

**La fraude financière et le contrôle interne en
entreprise : l'importance d'un SCI efficient pour
optimiser l'identification des risques de fraude et
réduire leur probabilité d'occurrence**

Travail de Bachelor réalisé en vue de l'obtention du Bachelor HES

Par :

Eric CASTRO

Conseillère au travail de Bachelor :

Ariane CHARGUERAUD, enseignante vacataire HEG

Genève, le 19 août 2016

Haute École de Gestion de Genève (HEG-GE)

Economie d'entreprise

Déclaration

Ce travail de Bachelor est réalisé dans le cadre de l'examen final de la Haute école de gestion de Genève, en vue de l'obtention du titre de Bachelor of Science en économie d'entreprise.

L'étudiant a envoyé ce document par email à l'adresse d'analyse remise par son conseiller au travail de Bachelor pour analyse par le logiciel de détection de plagiat URKUND. <http://www.orkund.com/fr/student/392-orkund-faq>

L'étudiant accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans le travail de Bachelor, sans préjuger de leur valeur, n'engage ni la responsabilité de l'auteur, ni celle du conseiller au travail de Bachelor, du juré et de la HEG.

« J'atteste avoir réalisé seul le présent travail, sans avoir utilisé des sources autres que celles citées dans la bibliographie. »

Fait à Genève, le 19 août 2016

Eric CASTRO

Remerciements

Je tiens à adresser mes remerciements les plus sincères aux différentes personnes qui m'ont été d'une grande aide dans l'élaboration de ce projet de recherche.

Tout d'abord, je remercie grandement les professionnels en audit et les experts en finance et en comptabilité, qui ont eu l'amabilité de répondre à mes questions en me transmettant leur avis, vision et de précieux conseils qui ont m'ont permis d'approfondir mes analyses.

Je tiens également à remercier ma conseillère, Madame Ariane Charguéraud, pour sa disponibilité et ses précieux *feedback*. Elle a su me guider dans la construction de ce mémoire et a su faire preuve d'une grande implication tout au long de l'étude.

J'adresse par la même occasion, mes sincères remerciements à Céline Marin qui a eu la gentillesse de relire l'intégralité de mon mémoire.

Enfin, un grand merci à mes parents ainsi qu'à tous mes proches pour leur soutien et leur patience durant toute la réalisation de cette étude.

Résumé

Cette étude portant sur une problématique émanant de la réalité professionnelle apportera un panorama sur les différents types de fraudes financières en entreprise et analysera les modes opératoires, les enjeux et conséquences ainsi que les vulnérabilités intrinsèques favorisant ce type de risque. L'objectif premier de ce travail est d'identifier les différents aspects d'un SCI qui permettent de lutter contre ce fléau afin de démontrer qu'il peut avoir une importance capitale dans la réduction de la probabilité d'occurrence et de l'impact du risque de fraude.

Tout d'abord, le détournement d'actifs, la fraude comptable ou encore la cybercriminalité sont différents types de fraudes financières qui ne cessent de se produire au sein des entreprises ayant certaines failles au niveau du SCI. Dans cette optique, le renouvellement du *framework* COSO entre 1992 et 2013 a permis d'apporter des améliorations au niveau des outils, garantissant ainsi une base solide pour la mise en place du SCI au sein des sociétés. A ce sujet, le *Risk Assessment* demeure un outil indispensable qui, avec une simple cartographie des risques, peut apporter une réelle valeur ajoutée dans la prévention et la détection des risques de fraude.

Bien que les mécanismes déclencheurs puissent avoir un début d'explication avec le triangle de la fraude de Donald R. Cressey, il ne faut pas oublier que le criminel économique reste avant tout un humain. De ce fait, l'aspect psychologique n'est pas à négliger dans le processus de réflexion pour le dissuader de toutes tentatives de fraude.

Par ailleurs, l'IT en entreprise devrait aussi être considéré comme une préoccupation majeure au sein d'une société, car c'est un aspect qui détient une importance grandissante, dû notamment à l'avancée technologique et surtout à l'augmentation fulgurante du nombre de cas de cybercriminalité. Cette dernière peut notamment s'expliquer par la création de cybermafia ciblant les entreprises avec des techniques tels que le *botnet*, le *phishing* ou encore l'attaque DDoS pouvant avoir de lourdes conséquences lorsque la sécurité informatique de l'organisation contient des failles.

Finalement, l'outil de réflexion que j'ai construit : « Le Trèfle Anti-Fraude », permettra à tout lecteur d'avoir en tête les différents aspects qui doivent être pris en considération au sein d'une entreprise : psychologie, SCI, technologie, et de les analyser à travers trois éléments interdépendants : prévention, détection et réaction, pour aboutir à la dissuasion de toute tentative de fraude d'un potentiel criminel économique.

Table des matières

Déclaration	i
Remerciements	ii
Résumé	iii
Liste des tableaux	vi
Liste des figures	vi
Introduction générale.....	1
1. Contexte et problématique	3
2. L'environnement du SCI et de la fraude financière.....	5
2.1 Définition et caractéristiques de la fraude.....	5
2.2 Eléments de définition du contrôle interne	6
2.2.1 Le COSO	6
2.2.2 Acteurs du contrôle interne	7
2.3 La gestion des risques en entreprise.....	9
2.4 La gouvernance d'entreprise	9
2.5 Les normes	10
3. Méthodologie adoptée	11
3.1 Entretiens semi-directifs.....	11
3.2 Recherche de références	12
3.3 Les chiffres	13
3.4 Analyse des données	13
3.5 Conception du modèle de réflexion	14
4. Analyse : Les données sur la fraude financière en entreprise.....	15
4.1 Les catégories de fraudes	15
4.2 Types de fraudes en entreprise	15
4.2.1 Détournement d'actifs.....	16
4.2.2 La fraude comptable.....	17
4.2.3 Corruption	18
4.2.4 <i>Management override</i>	18
4.2.5 La fraude au président.....	19
4.2.6 Cybercriminalité	19
4.3 Vulnérabilités intrinsèques favorisant la fraude financière	21
4.4 Conséquences pour l'entreprise.....	22
4.5 Signaux d'alerte	24
4.6 <i>Forensic accounting</i>	26

La fraude financière et le contrôle interne en entreprise : l'importance d'un SCI efficient pour optimiser l'identification des risques de fraude et réduire leur probabilité d'occurrence.

5. Analyse : Les données sur le fraudeur en entreprise	27
5.1 Le portrait-robot du fraudeur en entreprise	27
5.2 Le processus de la fraude financière	27
5.3 Causes et facteurs déclencheurs de la fraude financière	29
5.3.1 Triangle de la fraude.....	30
5.3.1.1 Motivation/Pression.....	30
5.3.1.2 Opportunité.....	31
5.3.1.3 Rationalisation.....	31
6. Résultats : Les aspects d'un SCI efficace face à la fraude financière ..	33
6.1 Composantes du COSO appliquées au risque de fraude	33
6.2 SCI face au triangle de la fraude : cibler l'opportunité	35
6.3 <i>Risk Assessment</i> : un dispositif indispensable.....	37
6.4 La cartographie des risques.....	39
6.5 L'importance de l'IT pour un SCI efficient	45
6.6 Au-delà des procédures : la culture d'entreprise	46
7. Synthèse : « Le Trèfle Anti-Fraude »	48
7.1 Prévention.....	48
7.2 Détection	50
7.3 Réaction	51
7.4 Dissuasion	52
8. Conclusion.....	54
Bibliographie	56
Annexes	59
Entretien n°1.....	59
Entretien n°2.....	66
Entretien n°3.....	72
Entretien n°4.....	75
Entretien n°5.....	82

Liste des tableaux

Tableau 1 : Les quatre lignes de défense	8
Tableau 2 : Inventaire des risques de fraude dans le domaine bancaire	39
Tableau 3 : Mesure et hiérarchisation des risques	40
Tableau 4 : Propositions d'actions pouvant réduire la criticité des risques.....	43
Tableau 5 : Fiche analytique pour les détournements d'actifs	44

Liste des figures

Figure 1 : Evolution du taux de fraude au niveau mondial	3
Figure 2 : Taux de fraude par taille d'entreprise en nombre d'employés	4
Figure 3 : Le cube COSO <i>Internal Control – Integrated Framework</i>	7
Figure 4 : Evolution des pertes monétaires en USD 2012-2016	22
Figure 5 : Coût de la fraude en USD au cours de 2014-2015	23
Figure 6 : Différentes formes de détection de fraudes en entreprise	26
Figure 7 : Le triangle de la fraude	32
Figure 8 : Processus du <i>Risk Assessment</i>	37
Figure 9 : Cartographie des risques en <i>Risk Map</i>	41
Figure 10 : Cartographie des risques en diagramme de KIVIAT	42
Figure 11 : « Le Trèfle Anti-Fraude »	53

Introduction générale

Les entreprises, quelle que soit leur taille et leur activité sont chaque jour confrontées à différents types de risques. Le risque qui, quand il est mal géré, se caractérise souvent par une perte monétaire. C'est surtout le cas lorsque l'entreprise fait face à un risque dont elle sait qu'il est permanent mais ne peut pas forcément le maîtriser. En effet, le risque de fraude reste un des risques les plus importants au sein des sociétés et peut avoir des conséquences graves pour l'entreprise.

L'évolution permanente de l'environnement économique mondial pousse les entreprises à sans cesse prendre des risques difficilement maîtrisables. C'est la complexité de cet environnement qui accroît le risque de fraude au sein de l'entreprise, c'est pourquoi il est primordial d'avoir un système permettant de le prévenir, le détecter, l'analyser et le gérer.

Ce travail portant sur un problème émanant de la réalité professionnelle et ciblant principalement les grandes entreprises, définira dans la première partie, les caractéristiques de la fraude, du contrôle interne ainsi que les différents acteurs en lien direct avec ce dernier de manière à pouvoir donner une vision globale des parties impliquées dans la lutte contre la fraude.

Ensuite, la deuxième partie présentera et analysera, à travers quelques exemples provenant de mes entretiens et recherches, les différents types de fraudes financières internes et externes : détournements d'actifs, fraude comptable, fraude au président, *management override*, corruption et cybercriminalité. Par conséquent, il ne s'agira pas ici d'inclure la fraude fiscale car c'est une problématique différente qui n'a pas pour victime directe l'entreprise. J'estime qu'il est plus intéressant de se focaliser uniquement sur ce qui l'impacte afin de pouvoir faire le parallèle avec le SCI.

Dit autrement, il s'agira ici d'aborder les modes opératoires de fraudes, les enjeux et conséquences ainsi que les vulnérabilités intrinsèques favorisant l'apparition de la fraude en entreprise, grâce à mes recherches et entretiens avec des experts dans le domaine de la finance et de la comptabilité. À travers les différentes analyses, ce mémoire a également comme objectif dans la deuxième partie d'identifier et d'analyser les mécanismes déclencheurs de la fraude avec le triangle de la fraude de Donald R. Cressey.

Puis, dans la troisième partie il s'agira d'analyser les différents aspects d'un SCI permettant de favoriser la prévention et la détection de la fraude afin de prouver qu'un système de contrôle interne efficace peut être la clé dans la lutte contre ce fléau. Le triangle de la fraude ainsi que le cube du COSO seront les deux éléments indispensables sur lesquels sera basée mon analyse. Il s'agira également de pousser la réflexion sur l'aspect humain en entreprise dans le but de démontrer l'importance de ce facteur dans le combat contre la fraude en entreprise.

Pour finir, je terminerai avec un modèle d'analyse : « Le Trèfle Anti-Fraude », élaboré par mes soins qui concentrera les différents éléments essentiels à prendre en considération pour qu'une entreprise puisse réduire la probabilité d'occurrence des risques de fraude.

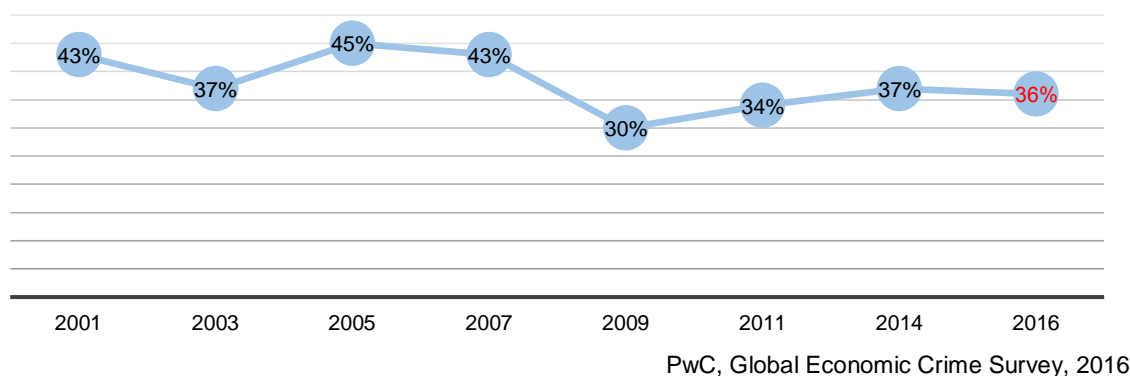
1. Contexte et problématique

La mondialisation, la fusion de grands groupes et la concurrence accrue sur les différents marchés, génèrent de grands espaces économiques dans lesquels les firmes prennent des risques considérables afin d'accroître leur rentabilité et leur part de marché.

Il est vrai que les entreprises sont de plus en plus amenées à se moderniser et se regroupent à travers des fusions pour générer des synergies, dominer le marché et faire des économies d'échelles.

En fusionnant, elles peuvent ainsi multiplier leurs activités dans le but d'accroître leur chiffre d'affaires et répondre favorablement aux attentes de leurs différentes parties prenantes et plus particulièrement à celles de leurs actionnaires. Cependant, ce développement peut générer une forte augmentation des opérations et complexifie ainsi l'organisation interne de la société. En effet, multiplier les activités au sein de l'entreprise ainsi que le nombre d'opérations engendre très souvent des vulnérabilités intrinsèques pour l'entreprise lorsque ces dernières sont mal maîtrisées, ceci étant notamment dû à un manque d'outils et de savoir-faire. Ainsi, ces types d'organisations se fragilisent et deviennent parfois des proies faciles pour les criminels économiques.

Figure 1 : Evolution du taux de fraude au niveau mondial



La problématique de la fraude est une réalité et il est du devoir de tout dirigeant et collaborateur d'une organisation d'avoir conscience que ce risque existe et qu'il doit être diagnostiqué.

En outre, il existe différents types de fraudes : internes et externes ou encore mixtes. La fraude se développe et apparait sous différentes formes ces derniers temps.

La fraude financière et le contrôle interne en entreprise : l'importance d'un SCI efficient pour optimiser l'identification des risques de fraude et réduire leur probabilité d'occurrence.

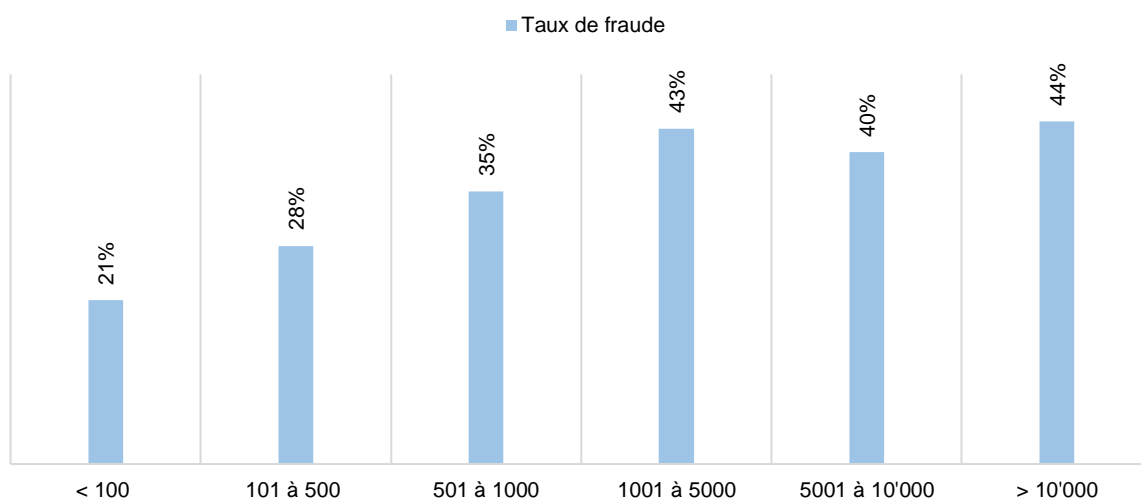
D'autre part, la préoccupation première des dirigeants d'entreprise est l'accroissement du chiffre d'affaires et des parts de marché. Néanmoins, la protection du patrimoine doit également être une priorité pour assurer la pérennité de l'entreprise à long terme. Ainsi, il s'avère qu'au sein de certaines sociétés, le SCI est présent sans être correctement défini avec des procédures mal formalisées et des outils mal utilisés. De plus, il arrive parfois qu'il n'y ait aucun système de contrôle interne existant au sein d'une organisation, ce qui est souvent le cas pour les petites structures (PME).

Dit autrement, une organisation n'ayant aucune culture d'honnêteté, tenant une mauvaise comptabilité et tenant une faible fréquence de contrôles est susceptible de favoriser la probabilité d'occurrence du risque de fraude quelles que soient ses procédures et les différents outils mis en place.

D'autre part, cette problématique de la fraude financière en entreprise est un risque qui doit être considéré comme un des *top risk* au sein de toute organisation, quelle que soit sa taille, car il peut mettre à mal la stabilité d'une entreprise voire même détruire un grand Groupe.

Pour récapituler, les entreprises doivent faire face à de nombreuses menaces telles que le détournement d'actifs, la cybercriminalité, la fraude comptable, le *management override* ou encore l'arnaque au président. La question qui se pose donc est la suivante : Un SCI au sein d'une entreprise suffit-il à mieux maîtriser le risque de fraude et à réduire sa probabilité d'occurrence ?

Figure 2 : Taux de fraude par taille d'entreprise en nombre d'employés



PwC, Economic Global Crime Survey, 2016

La fraude financière et le contrôle interne en entreprise : l'importance d'un SCI efficient pour optimiser l'identification des risques de fraude et réduire leur probabilité d'occurrence.

2. L'environnement du SCI et de la fraude financière

2.1 Définition et caractéristiques de la fraude

« On entend par fraude, 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. »

(Normes ISA 240, p.7 paragraphe 11)

Avant d'entamer la première partie dans ce mémoire il me paraît important de bien définir cette notion de « fraude » qui restera le fil conducteur durant tout ce travail afin d'être sûr que ce terme soit bien compris par tous les lecteurs. En effet, quand on entend le mot « fraude » on pense souvent aux fraudes fiscales ou à la fraude aux consommateurs. Cependant, dans ce mémoire, il s'agira d'étudier les fraudes dont sont victimes les entreprises du fait de l'agissement en interne de leurs collaborateurs ou en externe d'individus anonymes.

Si l'on se reporte à la définition de la norme ISA 240, la fraude est un « acte intentionnel ». En conséquence, pour que l'acte soit considéré comme frauduleux et non comme une erreur, il faut impérativement qu'il y ait cette notion d'intention de nuire volontairement. La fraude est donc un mot qui englobe tout acte intentionnel qui va à l'encontre des lois et règlements et qui implique des modes opératoires malhonnêtes dans le but de s'attribuer illégalement des biens (trésorerie, marchandises) ou des données confidentielles de la firme.

La fraude en entreprise a toujours existé en tant que risque en entreprise, cependant elle s'est répandue d'année en année à cause des différents cas qui ont été découverts. Elle peut porter sur des sommes astronomiques et détruire une carrière, une organisation voire même une vie dans les cas les plus extrêmes. La différence réside donc dans le fait que dorénavant la fraude doit être considérée comme un risque majeur au sein des entreprises qui doit être diagnostiqué spécifiquement. Effectivement, l'étude de PwC¹ assure que plus d'un tiers des entreprises (36%) ont confirmé avoir été victime de fraude durant les deux années précédentes, ce qui démontre bien l'ampleur de ce risque critique.

¹ Global Economic Crime Survey 2016

2.2 Eléments de définition du contrôle interne

« Le contrôle interne est un ensemble de principes et procédure prescrits par la direction d'une entreprise, servant à garantir une gestion des affaires correcte et efficace, à protéger les actifs, à empêcher ou à détecter des fraudes et des erreurs, à garantir l'exactitude et l'intégralité des enregistrements comptables ainsi qu'à compiler en temps utile les informations financières fiables, dans la mesure du possible. Vont au-delà des aspects qui dépendent directement de fonctions du système comptable ; englobent l'environnement de contrôle. »

(EXPERT SUISSE. Manuel suisse d'audit MSA « Tome 2 - Audit des comptes annuels », 2009)

En d'autres termes, le contrôle interne se définit comme étant un outil de gestion qui donne la possibilité à une entreprise de pouvoir maîtriser la gestion de ses activités en ayant à sa disposition un ensemble d'outils et d'actions. La mise en place de cet outil de gestion donne à l'entreprise un moyen d'assurer une certaine efficacité dans l'accomplissement de ses opérations, une bonne utilisation de ses ressources et d'agir en accord avec la conformité. Cet outil de gestion apporte une réelle valeur ajoutée à l'entreprise qui sait adapter le dispositif en fonction de sa structure, de son environnement et des changements. Il s'inscrit dans un processus d'amélioration continue et doit viser tout d'abord l'efficacité (atteinte des objectifs) puis l'efficience (atteinte des objectifs du mieux possible, « coût/profit »).

Pour résumer le contrôle interne sert à assurer la conformité aux lois et règlements ainsi que d'assurer le respect des instructions de la stratégie de l'entreprise fixés par la hiérarchie. Il assure également le bon déroulement des processus de la société ainsi qu'une certaine transparence et fiabilité dans la communication des informations financières.

2.2.1 Le COSO

Le *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) est une commission à but non lucratif qui a élaboré un référentiel présentant un cadre permettant la mise en place d'un système de contrôle interne (ou bien pour évaluer et mettre à jour les procédés en place). Ce référentiel définit les lignes directrices à travers cinq composantes et 17 principes permettant la constitution d'un dispositif de contrôle interne efficace au sein d'une organisation.

Figure 3 : Le cube COSO *Internal Control – Integrated Framework*



The Updated COSO Internal Control Framework, 2014

Le référentiel d'origine établi en 1992 a subi quelques évolutions dues notamment aux nouvelles réglementations (*Sarbanes-Oxley*, loi sur la sécurité financière) instaurées à cause des différents scandales financiers et comptables tels que WorldCom ou encore Enron. Il y a eu plusieurs évolutions entre le premier COSO (*Internal Control – Integrated Framework*, 1992) et sa mise à jour (2013) qui sont apparues dont l'insertion de principes (17) qui prennent notamment en compte l'avancée technologique et la fraude dans l'évaluation des risques (principe n°8) que j'évoquerai dans la troisième partie. Il ne s'intéresse plus uniquement au *reporting* financier mais également aux objectifs opérationnels et de conformité. D'autre part, il s'intéresse aussi à la RSE (responsabilité sociétale et environnementale), à la sécurité et a notamment articulé la notion de « tone at the top ».

Une autre nouveauté du COSO (2013) est l'instauration des « lignes de défense » dans l'organisation, ce qui est primordial dans la lutte contre la fraude. Effectivement, plusieurs acteurs du contrôle interne ayant chacun un rôle bien précis à respecter, se distinguent au sein d'une entreprise et il me paraît important de les décrire en quelques mots pour bien les différencier.

2.2.2 Acteurs du contrôle interne

Il y a tout d'abord, l'Audit interne qui est une activité indépendante et qui a donc un devoir de neutralité. Il s'occupe d'analyser le SCI de l'entreprise en mesurant son efficacité et l'application par les collaborateurs. Il peut par ailleurs, proposer des solutions afin de l'améliorer.

Ensuite, il y a le contrôleur de gestion qui lui fait office de pilote au sein de la société. Il s'occupe de la comptabilité analytique, d'analyser les écarts et fournit les informations

La fraude financière et le contrôle interne en entreprise : l'importance d'un SCI efficient pour optimiser l'identification des risques de fraude et réduire leur probabilité d'occurrence.

financières à sa hiérarchie afin de pouvoir faire les bons choix stratégiques pour atteindre les objectifs.

Un autre acteur qui lui est externe à l'entreprise est l'Audit externe. Cet organe de révision mandaté par la société certifie les comptes et vérifie, en Suisse, l'existence du SCI selon l'article 728 a. du CO en cas de contrôle ordinaire. Il est important de souligner que ce dernier ne vient pas chercher la fraude au sein d'une entreprise, il doit seulement s'assurer que les états financiers sont conformes aux lois et règlements afin de garantir une communication transparente avec les parties prenantes de la société. Il établit entre autre un rapport pour l'assemblée générale et le conseil d'administration.

Le conseil d'administration est responsable de la mise en place du système de contrôle interne en fonction des risques majeurs identifiés au préalable. Il doit être de préférence composé de différents profils (finance, ressources humaines, production) afin d'assurer une diversité des savoirs de manière à comprendre l'environnement globale de la firme.

Par ailleurs, en fonction de la taille de l'entreprise on pourrait également inclure le comité d'audit comme acteur supplémentaire. Ce dernier assurant une surveillance régulière du SCI, émane du conseil d'administration et lui rend des comptes.

La direction générale a aussi une fonction primordiale car elle doit mettre en œuvre le SCI pour ensuite avoir un rôle de surveillance permanent sur l'implication des collaborateurs et un devoir d'exemplarité. En effet, cet acteur donne le ton et montre l'exemple (« tone at the top ») à son personnel.

Enfin, le dernier acteur et pas des moindres, le personnel de l'entreprise. J'estime que le personnel joue un rôle majeur dans un système de contrôle interne car il est au cœur du *business*. C'est donc lui qui effectue les contrôles, c'est lui qui est au contact des clients et fournisseurs et c'est donc lui qui détient la responsabilité ultime dans le bon fonctionnement de l'organisation. Les responsables opérationnels sont tout aussi importants que les collaborateurs car ils doivent pouvoir remonter les informations et doivent savoir motiver et superviser leur équipe de façon à éviter des risques de fraude.

Voici un tableau qui récapitule les quatre lignes de défense :

Tableau 1 : Les quatre lignes de défense

1 ^{ère} ligne	2 ^e ligne	3 ^e ligne	4 ^e ligne
Collaborateurs	Direction générale	Audit interne	Audit externe

La fraude financière et le contrôle interne en entreprise : l'importance d'un SCI efficient pour optimiser l'identification des risques de fraude et réduire leur probabilité d'occurrence.

2.3 La gestion des risques en entreprise

En ce qui concerne la gestion des risques en entreprise, comme je l'ai dit précédemment, la prise de risque au sein de toute société est inévitable. L'émergence de marchés de plus en plus concurrentiels fait apparaître un nombre de risques croissant. En effet, pour maximiser son profit, obtenir de la croissance, gagner des parts de marché, il est nécessaire pour l'entreprise de prendre des risques afin de pouvoir créer de la valeur et ainsi écraser la concurrence. Cependant, il est essentiel pour une société d'avoir un dispositif de gestion des risques de manière à pouvoir structurer leur approche et construire une base solide lui permettant de gérer au mieux les différents risques. Un tel dispositif permettra d'identifier, d'analyser, d'évaluer et de contrôler les différents risques en fonction de leur probabilité d'occurrence et de leur degré de gravité. Il est important de raisonner en termes de « coût/profit » et d'avoir en tête la notion de « l'optimum économique » en vue de pouvoir prendre les meilleures décisions dans l'intérêt de l'entreprise.

Tout comme le contrôle interne, cela reste un processus continu et dynamique qui concerne l'ensemble des activités et fonctions de l'entreprise. Effectivement, l'efficacité d'un tel dispositif repose essentiellement sur l'investissement de chacun au sein de l'entreprise. En d'autres termes, la circulation de l'information doit être permanente et transparente de manière à pouvoir responsabiliser l'ensemble des collaborateurs et pouvoir recenser tous les risques de l'entreprise.

En somme, mettre en place une gestion des risques permet de mieux piloter les affaires d'une entreprise. J'y reviendrai dans la troisième partie de ce mémoire lorsque j'aborderai l'outil indispensable pour le *Risk Assessment* : la cartographie des risques. Cela reste d'ailleurs un enjeu majeur dans la gestion d'entreprise, car maîtriser ses risques doit permettre à toute société de pouvoir atteindre plus facilement ses objectifs en minimisant ses coûts afin d'assurer des performances en constante progression.

2.4 La gouvernance d'entreprise

La gouvernance d'entreprise est un système indispensable qui encadre les limites de l'exercice du pouvoir. L'entreprise ayant différents organes tels que les actionnaires, l'organe de révision, le conseil d'administration ou encore la direction générale, avec chacun des rôles et responsabilités, doit pouvoir déterminer une structure dans laquelle chacun connaît ses responsabilités.

C'est justement dans la répartition des missions que la gouvernance intervient, en proposant une définition claire des rôles de chacun tout en ayant comme objectif la diffusion d'informations transparentes entre les différents acteurs. En d'autres termes, c'est un mécanisme qui permet de définir la façon dont la société doit diriger et gérer ses affaires tout en assurant une certaine clarté dans l'équilibre des pouvoirs entre les différents acteurs de l'entreprise.

La gouvernance d'entreprise a par ailleurs un rôle très important dans la dissuasion de tentatives de fraude. Elle doit évidemment faire en sorte que les différents acteurs respectent une certaine éthique des affaires et les valeurs de l'entreprise en exerçant une surveillance constante sur la direction générale afin d'avoir la certitude que l'accent est mis sur la prévention et la détection de la fraude auprès des salariés, réduisant ainsi la probabilité d'occurrence. Cette surveillance exercée sur la direction pourrait par la même occasion permettre de dissuader cet acteur de contourner les règles, d'où son importance dans la prévention et la lutte contre la fraude financière en entreprise.

2.5 Les normes

Pour terminer cette première partie, j'estime également important de faire le point sur le rôle des normes dans l'environnement de la fraude. La norme est un moyen qui définit les pratiques fondamentales et lignes directrices dans différents domaines. En matière de comptabilité par exemple, ce sont les normes IFRS qui dictent les règles de présentation des états financiers au niveau international et en matière d'audit externe, il y a la norme ISA 240. Cette dernière est une norme qui détaille les responsabilités de l'auditeur face à la fraude dans les états financiers. Le non-respect des normes peut avoir de lourdes conséquences pour une entreprise. Le cas Enron en est la parfaite illustration. En effet, le cabinet Arthur Andersen, qui avait comme mission de certifier les comptes de cette société, a failli dans sa mission et les conséquences ont été immédiates. L'organe de révision de la société américaine a incontestablement certifié des comptes falsifiés, ce qui lui a valu sa disparition alors qu'il était l'un des cinq plus grands cabinets d'audits au monde.

Voici quelques exemples de normes :

- ISA : *International Standards on Auditing*
- IFRS : *International Financial Reporting Standards*
- NAS : Normes d'audit suisse

3. Méthodologie adoptée

3.1 Entretiens semi-directifs

Pour ce travail de recherche, j'ai décidé dans un premier temps d'obtenir des interviews auprès de personnes ayant une certaine expertise dans le domaine financier ou comptable et en possession d'une expérience dans l'audit. Le but étant de pouvoir obtenir des entretiens dits semi-directifs me permettant de pouvoir dialoguer et interagir directement avec la personne en face de moi. Cette méthode m'a permis de pouvoir pousser la réflexion plus loin qu'avec un simple questionnaire envoyé en ligne, car j'ai pu directement poser d'autres questions et l'interlocuteur n'a pas hésité à me faire part de leurs précieux avis, conseils et anecdotes sur le sujet.

Ma méthodologie pour les entretiens semi-directifs se décompose en quatre étapes.

La première est l'élaboration du questionnaire présent en annexe, en cherchant toujours à cibler mes questions en sorte de pouvoir obtenir l'information que je souhaite. Ce questionnaire m'a servi de fil conducteur sans pour autant procéder en un entretien journalistique. En effet, l'objectif était vraiment de pouvoir discuter de manière ouverte sur cette problématique, afin de pouvoir enrichir mes analyses et mes recherches.

Dans la deuxième étape, j'ai procédé à une recherche approfondie dans le but de vraiment cibler des personnes potentiellement intéressées par mon projet de recherche. Une fois les professionnels ciblés, je me suis permis de leur présenter mon projet de recherche, afin de voir s'ils étaient aussi curieux que moi par ce sujet et s'ils étaient aptes à répondre à mes questions.

Suite à cela, j'ai obtenu des réponses favorables des personnes suivantes :

- Une Responsable contrôle et audit interne dans le domaine de la santé (Experte en controlling et finance)
- Un Responsable de l'audit Interne dans le domaine bancaire (Expert-comptable)
- Un *Senior Banking Auditor* actif dans un *Big Four* (B.A. Sc)
- Un *Senior Audit Financial Services* actif dans un *Big Four* (B.A Sc.)
- Un *Assistant Manager Internal Audit* actif dans un *Big Four* (Certifié CIA, CRMA)

La troisième étape a été l'entretien avec la personne. Ainsi, j'ai eu la chance de pouvoir rencontrer des professionnels expérimentés qui ont su me fournir de précieux avis et conseils durant les entretiens tout en m'apprenant énormément de choses sur des actes en entreprise parfois allant jusqu'à l'extrême. Suite à ces entretiens, j'ai vraiment réalisé à quel point mon projet de recherche intéresse les professionnels du secteur et qu'il s'agit d'un thème sur lequel il est intéressant de se pencher. D'ailleurs, durant ces différents entretiens riches en contenu, j'ai eu connaissance de cas réels qui seront décrits tout au long de ce mémoire.

Pour finir, la quatrième et dernière étape a été d'analyser tout le contenu des entretiens afin de pouvoir trouver des pistes de solutions et des preuves qui démontrent qu'un système de contrôle interne peut être un dispositif clé dans la prévention et la détection de la fraude.

3.2 Recherche de références

En ce qui concerne la recherche de références, cela a été la période la plus longue en termes de temps. En fait, je n'ai pas arrêté de faire des recherches sur le web, dans les médias, dans les journaux, dans les livres et ce dans le but de pouvoir maîtriser mon sujet et avoir les idées structurées. Ce qui m'a particulièrement aidé, ce sont les enquêtes et sondages menés par différents organismes sur la fraude financière dans le monde. L'analyse des résultats et la comparaison à travers plusieurs années m'ont permis de faire ressortir les chiffres clés qui permettent de démontrer sur quels types de fraude il faut se concentrer et celles qui sont les plus importantes au niveau de l'impact. Je me suis également intéressé à différents documentaires qui étaient soit en lien direct avec la fraude, ou qui pouvaient m'apporter des éclaircissements sur les méthodes adoptées et les conséquences.

Je me suis notamment intéressé aux cas Enron et WorldCom qui démontrent bien l'ampleur que peut prendre une fraude, mais également au cas Madoff qui prouve que la capacité de persuasion et de manipulation d'un individu peut être la clé dans l'accomplissement d'une fraude et qu'il ne faut pas simplement s'attarder sur les processus et procédures, mais avoir une certaine intelligence émotionnelle afin de ne pas tomber dans le piège et être victime d'une telle fraude. Par ailleurs, je me suis également intéressé au cas Kerviel qui m'a fait comprendre que le manque de contrôle au sein d'une banque pour un trader peut être un élément dévastateur pour la banque et ses parties prenantes.

3.3 Les chiffres

En ce qui concerne les chiffres sur la fraude financière, je me suis basé sur différentes études et rapports statistiques pour mettre en évidence les résultats qui me paraissent forts intéressants et qui permettent ainsi d'avoir une vue plus concrète de la situation dans le monde. Les études et rapports statistiques sur les fraudes découvertes ont relativement augmenté ces derniers temps, démontrant ainsi l'importance du phénomène. Je me suis notamment basé sur les différentes enquêtes menées par PwC (*PricewaterhouseCoopers*) qui m'ont permis justement de voir l'évolution de la fraude au niveau mondial. Pour ce faire, j'ai étudié l'enquête sur la fraude de 2014 ainsi que celle de 2016, puis j'ai complété mes statistiques à travers d'autres enquêtes publiées par KPMG, EY et l'ACFE (*Association of Certified Fraud Examiners*). Cette dernière est une association américaine qui délivre le diplôme d'examineur certifié et qui propose à ses adhérents une base de données regroupant des documents réels sur la fraude en entreprise. Son rapport publié dernièrement en 2016, recense 2'410 cas de fraudes (qui ont eu lieu dans 114 pays) enquêtées par des experts en fraude de l'association.

3.4 Analyse des données

Tout d'abord, j'ai décidé d'apporter, lorsque j'en estimais l'utilité, une vision chiffrée sur mes dits. Effectivement, j'ai pu faire ressortir les chiffres qui me sont parus les plus intéressants, tels que le profil type du fraudeur, les types de fraudes étant les plus courantes ou encore le type de fraude ayant eu la plus forte progression. Ces éléments m'ont permis d'avoir vraiment une vision globale de ce qui se passe actuellement dans le monde professionnel en ce qui concerne la fraude et m'ont aidé à définir les outils, méthodes et pratiques qu'il faut mettre en place dans le but de protéger l'entreprise face à ce fléau. Cependant, il me paraît évident de préciser que le risque zéro n'existe pas, en revanche, il n'est pas impossible de réduire la probabilité d'occurrence et l'impact des risques de fraude qui causent d'énormes pertes à la société.

Par ailleurs, dans le cadre de ma spécialisation en « Controlling, Financement et Investissement », ainsi que dans le cadre de mon option mineure « Du contrôle interne à l'audit : une approche risque », j'ai eu la chance de pouvoir assister à une dizaine de conférences en lien direct parfois avec mon sujet ce qui m'a permis d'avoir la vision d'un responsable travaillant en audit interne et mettant en place des dispositifs dans le but de réduire la probabilité d'occurrence de certains risques, notamment celui de fraude. Mon expérience dans le domaine bancaire a également été une source d'analyse pour moi et

une façon de guider ma réflexion car le service dans lequel je me trouvais était certainement celui dans lequel le risque de fraude était le plus élevé.

En outre, j'ai également pris le soin d'analyser une série de documentaires qui retracent la vie d'un *hacker* créant une société visant à dérober des données confidentielles d'une grosse multinationale dans le but de la faire disparaître. Cette analyse m'a permis de comprendre quelques techniques de cyberattaques et démontre l'importance du phénomène, car comme nous pouvons le voir actuellement, les individus que l'on surnomme *Anonymous* ou encore pirates du Net sont capables de s'introduire dans la plupart des systèmes informatiques, mêmes les plus sécurisés, ce qui prouve qu'il y a un enjeu majeur dans la lutte contre la cybercriminalité et que cette affaire devrait être l'une des priorités pour tout dirigeant d'entreprise.

Cette méthodologie divisée en quatre phases m'a permis de pouvoir couvrir la problématique de la fraude sous différents angles, dans le but de déterminer si le SCI a son importance dans la prévention et la détection de la fraude.

3.5 Conception du modèle de réflexion

Finalement, pour apporter une réelle plus-value dans mon étude, j'ai décidé de ne pas boucler ce projet de recherche uniquement avec une simple conclusion permettant de savoir si un SCI est suffisant pour réduire la probabilité d'occurrence et l'impact du risque de fraude. En effet, j'ai pris l'initiative de synthétiser mes recherches et analyses sous la forme d'un concept présenté d'une certaine forme, dans le but que cela devienne une source de réflexion pour tout individu qui s'intéresserait à combattre la fraude financière en entreprise. Le but de mon concept est de condenser tous les éléments fondamentaux permettant à une entreprise de pouvoir assurer la dissuasion de tentatives de fraude au sein d'une société. Je me suis d'ailleurs inspiré du triangle de la fraude que je détaillerai dans la deuxième partie, pour guider ma réflexion. En bref, j'ai décidé de nommer mon concept : « Le Trèfle Anti-Fraude » et je vous invite à lire les détails en fin de mémoire.

4. Analyse : Les données sur la fraude financière en entreprise

4.1 Les catégories de fraudes

Il s'avère que j'ai pu répartir les différents types fraudes sous trois catégories. Par conséquent, j'ai distingué les fraudes internes, externes et mixtes.

La première catégorie concerne les événements impliquant un collaborateur de la société qui va à l'encontre de la législation et du règlement interne, en commettant l'acte à l'intérieur de l'entreprise :

- Manipulation comptable
- Abus de pouvoir
- Détournements de fonds

En ce qui concerne la seconde catégorie, elle regroupe les agissements d'un individu externe au détriment d'une firme :

- Cybercriminalité
- Usage de faux documents

La troisième catégorie résulte d'une coopération entre un membre interne de la société et d'un individu externe.

- Falsification de facture en collaboration avec un fournisseur
- Transmission d'un fichier client confidentiel à un proche

4.2 Types de fraudes en entreprise

L'entreprise peut être confrontée à différents types de fraudes et dans cette optique j'ai pu en identifier à travers l'analyse de mes différentes données provenant de mes entretiens et références. Il y a plusieurs catégories de fraudes qui sont souvent revenues chez les professionnels en audit que j'ai questionnés ainsi que dans les différents ouvrages et articles de presse que j'ai pu lire. Il y a en premier lieu le détournement d'actifs qui est la fraude la plus répandue au sein des entreprises, en témoigne sa première place au classement dans le rapport de PwC² avec un taux de 64%. D'autre part, j'ai pu identifier la fraude comptable ainsi que la corruption, le

² Global Economic Crime Survey 2016

management override, la fraude au président et une catégorie qui arrive en seconde position du classement des types de fraude reportés au niveau mondial et qui prend de plus en plus d'ampleur avec un taux passant de 24% à 32% en l'espace de deux ans, dans la même étude de PwC citée précédemment : la cybercriminalité.

4.2.1 Détournement d'actifs

En premier lieu, le détournement d'actifs peut impliquer autant des biens corporels qu'incorporels et se caractérise par un vol d'actif de l'entreprise tel que du numéraire, des matières premières ou des marchandises présentes en stock. Il m'a d'ailleurs été confié lors d'un entretien qu'une certaine préoccupation régnait au sein des hôpitaux dans tout ce qui est le vol de produits médicaux. En effet, la personne m'a assuré que certes les stocks sont toujours hautement sécurisés, mais elle n'écartait pas ce risque pour autant.

Elle m'a également fait part d'un cas de fraude standard qui peut se produire dans n'importe quelle organisation. Je parle évidemment du détournement de *cash*. Pour ainsi dire, un individu interne à l'hôpital avait retiré à plusieurs reprises de l'argent en caisse sans que personne ne s'en rende compte dû au fait que le supérieur hiérarchique ne faisait pas de contrôle en fin de journée. La fraude a pu être découverte au bout de quelques mois, lorsqu'un audit a eu lieu et qu'il a fallu demander des justificatifs qui n'existaient pas.

Par ailleurs, le *Senior Banking Auditor* m'a également confirmé qu'il avait rencontré à plusieurs reprises des cas de vols dans l'industrie, en me précisant que l'inventaire du stock n'était pas toujours mis à jour et que la variation de stock n'était donc pas contrôlée scrupuleusement, ce qui rendait difficile la détection de la fraude. Cette dernière a malgré tout été remarquée grâce à un audit externe.

Autrement dit, ce type de fraude consiste à détourner illégalement des actifs monétaires (caisse) ou physiques (médicaments) au sein d'une organisation.

En dernier lieu, les exemples de l'hôpital et de l'industrie cités précédemment, révèlent que le fraudeur en question a commis cet acte car il s'est aperçu que son supérieur hiérarchique ne suivait pas la procédure initialement prévue. En d'autres mots, il y avait une faille dans le système de contrôle interne de ces organisations et le resquilleur l'a exploité afin de s'approprier les biens de l'organisation tout en s'enrichissant frauduleusement.

4.2.2 La fraude comptable

En ce qui concerne la fraude comptable, elle a été médiatisée notamment à travers les scandales Enron, Worldcom ou encore Satyam Computers. Ce deuxième type de fraude consiste à modifier et présenter intentionnellement des états financiers qui ne représentent pas la réalité économique de la société et ne respectant pas le principe de transparence dans la communication financière. Différentes catégories telles que l'augmentation fictive des produits, la dissimulation des charges ou encore l'enregistrement d'actifs fictifs sont différents procédés qui concernent la fraude comptable.

Cette catégorie de fraude se traduit donc par une manipulation volontaire des chiffres de l'entreprise dans le but de tromper les différents lecteurs sur la situation économique de l'entité. Cependant, soulignons que la fraude comptable est relativement moins fréquente que le détournement d'actifs. Je pense que c'est notamment dû au fait que très peu de personnes au sein d'une organisation maîtrisent les techniques comptables. C'est pourquoi, pour ce genre de fraude, le profil type de l'auteur de cet acte serait généralement un membre de l'entreprise avec un certain niveau hiérarchique, détenant une excellente habileté des outils comptables.

Revenons-en au troisième scandale cité plus haut : Satyam Computers. Ce groupe indien fondé en 1987 a été le responsable du plus gros scandale en matière de fraude dans son pays. Le fondateur du groupe avait volontairement gonflé les comptes de l'entreprise durant plusieurs années. Il a notamment falsifié la trésorerie de l'entreprise (cash, banque) et a créé plus de dix mille employés fantômes pour lesquels un salaire était versé chaque mois, atterrissant probablement dans sa poche.

Enfin, dans le domaine bancaire, l'auditeur expérimenté m'a également fait part d'un événement de fraude auquel il a dû faire face. Il s'agissait d'un gestionnaire de fortune qui, suite au dépôt d'un client (plusieurs millions), avait falsifié le document des frais de gestion. Le client étant fortuné et ayant pleinement confiance en son banquier, signa le document sans poser de questions. L'écriture a été ensuite saisie et validée sans avoir fait un *call back* auprès du client. Ce manque de contrôle a laissé l'opportunité au gestionnaire de passer inaperçu et démontre bien l'importance d'une simple vérification telle que le contrôle quatre yeux, au sein d'un établissement bancaire.

4.2.3 Corruption

On peut la définir comme étant le détournement du pouvoir (abus de pouvoir ou de confiance) qu'un collaborateur utilise lors d'une transaction commerciale dans le but d'obtenir un avantage direct ou indirect. La corruption peut prendre différentes formes comme les pots-de-vin, l'affaire « Qatargate » de la FIFA en est une parfaite illustration.

Cette fraude demeure une menace pour l'entreprise à ne surtout pas négliger, qui reste tout de même une préoccupation majeure pour les dirigeants avec 55% selon l'étude de PwC³. Je trouve cela paradoxal car dans la même enquête, la corruption arrive en troisième position avec un taux des types de fraude reportés au niveau mondial de 24%.

Par ailleurs, une étude de EY⁴ conduite auprès de 2'825 dirigeants de 62 pays, met en avant l'importance des problèmes de corruption. Cette dernière rapporte que 39% des sociétés interrogées affirment que la corruption est très répandue dans leur pays et reste donc une menace permanente.

4.2.4 *Management override*

Durant mes entretiens, on m'a souvent parlé du terme *Management override*. Ce dernier, m'étant inconnu auparavant, m'a permis d'élargir mon champ d'analyse. Je m'autorise donc à le classer parmi les autres types de fraudes car cela en reste une à part entière. Ce terme signifie tout simplement le fait qu'un manager passe au-dessus des règles et procédures internes de l'entreprise dans le but d'obtenir un gain personnel injustifié au détriment de l'entreprise. Il use de son pouvoir pour frauder et agit de manière volontaire et illégale. Ce type de fraude est particulièrement compliqué à détecter d'après les professionnels que j'ai interrogés, en raison du niveau hiérarchique de l'auteur de la fraude. En effet, c'est souvent une personne *SMART* qui détient tous les outils, contrôles et qui dans certains cas s'occupe même de mettre en place les contrôles pour l'entreprise, ce qui lui laisse le champ libre pour élaborer une fraude de A à Z en vue de garder une maîtrise absolue de cette dernière.

³ Global Economic Crime Survey 2016

⁴ 14th Global Fraud Survey 2016

4.2.5 La fraude au président

Un nouveau type de fraude est apparu de plus en plus souvent ces dernières années et est particulièrement nuisible pour l'entreprise, il s'agit de la fraude au président. Concrètement, l'expert-comptable, responsable en audit interne dans une banque m'a confié que c'est une fraude assez récurrente. Cette dernière repose sur une technique de manipulation de la part du criminel économique et sur une bonne connaissance du fonctionnement de l'organisation (jargon interne, organigramme).

Le processus de la fraude au président peut être décrit de la manière suivante :

Le criminel économique collecte dans un premier temps toutes les informations lui permettant de connaître l'entreprise et ses dirigeants, et ce en se basant principalement sur les réseaux sociaux et l'organigramme de la société.

Puis, se faisant passer pour le dirigeant de l'entreprise, le manipulateur prétexte une opération financière urgente et confidentielle comme une fusion ou une acquisition. Sous la pression ou en confiance, l'entreprise exécute la transaction rapidement sans véritablement faire une vérification au préalable.

Une fois la transaction réalisée, le criminel économique transfère immédiatement l'argent vers des comptes basés à l'étranger dans le seul et unique but de brouiller les pistes et ainsi s'enrichir illégalement.

4.2.6 Cybercriminalité

D'autre part, comme je l'ai stipulé précédemment, la cybercriminalité est une catégorie de fraude qui prend de plus en plus d'ampleur ces derniers temps.

« Selon l'étude indépendante publiée en 2015 à la demande de McAfee par un expert indépendant de la sécurité sur Internet, le Dr Peter Troxler, la cybercriminalité n'est plus seulement le fait de pirates informatiques isolés attaquant les ordinateurs personnels depuis leurs chambres et animés par l'esprit de défi et d'exploit personnel, mais celui d'une cybermafia organisée qui mobilise des milliers de réseaux informatiques invisibles pour commettre ses méfaits à l'échelle mondiale. »
(Mikael Ouaniche, 2015)

Effectivement, cette criminalité moderne s'est rapidement adaptée à ce nouveau monde digitalisé et a fortement évolué avec les avancées technologiques. Les nouvelles catégories d'appareils, de réseaux virtuels, d'architectures informatiques, permettent à ces pirates informatiques d'innover dans leurs attaques et d'exploiter les failles dans des nouveaux systèmes mal maîtrisés et donc mal protégés par les sociétés. Si l'on se

tourne vers l'enquête de PwC⁵, les chiffres démontrent que ce type de fraude a doublé au cours de l'année 2015.

Cette nouvelle menace virtuelle peut être très puissante et efficace lorsqu'il s'agit de dérober des données confidentielles. Les pirates utilisent notamment le *botnet* qui peut se décrire comme étant un réseau-robot reliant plusieurs milliers de machines utilisées dans les cyberattaques pour prendre en otage des sociétés.

Un exemple récent concernant la cybercriminalité prouve que ce genre d'attaque peut arriver à tout moment au sein d'une organisation. En effet, l'entreprise RUAG active dans l'aviation a été victime d'une attaque ciblée de la part de pirates informatiques. D'après les informations publiées cette année, l'attaque a été menée de façon professionnelle avec l'introduction très discrète d'un logiciel malveillant (Cheval de Troie) qui est passé inaperçu pendant plusieurs mois et qui a piraté 20 Go de données. L'attaque aurait commencé en décembre 2014 et c'est seulement en janvier 2016, suite à un signal provenant de l'étranger, qu'il y a eu une réaction de RUAG.

En bref, la cybercriminalité recouvre donc les vols de données, notamment les codes d'accès de comptes bancaires, mais également d'autres types de données confidentielles stockées dans les systèmes informatiques des entreprises, telles que des conversations téléphoniques, des mails ou encore des secrets de fabrication. Dans l'étude 2016 de PwC sur la cybersécurité, les chiffres démontrent effectivement que le vol de données clients est le type de données le plus recherché par les cybercriminels avec 37%. Vient ensuite le vol de données des collaborateurs avec 32% puis en troisième position les données relatives à la propriété intellectuelle de l'entreprise avec 26%.

L'objectif ultime pour les cybercriminels est donc d'utiliser les différentes données récoltées illégalement afin de pouvoir, par exemple, lancer des campagnes de spam (technique du *phishing*) ou lancer des attaques DDoS (*Distributed Denial of Service*)⁶ afin de pouvoir rendre hors-service un réseau entier et exiger une rançon pour arrêter l'attaque. Ce genre d'opération, minutieusement orchestrée, est capable d'avoir un impact considérable au sein de l'entreprise et peut engendrer des dommages

⁵ The Global State of Information Security Survey 2016

⁶ Multitude de requêtes envoyées sur la bande passante pour surcharger un serveur et le rendre indisponible.

économiques immenses mais peut, par la même occasion, affecter la réputation de l'organisation et sa marche des affaires.

Finalement, un résultat que je trouve intéressant témoigne du manque de prise de conscience des entreprises sur la gravité que peut engendrer une attaque dans le réseau informatique. Il y a seulement 37%⁷ des entreprises à travers le monde assure avoir un plan opérationnel pouvant répondre aux incidents de cybercriminalité. Je pense que c'est notamment dû au fait que les petites structures sont incluses dans l'échantillon et qu'elles n'ont pas forcément les ressources nécessaires pour mettre en place un tel dispositif. Cette hypothèse a été confirmée par la comparaison que j'ai pu faire entre les dispositifs d'une multinationale dans laquelle j'ai évolué et une PME de trente salariés dans laquelle j'ai dû effectuer une analyse. Concrètement, je peux affirmer qu'il y a une grande différence entre ces deux types d'organisation en termes de sécurité informatique.

4.3 Vulnérabilités intrinsèques favorisant la fraude financière

Durant mes entretiens, il a été également question des vulnérabilités de l'entreprise qui pouvaient favoriser les tentatives de fraude, en voici un condensé des différents propos recueillis.

Tout d'abord, il y a le fait que l'entreprise n'accorde pas une réelle importance à son SCI. Certes, dans les multinationales il y a énormément de directives et beaucoup de procédures qui sont mises en place, néanmoins elles ne sont pas toujours appliquées avec rigueur et précision.

Le manque de séparation des fonctions est aussi très important dans le monde du travail et peut être perçu comme une vulnérabilité à part entière. Autrement dit, lorsqu'un même employé prépare et valide les factures, cela lui laisse l'opportunité de créer un fournisseur fictif.

Par ailleurs, une autre vulnérabilité citée lors d'un entretien est le fait que l'entreprise détienne beaucoup d'actifs fongibles, tels que des stocks, des caisses ou encore des coffres. En effet, cela peut rendre l'entreprise vulnérable si elle n'a pas mis en place des mesures adéquates pouvant protéger ce genre d'actifs tangibles.

⁷ Global Economic Crime Survey 2016

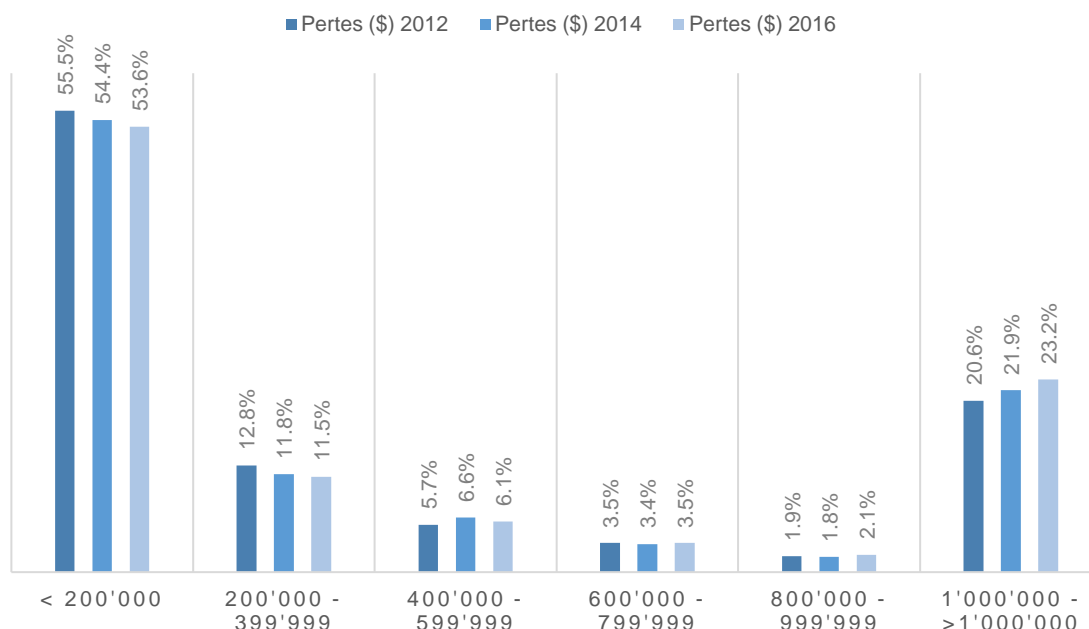
Puis, le recrutement d'employés avec peu d'éthique a également été considéré comme un élément pouvant rendre une entreprise vulnérable. On pense souvent que la lutte contre la fraude se déroule uniquement lorsque la fraude pointe le bout de son nez. Néanmoins, il me paraît important de souligner que les services de recrutement au sein des entreprises doivent également être sensibilisés au sujet des fraudes car je pense qu'il suffit d'avoir un processus de recrutement adapté à cette thématique pour réduire le nombre de fraudes en entreprise.

Finalement, une dernière vulnérabilité qui me paraît être très importante et celle de la mauvaise gestion des outils informatiques. L'avancée technologique permet certes à l'entreprise d'optimiser sa gestion à travers un ERP (*Entreprise Ressources Planning*) ou encore le *E-Banking* dans le domaine bancaire, mais une entreprise ayant les outils les plus sophistiqués en matière informatique sans posséder le savoir-faire nécessaire pour exploiter la puissance de ces derniers pourrait devenir une grande faiblesse.

4.4 Conséquences pour l'entreprise

La fraude peut avoir différents impacts négatifs au sein d'une société. Effectivement, pour les sociétés cotées en bourse par exemple, le premier impact important pourrait être la chute du cours de bourse. Cependant, deux conséquences majeures se sont distinguées lors de mes entretiens : les pertes financières et l'impact sur la réputation.

Figure 4 : Evolution des pertes monétaires en USD 2012-2016

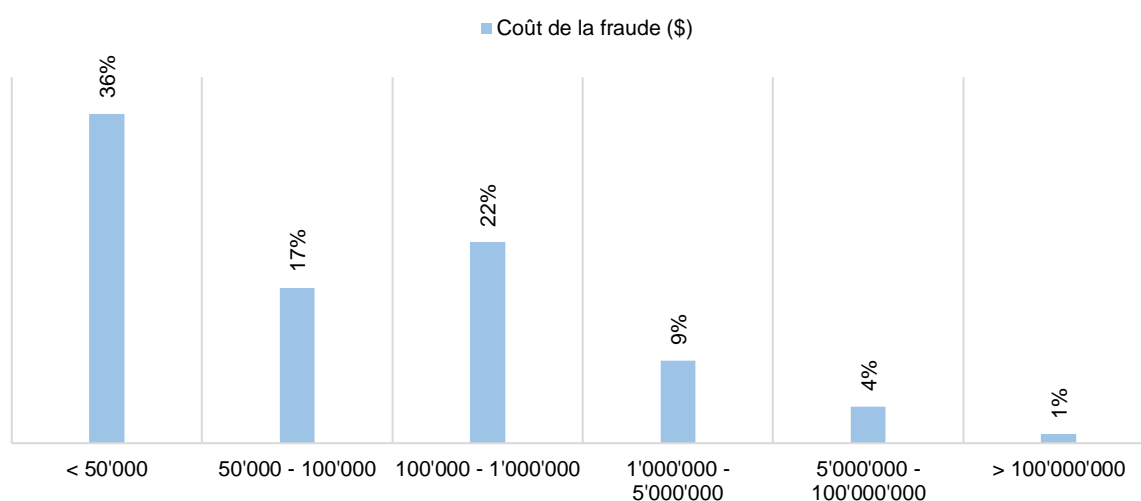


ACFE, Report to the Nations on Occupational Fraud and Abuse, 2016

Les pertes monétaires engendrées par la fraude peuvent varier en fonction de l'auteur de celle-ci, atteignant parfois des pertes colossales, surtout lorsqu'il s'agit de détournements commis par des collaborateurs ayant un certain niveau hiérarchique. Le niveau de complexité des fraudes commises par les dirigeants devient nettement supérieur à la moyenne et amène donc des conséquences financières bien plus importantes, ce qui indique qu'il y a une corrélation positive entre ces deux facteurs.

A ce sujet, l'étude PwC⁸ confirme que dans 5% des cas le coût de la fraude peut aller jusqu'à plus de cinq millions de dollars au niveau mondial et que 1% des fraudes les plus coûteuses ont atteint plus de cent millions de dollars au cours des deux années précédentes.

Figure 5 : Coût de la fraude en USD au cours de 2014-2015



PwC, Global Economic Crime Survey, 2016

D'autre part, la fraude comptable est certainement celle qui engendre les pertes les plus élevées en termes d'impact direct, car lorsque le fraudeur manipule les états financiers, il essaie de cacher d'une certaine manière les mauvais résultats de l'entreprise et en conséquence retarde l'adoption de nouvelles actions qui auraient pu faire passer les indicateurs au vert. En termes de chiffres, l'étude ACFE⁹ confirme justement que la fraude comptable est celle qui causerait la plus grande perte pour les entreprises avec une perte moyenne atteignant le million de dollar.

⁸ Global Economic Crime Survey 2016

⁹ Report to the Nations on Occupational Fraud and Abuse 2016

Néanmoins, la dégradation de l'image de l'entreprise est d'après moi l'élément le plus impactant pour cette dernière. En d'autres mots, l'impact monétaire est un impact à court terme tandis que l'impact sur l'image est à long terme et peut faire couler le navire, si des mesures radicales ne sont pas prises.

Il est vrai que pour une association, telle que la Croix-Rouge ou Médecins Sans Frontières (MSF) par exemple, l'impact sur la réputation sera très fort et de ce fait les donateurs ne lui feront plus confiance et les pertes pourraient accroître davantage. Dans le domaine bancaire ou commercial également il faut savoir garder une bonne réputation pour ne pas perdre de clients et d'employés.

Somme toute, je pense que le moral du personnel d'une organisation ayant vécu une fraude est également impacté par un tel événement car lorsqu'un dirigeant par exemple, commet cet acte illégal, les employés ne sont pas au courant et la plupart du temps se sont les premiers à en faire les frais : licenciements, baisse de motivation, plus de raison de travailler dans un tel environnement.

4.5 Signaux d'alerte

A l'occasion des interviews, j'ai également pu aborder le thème des signes qui permettent d'identifier des situations suspectes entachées de fraude. En effet, plusieurs indices distincts ont été cités comme l'erreur dans les états financiers ou encore l'agissement étrange de certains employés lorsqu'il y a lieu de faire un audit.

Ce deuxième élément est important dans la détection de la fraude. A ce sujet, l'un des interlocuteurs m'a affirmé qu'il peut y avoir des signes forts lorsqu'on est conscient de l'environnement dans lequel on se trouve.

Autrement dit, il faut pouvoir ressentir ce qu'il se passe autour de soi et détecter des situations étranges. Ces dernières peuvent se traduire par des informations contradictoires d'employés d'un même département ou par de la rétention d'informations. Le responsable d'audit interne que j'ai questionné m'a fait part de son expérience en m'affirmant qu'il faisait très attention à ce qu'on lui disait car il avait déjà rencontré des responsables de services qui s'assuraient que toutes les informations passent par eux avant d'être communiquées à l'audit interne. Un signal fort d'après lui, car cela sous-entend que ces collaborateurs veulent voir toutes les informations (pouvant certainement en masquer quelques-unes) avant de les fournir au responsable de l'audit interne.

Un autre indice fort intéressant qui m’a été reporté par le consultant expérimenté en audit était le facteur des vacances. Il s’avère qu’il a déjà rencontré des entreprises dans lesquelles un collaborateur ne prenait pas de vacances pendant une année et personne ne faisait attention à ce fait. Concrètement, cela pouvait sous-entendre que l’employé était dans la gestion d’une fraude qu’il avait construite de A à Z en prenant le soin qu’aucun autre employé ne puisse voir ce qu’il était en train de détourner. Je peux également citer d’autres *red flags* comme les transactions inhabituelles, la disparition de documents, l’évolution incohérente de ratios ou tout simplement un manque d’organisation dans la comptabilité.

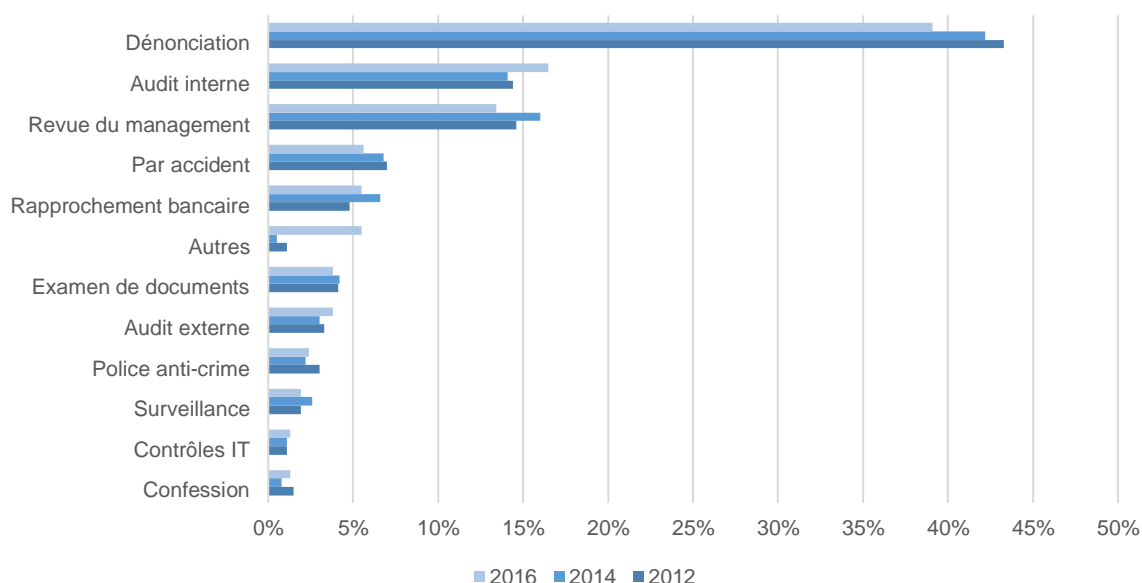
Par conséquent, ces signaux d’alerte permettent aux acteurs de pouvoir détecter la fraude plus rapidement. Cependant, si l’on se fie aux chiffres de l’étude de l’ACFE¹⁰ sous le chapitre des détections de fraude, il faut savoir que la durée moyenne d’une fraude est de 18 mois et a une corrélation positive avec les pertes monétaires. Cela prouve qu’il faut être attentif à ce qui se passe autour de soi lorsque les contrôles sont déficients au sein d’une organisation de manière à éviter qu’une fraude se mette en place sans qu’on s’en rende compte.

De plus, d’après cette même étude, la fraude a été détectée suite à une dénonciation dans 39.1% des cas et dans 5.6% des cas par accident, tandis que 3.8% seulement ont été repérés grâce au contrôle externe qui, je le rappelle, n’a pas comme mission principale de détecter la fraude. Ces chiffres démontrent bien l’importance de la culture d’entreprise et plus particulièrement du *whistleblowing* qui permet de dénoncer de façon anonyme les agissements et opérations étranges d’un collaborateur grâce à différents dispositifs standards tels que le téléphone ou encore les mails.

Pour résumer, il y a différents signaux d’alerte permettant de détecter des fraudes et la plupart de ces dernières peuvent être découvertes par les dispositifs de contrôle, la culture d’entreprise ou par des réactions humaines. Néanmoins, il s’avère que les différentes études indiquent que la plupart des fraudes sont souvent découvertes suite à des dénonciations ou par hasard, et non à l’occasion de contrôles, ce qui prouve l’importance de l’aspect humain dans la lutte contre la fraude financière en entreprise.

¹⁰ Report to the Nations on Occupational Fraud and Abuse 2016

Figure 6 : Différentes formes de détection de fraudes en entreprise



ACFE, Report to the Nations on Occupational Fraud and Abuse, 2016

4.6 Forensic accounting

J'ai appris durant mes entretiens qu'il existe une profession fondamentale dans les investigations lorsque l'entreprise découvrait la fraude : le *forensic accounting*. En effet, l'objectif de l'audit interne n'est pas de découvrir une fraude mais d'identifier les faiblesses dans les processus et procédures qui pourraient avoir un impact sur la marche des affaires. C'est pourquoi le *forensic accounting* arrive pour soutenir l'audit dans les investigations de manière à pouvoir utiliser les travaux dans le cas d'un procès.

Pour ce faire, ces investigateurs vont faire une étude approfondie sur les agissements de la personne accusée en analysant les données personnelles stockées dans les ordinateurs comme les mails, les fichiers ou encore les transactions bancaires à travers des outils de *Big Data* spécialement conçus pour analyser une masse importante de données. L'objectif du *forensic accounting* est également d'étudier de près l'information financière de l'entreprise en étudiant en profondeur les écritures comptables. Ces deux analyses permettent à ces derniers de trouver des détails clés qui résolvent une partie de l'énigme. Puis, il y a souvent une partie de confrontation avec l'accusé en évoquant les données sensibles identifiées en vue de laisser toutes les informations nécessaires à la justice afin qu'elle détermine la condamnation.

5. Analyse : Les données sur le fraudeur en entreprise

5.1 Le portrait-robot du fraudeur en entreprise

Tout individu peut commettre une fraude et à ce sujet l'étude PwC¹¹ a proposé un portrait-robot du collaborateur fraudeur qui est dans la majorité des cas, un homme ayant une fonction de cadre, détenant un diplôme universitaire, entre 31 et 40 ans avec une ancienneté de trois à cinq ans au sein de la société.

C'est généralement un collaborateur apprécié de ses collègues, ayant la confiance de la hiérarchie qui commet des fraudes en entreprise. Aussi surprenant soit-il, cela démontre bien que le fraudeur est souvent quelqu'un que je caractériserais de normal à premier abord, mais qui va être poussé à commettre l'acte à cause de divers aspects psychologiques que je détaillerai lorsque j'aborderai le triangle de la fraude.

Une autre étude provenant de KPMG¹² a également proposé un profil-type du fraudeur en entreprise. Il s'avère que leur proposition a quelques similitudes avec celle de PwC. Pour KPMG, le fraudeur est un homme dans 80% des cas, qui a entre 36 et 55 ans. C'est dans 65% des cas un collaborateur interne de l'entreprise et dans 67% des cas une personne ayant des responsabilités dans l'entreprise.

Ces deux profils proposés mettent en évidence l'importance du *middle management* car ils ont souvent à disposition une masse d'informations sensibles et disposent d'une plus grande facilité à contourner les contrôles mis en place (*Management override*).

5.2 Le processus de la fraude financière

Il y a différentes étapes dans le processus de déroulement de la fraude. Ce processus appelé communément « les 5C » (commettre, camoufler, convertir, chercher, contrôler), est une approche qui m'a permis de mieux comprendre le déroulement de la fraude et la façon d'agir du fraudeur. Ce concept pourrait aider tout dirigeant dans la mise en place de contrôles servant à combattre la fraude financière.

Le processus comporte donc cinq étapes divisées en deux groupes. Le premier groupe comporte les trois premières phases qui concernent directement l'auteur de la fraude :

¹¹ Global Economic Crime Survey 2016

¹² Global profiles of the fraudster 2016

commettre, camoufler, convertir. Tandis que le second concerne la partie étant victime de l'acte : chercher, contrôler.

La première étape est l'accomplissement de la fraude. Cependant, il ne faut pas négliger la phase préparation et planification faite en amont par le fraudeur car c'est elle qui, à mon avis, est l'élément déclencheur de l'acte. J'y reviendrai dans la partie des facteurs déclencheurs de fraudes en illustrant mes propos avec le triangle de la fraude.

Deuxième étape, le fraudeur tentera de cacher son acte, par exemple en manipulant les états financiers ou en falsifiant de la documentation.

En troisième étape, la personne ayant commis l'acte aura comme objectif de convertir son acte par un avantage personnel indu. Un manager sous pression, qui maquille les comptes de l'entreprise de façon à obtenir un bonus supplémentaire dû au fait que son revenu est corrélé aux performances économiques de l'entreprise, aura converti sa fraude en un versement de bonus.

Suite à ces trois premières étapes, viennent ensuite la quatrième et la cinquième étape qui se concentrent plus sur la victime de la fraude, autrement dit l'entreprise. En effet, pour découvrir la fraude, l'organisation victime doit chercher et mener des enquêtes pour trouver le coupable, déterminer l'ampleur de la fraude et apporter des preuves suffisantes pour justifier les éventuelles accusations.

Enfin, la sixième et dernière étape de ce processus : contrôler, a comme objectif de mettre en place de nouveaux contrôles dans le but que la fraude détectée ne se reproduise plus. La revue du système de contrôle interne peut-être déterminant dans cette dernière étape

En résumé, ce déroulement standard de la fraude permet de comprendre le procédé du fraudeur. Néanmoins, pour pouvoir déterminer si un SCI est efficace dans la réduction de probabilité d'occurrence de la fraude il faudrait comprendre ce qu'il se passe avant le déroulement de celle-ci. Autrement dit, il est indispensable d'apporter un complément au SCI en analysant les facteurs déclencheurs de la fraude car c'est là où l'on voit si une fraude va être commise.

5.3 Causes et facteurs déclencheurs de la fraude financière

La deuxième interrogation de mon questionnaire porte sur les causes et facteurs déclencheurs de la fraude. Il me paraît important d'analyser ce qui pousse certains individus à la fraude dans le but d'avoir réellement en tête le cœur de cette problématique. En effet, après avoir discuté avec les différents interlocuteurs je me suis rendu compte que les mêmes causes revenaient sans cesse durant les entretiens.

Effectivement, j'ai pu distinguer deux catégories de causes, une première liée à l'entreprise et l'autre liée à la personne qui commet l'acte.

Concernant la première cause, il s'agit évidemment des failles dans le système de contrôle interne de l'entreprise. À vrai dire, j'ai constaté que dans certaines sociétés, la cause principale provoquant le plus souvent des tentatives de fraude est le manque de ségrégation des tâches dans les activités. A ce sujet, il s'avère que les professionnels de l'audit que j'ai questionnés m'ont affirmé que, dans les petites structures, les chefs de service ne contrôlent pas toujours le travail effectué par les employés en prétextant une confiance aveugle en leur équipe dû au fait qu'ils ont toujours excellé dans leurs missions.

Cependant, ce manque de rigueur dans les contrôles, qui devient par la suite une routine, peut devenir une vulnérabilité pour la société et inciter l'employé à utiliser cette confiance excessive dans le but de commettre une fraude.

De plus, il arrive fréquemment qu'en entreprise, des dirigeants soient mis sous pression lors de la présentation des objectifs. La pression sur les résultats de l'entreprise par exemple, pousse parfois certains dirigeants à utiliser la fraude comptable en enregistrant des revenus de manière décalée. Cela arrive souvent lorsque la rémunération d'un salarié est corrélée avec les performances de l'entreprise ou lorsque les dirigeants veulent masquer provisoirement les difficultés rencontrées afin de rassurer les actionnaires et démontrer que leur stratégie est la bonne. Ce procédé consiste à enregistrer le chiffre d'affaire du mois de janvier par exemple au mois de décembre, afin de pouvoir satisfaire la hiérarchie. Il m'a été expliqué par l'expert-comptable, responsable en audit interne et m'a confirmé avoir été confronté à ce genre de situation.

La deuxième catégorie, liée à la personne, concerne plus le côté éthique, les valeurs ainsi que la situation personnelle du fraudeur. Effectivement, on m'a souvent réitéré que le fraudeur a un style de vie extravagant en m'évoquant des employés instables financièrement étant accroc au casino ou aux stupéfiants. Certes, ce sont des cas extrêmes, mais qui existent bel et bien dans le monde professionnel. Par ailleurs, on m'a également parlé de personnes ayant une certaine pression sociale en ce qui concerne leur statut, les incitant à vivre au-delà de leurs moyens.

En d'autres mots, des individus n'ayant ni éthique ni valeurs, avec des problèmes d'argent et une envie de nuire à la société par manque de reconnaissance, pourraient devenir une menace au sein de l'entreprise.

Pour résumé, l'analyse du système de contrôle interne de l'entreprise est un facteur important dans la dissuasion des tentatives de fraude. Cependant, il est également important de prendre en considération l'aspect humain dans l'analyse des causes et facteurs déclencheurs. Je pense que le contexte dans lequel agit le fraudeur est incontestablement tout aussi important que la bonne application des procédures et processus dans l'entreprise. Autrement dit, analyser l'état d'esprit, le fonctionnement psychologique et la façon de procéder du fraudeur doit également être exécuté lorsque le sujet est abordé, afin de pouvoir compléter le processus d'identification et de prévention du risque de fraude.

5.3.1 Triangle de la fraude

Lors de mes entretiens, tous m'ont affirmé que les causes et facteurs déclencheurs de la fraude en entreprise peuvent être identifiés et avoir un début d'explication à travers l'analyse du triangle de la fraude de Donald R. Cressey. Ce dernier a créé en 1986 un outil d'analyse représentant l'environnement favorable aux actes de fraude. En effet, le schéma du triangle de la fraude distingue trois éléments interdépendants : la motivation (ou la pression), l'opportunité et la justification, pouvant aboutir à un acte de fraude dans une entreprise détenant des dysfonctionnements ou des failles au niveau de son système de contrôle interne.

5.3.1.1 Motivation/Pression

Pour commencer, comme je l'ai dit à plusieurs reprises, l'individu qui commet un acte est conscient d'enfreindre les règles de la société et sait qu'il pourrait y avoir des conséquences graves à assumer. Ces conséquences pourraient être une amende, une condamnation, un licenciement ou encore une carrière détruite (*blacklist*), voire même

un suicide. Cette notion de conscience est un élément essentiel dans l'analyse du premier facteur du triangle de la fraude car la motivation du fraudeur se manifeste par une prise de risque énorme pour lui. Il en est conscient mais une forte motivation ou une pression excessive subie par son environnement le pousse à vouloir agir.

Comme je l'ai dit précédemment un motif qui motive les fraudeurs à passer à l'acte est leur problème d'argent ou encore la pression sociale. D'autres facteurs peuvent également être liés à ce premier élément du triangle de fraude :

- Pression de la hiérarchie sur les performances de l'entreprise
- Envie de s'enrichir
- Volonté de diffuser une bonne image auprès des parties prenantes

5.3.1.2 Opportunité

Ensuite, il y a l'opportunité de passer à l'acte qui est souvent relative en fonction de la personne. C'est-à-dire que l'opportunité peut se présenter à tout moment pour un collaborateur au sein d'une entreprise dans laquelle le SCI n'est pas abouti ou mal utilisé. Malgré cela, le fait de saisir cette opportunité et d'exploiter les failles de l'entreprise ne sera pas fait par tout le monde. L'intégrité d'une personne et son éthique pourront empêcher le passage à l'acte. Par contre, si un individu parfaitement honnête se voit offrir une opportunité de commettre une fraude en sachant que la société ne la découvrira pas ; saisira-t-il cette opportunité ?

Prenons un exemple concret dont je vous ai fait part en début de mémoire. Le vol dans la caisse de l'hôpital est un fait simple mais qui illustre parfaitement ce deuxième élément du triangle de la fraude. Le collaborateur en question a profité du manque de rigueur de la part de son chef dans le contrôle de la caisse (faille dans le SCI, non-respect de la procédure) et en a donc profité pour saisir cette opportunité.

C'est donc l'absence ou une complexité trop élevée des contrôles au sein des organisations qui, d'une façon ou d'une autre, favorise le risque de fraude et permet au criminel économique d'avoir des occasions pour opérer.

5.3.1.3 Rationalisation

Enfin, le dernier composant du triangle de la fraude se distingue des autres car il apparaît lorsque l'acte a été commis : la rationalisation. Il est vrai que le fraudeur peut, dans une certaine mesure, tenter de justifier ses actes dans le but de garder une certaine perception positive de lui-même, d'où l'importance de comprendre le

fonctionnement psychologique de l'individu. Une justification souvent rencontrée dans les PME par l'un des professionnels que j'ai questionnés était « tout le monde le fait dans l'entreprise ». Ou encore, lorsqu'un dirigeant est élu à la place de son concurrent qui lui est en place depuis plus longtemps dans l'entreprise, il trouvera sa justification en s'appropriant un bonus indu de façon à se faire justice lui-même.

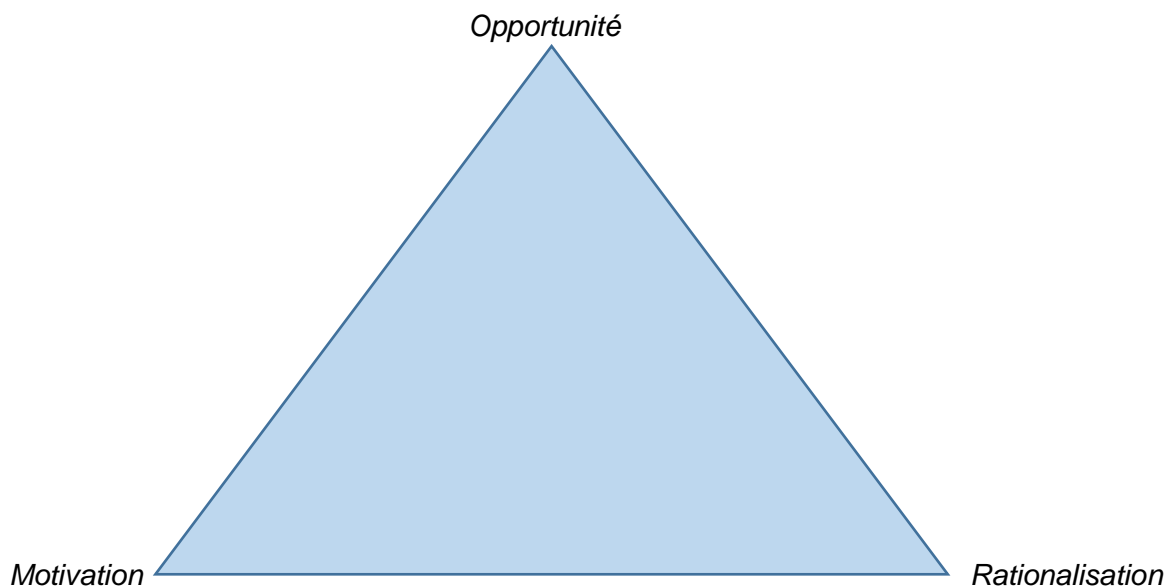
Ceci montre bien que les fraudeurs tentent toujours de rationaliser leurs actes afin de ne pas se sentir coupables d'un acte illégal.

D'autres formes de justification peuvent faire leur apparition, en voici quelques-unes :

- « Je protège les intérêts de l'entreprise, il n'y avait pas d'autres solutions que de frauder »
- « C'est une fraude temporaire, ne vous en faites pas, elle n'aura pas d'impact car j'ai joué avec des petits montants »
- « J'ai subi trop de pression, je n'avais pas d'autres choix que de frauder, sinon je perdais mon poste »

En résumé, le triangle de la fraude est un excellent modèle qui m'a permis de pouvoir guider mon analyse et d'identifier les éléments que le SCI peut cibler pour être efficace face à la fraude financière.

Figure 7 : Le triangle de la fraude



Donald R. Cressey, 1986

6. Résultats : Les aspects d'un SCI efficace face à la fraude financière

Suite à l'analyse de mes données, j'ai décidé de pousser la réflexion dans cette troisième partie en relevant différents éléments du COSO notamment, de manière à déterminer si le SCI recouvre bien tous les aspects pour assurer la protection d'une entreprise face à la fraude financière.

6.1 Composantes du COSO appliquées au risque de fraude

Il m'a paru important de faire un *focus* sur les aspects du COSO qui permettent aux entreprises utilisant le référentiel de lutter contre ce fléau. En effet, comme dit en début de mémoire, le COSO a cinq composantes qui peuvent cibler la fraude, chacune d'une manière différente, sous plusieurs angles. La combinaison entre les cinq composantes permet justement à la société de créer un environnement dans lequel la fraude n'est pas réalisable.

Environnement de contrôle : C'est la base de la pyramide et doit donc apporter à l'entreprise des piliers lui permettant de lutter contre la fraude comme par exemple :

- Charte de valeurs et éthique
- Cahier des charges
- Règlements et procédures internes documentées
- « Tone at the middle » et/ou « Tone at the top »

Evaluation des risques : L'évaluation des risques doit faire l'objet d'une étude approfondie de l'entreprise de façon à pouvoir recenser les risques de fraude en prenant en considération les facteurs favorisant les fraudes ainsi que les schémas. Il est important d'impliquer tout le personnel dans l'identification des risques de fraude et ce régulièrement.

Activités de contrôles : La ségrégation des tâches ainsi que les procédures et processus documentés doivent être suivis à la lettre au sein de la société afin d'éviter des tentatives de fraude.

Information et communication : L'importance dans la lutte contre la fraude réside également dans la circulation de l'information en interne et en externe. Faire comprendre à toutes les personnes concernées par ce sujet que l'entreprise dispose d'un programme de gestion du risque de fraude, de formation spécifique ou d'outils

performants permettra d'une part de sensibiliser ces derniers et de l'autre repoussera les *hackers* d'une éventuelle attaque.

Pilotage : Outre les tableaux de bords utilisés par le contrôle de gestion, le pilotage *focus fraud* sera plus utilisé par l'organe indépendant de la société qui tâchera d'évaluer le SCI, afin de l'améliorer en fonction des évolutions technologies ou légales.

D'un point de vue personnel et en prenant du recul sur mon année d'expérience au sein d'un grand groupe bancaire, je me suis rendu compte que les composantes du COSO étaient bel et bien présentes.

Tout d'abord si l'on reprend dans l'ordre les cinq composantes, au niveau de l'environnement de contrôle, j'ai tout de suite remarqué qu'il y avait énormément de procédures documentées, des processus bien précis à suivre, des contrôles rigoureux à faire ainsi qu'une certaine exemplarité de la part de mon supérieur dans la gestion de l'équipe. Me situant au sein d'un service où se trouvait tous les lingots d'or, les chèques, l'argent liquide et les titres de la banque, il était très important d'effectuer des contrôles permanents, notamment lors de réception de lingots d'or, de cash ainsi que des chèques. Par ailleurs, la caisse était contrôlée tous les jours en début et en fin de journée, ce qui démontre bien que l'opportunité de commettre une fraude était nulle.

En ce qui concerne l'évaluation des risques je dois dire que j'ai été chanceux de pouvoir évoluer dans un service riche en missions où à travers un seul service se concentrent trois activités importantes du *back-office* : Caisse-Coffres-Portefeuille. Une sorte d'évaluation des risques s'est faite lors d'une réunion où mes anciens collègues ont fait part de leur inquiétude quant aux protections de l'argent (peur de vivre un braquage ou un simple vol). Suite à cela, mon supérieur a directement remonté l'information afin de voir ce qu'il était possible de faire.

La troisième composante du COSO au sein d'une banque est certainement l'une des plus importantes. En effet, j'ai été impressionné de voir que tout était organisé de manière à ce que chacun ait des responsabilités et qu'un encaissement de chèque par exemple ne puisse pas se faire sans la validation de deux collaborateurs au minimum (contrôle quatre yeux) voire trois lorsqu'il s'agissait d'un certain montant. J'étais au sein d'un service où j'avais l'impression qu'il n'y avait aucune faille exploitable pour d'éventuels criminels économiques et je dois dire que j'appréciais me lever chaque jour

afin de pouvoir évoluer dans un environnement si structuré où l'on sentait que les valeurs et procédures étaient respectées.

Concernant l'information et la communication, en rentrant dans la banque j'ai suivi une semaine de formation assez intense et notamment une journée spécialement dédiée à la sécurité informatique (cybercriminalité) et au blanchiment d'argent. J'ai donc été sensibilisé à ces deux notions et durant toute mon année j'avais en tête les différents risques existants grâce à cette journée. Ceci démontre bien qu'une formation sur la fraude dans les premiers jours en entreprise pourrait éviter bon nombre de cas. Cependant, je pense qu'il serait plus important de recruter du personnel intègre, ne nécessitant pas de formation, mais comme dirait un célèbre proverbe : « mieux vaut prévenir que guérir ».

Enfin au niveau du pilotage, j'ai pu m'apercevoir que mon responsable devait fréquemment préparer la synthèse des différents résultats de l'équipe et des éventuels dysfonctionnements des systèmes informatiques, dans le but de pouvoir transmettre cela aux auditeurs, afin de voir les possibilités d'améliorations dans les processus du service dans lequel j'évoluais.

En résumé, les composantes du COSO peuvent être utilisées dans la lutte contre la fraude et donc un système de contrôle interne comme celui détaillé ci-dessus peut être un réel atout dans la prévention des tentatives de fraude.

6.2 SCI face au triangle de la fraude : cibler l'opportunité

Durant mon entretien avec l'expert-comptable, responsable d'audit interne dans le domaine bancaire, nous avons pu discuter longuement sur la fraude et il m'a fait réfléchir sur un aspect auquel je n'avais pas pensé au départ. En effet, il m'a guidé dans ma réflexion en me posant la question suivante : Est-ce que le triangle de fraude est bien pris en considération dans le COSO ? Comme je l'ai dit précédemment, le contrôle interne a plusieurs caractéristiques qui lui permettent d'apporter une plus-value à l'entreprise (cf. éléments de définition du contrôle interne) en termes de gestion globale. Effectivement, le fait de pouvoir évaluer son SCI afin de l'améliorer en adaptant les contrôles et processus à l'évolution des marchés lui permet d'avoir une certaine valeur ajoutée pour maîtriser sa marche des affaires, mais pas que.

Concrètement, la mise à jour du référentiel COSO, dont je vous ai parlé dans la toute première partie, a permis d'apporter des évolutions en prenant en compte cette

problématique majeure, ce qui donne à ce *framework* une valeur ajoutée certaine à ceux qui l'utilisent. Le principe n°8 portant sur l'évaluation de la fraude a été rajouté afin de permettre à ce référentiel d'être à jour par rapport à l'augmentation des tentatives de fraude en entreprise. Il est donc important de pouvoir intégrer dans sa gestion des risques la fraude, afin de pouvoir agir de manière proactive dans le but d'avoir une certaine maîtrise de ce dernier. Pour ce faire, il est important d'utiliser un outil essentiel : la cartographie des risques, dans le but de pouvoir calculer la probabilité d'occurrence de ce risque afin de mieux le gérer.

Durant mes entretiens il a été dit que le contrôle interne pouvait être la clé en ce qui concerne la maîtrise du risque de fraude, du moment que les contrôles sont bien exécutés et que le système soit réévalué au moins une fois par année. On ne pourra certes pas dire que grâce à cela le risque de fraude devient nul, mais si l'on s'assure qu'il y a un dispositif en place adapté, clair et suivi, alors cela donnera une assurance raisonnable dans la gestion de ce risque.

Pour démontrer la réelle valeur ajoutée du contrôle interne dans la maîtrise du risque de fraude, il me paraît important de faire le lien entre le triangle de la fraude, concept dont je vous ai parlé dans la deuxième partie et le COSO. Je rappelle que le COSO est un référentiel permettant à toute entreprise de mettre en place un système de contrôle interne, néanmoins il n'est pas là pour donner la solution ultime. C'est à la société de modéliser au mieux un SCI qui soit adapté à sa structure et aux évolutions.

D'autre part, dans le triangle de la fraude nous avons vu les trois éléments clés schématisant les causes et facteurs déclencheurs de la fraude. L'élément qui est directement en lien avec le SCI d'une entreprise est l'opportunité. La motivation ou la pression d'un employé est plus dans l'aspect éthique des affaires et psychologique de la personne, et la justification se produit lorsqu'il y a eu le passage à l'acte. Autrement dit, l'opportunité est un élément important du triangle de la fraude et c'est précisément là-dessus que le contrôle interne apporte sa valeur ajoutée.

En résumé, si au sein d'une entreprise il y a un SCI compris par tous les acteurs qui est appliqué rigoureusement avec des contrôles simples, efficaces et surtout avec un personnel impliqué, l'opportunité pour un employé de passer à l'acte devient quasi nulle, étant donné qu'il aura devant lui aucune faille à exploiter. D'après moi, cela démontre bien que le contrôle interne a une réelle valeur ajoutée dans la lutte contre la fraude et peut être une des clés pour réduire la probabilité d'occurrence du risque de fraude.

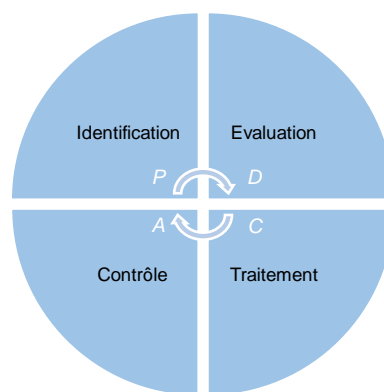
6.3 *Risk Assessment* : un dispositif indispensable

Pour compléter mon analyse et étant dans la partie concernant les aspects d'un SCI efficace pour la prévention et la détection de la fraude, il me paraît évident d'apporter quelques éclairages sur un modèle de gestion des risques que toute entreprise doit adopter en utilisant notamment la cartographie des risques, qui servira de document de base pour guider la gestion des risques.

Pour compléter le système de contrôle interne, il est primordial d'avoir une gestion des risques qui soit revue régulièrement de façon à identifier les nouveaux risques pouvant empêcher l'entreprise d'atteindre ces objectifs. Cette démarche doit s'inscrire dans un processus continu et dynamique.

Voici les quatre étapes qui me paraissent essentielles dans un dispositif de gestion des risques au sein d'une société :

Figure 8 : Processus du *Risk Assessment*



Identification des risques : Après avoir identifié les objectifs de l'entreprise, les activités et les processus de la société, il est important de lister tous les risques qui leurs sont liés. Cette première étape est indispensable, car chaque risque doit être recensé, quel que soit son degré d'impact ou de probabilité. Il est également important de toujours avoir en tête les facteurs d'influence externes lors de l'identification des risques. Des facteurs pouvant provenir de l'environnement : Politique, Economique, Social, Technologique, Environnemental et Légal (PESTEL).

Evaluation des risques : Ici il s'agit de procéder à l'analyse des risques de l'entreprise à partir des données internes et externes. C'est ici qu'il faudra évaluer la criticité des risques en multipliant l'impact par la probabilité. Par la suite, il sera possible de visualiser cela grâce à la cartographie des risques que la société mettra en place.

La fraude financière et le contrôle interne en entreprise : l'importance d'un SCI efficient pour optimiser l'identification des risques de fraude et réduire leur probabilité d'occurrence.

De plus, je pense qu'il peut être judicieux de classer les risques selon leurs catégories (financiers, opérationnels, sécurité, etc.).

Traitement du risque - Evaluation du degré d'aversion au risque : Une fois les risques identifiés et évalués, il me semble important de pouvoir discuter, avec le Conseil d'Administration et la Direction, du niveau de tolérance de la société. Selon le *risk appetite*, différents leviers seront actionnés. A savoir, s'il y a une faible tolérance, de fortes mesures seront mises en place. Au contraire, s'il y a une forte tolérance au risque, de plus faibles mesures seront proposées.

De plus, il est important d'avoir en tête l'optimum économique, c'est-à-dire évaluer le coût d'occurrence par rapport au coût de prévention du risque. Effectivement, il n'est pas pertinent de mettre en place des mesures de traitement de risques si les coûts de celles-ci sont supérieurs au coût d'occurrence. C'est donc dans cette troisième étape où l'on mettra en place un suivi et où l'on définira les mesures à adopter (éviter, réduire, supporter ou transférer).

Contrôle du risque – Formalisation / Surveillance : Dans cette dernière étape, il s'agira de formaliser les contrôles. Ce sera utile non seulement pour la Direction, mais également pour les collaborateurs de l'entreprise qui en seront les principaux acteurs. Pour formaliser, il sera important de nommer les différents risques choisis par processus et objectifs et décrire quels sont les contrôles ou mesures mis en place contre ceux-ci. Le Responsable du contrôle ainsi que la fréquence de contrôle devront également être mentionnés. Il sera également essentiel de procéder à une surveillance, en fonction de la situation, de façon à pouvoir s'assurer que le contrôle a été effectué correctement.

Enfin, il est également important de mentionner la situation avant et après la mise en place de mesures de contrôle. Ainsi, nous aurons le risque brut, les contrôles et ensuite le risque net.

En résumé, il y a différentes représentations possibles pour la cartographie des risques comme le *Risk Map* ou encore le diagramme de KIVIAT. Cela reste un outil de gestion qui doit évoluer au fil du temps et ne pas rester statique. Il sert principalement à avoir une vue d'ensemble des risques majeurs de l'entreprise en les hiérarchisant, de façon à pouvoir réduire leur probabilité d'occurrence en optant pour des actions bien spécifiques.

6.4 La cartographie des risques

J'ai décidé d'illustrer mes propos à travers un exemple concret de manière à prouver que la cartographie des risques a une réelle valeur ajoutée dans la maîtrise des risques de fraude. Pour ce faire, j'ai décidé de me baser sur mon expérience professionnelle au sein d'un établissement financier et de notamment me concentrer sur le service dans lequel j'étais : Caisse-Coffres-Portefeuille, qui est d'après moi un service qui pourrait être ciblé par les tentatives de fraude.

Mon approche ne recensera pas tous les risques du domaine bancaire mais uniquement des risques de fraude pour rester dans le sujet de ce mémoire. Dans cette optique, j'ai tout d'abord identifié dix risques de fraude répartis en deux familles de fraudes : internes et externes.

Voici donc l'inventaire des différents risques que j'ai pu identifier :

Tableau 2 : Inventaire des risques de fraude dans le domaine bancaire

Catégorie de fraude	Risque identifié	Référence
Fraude interne	Détournements d'actifs	R1
Fraude interne	Manipulation taux	R2
Fraude interne	<i>Management override</i>	R3
Fraude interne	Documents internes falsifiés	R4
Fraude interne	Fraude comptable	R5
Fraude externe	Cybercriminalité	R6
Fraude externe	Chèques frauduleux	R7
Fraude externe	Fraude en président	R8
Fraude externe	Braquage	R9
Fraude externe	Usage de faux documents	R10

Comme vous pouvez le voir, j'ai décidé de donner une référence à chaque risque afin de pouvoir les distinguer et les repérer rapidement dans la cartographie des risques. Par la suite, j'ai donc évalué les différents risques listés à la page précédente en mesurant la probabilité et l'impact de chacun dans le but d'avoir la criticité et pouvoir ainsi déterminer quels sont les risques prioritaires auxquels la banque devrait faire attention.

Tableau 3 : Mesure et hiérarchisation des risques

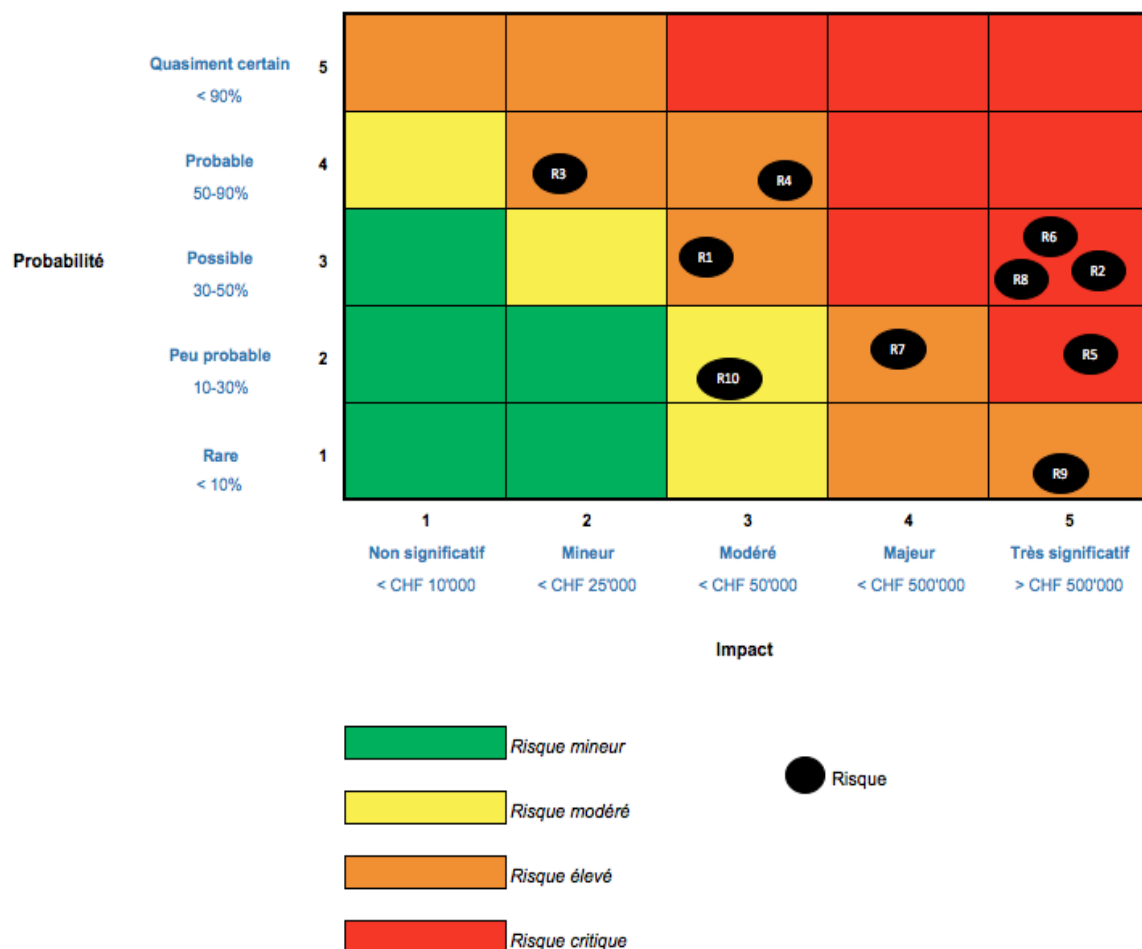
Référence	Probabilité	Impact	Criticité	Résultat	Risques majeurs
R1	3	3	9	Risque élevé	-
R2	3	5	15	Risque critique	Prioritaire
R3	4	2	8	Risque élevé	-
R4	4	3	12	Risque élevé	-
R5	2	5	10	Risque critique	Prioritaire
R6	3	5	15	Risque critique	Prioritaire
R7	2	4	8	Risque élevé	-
R8	3	5	15	Risque critique	Prioritaire
R9	1	5	5	Risque élevé	-
R10	2	3	6	Risque modéré	-

Une fois les dix risques évalués, j'ai pu obtenir la criticité de manière à pouvoir ensuite définir, grâce à la cartographie des risques, les plus dangereux pour l'entreprise.

Par conséquent, j'ai créé un *Risk map* avec le programme Excel, qui m'a permis de placer les différents risques dessus, me permettant de voir en moins de trente secondes les risques critiques de la banque.

Voici la cartographie des risques de fraude que j'ai créée sous la forme de *Risk Map* :

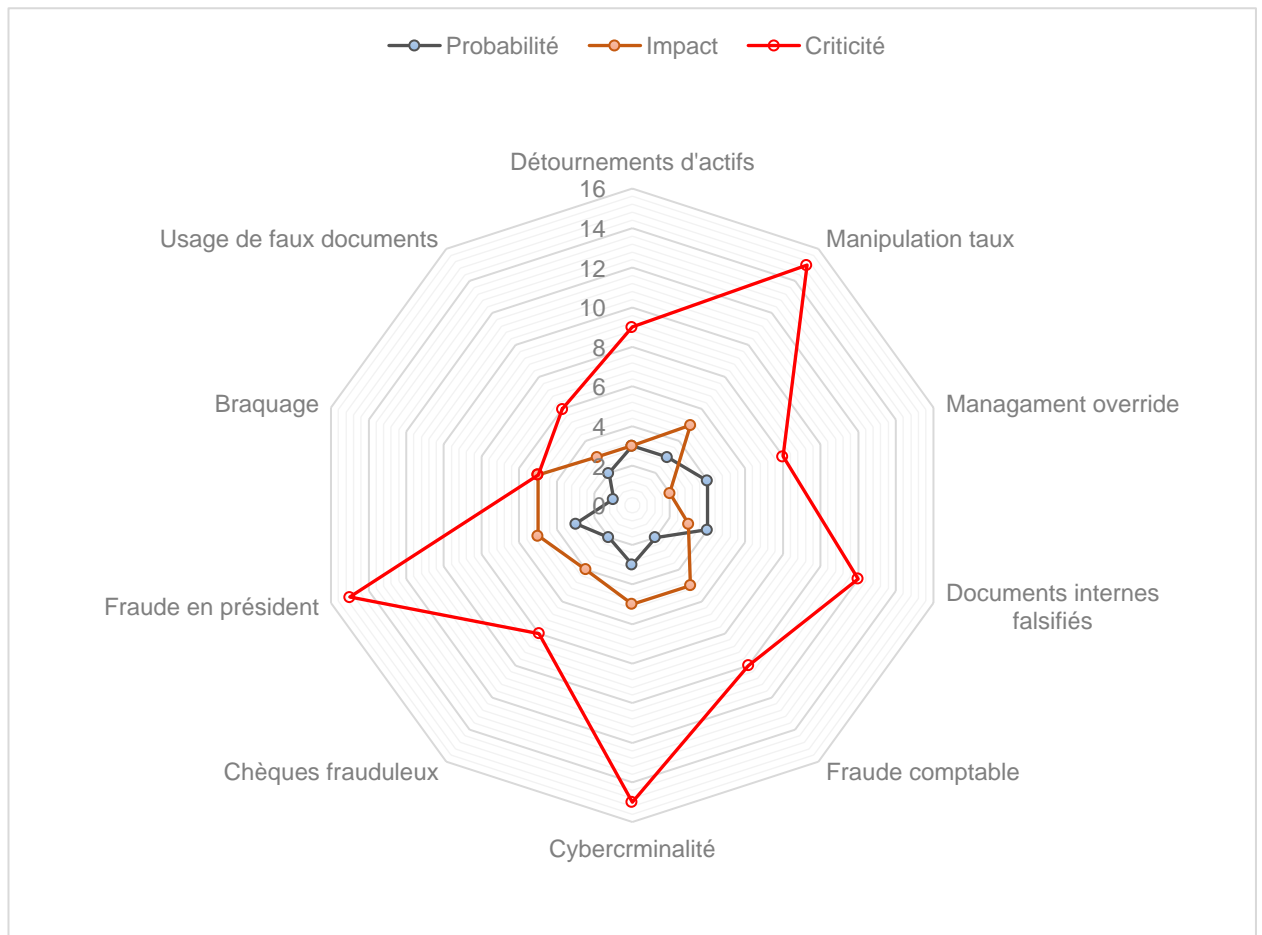
Figure 9 : Cartographie des risques en *Risk Map*



La cartographie ci-dessus démontre bien son importance dans la gestion des risques d'une entreprise. On peut voir très clairement les différents risques majeurs qui se distinguent des autres dans la zone rouge. Je pense que la force principale de cet outil réside dans sa capacité à synthétiser l'information de manière claire et efficace. En me basant donc sur cette cartographie de risque, je peux m'apercevoir qu'il y a quatre risques critiques qui doivent absolument être pris en charge. Il faudrait donc proposer différentes actions pouvant réduire la probabilité ou l'impact de ces derniers de façon à sortir du rouge.

De plus, j'ai également décidé de représenter les différents risques à travers le diagramme de KIVIAT, sous forme de radar car c'est également un excellent visuel pour distinguer les différents risques :

Figure 10 : Cartographie des risques en diagramme de KIVIAT



Selon le graphique ci-dessus, la criticité est le produit des deux facteurs : probabilité (bleu) et impact (orange) qui permettent de voir (en rouge) la hiérarchisation des risques critiques, autrement dit, la criticité. D'autre part, l'impact pourrait viser plusieurs aspects comme la réputation, le chiffre d'affaire ou encore le cours de bourse. En somme, cette deuxième forme de représentation permet de distinguer les différents risques majeurs en termes de fraude tout comme le premier tableau dans le but d'apporter des actions correctrices pour réduire la criticité de ces derniers.

Une fois la cartographie en place, il sera important d'opter pour des dispositifs de prévention pour réduire la probabilité d'occurrence de la fraude et des outils de détection pour réduire l'impact des différents risques. A ce sujet, si je reprends les différents risques identifiés en amont, je proposerai différentes actions qui permettrait de réduire la criticité :

Tableau 4 : Propositions d'actions pouvant réduire la criticité des risques

R1. Compter la caisse en fin de journée et avoir obligatoirement deux collaborateurs avec chacun un code pour ouvrir le coffre.
R2. Contrôle quatre yeux et validation manuelle.
R3. Sensibiliser les managers et faire des sondages anonymes auprès des collaborateurs. Ne pas attribuer tous les contrôles à un seul manager.
R4. Communication plus transparente avec le client en termes de contrat et utiliser le « call-back ».
R5. Ségrégation des tâches. Contrôle quatre yeux. Obligation de faire un « check » avant de valider les comptes.
R6. Former les collaborateurs IT aux nouvelles techniques de cyberattaque. Obtenir des serveurs de sauvegarde en cas d'urgence.
R7. Contrôle quatre yeux et faire attention aux profils d'utilisateurs dans les logiciels de façon à éviter qu'une personne puisse saisir et valider la transaction. Avoir une personne de contact dans chaque banque émettrice de chèques.
R8. Sensibiliser les collaborateurs à ce risque en mettant en place une formation spécifique démontrant les bonnes pratiques à avoir lors d'un cas exceptionnel. Mettre en place une requête dans le logiciel bloquant une transaction inhabituelle.
R9. Appliquer les normes de sécurité requises et s'assurer que les accès sont inconnus des individus externes à l'entreprise. Souscrire une assurance en cas de vol ou de casse.
R10. Contrôle quatre yeux et apporter un regard neutre lorsqu'un client habitué vient apporter de nouveaux documents afin de s'assurer que la procédure de contrôles est bien appliquée.

Une fois le traitement choisi pour chaque risque, il sera important de formaliser le tout dans le but d'avoir un suivi pour chacun. Pour ce faire, j'opterais pour la création d'une fiche analytique pour chaque risque afin d'assurer un suivi efficace.

Tableau 5 : Fiche analytique pour les détournements d'actifs

(R1) Détournements d'actifs : Risque élevé	
<i>Description</i>	Soustraction illicite d'actifs monétaires (caisse) ou physiques (lingots d'or, chèques, titres)
<i>Criticité (Probabilité & Impact)</i>	9 (3 & 3)
<i>Causes et facteurs déclencheurs</i>	<ul style="list-style-type: none"> • Comptage de la caisse effectué aléatoirement. • Facilité d'accès au coffre ou à la caisse. • Codes détenus uniquement par un collaborateur.
<i>Traitement</i>	A réduire la probabilité d'occurrence et l'impact.
<i>Objectif</i>	Réduire la criticité du risque pour assurer la maîtrise du risque et le faire passer en tant que risque mineur.
<i>Contrôles/Actions à effectuer</i>	<ul style="list-style-type: none"> • Compter la caisse quotidiennement. • Avoir obligatoirement deux collaborateurs avec chacun un code pour ouvrir le coffre. • Obtenir une assurance vol.
<i>Responsable</i>	Monsieur C.
<i>Mesure de l'efficacité des contrôles/actions</i>	Revu des contrôles mensuellement et feedback (rapport sur les lacunes) du responsable auprès de la hiérarchie.

Pour terminer, il s'avère qu'un dispositif de gestion des risques accompagné d'une cartographie des risques adéquate apporte au SCI de la société en question un moyen efficace pour lutter contre la fraude.

A travers cette démarche, j'ai pu identifier les risques de fraude, déterminer les causes et vulnérabilités ainsi que différentes actions à appliquer qui pourraient être bénéfiques pour l'entreprise.

J'ai pu avoir une approche préventive en me concentrant sur la probabilité d'occurrence du risque de fraude, en proposant par exemple le comptage quotidien de la caisse pour le détournement d'actifs. De plus, j'ai également pu avoir une approche détective en concentrant ma réflexion sur l'impact que ce risque pourrait avoir, et ce grâce au calcul de la criticité. En d'autres termes, grâce à une simple cartographie des risques, l'entreprise peut identifier les risques de fraude et ainsi déterminer des actions préventives et détectives pour assurer une bonne maîtrise de ces derniers. Ceci démontre bien que ce dispositif est un outil indispensable, permettant à l'entreprise d'agir de manière proactive et d'assurer un certain contrôle de ses activités.

6.5 L'importance de l'IT pour un SCI efficient

Pour faire le lien avec la dernière catégorie de fraude dont je vous ai parlé en fin de deuxième partie, il me semble important de consacrer une partie sur l'importance de l'informatique en entreprise dont on m'a fait part durant mes différents entretiens. En revenant toujours sur l'exemple de mon année au sein du grand groupe bancaire, j'ai pu remarquer que tout était informatisé. Autant vous dire qu'une panne informatique ou une cyberattaque pouvait bloquer une partie voire la totalité des activités du service. En effet, lors de mon entrée j'ai reçu un panel d'accès concernant les différents logiciels que j'allais devoir utiliser, ce qui est d'après moi un point d'attention très important dans la gestion du risque de fraude car une bonne gestion des mots de passe est primordiale au sein d'une organisation.

J'ai pu effectivement remarquer que tous au sein de l'équipe avions un profil d'utilisateur nous permettant de faire seulement certaines actions bien spécifiques. Par exemple, pour ouvrir le coffre de la banque, deux personnes étaient requises, chacune ayant un code différent qui lorsqu'ils étaient assemblés, permettaient d'ouvrir le coffre. Ou encore, lorsque j'encaissais les chèques pour un client, mon profil d'utilisateur me permettait uniquement d'introduire l'écriture dans le système, puis la validation se faisait par mon supérieur. Cette simple distinction à travers des profils utilisateurs est, je pense, un moyen efficace de prévention contre la fraude.

J'ai par ailleurs vécu un cas que je caractériserais d'exceptionnel durant cette année 2013 (on m'a assuré que ce n'était pas arrivé depuis longtemps). Effectivement, il y a

une matinée où certains logiciels et programmes étaient hors-service. C'était certainement dû à une simple panne informatique, mais ce qui est sûr c'est que le département IT a su réparer l'incident en peu de temps et a eu une communication continue avec notre service.

Le deuxième point d'attention donc, est la capacité de l'entreprise à gérer des situations extrêmes en peu de temps tout en gardant une certaine circulation de l'information. Disposer par exemple de serveurs de sauvetage ou encore garder les serveurs dans un local adapté (aération, espace) sont également des facteurs très importants pour éviter d'avoir des dysfonctionnements dans le système d'information.

En somme, je pense qu'une journée de formation ou sensibilisation à la sécurité informatique de la société dans laquelle on se trouve est primordial car les sociétés sont souvent bien protégées contre les virus et *hackers*, malgré que la menace interne reste permanente si l'on ne sait pas qui se trouve à côté de nous. Durant la formation, plusieurs exemples étonnants de ce qui pouvait se faire en entreprise dans la gestion des mots de passe par les employés ont été donnés comme le *post-it* avec le mot de passe, collé sous le clavier ou sur l'écran, ou encore quitter son lieu de travail en oubliant de fermer sa session. Cela peut paraître évident, mais démontre bien que l'application rigoureuse des procédures par les employés est quelque chose d'essentiel si l'entreprise veut éviter des intrusions, du sabotage ou tout simplement des vols de données.

6.6 Au-delà des procédures : la culture d'entreprise

Avant de boucler cette troisième partie, j'ai décidé de relever un aspect qui est tout aussi important que les procédures et qui doit être inclus dans l'ensemble du système de contrôle interne pour former une armure solide contre la fraude. En effet, la formation est un élément clé permettant aux employés d'être aptes à réaliser différentes missions avec précision au sein de la société et d'apporter une certaine motivation à ces derniers. Autrement dit, la formation peut servir d'une certaine manière à inculquer un « esprit contrôle interne » au sein de l'organisation dans laquelle les collaborateurs puissent comprendre les raisons de leurs contrôles. Il est important qu'ils connaissent également, les différents niveaux de contrôles et leur valeur ajoutée de ces derniers, afin qu'ils n'aient pas le sentiment d'être un pion parmi les autres, servant uniquement à contrôler et valider des opérations sans connaître la raison.

De plus, la communication sur la fraude est d'après moi un deuxième point très important. Toute société doit démontrer que ça ne doit plus être un sujet interdit en entreprise, mais qu'il existe bel et bien des risques de fraude pouvant arriver dans n'importe quelle structure. Comme je vous l'ai dit, les personnes ne parlent pas spontanément de fraude, y compris moi. J'ai effectivement choisi ce sujet, pourtant lorsque j'allais aux entretiens, j'avais une certaine appréhension par rapport aux réponses que j'allais obtenir (trop vagues, confidentielles). Au final, je me suis rendu compte que les professionnels avec qui j'ai pu discuter tout au long de mon mémoire ont été très clairs dans leur approche : « il faut parler de la fraude, c'est un sujet important dans le monde des entreprises qui doit être démocratisé ». Je veux dire par là que communiquer sur la fraude peut aider une entreprise à indirectement créer un environnement sûr pour les employés.

Comme dit précédemment, une entreprise qui communique sur la fraude et qui démontre qu'elle a des moyens en place et qu'elle consacre du temps dans la lutte contre cette dernière sera potentiellement moins ciblée par les resquilleurs. Au contraire, une entreprise dans laquelle on ressent une certaine inquiétude lorsque l'on parle de fraude, car considérée comme un sujet délicat, donnera le sentiment d'être dans une organisation qui n'est pas sûre de ses moyens et qui conserve donc certainement des failles exploitables pour les fraudeurs.

Pour finir, à travers mes différentes recherches, j'ai pu m'apercevoir que l'on parlait beaucoup de procédures, de systèmes informatiques ou encore d'outils utilisés contre la fraude. Cependant, je pense que l'aspect humain dans toute cette histoire est parfois oublié. Certes, il faut des machines pour contrer les tentatives de fraude. Certes, il faut des procédures qui doivent être suivies à la lettre pour avoir une organisation optimale. Or, le cœur du problème vient d'une personne qui commet l'acte et c'est donc sur cette base là qu'il faut creuser afin de savoir si une bonne culture d'entreprise permettrait d'éviter cela. En d'autres termes, il faut faire en sorte que le potentiel fraudeur trouve une raison de travailler, car le bien-être des employés est d'après moi un facteur important dans la prévention contre la fraude. Si l'on reprend le triangle de la fraude de Donald R. Cressey, un collaborateur ayant un certain bien-être dans l'entreprise n'aura pas de motivation (élément déclencheur) à proprement parler pour commettre un acte de fraude car il sera en adéquation avec les valeurs et la culture de l'entreprise, et ne pourra de ce fait pas agir à l'encontre de ses principes.

7. Synthèse : « Le Trèfle Anti-Fraude »

Après avoir analysé toutes mes données et les différents outils permettant à une entreprise de pouvoir gérer ses risques et plus particulièrement le risque de fraude, j'ai décidé d'apporter une proposition en matière de gestion du risque de fraude en m'inspirant notamment du triangle de la fraude. En effet, c'est d'après moi un risque particulier qui doit être analysé à travers un modèle bien spécifique. Je me permets donc de proposer un concept que j'ai décidé de nommer « Le Trèfle Anti-Fraude ».

Par ailleurs, sachant qu'il existe déjà un outil *Fraud Risk Assessment* dans le monde des auditeurs internes, j'ai décidé de centrer ma recommandation sur un concept plutôt qu'un outil de façon à pouvoir apporter un modèle conçu spécialement pour la fraude financière en entreprise. Le triangle de la fraude étant plus axé sur « pourquoi » la fraude est commise, mon concept aura l'axe du « comment » assurer une protection à long terme au sein d'une société pour que la fraude ne soit pas commise. Le concept que je vais vous détailler à présent rassemblera les différents éléments qui me paraissent essentiels pour permettre à l'entreprise de dissuader tout individu de commettre des fraudes.

En d'autres termes, j'ai décidé de pousser la réflexion là-dessus afin de pouvoir conceptualiser mes idées de façon à créer un trèfle (à trois feuilles) qui pourrait servir dans la réflexion des stratégies anti-fraude à adopter au sein des organisations.

Mon concept rassemble donc trois feuilles : la prévention, la détection et la réaction qui sont issues d'une même racine qui est l'objectif de l'entreprise, c'est-à-dire la dissuasion.

7.1 Prévention

J'ai opté tout d'abord pour la « prévention » car c'est, d'après moi, l'élément principal dans la lutte contre la fraude. Comme je l'ai indiqué dans la troisième partie de ce mémoire, un système de contrôle interne sans une culture d'entreprise bien établie ne peut pas avoir un impact positif à long terme au sein d'une entreprise. Effectivement, selon moi, l'aspect éthique au sein d'une entreprise a autant d'importance que les procédures et contrôles car le cœur du problème n'est pas la faille dans le système mais, la motivation du criminel économique.

La prévention contre la fraude peut être réalisée à travers différentes actions et outils qui décourageraient le fraudeur à commettre son acte. L'instauration d'un processus de recrutement bien spécifique ou encore d'une culture d'honnêteté par la gouvernance d'entreprise, ainsi que le « tone at the top » et « tone at the middle » sont des premiers facteurs qui pourraient grandement influencer la dissuasion. La sensibilisation et la formation sont aussi des moyens dissuasifs, permettant aux collaborateurs d'agir en connaissance de cause tout au long de leur mission dans l'entreprise.

Ceci étant dit, l'outil nécessaire pour anticiper la fraude, est le dispositif de gestion des risques qui permet d'avoir une vue d'ensemble rapide des principaux risques de fraude afin de les hiérarchiser et déterminer les zones d'ombres qui doivent être traitées.

Ensuite, j'estime que la ségrégation des tâches ainsi que des contrôles internes efficaces dans les opérations de l'entreprise sont aussi des éléments qui peuvent aider l'entreprise à agir en amont, de façon à réduire le nombre de tentatives. Concrètement, le fait de disposer de contrôles et de les appliquer peut avoir un effet dissuasif, car cela démontre à tous les collaborateurs qu'il y a de la rigueur à ce niveau-là. Ceci étant dit, le COSO permet d'avoir un début de solution dans la prévention contre la fraude. Encore faut-il que l'entreprise le comprenne et sache l'adapter correctement à son environnement et à sa structure.

En résumé, la prévention est un premier élément indispensable qui est en lien direct avec le triangle de la fraude. Autrement dit, si l'on se base sur les aspects culture d'entreprise, éthique, ou encore « tone at the top » c'est le premier élément du triangle de la fraude qui est ciblé : la motivation. Car comme je l'ai dit dans la deuxième partie de ce mémoire, la motivation est liée à l'aspect psychologique de la personne tout comme l'éthique et la culture d'entreprise alors que l'opportunité est liée aux failles du système de l'entreprise. C'est pourquoi les contrôles internes efficaces au sein de cette dernière sont un bon moyen d'enlever toute opportunité pour les fraudeurs, tandis que la culture d'entreprise cible davantage la motivation des potentiels fraudeurs : deux moyens de prévention efficace. En fait, les dirigeants devraient avoir en tête cette notion de prévention séparée en deux axes, ciblant la motivation et l'opportunité de la fraude, car cette simple réflexion aiderait grandement les entreprises à réduire la probabilité d'occurrence de ce type de risque.

7.2 Détection

Ensuite, il est important au sein d'une entreprise de disposer d'outils et d'actions permettant de détecter les différents risques de fraude. La prévention contre la fraude ne peut pas arrêter tous les criminels qui seraient susceptibles de commettre un acte illicite. Ceci étant dit, il est aussi important de souligner que les mesures préventives peuvent être clairement apparentes, comme les procédures, les règlements ou encore les chartes, tandis que les mesures de détection sont moins visibles par tous les collaborateurs.

A ce sujet, le *whistleblowing* est un moyen efficace pour détecter les fraudes au sein de l'organisation. Le lanceur d'alerte, étant anonyme, n'a aucune crainte de représailles et peut signaler des agissements frauduleux d'autres collaborateurs. Les entretiens d'évaluation ou de départ, ainsi que des sondages anonymes peuvent être également une grande source d'informations intéressantes pour détecter les tentatives de fraude. Les collaborateurs sont au cœur des affaires de l'entreprise et entretenir une discussion régulière avec eux pourrait être une façon de détecter d'éventuelles anomalies.

D'autre part, en termes de détection, il s'avère essentiel pour une société d'avoir en sa possession des outils de *Big Data* ou de vérification assistée par ordinateur (CAAT) donnant la possibilité d'analyser des masses de données selon différentes caractéristiques. Ces derniers, serviront à analyser des transactions inhabituelles qui sont faites durant le week-end par exemple et ainsi optimiser le processus de détection. Un autre moyen efficace de détection qui pourrait compléter les outils informatiques serait des audits aléatoires dans les zones d'ombres identifiées préalablement de manière à vérifier que les actions correctrices sont appliquées avec rigueur et précision.

En résumé, la détection joue un rôle majeur tout comme la prévention car l'un sans l'autre ne peut pas permettre à l'entreprise d'assurer une protection à long terme face à la fraude. En effet, pour dissuader les éventuels fraudeurs, il faut s'armer d'outils et d'actions qui puissent détecter rapidement une fraude afin d'éviter une augmentation des pertes et permettre à la société de réagir en conséquence.

7.3 Réaction

La réaction de l'entreprise, lorsqu'une fraude a été découverte, est également un élément essentiel dans ce « Trèfle Anti-Fraude ». Pour arriver au résultat escompté : la dissuasion, il est important de compléter cette approche préventive et détective par une approche réactive. Cette dernière apportera une crédibilité dans les actions de l'entreprise et démontrera que chaque acte de fraude est traité d'une manière bien spécifique et que les conséquences pour le fraudeur soient bien comprises de tous.

Comme je l'ai dit dans la dernière page de la troisième partie, la communication au sein d'une entreprise à propos de la fraude ne doit pas être considérée comme interdit. En effet, j'estime qu'il faudrait conscientiser tous les acteurs de l'entreprise que ce fléau existe bel et bien et qu'il peut arriver à tout moment. Par ailleurs, la réaction ne doit pas s'arrêter uniquement à une simple communication des conséquences de la part de l'entreprise, mais elle doit aussi être synonyme d'actions correctrices au niveau des contrôles internes. Le rôle de l'auditeur interne dans ce troisième élément est donc primordial car il a une activité indépendante qui lui permet d'analyser le SCI afin de réagir en conséquence.

C'est avant tout un élément qui donnera une image de l'entreprise vis-à-vis des collaborateurs et du monde extérieur. Soit c'est une entreprise sûre de ces moyens, qui sait gérer les risques de fraude et réagir de manière adéquate ou dans le cas contraire c'est une entreprise qui n'assume pas les différentes mesures mises en place, illustrant ainsi son manque de crédibilité et ses faiblesses.

En résumé, dans ce troisième élément, c'est la rapidité de réaction qui permettra à l'entreprise dans un premier temps de réduire l'impact d'un acte de fraude et dans un deuxième temps d'apporter des actions correctrices de façon à renforcer à nouveau le SCI afin d'éviter que le même type de risque se reproduise.

7.4 Dissuasion

La dissuasion de tentatives de fraude est donc le résultat des trois éléments cités précédemment. D'après moi, ce concept pourrait garantir une réflexion efficace dans la lutte contre la fraude car il synthétise à lui seul des actions et outils efficaces qui ont fait leur preuve, d'après mes recherches et les statistiques affichées tout au long de ce mémoire. En outre, ce concept pourrait être un complément à d'autres modèles tels que le triangle de la fraude, les « 5C » ou encore le référentiel COSO.

En outre, ce « Trèfle Anti-Fraude » démontre bien qu'il ne suffit pas à une entreprise de disposer uniquement de contrôles efficaces. Il faut aussi prendre en compte l'aspect psychologique de l'individu afin de pouvoir anticiper ou réagir en conséquence.

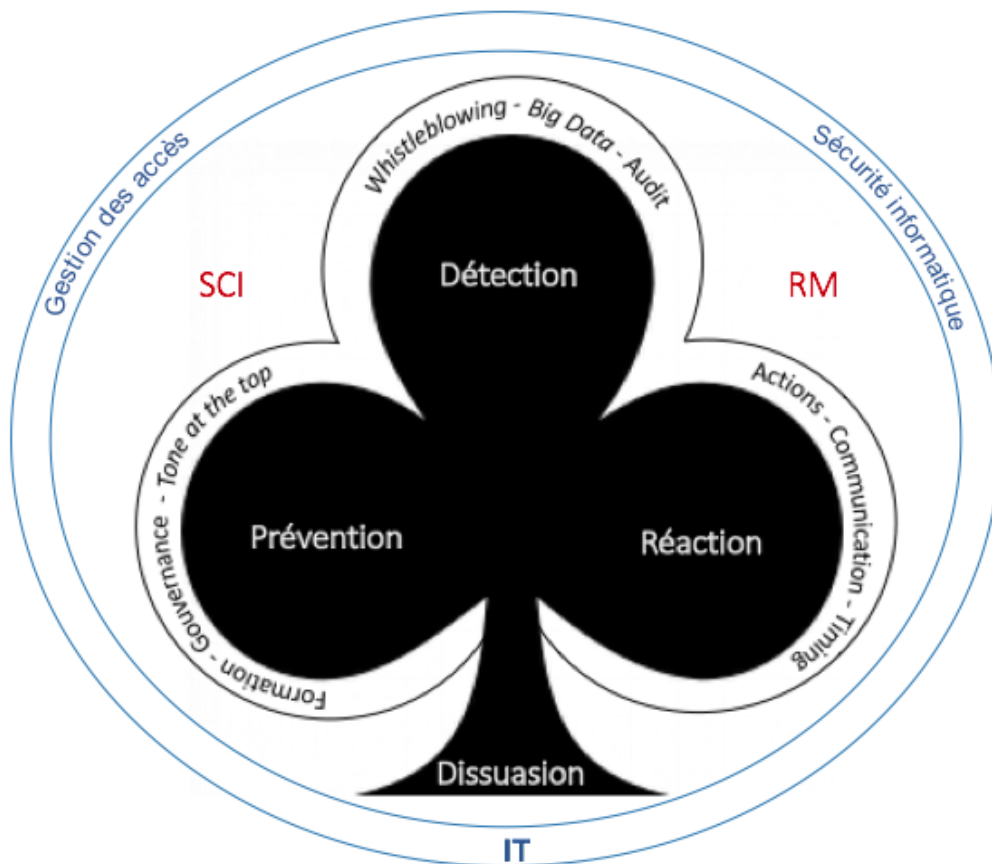
L'entreprise doit par ailleurs savoir être proactive en insistant sur la culture d'entreprise et sur l'éthique tout en sachant communiquer de manière subtile au sein de la société de façon à sensibiliser tous les collaborateurs à ce risque et démontrer ainsi que l'entreprise dispose des meilleures ressources et techniques pour combattre ce fléau.

Pour le reste, il ne faut pas oublier l'aspect IT en entreprise, qui est d'après moi, un autre élément important pour avoir un SCI efficient et qui aide davantage à réduire la probabilité d'occurrence du risque de fraude lorsqu'il est exploité correctement.

Effectivement, j'estime que c'est un point qui doit être mis en avant car comme vous avez pu le constater à travers ce mémoire, le risque de cybercriminalité est un risque qui prend de plus en plus d'ampleur et qui peut avoir de lourdes conséquences.

C'est pourquoi, j'inclus la sécurité informatique dans mon « Trèfle Anti-Fraude » car je pense qu'une entreprise qui n'a pas mis en place un tel dispositif adapté à sa structure pourrait être la cible de nombreuses attaques, et au pire des cas disparaître. Evidemment, le savoir-faire en IT a également son rôle à jouer car il ne suffit pas d'avoir les machines informatiques les plus puissantes, si l'entreprise n'arrive pas à maîtriser ces dernières.

Figure 11 : « Le Trèfle Anti-Fraude »



Eric Castro, 2016

En définitive, la valeur ajoutée de ce « Trèfle Anti-Fraude » réside dans le fait qu'il élargit son champ de vision en combinant, des actions liées au comportement des collaborateurs et des outils liés au système de contrôle interne de l'entreprise, tout en mettant un point d'attention sur l'aspect technologique. Cette combinaison : psychologie, SCI, technologie, est pour moi une approche pouvant réduire fortement la probabilité d'occurrence et l'impact des risques de fraude en entreprise.

8. Conclusion

En conclusion, la fraude financière en entreprise reste un risque critique dans le monde professionnel et doit être diagnostiquée de manière bien spécifique. Les différents acteurs du contrôle interne ont tous un rôle à jouer dans le combat contre ce fléau et doivent pouvoir assurer une circulation de l'information constante et transparente dans le but d'avoir la bonne approche.

Le détournement d'actifs, étant la fraude la plus courante en entreprise, n'a pas les mêmes conséquences que la fraude comptable, qui elle peut faire disparaître une entreprise, à elle seule. La corruption ainsi que la fraude au président restent des préoccupations majeures pour les dirigeants d'entreprise, tandis que le *management override* se transforme en une fraude récurrente et standard qui peut impacter directement le moral et le bien-être des collaborateurs. En ce qui concerne la cybercriminalité, son passage à la deuxième position du classement des fraudes les plus récurrentes, prouve que l'IT en entreprise doit devenir une priorité pour tout dirigeant de manière à garantir une sécurité informatique optimale à long terme au sein d'une entreprise.

Quant aux vulnérabilités intrinsèques favorisant la fraude financière, elles peuvent être synonymes de failles dans le SCI, d'un mauvais processus de recrutement ou encore de dysfonctionnements dans la gestion informatique. Ces dernières peuvent amener les criminels économiques à commettre une manipulation comptable douteuse ou un détournement de données confidentielles. Néanmoins, différents signaux d'alerte comme l'agissement étrange des collaborateurs ou bien l'évolution inhabituelle de ratios permettent d'identifier des anomalies.

Au demeurant, les causes et facteurs déclencheurs peuvent être analysés à travers le triangle de la fraude de Donald R. Cressey qui démontre l'importance de la combinaison : motivation, opportunité et rationalisation, dans le processus de la fraude.

En d'autres termes, un SCI basé sur le COSO est sans doute un dispositif permettant de réduire la probabilité d'occurrence et l'impact du risque de fraude, et ce grâce à ses cinq composantes qui ciblent sous plusieurs angles la fraude financière. En effet, le SCI dispose d'une approche préventive et détective à la fois, avec des procédures et outils tels que le *Risk Assessment* et sa cartographie des risques qui ont comme fonction d'identifier, d'évaluer, de traiter et de surveiller les risques de fraude en continu.

De plus, la prise en compte de l'aspect IT dans le SCI, à travers des sensibilisations et des formations apportent un soutien dans la lutte contre la fraude et par la même occasion, une certaine efficience dans la gestion de l'entreprise.

Toutefois, la culture d'entreprise et l'aspect humain doivent absolument être pris en considération, car il ne s'agit pas uniquement de procédures et processus mais également de psychologie et de comportement humain du criminel économique.

Par conséquent, la dissuasion de la fraude peut être garantie lorsque trois éléments sont réunis : la prévention, la détection et la réaction. L'outil de réflexion que j'ai imaginé : « Le Trèfle Anti-Fraude », synthétise les différents aspects à prendre en compte sous une approche : psychologie, SCI, technologie, dans le but de dissuader le criminel économique de toutes tentatives de fraude.

En définitive et d'un point de vue personnel, ce projet de recherche a été l'occasion pour moi de me pencher sur une problématique émanant de la réalité professionnelle et de collaborer avec des professionnels en audit, ainsi qu'avec des experts en finance et en comptabilité pour tenter de trouver des pistes de solutions face à ce fléau. Grâce à leurs visions et à de précieux conseils qui ont su orienter mes recherches et analyses, j'ai pu apprendre passablement de notions pour approfondir cette étude et ainsi créer un outil de réflexion. Ce dernier pourra m'être d'une grande utilité l'avenir, et saura guider tout lecteur dans le raisonnement de la réduction de l'impact et de la probabilité d'occurrence du risque de fraude en entreprise.

Bibliographie

Rapports

DI GIOVANNI, Jean-Louis, BORDE, Fabienne, ESTÈVE, Thomas, 2016. Global Economic Crime Survey 2016. *Pwc.fr* [en ligne]. Mars 2016. [Consulté le 7 mai 2016]. Disponible à l'adresse : http://www.pwc.fr/fr/assets/files/pdf/2016/03/pwc_ad_fraude_mars2016_v3.pdf

ARAJ, Farah, 2015. Faire face au risque de fraude – Exploration du rôle de l'audit interne. *Na.theiia.org* [en ligne]. 2015. [Consulté le 19 mai 2016]. Disponible à l'adresse : <https://na.theiia.org/translations/PublicDocuments/Responding-to-Fraud-Risk-French.pdf>

PWC, 2016. The Global State of Information Security Survey 2016. *pwc.lu* [en ligne]. 2016. [Consulté le 22 mai 2016]. Disponible à l'adresse : <https://www.pwc.lu/en/information-risk-management/docs/pwc-2016-gsiss.pdf>

PWC, 2013. COSO 2013 – Une opportunité pour optimiser votre contrôle interne dans un environnement en mutation. *Pwc.fr* [en ligne]. Juillet 2013. [Consulté le 4 juin 2016]. Disponible à l'adresse : http://www.pwc.fr/fr/assets/files/pdf/2013/10/ad_pocket_guide_coso_juillet2013.pdf

Committee of Sponsoring Organizations of the Treadway Commission, 2013. Internal Control – Integrated Framework. *Coso.org* [en ligne]. Mai 2013. [Consulté le 5 juin 2016]. Disponible à l'adresse : http://www.coso.org/documents/990025P_Executive_Summary_final_may20_e.pdf

ACFE. Managing the Business Risk of Fraud : A Practical Guide. *Acfe.com* [en ligne]. [Consulté le 5 juin 2016]. Disponible à l'adresse : https://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/managing-business-risk.pdf

The Institute of Internal Auditors, 2009. Internal auditing and fraud. *Louisiana.edu* [en ligne]. Décembre 2009. [Consulté le 17 juin 2016]. Disponible à l'adresse : https://www.louisiana.edu/sites/auditor/files/1011919_2029.dl_PG%20IA%20and%20Fraud.pdf

EY, 2016. Corporate misconduct individual consequences – 14th Global Fraud Survey. *Ey.com* [en ligne]. 2016. [Consulté le 19 juin 2016]. Disponible à l'adresse : [http://www.ey.com/Publication/vwLUAssets/EY-corporate-misconduct-individual-consequences/\\$FILE/EY-corporate-misconduct-individual-consequences.pdf](http://www.ey.com/Publication/vwLUAssets/EY-corporate-misconduct-individual-consequences/$FILE/EY-corporate-misconduct-individual-consequences.pdf)

KPMG, 2016. Global profiles of the fraudster. *Assets.kpmg.com* [en ligne]. Mai 2016. [Consulté le 12 juillet 2016]. Disponible à l'adresse : <https://assets.kpmg.com/content/dam/kpmg/pdf/2016/05/profiles-of-the-fraudster.pdf>

ACFE, 2016. Report to the Nations on Occupational Fraud and Abuse. *s3-us-west-2.amazonaws.com* [en ligne]. 2016. [Consulté le 15 juillet 2016]. Disponible à l'adresse : <https://s3-us-west-2.amazonaws.com/acfe-public/2016-report-to-the-nations.pdf>

CIMA, 2009. Fraud risk management : a guide to good practice. *Cimaglobal.com* [en ligne]. Janvier 2009. [Consulté le 15 juillet 2016]. Disponible à l'adresse : http://www.cimaglobal.com/Documents/ImportedDocuments/cid_techguide_fraud_risk_management_feb09.pdf.pdf

Articles

DALMASSO, Coralie. L'évolution du référentiel COSO : du contrôle interne au management des risques. *Bpms.info* [en ligne]. [Consulté le 9 mars 2016]. Disponible à l'adresse : <http://www.bpms.info/levolution-du-referentiel-coso-du-contrôle-interne-au-management-des-risques/>

VERSIGNY, Caroline, FERGUSON, Charles, L'enjeu des risques de Fraude : la maîtrise des flux de données ? *blog-finance.groupeonepoint.com* [en ligne]. [Consulté le 9 mars 2016]. Disponible à l'adresse : <http://blog-finance.groupeonepoint.com/lenjeu-des-risques-de-fraude-la-maitrise-des-flux-de-donnees/>

CRETTE, Olivier, 2014. Contrôle interne et prévention de la fraude dans les PME : une nécessité ? *Ledouble.fr* [en ligne]. Septembre 2014. [Consulté le 12 mars 2016]. Disponible à l'adresse : <http://www.ledouble.fr/wp/wp-content/uploads/2013/10/LEDOUBLE-SAS-Olivier-Cretté-étude-Analyse-offres-publiques-2013-FG-09.2014.pdf>

COLBY, Everett, La fraude et le contrôle interne – Première partie : l'importance des contrôles. *Cga-pdnet.org* [en ligne]. [Consulté le 15 avril 2016]. Disponible à l'adresse : https://www.cga-pdnet.org/Non_VerifiableProducts/ArticlePublication/FraudInternalControls_F/FraudInternalControls_p1_F.pdf

DUPRAT, Romain, Typologie des différentes catégories de fraude à caractère financier. *Pansard-associes.com* [en ligne]. [Consulté le 16 avril 2016]. Disponible à l'adresse : <http://www.pansard-associes.com/publications/audit-comptabilite/contrôle-interne-fraudes/typologie-fraudes-financier.htm>

DRAZ, Daniel, 2011. Fraud prevention : Improving internal controls. *Csoonline.com* [en ligne]. 28 mars 2011. [Consulté le 17 avril 2016]. Disponible à l'adresse : <http://www.csoonline.com/article/2127917/fraud-prevention/fraud-prevention-improving-internal-controls.html>

COLBY, Everett, La fraude et le contrôle interne – Troisième partie : les stratagèmes de fraude interne. *Cga-pdnet.org* [en ligne]. [Consulté le 23 avril 2016]. Disponible à l'adresse : https://www.cga-pdnet.org/Non_VerifiableProducts/ArticlePublication/FraudInternalControls_F/FraudInternalControls_p3_F.pdf

OUANICHE, Mikaël, 2013. Les modes opératoires de la fraude interne. *Oca-audit.com* [en ligne]. Février 2013. [Consulté le 25 mai 2016]. Disponible à l'adresse : http://www.oca-audit.com/offres/doc_inline_src/211/ARTICLE+CAHIER+DU+DROIT++LES+MODES+OPERATOIRES+DE+LA+FRAUDE+INTERNE.pdf

PERRUCHOUD, Jean-Yves, 2013. La fraude financière et comptable. *iframe.treuhaender.ch* [en ligne]. 2013. [Consulté le 2 juin 2016]. Disponible à l'adresse : <http://iframe.treuhaender.ch/GetAttachment.axd?attaName=a8d3179e-ad6d-474a-9afb-31040ea820d2>

KEOLASY, RATDAVONE, GENDRON, Yves, MALSCH, Bertrand, 2014. L'affaire WorldCom : Incompétence des auditeurs ou manquement à leur obligation d'indépendance ? *gestion.evalorix.com* [en ligne]. 2014. [Consulté le 5 juin 2016]. Disponible à l'adresse : <http://gestion.evalorix.com/cas/comptabilite-et-finance/laffaire-worldcom-incompetence-auditeurs-manquement-obligation-dindependance/>

GRONDIN, Anaëlle, 2016. Le boom inquiétant de la « fraude au président ». *Lesechos.fr* [en ligne]. 8 avril 2016. [Consulté le 26 juin 2016]. Disponible à l'adresse : http://www.lesechos.fr/08/04/2016/lesechos.fr/021827593152_le-boom-inquietant-de-la--fraude-au-president---.htm

GODART, Nina, 2016. Voici à quoi ressemble le fraudeur en entreprise. *bfmtv.com* [en ligne]. 12 juillet 2016. [Consulté le 13 juillet 2016]. Disponible à l'adresse : http://bfmtv.com/entreprise/voici-a-quoi-ressemble-le-fraudeur-en-entreprise-1004938.html?utm_campaign=Echobox&utm_medium=Social&utm_source=Twitter&link_time=1468331871#xtor=CS2-30

Supports de cours

Dre EQUEY, Catherine, 2015. *La mise en place d'un Système de Contrôle Interne (SCI) : Le cadre conceptuel du COSO* [document PDF]. 16 septembre 2015. Support de cours : Cours « Controlling, Investissement et Financement », Haute école de gestion de Genève, filière économie d'entreprise, année académique 2015-2016

Dre BRENDER, Nathalie, WIELAND, Sara, KONO, Laura, 2016. *Les composantes du SCI* [document PDF]. 10 février 2016. Support de cours : Cours « Du Contrôle interne à l'audit : une approche risque », Haute école de gestion de Genève, filière économie d'entreprise, année académique 2015-2016

Loi et Normes

IFAC, 2009. International Standard on Auditing 240, The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements. *Ifac.org* [en ligne]. 15 décembre 2009. [Consulté le 16 avril 2016]. Disponible à l'adresse : <http://www.ifac.org/system/files/downloads/a012-2010-iaasb-handbook-isa-240.pdf>

Code des obligations, Loi fédérale complétant le Code civil suisse, (Livre cinquième : Droit des obligations), L'Assemblée fédérale de la Confédération suisse, 30 mars 1911(CO ; RO 27.321) Etat le 1^{er} janvier 2010

Chambre fiduciaire. *Normes d'audit suisse (NAS)*. Edition 2013. Zurich : Schweizerische Kammer Wirtschaftsprüfer Steuerexperten, 2013. ISBN 9783906076119

Ouvrages

OUANICHE, Mikael, 2015. *La fraude en entreprise*. 2^e édition. Maxima Laurent du Mesnil, 24 juin 2015. Organisation et technique de gestion. ISBN 9782840018384

GALLET, Olivier, 2014. *Halte aux fraudes*. 3^e édition. Dunod, 26 mars 2014. Fonctions de l'entreprise. ISBN 9782100708017

RUUD, Flemming, 2009. *Ligne de conduite de l'audit interne*. 2^e édition. SVIR. ISBN 9783037750018

SCHICK, Pierre, VERA, Jacques, BOURROUILH-PAREGE, Olivier, 2014. *Audit interne et référentiels de risques*. 2^e édition. Dunod, 22 septembre 2010. Fonctions de l'entreprise. ISBN 9782100708024

BERNARD, Frederic, GAYRAUD, Remi, ROUSSEAU, Laurent, 2013. *Contrôle interne*. 4^e édition. Maxima Laurent du Mesnil. 13 juin 2013. ISBN 9782840017578

La fraude financière et le contrôle interne en entreprise : l'importance d'un SCI efficient pour optimiser l'identification des risques de fraude et réduire leur probabilité d'occurrence.

Annexes

Entretien n°1

Senior Banking Auditor

Q1. Pourriez-vous me citer différents types de fraudes que rencontrent souvent les entreprises ?

- Il y a souvent les paiements/ transferts de montants dissimulés. C'est d'ailleurs d'après moi une fraude qui peut être évitée grâce au SCI (par ex : avec un simple contrôle quatre yeux). Le manque de ségrégation des tâches d'une même activité reste une grande cause dans l'apparition des fraudes en entreprise.
- Concrètement, un gestionnaire de fortune saisie l'écriture et valide le paiement sans avoir au préalable été contrôlé par un autre collaborateur.
- Je pense également qu'une fraude peut mieux se dérouler lorsqu'il y a deux personnes qui collaborent pour commettre cet acte.
- Dans les petites entités, on retrouve souvent ce type de fraude car il y a très peu souvent une bonne ségrégation des tâches. Tandis que dans les grosses structures, une certaine rigueur est mise dans la séparation des tâches.
- Dans le domaine bancaire il peut aussi arriver qu'un collaborateur soustrait un montant cash suite à la visite d'un client pour un dépôt de plusieurs millions. Le banquier augmentera les frais de gestion à hauteur de CHF 20'000 sans que son client s'en aperçoive et signera le document sans poser de question. L'écriture est ensuite saisie puis validée. Dans ces cas-là, il est important de faire un call-back pour demander au client si le montant des frais était celui admis par le règlement.
- Il y a aussi des cas où un employé indique pour l'installation IT par exemple, un montant de CHF 30'000 alors que cela devrait être un montant inférieur et la validation est faite par le management sans avoir même effectué un contrôle. Ce manque de rigueur au sein du management est un facteur aggravant au sein d'une société.
- Un deuxième type de fraude que l'industrie rencontre souvent est le vol d'actifs. J'estime qu'une bonne gestion des stocks il ne devrait pas y avoir de soucis. Par contre, il s'avère que les entreprises n'ont pas toujours un inventaire à jour entre

le début et la fin du mois, ce qui est un moyen de noyer les investigateurs dans les recherches.

- Un troisième type qui me vient à l'esprit est le *managements override of control* ». Je t'assure que cela arrive en entreprise et cela rejoint ce que je t'ai dit concernant la ségrégation des tâches. Si je devais définir cela en quelques mots, je dirais que c'est le management qui effectue la fraude et qui la cache car il détient tous les contrôles en sa possession.

Q2. Quels sont les causes et facteurs déclencheurs de fraude ?

- Mon expérience peut t'assurer qu'il y a un facteur déclencheur de fraude et c'est l'opportunité. Je peux t'affirmer que lorsque les personnes sont dans une entreprise où le SCI est faible et qu'on a l'occasion de commettre l'acte on peut être tenté et rentrer dans le triangle de la fraude. Je te conseille de faire des recherches sur ce concept qui t'apportera des explications supplémentaires.
- On peut rajouter au triangle de la fraude, l'aide d'un tiers qui permet d'avoir une fraude bien préparée et qui peut avoir de plus lourdes conséquences. J'estime qu'il faut toujours une aide à l'interne afin de pouvoir commettre une fraude correctement.

Q3. Quelles peuvent-être les vulnérabilités d'une entreprise favorisant la fraude financière ?

- Je dirais que c'est le manque d'importance accordée à son SCI. Ceci dit, dans les multinationales il y a un paquet de directives et énormément de procédures en place. Le risque réside donc la non-application de ces directives qui peut ouvrir un engrenage dans la tentative de fraude.
- Par exemple, lorsque je reçois une facture informatique, je dois vérifier le montant et le fournisseur pour effectuer une validation. Par contre, si personne ne fait de contrôle la personne qui fait la facturation pourrait inventer des factures fictives d'un certain montant et les verser sur son compte.

Q4. Quels sont les facteurs qui poussent les gens à la fraude ?

- Voir en haut.

Q5. Avez-vous déjà été confronté à une fraude (en tant qu'auditeur, collaborateur ou autre) ?

- Oui, mais cela reste confidentiel, je ne peux pas t'en parler dans les détails. Je peux juste te dire que c'était lié à la soustraction de la clientèle dans le domaine bancaire.

Q5.1. Si oui, quelle réaction avez-vous eu ? Que s'est-il passé ensuite ?

- J'ai remis en question mon travail car je n'étais pas sûr de la fraude puis j'ai ensuite eu la confirmation de l'établissement victime. Suite à cela, j'ai approfondi à travers deux étapes. J'ai revu entièrement la directive, cela m'a pris énormément de temps pour ensuite pouvoir faire le rapport. L'information a bien entendu été remontée à la FINMA.
- Concernant l'entreprise victime, elle a eu connaissance de la fraude et a créé une provision afin de pouvoir rembourser le client. Concernant le gestionnaire de fortune, il a été licencié.

Q6. Comment découvre-t-on ces tentatives de fraude, quels sont les signes ?

- Il y a plusieurs signes qui peuvent être relevé comme par exemple, les erreurs dans les états financiers, les textes dans les PV de conseil d'administration, les mails mais également la rétention d'informations qui pour est moi un indice important tout comme la démission ou le renvoi d'un cadre ou d'un directeur.
- Il faut tout de même faire attention à la notion de l'ampleur. Un cas auquel j'ai dû faire face était assez paradoxal : Un collaborateur avait volé des sachets de thé et a ensuite été licencié. Cependant, l'affaire est remontée jusqu'au tribunal fédéral et le collaborateur a eu gain de cause car son licenciement a été considéré comme abusif.
- Je peux aussi te citer un cas de fraudes à l'extrême que j'ai vécu dans lequel un gestionnaire s'est suicidé suite à la découverte.
- Les médias peuvent également être donnés des indices. Il y a aussi les émissions comme cash investigations ou zone interdite qui font des enquêtes et dans lesquels on aperçoit parfois des entreprises qui commettent des irrégularités.

Q7. Quels sont les enjeux et conséquences pour l'entreprise ?

- Je répondrai à cette question à la fin de l'entretien.

Q8. Comment peut-on prévenir ces tentatives de fraude (outils, réactions humaines) ?

- En inculquant chez les collaborateurs la responsabilité et le respect de l'entreprise mais également rémunérer correctement les collaborateurs.
- Il est aussi important de former les collaborateurs au contrôle. Cela peut paraître simple mais il est important qu'au sein d'une entreprise les collaborateurs connaissent et comprennent les différents contrôles à faire et sachent dans quelle ligne de défense ils se trouvent.
- Un management de confiance doit aussi être de rigueur pour éviter la fraude. Ce n'est pas simplement le fait d'avoir des responsables formés au niveau universitaires car on ne mesure pas la confiance avec le niveau d'éducation. Il faudrait faire un focus sur les expériences passées de la personne pour avoir un avis pertinent.
- Avoir un SCI qui n'est pas en place de façon protocolaire, dans le sens où il n'est pas là juste pour être là. Il doit être clair et compris de tous les internes pour être bien appliqué. Au sein d'une entreprise, j'ai vu qu'une facture devait être validée par cinq personnes et il s'avère que c'était le comptable qui s'occupait de valider avant d'envoyer la facture sans passer par d'autres signatures.

Q9. Existe-il un profil type de fraudeur ?

- Etant donné que la fraude est motivée par l'argent ou par la pression de la hiérarchie. Donc je dirais que cela peut autant concerner un collaborateur qui est au cœur de la trésorerie d'une entreprise, qui puisse sortir directement l'argent de la caisse ou passer des écritures comptables par exemple ou alors un collaborateur ayant des responsabilités et devant assumer l'atteinte de certains objectifs parfois éloignés de la réalité.
- Je dirais donc deux types de profils : les financiers et ceux qui doivent faire de très bons résultats.

Q10. Pourriez-vous m'expliquer le lien entre la fraude et l'audit interne ?

- Je préfère t'expliquer le lien entre l'audit interne et l'audit externe car je pense que cela peut aussi être intéressant.
- L'audit interne s'occupe davantage d'effectuer des vérifications à travers des tests. Ce sont des membres non opérationnels de l'entreprise, ils ont un devoir d'indépendance dans leur mission.
- Concrètement, suite à une analyse des risques, l'audit interne va détecter des risques importants. Ces derniers peuvent être liés à la fraude, d'ailleurs il y en a toujours au moins un lié à la fraude. Une fois les tests effectués sur le processus de gestion de fortune par exemple, l'information est remontée au CA.
- On peut définir l'audit interne comme étant le bras droit du CA et l'audit externe comme étant le bras droit du régulateur.
- L'audit interne fait des rapports et l'audit externe lit ces rapports. Cependant c'est assez rare que l'audit externe se base uniquement sur le travail élaboré par l'audit interne car il donne rarement des assurances liées aux états financiers.
- Il y a une certaine complémentarité entre ces deux fonctions.

Q11. Est-ce que le contrôle interne amène une valeur ajoutée pour maîtriser le risque de fraude ?

- Pour le détecter oui, mais pour le prévenir non.
- Il y a trois types de contrôles, le contrôle exécutif, contrôle management et contrôle audit.
- Si le fraudeur décide de faire une fraude, l'audit interne ne le saura pas, il pourra uniquement la détecter une fois l'opération faite.

Q12. D'après vous, disposer d'un SCI efficace est-il suffisant pour réduire le nombre de tentatives de fraude ?

- Oui clairement ! Il doit être simple, compris, appliqué par des collaborateurs impliqués !
- Il est très important d'avoir un SCI simple à comprendre.

Q13. Quelles améliorations faut-il apporter au COSO 2013 pour pouvoir lutter contre les fraudes et réduire ce risque de façon plus net ?

- Cela reste relatif comme avis car le cube COSO n'amène pas de solution absolue à l'entreprise mais une idée de comment mettre en place un SCI. Mais pour répondre à votre question, je rajouterais une partie « education training » dans la base du cube, en dessous de contrôle environnement.

Q14. Qu'est-ce qu'il faudrait créer pour apporter un soutien au SCI afin de réduire le nombre de tentatives ?

- A la base le SCI évolue en fonction des évolutions et donc des fraudes. Il s'améliore d'années en années, donc je n'ai pas d'outil qui me vienne à l'esprit. Je pense que le SCI peut suffire à combattre la fraude.

Q15. Existe-t-il un outil élaboré spécialement pour lutter contre la fraude financière en entreprise ?

- Dans les banques, ils ont des « FinTool ». Ces outils donnent en temps réel toutes les positions ce qui permet à la direction de contrôler ses gestionnaires.

Q16. D'après votre expertise, qu'est-ce que vous feriez au sein d'une entreprise afin de réduire la probabilité d'occurrence du risque de fraude ?

- L'élément « education training » dont je t'ai parlé tout à l'heure est d'après moi une clé pour réduire la probabilité d'occurrence de ce risque. Il s'agirait en fait de proposer des formations, pour motiver les équipes et inculquer aux équipes le respect des valeurs de l'entreprise et l'esprit du contrôle interne.
- Il faudrait que tous les internes comprennent que leur travail ne se résume pas à valider des opérations sans raison mais qu'il y a une explication derrière tout ça et qu'il faut la comprendre. Il y a pourtant des sensibilisations lorsqu'on passe à un niveau supérieur au niveau de la hiérarchie, mais cela reste assez protocolaire je trouve.

Q17. L'avancée technologique est-elle bénéfique ou non pour une entreprise afin de combattre la fraude financière ?

- Cela dépend des entreprises. Il faut faire attention aux gens qui maîtrisent un minimum l'IT car ils peuvent être dangereux pour les sociétés. Il n'y a pas vraiment de SCI lié à l'IT et donc celui qui gère les techniques IT peut faire une fraude

La fraude financière et le contrôle interne en entreprise : l'importance d'un SCI efficient pour optimiser l'identification des risques de fraude et réduire leur probabilité d'occurrence.

extrêmement vite sans que personne ne s'en aperçoive. C'est au CA de dire s'il faut faire des contrôles à ce niveau-là et il s'agit souvent de personnes n'ayant pas assez de savoir-faire en matière informatique pour exprimer un avis pertinent. J'ai souvent vu qu'en IT, un collaborateur à lui seul peut passer et valider une transaction. Cependant, il ne peut pas maîtriser l'impact sur les états financiers et c'est là où intervient l'audit externe.

Q18. Avez quelque chose à ajouter / Avis personnel ?

- Ayant évolué dans le monde bancaire, je pense qu'on est dans une tourmente, on est en train de délaisser un modèle qui nous a été bien utile pendant une trentaine d'années pour laisser le modèle des « Fintechs » s'implanter et on doit s'adapter à la nouvelle vitesse des transactions bancaires.
- C'est là tout l'enjeu, les auditeurs doivent pouvoir s'assurer qu'une fraude peut être détectée assez rapidement afin de faire des recommandations cohérentes et remonter le point dès que possible à la FINMA.
- Je pense aussi qu'on a aujourd'hui à faire à des personnes très SMART, ce n'est plus comme avant, on voit la différence, surtout en banque. Les collaborateurs sont toujours de plus en plus formés et il est donc important d'avoir les compétences nécessaires en audit pour maîtriser son sujet de façon à pouvoir être apte à détecter la moindre incohérence.

Entretien n°2

Responsable contrôle et audit interne dans le domaine de la santé

Q1. Pourriez-vous me citer différents types de fraudes que rencontrent souvent les entreprises ?

- Oui, les détournements d'actifs comme par exemple le vol de cash ou de biens sont pour moi un type très répandu dans le monde des entreprises. Je peux aussi citer l'utilisation abusive de son statut pour se faire payer ses dépenses. Ou encore, le rapport privilégié avec ses fournisseurs pour obtenir un avantage matériel en échange d'une relation commerciale. C'est au code d'éthique de l'entreprise de préciser ce qui est acceptable ou non.

Q2. Quels sont les causes et facteurs déclencheurs de fraude ?

- Je pense que c'est clairement lié à la personne. Son éthique, ses valeurs et sa situation personnelle font de la personne un fraudeur ou non. Mais cela peut aussi être des lacunes de contrôles au sein d'une entreprise.

Q3. Quelles peuvent-être les vulnérabilités d'une entreprise favorisant la fraude financière ?

- Dans le SCI, le manque de séparation des tâches surtout dans les petites entreprises qui sont très vulnérables à ce niveau-là. Souvent, il arrive que le chef ne contrôle pas car il a une confiance aveugle en l'employé. L'employé peut profiter de cet excès de confiance pour commettre la fraude et ensuite rejeter la faute sur son chef qui n'effectuait pas les contrôles et se positionner en tant que victime. C'est très important de ne pas installer cette routine de valider aveuglement. Ce n'est parce que je fais confiance que je ne vais pas faire de contrôle.

Q4. Quels sont les facteurs qui poussent les gens à la fraude ?

- Comme je l'ai dit, la situation personnelle est la source du problème. L'addiction aux jeux, le besoin d'argent sont des facteurs qui peuvent pousser la personne à commettre la fraude. J'ai eu le cas d'une personne qui était accroc aux jeux et qui dépensait tout son salaire et qui en voulait toujours plus. Souvent, les fraudeurs ce sont des gens qui vivent au-dessus de leur moyen.

- Un autre cas peut-être celui d'un employé qui s'identifie tellement à son entreprise en pensant que c'est son argent qu'il va payer ses impôts avec l'argent de la société en ne faisant plus la distinction entre son patrimoine et celui de l'entreprise.

Q5. Avez-vous déjà été confronté à une fraude (en tant qu'auditeur, collaborateur ou autre) ?

- Oui, le premier cas s'est déroulé chez mon ancien employeur dans lequel une tierce personne nous a alerté et on a dû lancer un audit « surprise » de fraude. C'est une procédure très spéciale qui arrive lorsqu'il y a une fraude identifiée.
- Le deuxième cas est arrivé lorsque l'on faisait des contrôles, on a détecté une fraude. A ce moment-là j'ai remis en doute l'intégrité de la personne et j'ai immédiatement remonté l'information à la direction.
- Le troisième cas était on va dire un cas standard. Une personne avait retiré de l'argent dans la caisse et son chef ne faisait pas de contrôle. Ça a quand même tenu quelques mois avant qu'on demande des justificatifs qui n'existaient pas.

Q5.1. Si oui, quelle réaction avez-vous eu ? Que s'est-il passé ensuite ?

- On lance l'audit détaillé. C'est à dire sur quels éléments, quels comptes, etc.
- Je vous avoue que ce n'est pas simple en termes de communication, il faut bétonner nos propos. Ensuite, il fallait qu'on détermine le montant qui avait été détourné par la personne. Pour résumer, il faut beaucoup creuser, c'est une approche de détective qu'on doit adopter et faire des recherches très précises.
- Ensuite, une fois notre travail terminé cela passe par la justice et souvent la personne se fait virer immédiatement.

Q6. Comment découvre-t-on ces tentatives de fraude, quels sont les signes ?

- En faisant un focus sur le comportement de la personne. Quand on commence à poser des questions, on voit qu'elle se perd dans ses propos et a une communication non-verbale assez étrange. Donc encore une fois, c'est lié à la personne.
- Au niveau des contrôles analytiques, il s'agit de se baser sur le cash, les écritures comptables et vérifier s'il n'y a pas des anomalies. On repère assez vite ces anomalies lorsqu'on a une certaine expérience dans la comptabilité.

Plus généralement quand on détecte une fraude c'est souvent un lanceur d'alerte qui la dénonce.

Q7. Quels sont les enjeux et conséquences pour l'entreprise ?

- Il y a bien sûr le risque financier qui peut avoir un gros impact pour l'entreprise. Mais également, l'impact sur l'image qui peut faire très mal. L'exemple du scandale des HUG est assez parlant. La publication dans les médias de la mauvaise gestion au sein des HUG a donné un coup sur sa réputation.

Q8. Comment peut-on prévenir ces tentatives de fraude (outils, réactions humaines) ?

- Disposer d'un SCI c'est la base au sein d'une organisation mais ça ne fait pas tout, effectivement. Pour moi, il n'y a pas d'outils miracles. C'est plutôt, l'information qui est primordial pour réagir face à cette problématique. Il est essentiel de rappeler aux collaborateurs les valeurs de l'entreprise, l'éthique et les sensibiliser à la fraude. Par exemple, en parlant des conséquences s'ils ne respectent pas les règles afin de vraiment être sûr qu'ils n'oseront pas frauder.

Q9. Existe-il un profil type de fraudeur ?

- Pas vraiment, je pense par contre qu'un fraudeur est une personne opportuniste. Ce n'est pas toujours lié au top management comme peut le dire certaines études, cela peut concerner aussi une simple secrétaire. C'est plus lié au profil, toute personne qui est en situation difficile et qui vit au-dessus de ses moyens pourrait être susceptible de commettre l'acte. C'est vraiment lié aux traits de personnalité et non à la fonction dans l'entreprise.

Q10. Pourriez-vous m'expliquer le lien entre la fraude financière et le contrôle interne ou l'audit interne ?

- L'objectif de l'audit interne c'est de donner une assurance raisonnable au CA ou au comité d'audit. Il doit donc s'assurer qu'il n'y aura pas de fraude même s'il y a toujours un risque de fraude dans les scénarios extrêmes.

Q11. Est-ce que le contrôle interne amène une valeur ajoutée pour maîtriser le risque de fraude ?

- Dans le cadre du SCI, l'audit interne doit s'assurer que les contrôles sont bien effectués et bien fait et que le système est réévalué chaque année. Je ne peux vous affirmer avec certitude que ça permet d'éviter les fraudes mais si on s'assure que tout est bien fait, ça donne déjà une bonne assurance.

Q12. D'après vous, disposer d'un SCI efficace est-il suffisant pour réduire le nombre de tentatives de fraude ?

- Non, car il y a toujours une problématique au niveau de la personne. Donc ça ne suffit pas, il faut vraiment rappeler aux gens l'utilité de ce dispositif. De toute manière, j'estime qu'une assurance à 100% n'est pas possible, il y aura toujours un défaut.
- Pour que le SCI soit efficace il faut qu'il soit mis à jour, en fonction du contrôle ordinaire ou restreint, chaque année. Le fiduciaire va de toute manière vérifier que cela a bien été revu une fois dans l'année car c'est une obligation légale.

Q13. Quelles améliorations faut-il apporter au COSO 2013 pour pouvoir lutter contre les fraudes et réduire ce risque de façon plus net ?

- Je n'ai pas de réponse pour cette question. Ça reste un modèle qui après doit être modulé dans chaque entreprise. Je dirais donc qu'il ne faut pas améliorer le COSO mais améliorer son adaptation par les entreprises.

Q14. Qu'est-ce qu'il faudrait créer pour apporter un soutien au SCI afin de réduire le nombre de tentatives ?

- Personnellement, je suis en train d'essayer de monter un projet dans lequel l'objectif est d'avoir des répondants de contrôle interne, qui sont en mesure de faire des contrôles. L'idée serait de trouver une personne qui puisse réaliser un certain nombre de contrôles et ensuite m'apporter un feedback.
- Dans certaines structures, il y a une personne qui est responsable du contrôle interne et parfois il lui manque la connaissance du terrain et du coup il ne sait pas trop comment l'activité fonctionne. Ce n'est pas toujours très simple, c'est pourquoi avoir une personne qui contrôle au sein de l'opérationnel pourrait être un atout pour l'audit interne au sein d'une société.

- Sinon je pense tout simplement qu'il est Important pour le top management de prouver l'utilité d'un SCI pour que tout le monde adhère à ce système.

Q15. Existe-t-il un outil élaboré spécialement pour lutter contre la fraude financière en entreprise ?

- Pas à ma connaissance. Le fiduciaire peut utiliser des outils pour contrôler un certain nombre d'opérations rapidement. Ces logiciels moulinent les opérations comptables (ACL). On donne un certain nombre de critères et l'outil contrôle répertorie les écritures. Par exemple, je lui demande de me sortir toutes les écritures comptables qui sont passées durant la nuit. C'est un outil qui permet de faire des analyses à partir de gros volumes de données. Mais ce n'est pas des outils spécifiques à la fraude.

Q16. D'après votre expertise, qu'est-ce que vous feriez au sein d'une entreprise afin de réduire la probabilité d'occurrence du risque de fraude ?

- Je peux vous assurer que la séparation des tâches est un élément primordial dans toute organisation même si c'est difficile dans les petites structures. Mais une chose que je mettrais en place serait une politique des droits d'accès informatiques car l'accès à l'information est quelque chose de très sensible. La personne ayant accès à toutes les informations peut devenir un réel danger pour l'entreprise s'il n'en fait mauvais usage.

Q17. Enfin, l'avancée technologique est-elle bénéfique ou non pour une entreprise afin de combattre la fraude financière ?

- Ça dépend pour qui. On a quand même des systèmes informatiques de plus en plus performant, donc ça devient opaque pour certains. Mais ça nous permet de voir qui a saisi quoi, on a l'historique de toutes les transactions ce qui nous permet de tracer l'information plus facilement et avec un gain de temps énorme. Mais pour moi, le fait que les systèmes deviennent de plus en plus opaque est un réel point faible pour les entreprises car peu de gens ont une vraie maîtrise de l'informatique.

Q18. Avez quelque chose à ajouter / Avis personnel ?

- A mon avis, la fraude est un problème auquel toute entreprise doit faire face actuellement. Ce qui me préoccupe le plus à l'hôpital c'est le vol d'actif car on a

un stock avec des produits dangereux et coûteux qui sont les produits médicaux. L'enjeu est de savoir si on est OK dans la manière dont on sécurise nos biens.

- Plus généralement, on a quand même des systèmes de double validation donc c'est moins faisable de détourner de l'argent. Je vois mal qu'on puisse voler de l'argent comme ça sans se faire attraper. Donc généralement il y a toujours un système qui permettra de le repérer.
- Le SCI, quand il est bien appliqué, est un système bien rodé qui tôt ou tard pourra détecter une fraude. Je pense donc que le SCI joue un rôle majeur dans la détection de la fraude.

Entretien n°3

Senior Audit Financial Services

Q1. Pourriez-vous me citer différents types de fraudes que rencontrent souvent les entreprises ?

- Détournement d'actifs : Vol par des employés des actifs de l'entreprise (souvent du cash, transferts bancaires)
- Surestimation du revenu, exagération dans les chiffres publiés par l'entreprise pour donner une meilleure image. Souvent lorsque les bonus de la direction dépendent fortement des résultats de l'entreprise.

Q2. Quels sont les causes et facteurs déclencheurs de fraude ?

- Problèmes personnels (d'argent), instabilité des employés, addiction (casino, drogue par exemple).
- Manque d'éthique des employés

Q3. Quelles peuvent-être les vulnérabilités d'une entreprise favorisant la fraude financière ?

- Je ne pense pas qu'une entreprise favorise la fraude financière... Elle pourrait être laxiste sur les contrôles et les facteurs permettant de détecter la fraude (système de contrôle interne défaillant, engagement d'employés avec peu d'éthique)

Q4. Quels sont les facteurs qui poussent les gens à la fraude ?

- Voir question 2

Q5. Avez-vous déjà été confronté à une fraude (en tant qu'auditeur, collaborateur ou autre) ?

- Non jamais

Q5.1. Si oui, quelle réaction avez-vous eu ? Que s'est-il passé ensuite ?

- ...

Q6. Comment découvre-t-on ces tentatives de fraude, quels sont les signes ?

- Le plus souvent, par hasard.... Comme deuxième facteurs, je dirai un contrôle interne efficace (contrôles en place, audit interne, etc.).

Q7. Quels sont les enjeux et conséquences pour l'entreprise ?

- Pertes financières, mais surtout perte d'image

Q8. Comment peut-on prévenir ces tentatives de fraude (outils, réactions humaines) ?

- Bon système de contrôle interne, éthique d'entreprise (plus important d'anticiper, de montrer aux employés qu'une fraude serait découverte). Voir sur internet le triangle de la fraude.

Q9. Existe-il un profil type de fraudeur ?

- Non, apparemment pas. Mais il existe des symptômes (stress importants, problèmes personnels, etc.)

Q10. Pourriez-vous m'expliquer le lien entre la fraude financière et le contrôle interne ou l'audit interne ?

- Voir explications ci-dessus.

Q11. Est-ce que le contrôle interne amène une valeur ajoutée pour maîtriser le risque de fraude ?

- Bien entendu. Surtout pour la prévention de fraude (pas d'opportunité pour les employés de frauder)

Q12. D'après vous, disposer d'un SCI efficace est-il suffisant pour réduire le nombre de tentatives de fraude ?

- Non, il faut insister sur l'éthique au sein de l'entreprise.

Q13. Quelles améliorations faut-il apporter au COSO 2013 pour pouvoir lutter contre les fraudes et réduire ce risque de façon plus net ?

- La fraude ne peut pas être évitée par un modèle ou le respect d'une norme. C'est avant tout une question de culture d'entreprise, à mettre en place par la direction notamment.

Q14. Qu'est-ce qu'il faudrait créer pour apporter un soutien au SCI afin de réduire le nombre de tentatives ?

- Voir réponses ci-dessus

Q15. Existe-t-il un outil élaboré spécialement pour lutter contre la fraude financière en entreprise ?

- Non. C'est du cas par cas (dépend du type de business)

Q16. D'après votre expertise, qu'est-ce que vous feriez au sein d'une entreprise afin de réduire la probabilité d'occurrence du risque de fraude ?

- Voir réponses ci-dessus (éthique + culture d'entreprise + SCI)

Q17. Enfin, l'avancée technologique est-elle bénéfique ou non pour une entreprise afin de combattre la fraude financière ?

- Oui bien sûr. Les ordinateurs sont plus fiables que les humains... Encore faut-il savoir maîtriser son informatique.

Entretien n°4

Responsable d'audit interne dans le domaine bancaire

Q1. Pourriez-vous me citer différents types de fraudes que rencontrent souvent les entreprises ?

- Dans la fraude financière, il y a la fraude externe et interne ça c'est vraiment important. Il est important de savoir si l'attaque vient de l'extérieur en essayant par exemple de transférer de l'argent en dehors de la banque ou des encaissements de chèques frauduleux. La fraude interne arrive lorsque le collaborateur s'enrichit de manière illicite avec par exemple des vols dans la caisse.
- Une autre problématique qui se pose par rapport au contrôle interne, c'est de dire, plus une personne est élevée dans la hiérarchie plus elle a des compétences et des droits. Le risque du *management override* est donc un autre type de fraude qui me paraît être important à citer. L'idée c'est de se dire que tout le monde obéit au management sans rien dire de manière à ce qu'il puisse faire ce qu'il veut. Les contrôles fonctionnent bien dans la première ligne de défense mais plus on monte dans la hiérarchie moins les contrôles atteignent les managements.
- Il y a aussi le détournement d'actifs. C'est un type de fraude plus vaste car plus un actif est fongible/liquide plus c'est compliqué. Les fraudeurs seraient plus pousser à voler un diamant qu'une pelleteuse par exemple, il faut donc savoir adapter ses contrôles en fonction des actifs de l'entreprise.
- Une fraude à la mode, qui est assez connu du moins dans mon domaine c'est la fraude au président.
- Il arrive aussi dans le monde bancaire que les collaborateurs falsifient de la documentation voire même créé de faux clients de façon à pouvoir se verser l'argent sur un compte à eux. Cela existe vraiment.
- La fraude comptable est aussi un type de fraude qui me vient à l'esprit. Certains types de compte qui sont à risque. C'est ceux qui ne sont quasiment jamais utilisés, comme banque restante. C'est surtout dans ces comptes où le SCI doit se concentrer. Ou il y a aussi des comptes dormants qui restent inactifs et personne ne le voit comme par exemple la perte de contact avec un client suite

à un décès qui n'est pas communiqué. Le risque ici est que le conseiller le remarque et s'approprie ce compte.

- Il y a aussi les cybercriminels qui deviennent de vrais criminels une fois qu'ils ont opéré alors que ce sont d'après moi des gens normaux qui se foutent en l'air pour un simple challenge.

Q2. Quels sont les causes et facteurs déclencheurs de fraude ?

- Pour moi le triangle de la fraude résume bien les causes de la fraude. La motivation et la pression sont vraiment des facteurs importants. Les gens ont des pressions sociales et se fichent en l'air avec les cas de fraude. Ils sont malades du jeu et n'arrivent pas à suivre leur train de vie notamment avec les femmes et le casino. Le besoin d'argent est clairement un facteur déclencheur.
- La pression sur le chiffre d'affaires incite aussi à la fraude mais cette fois-ci comptable. L'employé sous pression va enregistrer des revenus en plus afin de satisfaire la demande des dirigeants. La méthode de l'enregistrement décalé est aussi utilisée dans laquelle on va enregistrer le chiffre d'affaires de janvier au mois de décembre afin de pouvoir satisfaire le patron.
- Ou alors, lorsque les dirigeants veulent payer moins d'impôts, ils augmentent les charges de façon à optimiser la charge fiscale. Ceci se fait très souvent dans les PME.
- La justification peut aussi être un facteur car dans les PME les fraudeurs justifient leurs agissement en disant : « tout le monde le fait ».

Q3. Quelles peuvent-être les vulnérabilités d'une entreprise favorisant la fraude financière ?

- Comme je l'ai évoqué dans la question une, le fait d'avoir des actifs fongibles mais aussi le manque de contrôle, même si on sous-estime la motivation et la justification dans les approches pour étudier le problème.

Q4. Quels sont les facteurs qui poussent les gens à la fraude ?

- Opportunité : *Hard fact*
- Motivation : *Soft fact*
- Justification : *Soft fact*

Q5. Avez-vous déjà été confronté à une fraude (en tant qu'auditeur, collaborateur ou autre) ?

- Oui, et souvent, on détecte ça d'une manière aléatoire en s'apercevant qu'il y a quelque chose d'étrange. Ensuite on creuse et on détecte la fraude. On se base par exemple sur la fluctuation du chiffres d'affaires ou alors sur le nombre de fautes d'orthographe d'un mail que l'on vient de recevoir. Toutes ces choses inhabituelles peuvent être le signal fort qu'une fraude est en train de se dérouler.

Q5.1. Si oui, quelle réaction avez-vous eu ? Que s'est-il passé ensuite ?

- Il y a différentes manières de traiter une affaire. Soit des spécialistes de fraudes viennent en aide soit la révision interne peut s'occuper directement du cas suivant l'ampleur de la fraude. Lorsqu'il y a plusieurs personnes impliquées dans la fraude cela devient assez compliqué et nous devons recourir aux spécialistes de la fraude.
- Les fraudes peuvent aboutir à des plaintes pénales lorsqu'en interne personne ne trouve de compromis. Les investigations sont faites par le réviseur externe ou interne mais si la FINMA a des doutes et sent qu'il y a des manipulations douteuses de cours de bourse par exemple, elle peut ordonner des contrôles à une société d'audit.
- Il arrive parfois que personne ne sorte l'information de la fraude à l'extérieur de façon à éviter d'apparaître dans les médias. C'est silence radio.

Q6. Comment découvre-t-on ces tentatives de fraude, quels sont les signes ?

- Les bons fraudeurs on ne les identifie pas facilement avec un système. Car ça arrive souvent lorsqu'il y a des failles dans l'entreprise et ce sont des gens qui maîtrisent les techniques utilisées. Mais avec de simples contrôles et un SCI bien en place, la probabilité de détecter des fraudes augmente.
- En revanche, je pense que l'esprit critique joue un rôle à joué chez les auditeurs internes. Il faut ressentir de ce qu'il se passe autour de soi. Quand on reçoit des informations contradictoires, quand on sent qu'il y a une rétention d'informations, ce n'est pas très logique, donc on se pose des questions. Il y a des signes qui ne trompent pas chez la personne. Son attitude, ses propos, sa façon de parler. Il est vraiment très important d'écouter attentivement ce que les collaborateurs peuvent dire par exemple « on est sans cesse sous pression dans

le département ventes ». Ce genre d'informations doit pouvoir nous signaler que des tentatives de fraude peuvent être commises.

Q7. Quels sont les enjeux et conséquences pour l'entreprise ?

- Le risque de réputation peut être énorme. C'est un risque très important à gérer pour l'entreprise car la perte en réputation peut faire perdre des fournisseurs et d'autres parties prenantes vitales pour l'entreprise.

Q8. Comment peut-on prévenir ces tentatives de fraude (outils, réactions humaines) ?

- Le SCI est quand même un outil qui fonctionne très bien sur l'opportunité. Mais je pense que par une bonne gouvernance éthique et une culture d'entreprise la fraude peut-être davantage éviter. La bonne gouvernance est porteuse de l'esprit de l'entreprise et doit donc s'assurer qu'il y a un management honnête pour permettre aux collaborateurs de suivre l'exemple. La complémentarité entre le SCI et une bonne gouvernance est d'après moi une bonne manière de prévenir.
- On est plus dans l'authenticité des personnes que sur les chartes. Il faut savoir appliquer ce qui est dit et ne pas juste avoir pleins de documents qui ne sont pas respectés.
- En gros, il faut faire connaître l'essence même de l'entreprise, impliquer les collaborateurs et les sensibiliser à cette problématique.

Q9. Existe-il un profil type de fraudeur ?

- Je dirais que c'est souvent un individu issu d'une fonction élevée dans la hiérarchie avec un certain nombre d'années d'expériences dans l'entreprise. C'est souvent des hommes. C'est avant tout parce qu'il y a plus d'hommes dans les postes à responsabilités et on a cette opportunité du *management override* qui est souvent présente.

Q10. Pourriez-vous m'expliquer le lien entre la fraude financière et le contrôle interne et l'audit interne ?

- Le principe des lignes de défense peut expliquer le lien. L'opérationnel fait des contrôles de premier niveau sur toutes les opérations et ensuite le contrôle interne s'assure que tout va bien en contrôlant par exemple les contrats les plus

La fraude financière et le contrôle interne en entreprise : l'importance d'un SCI efficient pour optimiser l'identification des risques de fraude et réduire leur probabilité d'occurrence.

importants et agit surtout sur l'opportunité de la fraude. Derrière ça, l'auditeur réunit le travail de l'opérationnel et du contrôle interne et fait une appréciation du SCI dans sa globalité de manière à s'assurer que tout est OK.

Q11. Est-ce que le contrôle interne amène une valeur ajoutée pour maîtriser le risque de fraude ?

- Oui, clairement. Dans la pratique, l'auditeur interne détecte rarement la fraude.
- Il ne faut pas oublier que le risque de fraude reste un risque secondaire, la principale préoccupation du SCI c'est que la marche des affaires se déroule correctement.
- Le but d'un SCI est de favoriser les bons contrôles à chaque niveau pour avoir une bonne gestion et éviter la fraude et ce n'est pas l'inverse.

Q12. D'après vous, disposer d'un SCI efficace est-il suffisant pour réduire le nombre de tentatives de fraude ?

- Non, car il faut agir sur la motivation et la justification et s'aider de la bonne gouvernance.

Q13. Quelles améliorations faut-il apporter au COSO 2013 pour pouvoir lutter contre les fraudes et réduire ce risque de façon plus net ?

- C'est un concept générique pour moi, ça récapitule bien différents points, sa force c'est de bien résumer tout ce qu'il y a dans l'entreprise. Sa force c'est vraiment que c'est un référentiel, après à chaque entreprise de l'adapter.
- Une autre question serait de savoir si le triangle de la fraude est bien pris en considération dans le COSO 2013. Je pense que ce genre d'analyse peut vous aider à trouver une piste de solution.

Q14. Qu'est-ce qu'il faudrait créer pour apporter un soutien au SCI afin de réduire le nombre de tentatives ?

- C'est plutôt d'une manière inhérente, on pense à un processus, on pense à le sécuriser. Comment créer un processus ? On réfléchit à tout le contrôle interne et par ce biais, cela permet de réduire le risque de fraude.
- Quand il y a l'évolution du SCI, soit parce que le business évolue, soit parce que les processus évoluent, il faut à ce moment-là réfléchir à la fraude. Attention aussi à toujours penser au coût/bénéfice. Si je prends l'exemple de l'avion qui a

plongé en Allemagne. Certains assurent qu'il faudrait rajouter un copilote d'autres non. Il faut savoir vivre avec un niveau de risque, ça fait partie du jeu. Il suffit simplement que le SCI soit adapté à la société et que ce ne soit pas la sclérose pour être efficace.

Q15. Existe-t-il un outil élaboré spécialement pour lutter contre la fraude financière en entreprise ?

- Dans le monde bancaire il existe des logiciels spécialement conçus pour analyser les transactions. Il faut d'ailleurs faire attention à la gestion des accès de ce genre de logiciels et savoir distinguer la limite entre la fraude et l'erreur. Quand on fait un contrôle, et qu'on tombe sur une irrégularité, savoir si c'est une erreur ou une fraude.
- Ça reste objectif, mais le monde bancaire est impitoyable par rapport à ça. On veut que les personnes à responsabilité aient une activité irréprochable, donc on ne prend pas de risque. Au niveau de la fraude en banque, c'est souvent un licenciement qui accompagne le fraudeur tandis que dans un hôpital par exemple ce sera un avertissement car le risque sur la réputation est moins élevé pour un hôpital que pour une banque.

Q16. D'après votre expertise, qu'est-ce que vous feriez au sein d'une entreprise afin de réduire la probabilité d'occurrence du risque de fraude ?

- Je réfléchirais sur les actifs et charges facilement retournable. Je regarderais dans quelles activités il y a le plus de pression pour justement agir sur la justification du triangle de la fraude et ensuite je ferais une évaluation du SCI qui est en place par rapport à ces éléments à risques.

Q17. Enfin, l'avancée technologique est-elle bénéfique ou non pour une entreprise afin de combattre la fraude financière ?

- La new technologie permet de faire des systèmes plus rigides, typiquement avec ces contrôles qui sont « embaded » comme par exemple la double validation. C'est d'après moi un grand avantage.
- Par contre, ça amène une perte de sens du réel. On perd la valeur de l'argent notamment chez les traders. Cette notion de perte du réel permet clairement de passer à l'acte plus facilement. En plus de ça, le fraudeur évolue avec les nouvelles technologies et surtout le cybercriminel.

- Je ne vois donc pas l'utilité de détenir un système super rigide si les collaborateurs ne font pas attention.
- Je trouve que ça ne change rien, le fraudeur évolue et les entreprises évoluent aussi avec. Il faut savoir adapter sa stratégie de défense car au final le danger reste le même.

Q18. Avez-vous quelque chose à ajouter / Avis personnel ?

- Je reste toujours convaincu que le plus faible restera l'humain et ce à tous les niveaux. Vous pouvez mettre en place des contrôles 4 yeux, une gestion des accès, des lignes de défense, etc. Mais au final si la personne ne respecte pas la culture de l'entreprise et agit de manière irresponsable vous aurez dépensez votre énergie pour rien.
- Encore une fois je pense que toute entreprise tolère un niveau de risque mais il est important d'agir de manière proactive afin d'anticiper les différents risques.
- Les normes ont également un rôle à jouer dans cette problématique. Ce n'est pas uniquement à l'entreprise de gérer la fraude mais c'est également le devoir de la réglementation de mettre des lois en place afin de dissuader les fraudeurs d'agir en démontrant qu'il y a des sanctions graves.
- D'une manière générale, je pense que la combinaison entre un SCl efficace et une bonne gouvernance d'entreprise peut suffire à réduire la fraude en entreprise.

Entretien n°5

Assistant Manager Internal Audit

Q1. Pourriez-vous me citer différents types de fraudes que rencontrent souvent les entreprises ?

- Oui, le premier qui me vient à l'esprit est le détournement d'actifs. Au niveau des fournisseurs par exemple ou le détournement de cash. La fraude dans les rabais est aussi un type de fraude que rencontrent souvent les entreprises.
- Il peut aussi y avoir la fraude aux commissions. Si je prends l'exemple de Tissot qui vend à travers des « retailers » et ces derniers vont à Manor et le modèle est proposé à moins 20% par contre ils demandent 10% du chiffre d'affaires à la fin des ventes et là il y a un potentiel acte de fraude.
- A mon avis, il faut toujours regarder l'argent qui sort de l'entreprise mais attention aux fournisseurs pour les retro commission. Au niveau des achats tu peux aussi avoir un cas de fraude.

Q2. Quels sont les causes et facteurs déclencheurs de fraude ?

- Il faut se baser sur le triangle de la fraude. Si tu veux agir au niveau du triangle, tu vas agir avec le SCI.
- L'élément « motivation » du triangle de la fraude, est souvent le synonyme de ceux qui ont des dettes, ou qui ont dans la sphère privée des choses qui les motive à commettre la fraude comme le problème d'argent.
- La justification est liée à la psychologie humaine du fraudeur. Il perçoit un manque de reconnaissance au niveau professionnel et cherche à justifier son acte.
- L'opportunité est un *hard fact*. Si on voit que l'entreprise a des failles on passe à l'action et on tente la fraude. Je pense que le SCI doit être préventif et agir sur ce facteur.
- Je trouve qu'on parle souvent de processus et moins de personne. Il faut donc aussi faire un focus sur la personne de manière intuitive. Ce n'est pas le travail de l'audit mais si on découvre qu'il y a une fraude on va creuser dans la sphère privée du fraudeur.

Q3. Quelles peuvent-être les vulnérabilités d'une entreprise favorisant la fraude financière ?

La fraude financière et le contrôle interne en entreprise : l'importance d'un SCI efficient pour optimiser l'identification des risques de fraude et réduire leur probabilité d'occurrence.

- Dans l'opportunité du triangle se concentre les vulnérabilités. On a par exemple le manquement dans le contrôle interne, le manque d'application des collaborateurs mais aussi le cumul de fonctions compatibles. Une personne qui prépare et valide les factures sans contrôle préalable peut être poussée à commettre une fraude. La création d'un fournisseur fictif avec un compte fictif permettrait au fraudeur de se transférer l'argent indirectement. Le manque de séparation des fonctions (SOD) est donc la vulnérabilité clé pour moi car c'est très important dans le monde du travail.

Q4. Quels sont les facteurs qui poussent les gens à la fraude ?

- Le manque d'argent, l'addiction aux jeux, tous ces éléments peuvent être des faits qui motivent le fraudeur. Le manque de reconnaissance peut aussi être un facteur qui pousse à la fraude même si celui-ci est considéré comme un élément de justification dans le triangle de la fraude.

Q5. Avez-vous déjà été confronté à une fraude (en tant qu'auditeur, collaborateur ou autre) ?

- Oui mais je vais parler d'une manière générale car je ne vais pas pouvoir te détailler les faits.
- Il faut toujours avoir en tête les lignes de défense car l'audit interne ne va jamais chercher à identifier une fraude, ce n'est pas son objectif. Son objectif c'est vraiment d'identifier les vulnérabilités dans les processus et procédures et proposer des améliorations.
- Les *red flags* sont également à prendre en considération.
- Lorsque j'ai été confronté à la découverte d'une fraude, j'ai dû arrêter le mandat et creuser afin d'être sûr de la fraude identifiée.

Q5.1. Si oui, quelle réaction avez-vous eu ? Que s'est-il passé ensuite ?

- Il faut impérativement que tu remontes l'information en signalant qu'il y a eu une fraude. Ensuite, soit on regarde en détails. Soit l'entreprise victime fait appel à des experts de fraude certifiés. C'est le *forensic accounting*.
- Car ces experts en fraude ont la possibilité de faire un travail qui puisse être utilisable dans le cas d'un procès. Ils savent rendre le détail utile pour les avocats alors que l'audit lui est plus focus audit processus et moins juridique.

- L'audit interne peut recommander le *forensic* et les aider avec leur connaissance dans les processus de l'entreprise pour optimiser le temps d'investigation.
- Mais pour le *forensic*, on va toujours tracer le mouvement d'argent car il est difficilement falsifiable, alors que la documentation est plus simple à falsifier. On peut donc tracer le cash et voir l'historique réel des transactions bancaires.
- Ensuite, les experts en fraude vont analyser les données personnelles du fraudeur avec des outils bien spécifiques. A travers cette analyse ils peuvent trouver un petit détail qui nous permette de détecter le détail décisif. Après la partie analyse, il y a une partie confrontation entre le fraudeur et les *forensic*. On confronte les gens avec les données étranges qui ont été détectées et ensuite l'avocat rentre en jeu.

Q6. Comment découvre-t-on ces tentatives de fraude, quels sont les signes ?

- Comme je l'ai dit, ce sont les manquements dans les processus en terme de contrôle.
- Pour être plus clair, un contrôle préventif peut être la séparation des fonctions, car il agit en amont et bloque la possibilité de faire la fraude ou encore l'analyse d'un fournisseur avant de le faire valider par les finances. Mais on peut aussi avoir des contrôles défectifs comme le contrôle d'un responsable financier dans lequel il check chaque semestre la fluctuation des chiffres de manière à s'assurer que tout est OK.

Q7. Quels sont les enjeux et conséquences pour l'entreprise ?

- La perte d'actifs me vient tout de suite à l'esprit. Mais il faut savoir que certaines entreprises ont des tolérances de fraudes. Aux USA, dans les casinos il y a logiquement une certaine tolérance au risque de cambriolage par exemple.
- Par contre, pour des associations comme MSF ou la Croix rouge, un simple problème peut ruiner leur réputation. Tous les donateurs se sentent directement concernées s'il y a une fraude en interne, donc forcément la tolérance est moins élevée et donc le risque de réputation devient plus important. Ça varie beaucoup
- Dans le domaine bancaire, c'est très important la réputation. Avant ils n'allaient pas aux tribunaux mais maintenant ils doivent rendre de plus en plus de compte même si ça reste très important de garder ce genre d'évènements secret. N'oublie pas de toujours réfléchir en termes de coût/bénéfice.

Q8. Comment peut-on prévenir ces tentatives de fraudes (outils, réactions humaines) ?

- Il faut que tu aies en tête la notion du contrôle préventif et du contrôle défectif et des lignes de défense.
- Pour moi, le « tone at the top » est clairement un élément très important. Il faut savoir montrer l'exemple au sein d'une entreprise et se baser sur des valeurs. Il y a aussi la communication qui est essentielle. Le management peut maintenir une sorte de pression sur les collaborateurs quant aux risques et conséquences de la fraude.

Q9. Existe-il un profil type de fraudeur ?

- Si je me base sur mon expérience, c'est souvent des gens qui ne prennent jamais de vacances car ça démontre que la personne veut garder sa fraude en place. Personnellement, j'obligerai un collaborateur à prendre au moins deux semaines de vacances de suite de façon à avoir un contrôle préventif contre la fraude. D'ailleurs dans l'exemple que je t'ai cité tout à l'heure, la personne s'est fait avoir lorsqu'elle s'est absentée.

Q10. Pourriez-vous m'expliquer le lien entre la fraude financière et le contrôle interne ou l'audit interne ?

- Le contrôle interne agit sur la fraude avec des contrôles préventifs et défectifs. Si c'est pour la prévenir on n'a pas de pertes financières. En ce qui concerne le contrôle défectif, il doit intervenir rapidement de manière à éviter un impact trop important.
Ces deux contrôles, préventifs et défectif, sont liés, car le premier agit sur la probabilité et le second sur l'impact. Il faut donc agir rapidement une fois que la fraude est détectée pour avoir un impact moins conséquent.
- L'audit interne est la troisième ligne de défense et peut identifier les indices de fraudes ou les manquements dans les contrôles.
- Je te donne un exemple. Si je constate qu'il y a des personnes qui n'ont pas pris des vacances pendant un an, je le signale immédiatement car j'estime que c'est un indice de fraude et qu'il peut y avoir potentiellement une fraude en cours et je recommande qu'il lui faut deux semaines de vacances immédiatement. L'indice des vacances est réellement un indice très fort qui marche tout le temps.

Q11. Est-ce que le contrôle interne amène une valeur ajoutée pour maîtriser le risque de fraude ?

- Comme je l'ai dit à la question précédente, il agit sur la probabilité et l'impact du risque, donc je dirai que oui.

Q12. D'après vous, disposer d'un SCI efficace est-il suffisant pour réduire le nombre de tentatives de fraude ?

- Oui, le SCI c'est l'élément le plus important. Attention à ne pas oublier les éléments *hards* et *softs* contrôles. La culture d'entreprise par exemple c'est un « soft ».

Q13. Quelles améliorations faut-il apporter au COSO 2013 pour pouvoir lutter contre les fraudes et réduire ce risque de façon plus net ?

- Je ne saurais répondre à cette question car ça reste un référentiel qui ne viendra pas nous donner la solution ultime. Il doit s'adapter en fonction du type de l'entreprise. Et je dois dire que le nouveau COSO 2013 a déjà connu une évolution importante par rapport à la fraude.

Q14. Qu'est-ce qu'il faudrait créer pour apporter un soutien au SCI afin de réduire le nombre de tentatives ?

- En gros, il faut se baser sur les concepts que je t'ai détaillés avant et compléter tout ça avec une gestion des risques et à ce moment-là tu as tous les éléments qui complètent un SCI efficace.

Q15. Existe-t-il un outil élaboré spécialement pour lutter contre la fraude financière en entreprise ?

- Il faudrait voir sur internet s'il existe des techniques de détection de fraude car je ne saurais pas te dire. Par contre, il existe des outils spécialement élaboré pour analyser des transactions en fonction de plusieurs caractéristiques. Ce sont les *Computer-Assisted Audit Tools* (CAAT)

Q16. D'après votre expertise, qu'est-ce que vous feriez au sein d'une entreprise afin de réduire la probabilité d'occurrence du risque de fraude ?

- Je me baserai sur les contrôles préventifs car ça permet d'avoir une anticipation.

Q17. Enfin, l'avancée technologique est-elle bénéfique ou non pour une entreprise afin de combattre la fraude financière ?

- Oui et non, car avec l'IT tout devient difficile à comprendre mais avec les nouvelles technologies, tu as de nouveaux outils qui permettent d'identifier les fraudes plus rapidement.
- Par contre au niveau IT, il est important d'avoir une séparation entre la programmation d'un outil et le test, car sinon le programmeur peut faire ce qu'il veut ensuite et personne d'autre n'aura le contrôle. La notion d'ITGC est très importante. La séparation des fonctions entre la personne qui développe et celle qui met en production est capitale.

Q18. Avez-vous quelque chose à ajouter / Avis personnel ?

- A mon avis, il y a vraiment les aspects SCI et IT. Ce n'est pas parce que tu as un système financier efficace que derrière l'IT ne pourra rien faire. N'oublie jamais que la culture d'entreprise est aussi très importante dans la lutte contre ce genre de risque et notamment le « tone at the top ».