En guise d'avant-propos, j'aimerais remercier l'ensemble des acteurs ayant participés de près ou de loin à la rédaction de ce mémoire.

Merci à mon promoteur, Pr. Gerrit Sarens, m'ayant accompagné et aidé tout au long de la rédaction.

Merci à ma famille et à mes amis pour l'aide apportée lors de la recherche des intervenants, mais aussi pour la relecture de ce mémoire.

Enfin, merci aux intervenants pour leur temps consacré à répondre aux interviews, sans qui il n'aurait pas été possible de réaliser ce mémoire.

Table des matières

INTRODUCTION

La conjoncture économique actuelle et les événements importants qui se sont déroulés au cours des dernières décennies ont eu pour conséquence de sensibiliser à nouveau les entreprises à la gestion des risques. (Ernst & Young, 2013). De par la concurrence féroce et accrue entre les entreprises, ainsi que les modifications permanentes du marché, des technologies, et des réglementations, les organisations ont pour obligation de repenser et de maitriser en temps voulu, l'ensemble des risques les plus variés et les plus complexes (Luburic, Perovic & Sekulovic, 2015).

Les dirigeants d'entreprises doivent dès lors relever d'importants défis en matière de gouvernance, et répondre aux problématiques organisationnelles. Est-ce que les risques sont identifiés et évalués dans tous les domaines de l'organisation ? Est-ce que les dirigeants d'entreprise peuvent apportés une réponse appropriée et alignées avec l'appétence au risque de l'entreprise ? Est-ce que les rôles et les responsabilités sont clairement définis au sein de l'organisation ? Voici une liste non exhaustive de problématiques organisationnelles courantes, auxquelles il y a un besoin de répondre de manière efficace et efficiente. (AMRAE & IFACI, 2013).

D'importants montants ont été consacrés par de nombreuses grandes et moyennes entreprises dans les activités liées aux systèmes de gestion des risques, aux systèmes de contrôles financiers, de contrôles internes, et de gestion de conformité. Toutefois les résultats espérés n'ont pas été au rendez-vous (Ernst & Young, 2013).

Les fonctions telles que la gestion des risques, le contrôle interne et l'audit interne représentent les meilleurs moyens pour répondre aux problématiques organisationnelles précitées. La question est de savoir comment ces fonctions doivent collaborer pour intégrer les différents systèmes afin de les faire fonctionner efficacement. Un nouveau modèle de gouvernance a dès lors gagné en popularité ces dernières années, le modèle des 3LoD (Klotz, 2015).

Ce modèle relève d'une importance capitale pour les entreprises actuelles. En effet, les organisations disposant d'un système des trois lignes de défense robuste auront tendance à être plus sensibles aux risques. Celles-ci pourront réagir plus efficacement et plus rapidement lorsque de nouveaux risques seront identifiés, elles pourront en outre

déployer de manière efficace les ressources nécessaires quant à la gestion de ces risques. Le modèle permet avant tout d'assigner des rôles et des responsabilités clairement définis aux différents acteurs de l'entreprise. Ces éléments contribuent à diminuer les pertes inattendues ainsi qu'à accroitre les chances d'atteinte des objectifs stratégiques de l'organisation.

Ce mémoire aura donc pour objectif d'étudier en quoi le modèle des 3LoD est efficace, ainsi que les facteurs pouvant potentiellement influencer l'effectiveness du modèle. Nous apprendrons notamment que le type d'interaction entre les lignes de défense, l'appétence au risque définie par les organes de gouvernance ainsi que la culture de l'entreprise influence l'effectiveness du modèle des 3LoD.

Deux parties composeront ce mémoire, à savoir la revue de littérature ainsi que la partie empirique.

La revue de littérature aura pour but de mettre en contexte le modèle des 3LoD, d'en extraire les composantes principales, pour en déduire les problématiques de recherche. Dès lors, les deux premières parties seront consacrées à la gestion des risques et à l'audit interne, alors que la troisième partie sera consacrée au modèle des 3LoD en lui-même.

La partie empirique consistera à étudier la problématique de recherche de manière pratique, plus précisément de manière qualitative. Il sera exposé, dans un premier temps, la méthodologie utilisée et la méthode de collecte de données, pour ensuite révéler l'analyse des entretiens réalisés.

PARTIE 1 : REVUE DE LITTERATURE

1. Le système de gestion des risques

1.1 La gestion des risques en entreprise

1.1.1 Définitions

Approches traditionnelle et globale de la gestion des risques

L'étude de la gestion des risques a débuté après la seconde guerre mondiale, exclusivement dans le secteur des assurances, ceci dans le but de protéger les entreprises mais aussi les particuliers. Dès les années 50', les compagnies d'assurance n'ont plus été en mesure d'établir des analyses pertinentes pour les nouveaux types de risques, tels que les risques financiers. Les entreprises ont, par ailleurs, pris conscience qu'elles pouvaient éviter les compagnies d'assurance en intégrant les risques via des systèmes de prévention de pertes et de contrôles. En conséquence, l'étude de la gestion de risques a été approfondie, et a été progressivement intégrée dans le secteur bancaire (Dickinson, 2011 & Whitman, 2015).

Dans les années 80', l'approche traditionnelle de gestion des risques est la plus répandue. Celle-ci est considérée comme étant une méthode désagrégée, la gestion des risques y est segmentée, et conduit à une multitude d'entités différenciées dans l'organisation (Liebenberg & Hoyt, 2003). Chaque silo dans la compagnie possède les capacités, et les responsabilités nécessaires pour affronter les risques potentiels encourus (Casualty Actuarial Society [CAS], 2003)

L'approche traditionnelle gère « les conséquences des variations négatives des revenus espérés dans le temps » (Whitman, 2015, p.23), menant les experts à se préoccuper seulement aux quantifications et impacts connus (Arena, Anaboldi & Azzone, 2010).

Ce postulat démontre, toutefois, les difficultés de lier la gestion des risques à la stratégie d'entreprise, de faibles procédures de conformité ou encore des contrôles inadéquats sur les rapports financiers, créant ainsi une coordination inefficace et dupliquant les coûts organisationnels (CAS, 2003).

Dans les années 90', un changement de paradigme s'opère, puisqu'une vision holistique de la gestion des risques s'impose (Gordon, Loeb & Tseng, 2009). En effet, « le but de la gestion des risques n'est pas de minimiser le risque total auquel fait face une organisation,

mais de choisir le niveau optimum de risques afin de maximiser la valeur des actions ». (Farrell & Gallagher, 2014, p. 32)

Le concept d'Enterprise Risk Management emboite dès lors le pas. Bien que l'ERM n'ait pas évolué de manière uniforme dans les différents secteurs, il peut être rapporté quelques facteurs communs caractérisant celui-ci.

Premièrement, l'apparition d'une multitude de risques complexes auxquels doivent faire face les entreprises actuelles, tels les risques financiers, les risques opérationnels et stratégiques. Deuxièmement, la participation croissante des parties prenantes externes à l'organisation, poussant les managers à prendre plus de responsabilités dans l'établissement d'une vision globale des risques. Pour exemple, les prévisions financières détaillées et exigées par les actionnaires, ou encore les multiples obligations de publications réclamées par les instances régulatrices. Troisièmement, le développement de la quantification des risques, permettant aux entreprises d'effectuer un ensemble de scénarios plausibles afin de prendre des décisions informées et éclairées. Quatrièmement, le partage grandissant entre entreprises non concurrentes de l'information, permettant l'amélioration des processus organisationnels et ouvrant la voie aux meilleures pratiques de gestion des risques (CAS, 2003).

En bref, l'ERM a « le potentiel de réduire les coûts de conformité, d'améliorer les performances opérationnelles, de renforcer la gouvernance d'entreprise ainsi que de délivrer une augmentation de la valeur des actions » (Bowling & Rieger, 2005, p.32). Ce concept a pour but de « créer le niveau désiré de variation des revenus espérés sur le temps pour l'ensemble des opportunités et des menaces de l'entreprise » (Whitman, 2015, p. 173).

Le processus de gestion des risques

Le processus de gestion des risques en entreprise représente la clef pour qu'un ERM soit *effective*. Ce processus consiste en une boucle infinie, mettant en avant un ensemble d'éléments primordiaux et de principes, dans le but de répondre aux besoins de mitigation des risques d'une entreprise (Decaux, 2017).

Premièrement, le management doit proposer une philosophie claire de la gestion des risques à l'entreprise, tout en étant attentif à la perception du risque par les collaborateurs de cette même entreprise (Decaux, 2017).

Deuxièmement, le management se doit de fixer les objectifs et de planifier la stratégie, tout en respectant *l'appétence pour le risque*, à savoir le montant et le type de risque qu'une entité est prête à accepter, et *la tolérance pour le risque*, à savoir le maximum de risques spécifiques qu'une entité est prête à prendre en fonction des autres risques. Ceci doit être en accord avec la vision et les valeurs de l'entité, pour ensuite être traduit en budget et actions quotidiennes (Decaux, 2017).

Troisièmement, l'identification des différents types de risque doit être établie, afin de déterminer si ceux-ci représenteront des opportunités ou à l'inverse affecteront l'atteinte des objectifs. Il existe différentes méthodes pour l'identification, telles que les interviews, l'audit interne, les workshops ou encore les analyses de scénarios (Decaux, 2017).

Quatrièmement, l'évaluation des risques permet de considérer quels événements auront un impact sur l'atteinte des objectifs. Cette étape prend en compte le *risque inhérent*, à savoir le risque précédant toute intervention, et le *risque résiduel*, à savoir le risque restant suite aux efforts effectués pour mitiger le risque. L'évaluation permet dès lors de définir la probabilité avec laquelle le risque apparait et la sévérité de ce dernier. Les méthodes utilisées peuvent être qualitatives ou quantitatives (Decaux, 2017).

Cinquièmement, le management détermine de quelle manière répondre aux risques. Il existe différentes possibilités, telles que les supprimer, les traiter, les transférer ou les tolérer. Les politiques ou procédures utilisées pour répondre aux risques peuvent être définies par les activités de contrôle, telles que la séparation des fonctions, les indicateurs de performance, les contrôles physiques ou encore les révisions effectuées par les directions (Decaux, 2017).

Sixièmement, il est essentiel de développer des rapports sur les risques, identifiant l'ensemble des informations pertinentes, pouvant être communiquées de manière à ce que le management assume sa responsabilité (Decaux, 2017).

Dernièrement, afin d'assurer l'*effectiveness* de l'ERM, le management se doit d'évaluer la présence et le fonctionnement des composants de l'ERM à travers le temps. En effet, l'ERM n'est pas un projet ponctuel, mais continu. Les objectifs, l'environnement, et par conséquence les risques associés varient pendant le temps. Ce monitoring peut être effectué via des activités de monitoring continues, des évaluations séparées ou indicateurs clés de risques (Decaux, 2017).

1.1.2 Limites ERM

Le concept de gestion des risques en entreprises soulève toutefois quelques questions. Grose (n.d.), fondateur et président d'Omega System Group Incorporation, met en évidence cinq faiblesses que constituent l'ERM.

Ce concept ne présente, tout d'abord, pas de processus défini assurant une gestion des risques totale. Il n'existe pas de mécanismes universels permettant de consolider l'ensemble des fonctions, des activités et des intérêts de l'entreprise. Jusqu'à ce que la gestion devienne systématique, le concept souffrira d'une mauvaise compréhension, de fragmentations et de réactions confuses (Grose, n.d.).

Deuxièmement, malgré les processus de gestion de risques mis en place par les différents référentiels, permettant une évaluation continue des risques, aucune entreprise ne peut prédire des événements qui ne se sont pas encore déroulés. L'approche globale de gestion des risques peut être définie comme étant une approche réactive et non proactive (Grose, n.d.).

Troisièmement, une entreprise ne sait prédire les coûts et les bénéfices de l'implémentation d'un ERM au sein d'une entreprise. Il est difficile de savoir si l'entreprise en sortira gagnante. De plus, les mesures de l'ERM ne portent que sur deux dimensions, la probabilité et la sévérité du risque. Tant que la dimension du coût de mitigation ne sera pas prise en compte, il pourra subsister un désintéressement de la part du comité exécutif dans la gestion des risques, et dès lors l'impact n'en sera qu'amoindri (Grose, n.d.).

Dernièrement, il est difficile d'établir une hiérarchie exacte de chaque risque. Bien que le principe d'identification des risques devrait, en théorie, permettre cette sélection, en pratique ce dernier pourrait être influencé ou favorisé de par l'allocation des ressources. L'identification des risques n'est pas immune à la pression politique ou sociale. Lorsque l'industrie du tabac affirmait que ce dernier n'était pas nocif pour la santé, il est clair que le processus d'identification du risque n'a pas été établi en toute objectivité (Grose, n.d.).

1.2 Le contrôle interne

1.2.1 Définitions

Il existe une multitude de définitions du contrôle interne inscrite dans le référentiel scientifique à ce jour, néanmoins celles-ci ont évolué au cours des dernières décennies. Sans effectuer une liste exhaustive et sans entrer dans les détails des différentes

définitions existantes, il est toutefois intéressant de parcourir brièvement les divergentes notions du contrôle interne de la littérature académique.

Une conception apparue en 1948, par Fain et Faure, explique le contrôle interne comme étant « l'organisation rationnelle de la comptabilité et du service comptable visant à prévenir ou tout au moins à découvrir sans retard les erreurs et les fraudes » (Ebondo, 2004, p.72). Cette approche est toutefois restreinte à une vision purement comptable, et non organisationnelle. Selon Gumb & Noël, (2006, p.3) « le contrôle interne s'est d'abord constitué comme un dispositif destiné à prévenir les erreurs et les fraudes dans le domaine comptable ».

Le concept du contrôle interne a été élargi par la suite, les définitions couvrent en effet de nombreux autres contrôles en plus des contrôles comptables (Maijoor, 2000). Dans la fin des années 1990, début des années 2000, plusieurs auteurs ont proposé leur vision du contrôle interne.

Henri Bouquin se permet, tout d'abord, d'interpréter la notion de contrôle interne en fonction de son origine linguistique. Le terme contrôle tient sa définition d'une part du registre anglo-saxon, d'autre part du registre français. C'est pourquoi différentes significations en découlent, à savoir ; la vérification et avoir le contrôle. Il précise entre autres ; « C'est le vrai sens du « contrôle interne » : la maitrise des activités, à ne pas confondre avec l'audit, qui lui, est un processus de vérification. Le *control* s'exerce plutôt avant l'acte, le *contrôle*, après ». (Bouquin, 2005, p. 3). Outre les déviances linguistiques, Henri Bouquin propose une définition plus large de ce qu'est le contrôle interne, et considère ceci comme étant « une somme du contrôle stratégique, du contrôle opérationnel et du contrôle de gestion. » (Bouquin, 2004, p. 49).

Selon Benoit Pigé, le contrôle interne permet « de s'assurer que les salariés qui représentent l'entreprise vis-à-vis de l'extérieur agissent dans l'intérêt de l'entreprise. Il permet de vérifier que la coordination hiérarchique, formelle et informelle fonctionne correctement et assure une coordination efficace entre les individus. Il garantit que les décisions prises par les dirigeants sont mises en œuvre par l'ensemble des salariés de l'entreprise » (Gumb & Noël, 2006, pg.8).

COSO (2013, pg.3), définit le contrôle interne comme étant « un processus mis en œuvre par le Conseil d'administration, les dirigeants et le personnel d'une organisation, destiné à fournir une assurance raisonnable quant à la réalisation des objectifs suivants :

- La réalisation et l'optimisation des opérations.
- La fiabilité des informations financières et de gestion.
- La conformité aux lois et aux réglementations en vigueur. »

Cette définition offre une approche plus flexible du contrôle interne, se concentre sur l'aspect processus et non sur l'aspect rigide tel que le système ou la structure.

1.2.2 Limites du contrôle interne

Premièrement, Gumb et Noël (2007, p. 105) critiquent les définitions émises par Bouquin et Pigé. Concernant l'idée de Bouquin, celle-ci « renverrait à une conception hiérarchique et délégataire du système de contrôle ». De même, pour la définition donnée par Pigé, celle-ci serait trop vague et en oublierait les dimensions financières et comptables.

Deuxièmement, Ebondo & Pigé (2002) offre, eux, une définition décalée du contrôle interne. Ce dernier permettrait une maîtrise voire une réduction des coûts de transactions, et dès lors une meilleure efficience de l'organisation au sein du marché. Néanmoins, cette définition paraît peu convaincante lorsque des opérations d'externalisation sont effectuées au sein des organisations. Les dirigeants doivent garder une partie des activités centrales pour que puisse demeurer l'entreprise dans le marché.

Troisièmement, en ce qui concerne la définition émise par COSO, Maijor (2000) pointe un manque de clarté dans les limites du contrôle interne. Les trois objectifs, à savoir, la conformité aux normes, l'effectiveness des opérations de management et la pertinence des rapports financiers ; semblent trop larges, trop peu explicites. L'ensemble des mesures organisationnelles pourrait dès lors intégrer le champ d'action du contrôle interne, et ce dernier n'aurait plus mesure à être effective. Maijor (2000) explique par ailleurs que le contrôle interne vu par COSO se rapproche fortement de la notion présente dans la littérature comptable, et qu'il est difficile d'en distinguer les deux.

Enfin, en ce qui concerne la normalisation du contrôle interne, l'étude de Cappelletti (2006, p.37), sur l'application de la Loi sur la Sécurité Financière par les entreprises, démontre l'impact organisationnel et humain de cette mise en œuvre. Selon ses recherches, la normalisation provoque un alourdissement des procédures. Cela « pourrait

conduire les entreprises à animer le contrôle interne comme une fonction », menant à un contrôle « plus permanent et actif, et non plus ponctuel et subi ». Dès lors, il serait impératif pour les entreprises de mettre en place des dispositifs, méthodes et autres outils de gestion afin de pallier les manquements institutionnels.

1.3 Référentiels existants

Plusieurs référentiels sont apparus au cours des deux dernières décennies, ayant la principale qualité, d'établir des méthodes organisationnelles, de fournir des lignes directrices, tout en décrivant « un set spécifique d'activités fonctionnelles et de définitions associées à l'ERM » (CAS, 2003, p. 62).

1.3.1 COSO – ERM Integrated Framework

Un premier référentiel essentiel concerne celui réalisé par COSO en 2004, à savoir *COSO – ERM Integrated Framework*, représentant par ailleurs l'extension du référentiel sur le contrôle interne réalisé en 1992, *COSO – Internal Control Integrated Framework*. Il est important de spécifier que le référentiel de 1992 n'est pas remplacé par celui de 2004, il y est seulement intégré.

L'ERM est définit par COSO comme étant un « processus, effectué par le comité de direction, le management et le personnel, appliqué dans le cadre de la stratégie et à travers l'entreprise, conçu pour identifier d'éventuels événements pouvant affecter l'entité, et fournissant une assurance raisonnable quant à la réalisation des objectifs de l'entité » (COSO, 2004, p.2). Ce positionnement de COSO démontre le besoin d'intégrer les processus ERM avec le business modèle de l'entité et les initiatives stratégiques. L'output des processus ERM pourrait être donc un input à l'exécution et la planification stratégique de l'entité (Beasley, Hermanson & Viscelli, 2017).

En 2017, *COSO – ERM Integrated Framework* a été mis à jour, afin de répondre aux changements technologiques, opérationnels et organisationnels. Les composants de ce nouveau référentiel seront détaillés au point ci-après.

Ce cadre de référence, inclut dès lors les cinq composants essentiels du référentiel sur le contrôle interne, à savoir l'environnement, l'information, la communication, le pilotage et les activités de contrôle, se déclinant chacune sur les activités et les fonctions de l'entreprise (Gumb & Noël, 2006 et Cappelletti, 2006). Ce référentiel est pionnier dans son domaine, servant de base aux différentes régulations créées depuis, telles que le

Combined Code en Grande Bretagne, la Loi sur la Sécurité Financière en France ou encore la loi Sorbane-Oxlay aux Etats-Unis (Kinney, 2000).

1.3.2 CobiT

Un deuxième référentiel existant se nomme *CobiT,* « Control Objectives for Information and related Technologies ». Il constitue un cadre complet pour la gouvernance et la gestion de l'informatique dans son ensemble, comprenant cinq domaines, 37 processus informatiques et plus de 200 pratiques de gouvernance et de gestion. Il classe l'informatique dans quatre domaines ; à savoir planifier et organiser, acquérir et implémenter des solutions automatisées, livrer et prendre en charge et surveiller et évaluer 34 processus de haut niveau et intégrer de nombreux objectifs de contrôle (Khter & Othman, 2013).

Le *CobiT* se concentre donc principalement sur l'informatique, et est largement utilisé par les entreprises en complément du COSO, alors que ce dernier se concentre particulièrement sur les processus et les contrôles pour les rapports financiers.

1.3.3 ISO 31000 :2018

Un troisième référentiel présent dans la littérature académique est celui publié par l'Organisation Internationale pour la Normalisation, à savoir *ISO 31000 :2018*. Précédemment nommé *ISO 31000-2009*, cette version révisée fournit des lignes directrices ainsi qu'une approche générique non spécifique à une industrie ou un secteur, et peut être appliquée tout le long de la vie d'une entreprise, ce à tous les niveaux de décision (ISO, 2018).

Le corps du référentiel se compose de 4 points essentiels, tels que la création d'un vocabulaire commun pour le management des risques, le développement de critères de performances, un processus de gestion des risques, ainsi qu'un cadre pour l'implémentation de la gestion des risques au sein de l'organisation. Le processus de gestion des risques est fortement semblable à celui développé par le CAS, incluant l'identification, l'analyse et l'évaluation des risques (Lalonde & Boiral, 2012).

L'objectif principal de la norme ISO 31000 est de créer un processus d'amélioration continue, en renforçant notamment le point *surveillance et révision*, permettant ainsi de créer une « boucle fermée » (Lalonde & Boiral, 2012, p. 283 et Curkovic, Scannell & Wagner, 2013).

1.3.4 Turnbull Guidance

En 1999, l'organisme anglais responsable de la promotion de la bonne gouvernance en entreprise, le Financial Reporting Council, a développé le référentiel nommé *Internal Control : Guidance for Directors on the Combined Code*, plus connu sous le nom, *Turnbull Guidance*. Ce guide fournit de meilleures pratiques de contrôle interne pour les entreprises cotées au Royaume-Uni (Spira & Page, 2010) et responsabilise directement les directeurs et managers des institutions. En effet, il leur est requis d'instaurer une approche systématique de la gestion des risques et une approche du contrôle interne basée sur les risques (McCrae & Balthazor, 2000).

Selon McCrae & Balthazor (2000), le Turnbull Guidance se divise en quatre points distincts :

- Le développement d'une politique pour la gestion des risques.
- L'implémentation de cette politique à travers une approche systématique de contrôle interne basé sur la gestion des risques, capable de surveiller continuellement l'ensemble des risques internes et externes.
- La révision périodique du système de contrôle interne afin d'assurer la qualité des processus mis en place.
- La création de rapports annuels sur les différentes politiques de gestion des risques.

1.4 Principaux éléments du référentiel COSO

Comme dis précédemment, le référentiel COSO, constitue la base des différentes régulations mises en place au cours des dernières décennies, telles que le *Combined Code*, le *SOX*, ou la *LSF*. C'est pourquoi, il paraît intéressant d'analyser en profondeur les principaux composants de ce guide.

Le COSO – ERM Integrated Framework 2017, est constitué d'un ensemble de principes organisés en cinq composants inter reliés.

Le premier point constitue la *gouvernance et la culture*, fixant le ton de l'entreprise, renforçant l'importance des responsabilités de la gestion des risques. La culture s'en remet aux valeurs et aux comportements souhaités ainsi qu'à la compréhension du risque de l'entité. (Decaux, 2017)

Le deuxième point réside dans *la stratégie d'entreprise et la fixation d'objectifs*, établissant entre autres le niveau de risque souhaité par l'entreprise. (Decaux, 2017)

Troisièmement, la *performance* constitue l'identification, l'évaluation et la priorisation de l'ensemble des risques pouvant impacter la réalisation de la stratégie et des objectifs. Ce point conçoit aussi l'implémentation et le développement de méthodes pour répondre aux risques. (Decaux, 2017)

Quatrièmement, le point *Review and Revision,* évalue les changements substantiels au sein de l'organisation, revoit les risques et les performances, et poursuit l'amélioration de l'ERM. (Decaux, 2017)

Enfin, le dernier point s'attelle à *l'Information, la Communication et le Reporting*, ayant pour but de tirer profit de l'information et de la technologie, de communiquer les informations sur le risque et de publier des rapports sur le risque, la culture et la performance. (Decaux, 2017)

1.5 Régulations

Il existe plusieurs normes étatiques en matière de gestion des risques et de contrôles internes, ou plus généralement sur la bonne gouvernance des entreprises.

Premièrement, le Turnbull Guidance permet aux entreprises anglaises de s'accorder au Combined Code, à savoir l'ensemble des lois régissant les pratiques de bonne gouvernance d'entreprise en Grande-Bretagne. Ce dernier se base entre autres sur le Cadbury Code, mettant en avant le principe du c*omply or explain.* Plutôt que d'établir des lois contraignantes, le régulateur a défini un ensemble de principes que les sociétés cotées peuvent soit respecter, soit, dans le cas inverse, expliquer pourquoi elles ne l'appliquent pas (Arwinge, 2013).

En ce qui concerne les normes américaines de gouvernance d'entreprises, plus précisément la loi Sarbanes-Oxley, apparue en 2002, la SEC (Securities Exchange Commission) a admis que le Turnbull Guidance rassemblait les critères nécessaires afin de s'adapter aux régulations étatiques (Arwinge, 2013). La section 404 de cette loi « renforce les exigences imposées aux entreprises en matière de contrôle interne » (Gumb & Noël, 2006, p. 10). Elle impose aux dirigeants d'évaluer le contrôle interne de la compagnie sur les rapports financiers. Plus précisément, il est établi que les CFO et les CEO doivent publier trimestriellement et annuellement, les procédures ainsi que

l'effectiveness du contrôle interne de leur entreprise (Krishnan, 2005 et Van de Poel & Vanstraelen, 2011).

Cette loi diffère du Combined Code au Royaume-Uni par le fait qu'elle est obligatoire, que l'entreprise est fortement sanctionnée en cas de manquements et qu'elle ne porte que sur l'aspect financier. Bien que le Turnbull Guidance soit conforme aux exigences américaines, le *COSO* est mentionné par l'autorité des marchés américains, comme étant le modèle à privilégier (Gumb & Noël, 2006).

La directive européenne 2006/46/EC permet d'affirmer que l'Union Européenne se dirige vers un système de *comply or explain*, tel qu'établi par la Grande-Bretagne. Les entreprises ont le choix de se soumettre aux normes de leurs états membres, soit de dévier de ces mêmes normes tout en expliquant pourquoi elles ne s'y soumettent pas (Van de Poel & Vanstraelen, 2011).

Pourquoi les législateurs, qu'ils soient américains, anglais ou européens, ont voulu renforcer les exigences imposées aux entreprises en ce qui concerne le contrôle interne au début des années 2000 ?

Selon Gumb et Noël (2007), ceci responsabiliserait des dirigeants d'entreprise, en les poussant à justifier les différents processus de contrôle interne mis en place. L'obligation de publication permettrait aussi la « formalisation et la systématisation du contrôle interne » et améliorerait la transparence des informations vis-à-vis des parties prenantes. Cette normalisation ne serait qu'une suite logique dans l'évolution du contrôle interne. Toutefois, les rectifications opérées ne sont que des réactions aux conséquences des faiblesses managériales au sein des entreprises. Peu de mesures proactives ont été réalisées afin de traiter les problèmes des rapports d'entreprises résultants de contrôle inadéquats (Dugan, Heier & Sayers, 2005).

2. L'audit interne

2.1 Définitions

Dans le passé, l'audit interne consistait en une vérification de l'ensemble des transactions financières effectué par une entreprise. Une batterie de tests était réalisée dans le but d'isoler les erreurs et les irrégularités, ce qui nécessitait la mise en place de programmes conséquents et difficiles à réaliser. Aujourd'hui, l'audit interne s'intègre dans la stratégie de risque de l'entreprise, en facilitant le développement de contrôles adaptés et en fournissant l'assurance que ceux-ci soient pertinents. Les fonctions des auditeurs internes se sont donc étendues à la gestion des risques, aux contrôles et au processus de gouvernance (Arena et al 2009).

Cette évolution de l'audit interne ne s'est pas faite en une fois, selon Renard (2013), celle-ci peut être perçue comme une stratification, chaque période ajoutant de nouveaux objectifs et de nouvelles complexités aux périodes antérieures. L'audit interne peut se décliner en quatre catégories opérationnelles correspondant aux fonctions de l'entreprise.

Premièrement, l'audit de conformité ayant pour rôle la vérification de la bonne application des règles, des normes par l'entreprise. Deuxièmement, l'audit d'efficacité, qui englobe les notions d'efficacité et d'efficience. L'auditeur émet des opinions, de recommandations, non plus seulement sur l'application des règles, mais aussi sur leur qualité. Troisièmement, l'audit de management, permettant d'attirer l'attention sur les risques ou les incohérences provenant des choix ou décisions effectuées par l'entité. L'auditeur ne remet pas en question la stratégie ou la politique adoptée par la direction, mais émet des avis sur les risques qui en découlent. Enfin, l'audit de stratégie, pouvant être défini comme étant « confrontation de l'ensemble des politiques et stratégies de l'entreprise avec le milieu dans lequel elles se situent pour en vérifier la cohérence globale » (Renard, 2013, p.41). Cet audit exige des compétences sérieuses et de haut niveau.

Pour conclure, nous reprendrons la définition à ce jour la plus utilisée et la plus complète, donnée par l'Institut de l'Audit Interne, « une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée. Il aide cette organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle, et de gouvernance,

et en faisant des propositions pour renforcer leur efficacité. » (de Zwaan, Stewart & Subramaniam, 2011, p.3).

Le rôle d'un auditeur interne consiste donc à assister les managers et leurs équipes, tout en établissant des rapports à un comité d'audit indépendant.

2.2 Valeur ajoutée

De cette évolution, un point important à noter est que l'audit interne constitue à ce jour une valeur ajoutée à l'entreprise. Pour atteindre ce but, plusieurs caractéristiques sont mises en avant.

Premièrement, les auditeurs internes peuvent conscientiser les managers aux responsabilités qui leur incombent, concernant notamment les risques et les contrôles. Les auditeurs internes peuvent aussi jouer le rôle de consultant, en surveillant les risques, en identifiant les faiblesses dans les systèmes de contrôle et en facilitant l'implémentation des ERM. Enfin, les auditeurs internes peuvent aider le comité d'audit et les auditeurs externes dans leurs tâches, précisément lorsque le comité d'audit est en charge de la surveillance du système de contrôle interne. (Arena & al., 2009).

2.3 Indépendance et objectivité

Une caractéristique fondamentale de l'auditeur interne est qu'il doit exécuter sa fonction en toute indépendance et objectivité. L'auditeur interne ne peut subir aucune influence pouvant altérer l'atteinte des objectifs qui lui sont infligés. L'Institut des Auditeurs Internes a d'ailleurs établit une norme en ce qui concerne l'indépendance, à savoir « le responsable de l'audit interne doit relever d'un niveau hiérarchique suffisant au sein de l'organisation pour permettre au service d'audit interne d'exercer ses responsabilités » (Renard, 2013, p.22). La notion d'objectivité ne peut dès lors pas être détachée de cette notion d'indépendance.

Selon l'IIA, certains critères doivent être remplis afin de favoriser ce degré élevé d'indépendance. Premièrement, les entreprises doivent « appliquer les normes internationales généralement admises pour la pratique de l'audit interne » (IIA, 2013, pg.5). Deuxièmement, les auditeurs internes doivent être « rattachés à un niveau suffisamment élevé dans l'organisation pour pouvoir assurer leurs responsabilités de manière indépendante » (IIA, 2013, pg.5). Enfin, les auditeurs internes doivent « avoir une

relation étroite et effective avec le Conseil ou l'organe de gouvernance équivalent » (IIA, 2013, pg.5).

2.4 Le comité d'audit

Le comité d'audit n'a pas la faculté de décider au sein d'une organisation, mais constitue toutefois un élément clé de la gouvernance d'entreprise.

Son rôle premier est d'effectuer des recommandations pour le Conseil d'Administration, il agit donc en tant que consultant (Spira & Page, 2003). Le comité d'audit supervise et surveille les processus de reporting financier conduits par le management de l'entité. Il existe une collaboration directe entre le management et le comité d'audit, dans le but d'assurer une administration propre des activités de l'organisation. Il travaille donc directement avec les directeurs financiers, comptables, et communique ses objectifs et ses attentes en ce qui concerne le management de l'organisation

De plus, le comité d'audit supervise les fonctions d'audit interne et en renforce les relations entre les managers de l'entreprise et les auditeurs internes. Il peut exiger de ces derniers la vérification des décisions, processus et procédures réalisés par le management de l'entreprise (Renard, 2013).

Le comité d'audit évalue le plan de travail annuel des auditeurs internes et le compare avec ses attentes et ses besoins. Il assure entre autres que les auditeurs internes planifient et utilisent les ressources à bon escient. Les auditeurs internes doivent dès lors avoir un accès direct au comité d'audit, et doivent pouvoir établir des relations privilégiées avec celui-ci (Renard, 2013).

3. Le modèle des trois lignes de défense

3.1 Mise en contexte

La première référence au concept des trois lignes de défense, dans le secteur financier, est évoquée dans la thèse de Roman Kräussl (2003), parlant des trois lignes de défense comme étant un moyen de contrer le risque systématique dans les marchés des institutions financières. La même année, le Financial Security Advisory, l'organisme britannique de régulation financière, évoquait ce concept dans un rapport sur la gestion des risques au sein des entités britanniques, et le degré d'utilisation par ces dernières de ce modèle. Il n'est néanmoins pas clair si c'est le régulateur qui ait requis les entreprises d'adopter ce modèle, ou si ce sont les entreprises qui l'ont adopté de manière autonome (Zhivitskaya, 2015).

Toutefois, ce n'est qu'après la crise économique de 2008 que le modèle a commencé à prendre de l'importance.

En effet, la conjoncture économique et les événements significatifs de la fin de la décennie précédente ont incité les régulateurs à renforcer leurs revendications dans le but d'une plus grande transparence et d'une diminution des risques de la part des entreprises. Nombre d'entre elles ont bien augmenté les investissements dans les différents secteurs concernés, à savoir l'identification des risques, les contrôles internes, les assurances ou encore l'implémentation de systèmes ERP. Toutefois, les résultats n'ont pas été à la hauteur de leur espérance, de nombreuses failles dans les contrôles subsistaient, et des évènements imprévus faisaient toujours apparition. En cause, une mauvaise définition et compréhension du profil de risque de l'entreprise, une non-coordination entre les fonctions d'assurance et les types de risques, mais aussi un manque de clarification des responsabilités au sein de la société (Ernst & Young, 2013).

En 2013, l'Institut des Auditeurs Internes (IIA) publiait « *Les trois lignes de maitrise pour une gestion des risques et un contrôle efficaces* », une prise de position listant un ensemble non-exhaustif des risques potentiels dans l'entreprise d'aujourd'hui. Cette prise de position n'a toutefois pas force de loi, la conformité n'y est pas obligatoire, mais y est fortement recommandée (Seago, 2015). Selon l'IIA (2013, p. 10), « ce type de document n'a pas pour but de fournir des réponses définitives à des circonstances particulières et, en tant que tel, n'est destiné qu'à être utilisé comme guide ».

Bien que l'IIA ait été pionnière dans la prise de position, le terme « *trois lignes de défense* » a été utilisé par de nombreux auditeurs des années auparavant. En effet, le document « Guidance on the 8th EU Company Law Directive – article 41", publié par FERMA (Federation of European Risk Management Association) & ECIIA (European Confederation of Institutes of Internal Auditing) en 2010, présentait déjà le modèle graphique (Klotz, 2015). Ceux-ci se basaient sur la section 2b de l'article 41 de cette directive, à savoir : " […] the audit committee shall, inter alia : monitor the effectiveness of the company's internal control, internal audit where applicable, and risk management systems […]." (ECIIA & FERMA, 2011, p. 2) pour y développer des lignes directrices.

Le modèle des 3LoD apparaît donc comme une conséquence de la crise financière de 2008, bien qu'il ne soit pas obligatoire pour les entreprises, il permet de s'ajuster aux différentes normes rentrées en vigueur.

Aujourd'hui, ce modèle est utilisé par un grand nombre d'entreprises. Selon l'étude réalisée en 2015 par « The Global Internal Audit Common Body of Knowledge » (CBOK), la fondation de recherche de l'Institut des Auditeurs Internes, 55% des entreprises cotées en bourse, 43% du secteur public, 41% des organisations sans but lucratif, et 40% des compagnies privées disent faire utilisation de ce modèle. Si nous regardons par secteurs d'activités, on remarque que cela est plus frappant pour les entreprises financières, en effet 78% disent utiliser l'audit interne comme troisième ligne de défense (Seago, 2015).

3.2 Définitions

Le modèle des 3LoD permet à l'organisation de se structurer elle-même, et est utilisé traditionnellement pour modéliser l'interaction entre la gouvernance d'entreprise et les systèmes de contrôles internes (Arndorfer & Minto, 2015). Il coordonne les différents acteurs et leurs activités, en optimisant la collaboration des acteurs dans la procédure de gestion des risques et de contrôle, et en assignant des responsabilités et des rôles précis aux différents acteurs de l'entité, contrairement aux référentiels ERM.

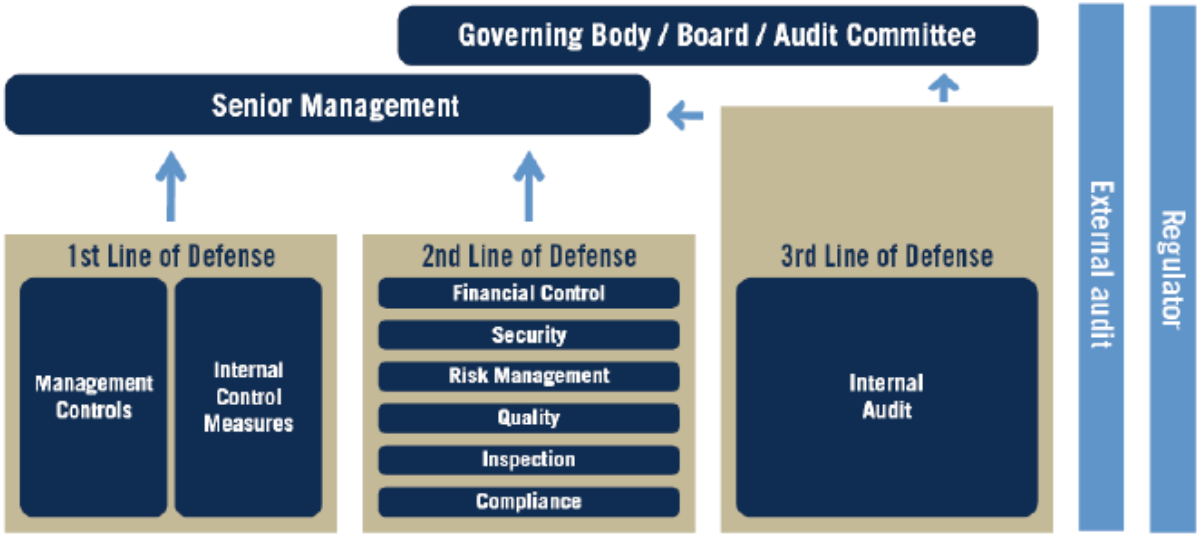
Cet outil d'aide à la décision fournit un moyen simple et efficace pour améliorer la communication en matière de gestion des risques, permet une utilisation efficace des ressources limitées affectées à ce domaine (IIA, 2013), ceci dans le but d'éviter une duplication des efforts et d'assurer une homogénéité dans les contrôles (Leech & Halon, 2016).

Le modèle intervient notamment pour clarifier la différence et la relation entre les activités de monitoring (contrôle interne / gestion risques) et l'assurance indépendante de l'organisation (audit interne) (Anderson & Eubanks, 2015).

Ce concept s'applique à tous types d'organisations, il s'intègre de manière différente en fonction de la taille de l'entreprise ou de la culture de l'entreprise (ECIIA & FERMA, 2011). Bien que la structure du modèle soit définie de manière spécifique, celui-ci n'est pas inflexible. Même dans les organisations ne possédant pas de référentiels de gestion des risques, celui-ci peut contribuer à l'efficacité des systèmes de gestion des risques (IIA, 2013).

Le modèle des 3LoD s'articule, comme son nom l'indique, sur trois axes distincts, le contrôle interne, la gestion des risques et l'audit interne. Ceux-ci sont dirigés par le senior management, le comité de direction et le comité d'audit. Une quatrième ligne de défense intervient dans certains cas, à savoir l'audit externe.

Ces lignes sont expliquées plus en détail ci-après.



Graphe n°1 : Le modèle des 3LoD (IIA, 2013).

3.2.1 Première ligne de défense

La première ligne de défense, à savoir le management opérationnel et/ou le contrôle interne, se concentre sur la gestion quotidienne des activités de l'entreprise, englobant l'ensemble des unités de l'entité générant des revenus (Arndorfer & Minto, 2015). Les managers opérationnels en sont les acteurs principaux, leur tâche première consiste en l'identification, l'évaluation et la gestion des risques journaliers, selon les procédures, les standards, et les processus définis (Klotz, 2015). Ils pilotent l'élaboration et la mise en œuvre des règles et des procédures internes, supervisent la conception des contrôles et leur intégration dans les systèmes et les processus, et s'assurent que les activités soient compatibles avec les objectifs fixés.

Dépendant des activités de l'entreprise, les contrôles peuvent se tourner sur la production des biens physiques, la provision des services financiers tels que le trading, les ventes, la gestion d'actifs et les relations clients (Arndorfer & Minto, 2015). En fonction de leur analyse, ils devront suggérer/communiquer des processus de contrôle adéquats aux différentes parties prenantes, plus particulièrement aux fonctions managériales de la deuxième ligne de défense.

3.2.2 Deuxième ligne de défense

La deuxième ligne de défense rassemble, elle, l'ensemble des fonctions de gestion de l'entreprise, plus précisément, l'ensemble des acteurs ayant un rôle de management au sein de l'entreprise.

L'IIA (2013), définit trois types de fonctions au sein de la deuxième ligne. Tout d'abord, les fonctions de gestion des risques, ayant pour buts de faciliter et surveiller la mise en œuvre des dispositifs efficaces de gestion des risques, tels que l'élaboration et l'implémentation de référentiels de gestion des risques, de définir l'appétence pour le risque de l'entité et de communiquer les informations adéquates.

Ensuite, les fonctions de conformité, ayant pour buts de surveiller divers risques spécifiques tels que le non-respect des lois et des réglementations en vigueur. Celles-ci sont directement rattachées à la direction générale, voir au conseil d'administration (IIA, 2013).

Enfin les fonctions de gestion, devant essentiellement effectuer le suivi des risques financiers et des divers reporting financiers (IIA, 2013).

De manière générale, la deuxième ligne de défense contribue à la mise au point et à la surveillance des contrôles relevant de la première ligne, de conseiller la direction opérationnelle, et si nécessaire de prendre des mesures correctives (Sébéloué & Zanvit, 2015). Dans le cas où la première ligne devient ineffective, le rôle de la deuxième prend alors plus d'ampleur et devient plus importante.

L'ensemble de ces fonctions dépendent fortement de la taille de l'entreprise. En effet, au plus l'entreprise sera de petite taille, au plus les fonctions auront tendance à être combinées voire supprimées (IIA, 2013).

3.2.3 Troisième ligne de défense

La troisième ligne de défense concerne l'audit interne. Celle-ci a pour rôle de réviser les contrôles et les procédures de gestion des risques, d'identifier les problèmes, et de garder les organes de gouvernances informés. Le comité d'audit leur fournit une vision globale de la gestion de l'organisation, une assurance pertinente sur l'efficacité de la gouvernance, de la gestion des risques et du contrôle interne, y compris sur l'atteinte des objectifs des deux premières lignes de défense (IIA, 2013).

Il n'est pas rare que le comité de direction fasse appel aux auditeurs internes lorsqu'une nouvelle loi ou norme est mise en application par le régulateur. Pour exemple, lors de l'implémentation de la loi Sarbanes-Oxley aux Etats-Unis en 2002, les managers opérationnels ainsi que les fonctions managerielles dans leur ensemble ne possédaient pas les compétences nécessaires pour redéfinir les contours des processus de contrôles internes ou de gestion des risques de l'entreprise. Il était dès lors demander aux auditeurs internes d'appliquer les mesures nécessaires au renouvellement du dispositif interne (IIA, 2013).

Il est conseillé au comité d'audit d'effectuer au minimum une évaluation annuelle du niveau de risque de l'entreprise (Arndorfer & Minto, 2015).

3.2.4 Quatrième ligne de défense

Le modèle peut s'étendre à une quatrième ligne de défense, reprenant les auditeurs externes et/ou les régulateurs.

Ceux-ci établissent des exigences dans le but de renforcer la gouvernance et le contrôle, mais peuvent aussi fournir des évaluations et des observations sur les rapports financiers ou autres. À la différence des trois axes principaux, celui-ci agit dans un cadre plus étroit

et possède des objectifs différents et plus ciblés que les lignes de défense internes (Anderson & Eubanks, 2015).

Toutefois, dans le cadre de ce mémoire, l'audit externe ne sera pas pris en considération comme étant une quatrième ligne de défense.

3.3 Coordination et interaction entre les lignes de défense

3.3.1 Définitions

La structure du modèle des 3LoD se doit d'être flexible, et adapté au modèle de gouvernance d'entreprise. Quelle que soit la taille ou la complexité d'une organisation, chacune des trois lignes de défense doit demeurer sous une forme ou une autre (IIA, 2013). Les rôles et les responsabilités doivent être séparés à travers les lignes de défense, et articulées autour des politiques et des procédures de l'entreprise (Anderson & Eubanks, 2015).

Bien que les lignes soient distinctes, possédant des fonctions précises, elles conservent un but commun, celui d'atteindre les objectifs fixés par l'entreprise en termes de gestion des risques. En effet, l'ensemble des acteurs sert les mêmes parties prenantes, à savoir la Direction Générale et le Conseil d'Administration, et dès lors se concentrent sur les mêmes notions de risques et de contrôles (Anderson & Eubanks, 2015).

Les organes de gouvernance doivent transmettre leur attente en ce qui concerne la coordination des activités et le partage des informations, dans le but d'éviter une duplication des efforts de la part des lignes de défense. Pour exemple, il est essentiel que les deux premières lignes travaillent main dans la main, en créant une terminologie commune, un ensemble d'outils et de processus possibles, mais aussi en comprenant comme les risques sont évalués par leur confrère. La troisième ligne de défense, elle, doit intensifier les communications avec les deux premières, afin de s'imprégner de la terminologie utilisée et de comprendre l'évaluation des risques réalisée (Seago, 2015).

Les fonctions de gestion des risques, de conformité et d'audit interne doivent former un ensemble cohérent de fonctions de contrôle transversales. Ces fonctions de contrôle étant semblables, elles doivent veiller à un échange approprié d'informations pertinentes (BNB, 2018).

Cette coordination permet donc de favoriser l'efficacité et l'efficience du modèle, même s'il ne faut pas perdre de vue que chacune des lignes se doit de garder un minimum d'indépendance.

3.3.2 Modèles d'interaction

L'étude de Paul Sweeting (as cited in Zhivitskaya, 2015) démontre trois différents types d'interaction de gestion des risques à travers le modèle des 3LoD, dans le but d'expliquer les pratiques d'implémentations du modèle.

« Offense vs defense » modèle

Premièrement, Paul Sweeting énonce le modèle « offense vs defense » (as cited in Zhivitskaya, 2015), expliquant que les deux premières lignes de défense sont en constante opposition. Dans ce cas-ci la première ligne représente purement le générateur de revenus de l'entreprise, ayant pour but de maximiser les profits alors que la seconde ligne a pour objectif principal de minimiser les risques de l'entreprise. De par ce modèle, il existerait donc un conflit entre les deux premières lignes, puisque la première ligne ne serait absolument pas incitée à prendre en compte les risques de l'entreprise, alors que la deuxième ligne serait une incitation à étouffer toute prise de risque, ce qui est contraire à la nature de toute entreprise (Zhivitskaya, 2015).

« Policy and policing » modèle

Deuxièmement, Paul Sweeting énonce le modèle « policy and policing » (as cited in Zhivitskaya, 2015), expliquant que la deuxième ligne de défense doit à la fois émettre des politiques et des procédures, pour ensuite vérifier les résultats à ceux qui ont appliqués ces politiques et procédures. La deuxième ligne de défense est alors vue comme une véritable ligne de supervision, car elle surveille si la première ligne est en accord avec les cadres et les exigences émises, plutôt que d'avoir une réelle confrontation avec celle-ci (Zhivitskaya, 2015).

« Partnership » modèle

Troisièmement, le « partnership » modèle de Paul Sweeting, impliquant que les deux premières lignes de défense « travaillent ensemble pour maximiser les rendements sous réserve d'un niveau de risque acceptable. Cela peut être notamment obtenu en incluant la responsabilité de la gestion des risques au sein même de la première ligne de défense, et en assurant un dialogue constant » (as cited in Zhivitskaya, 2015). La gestion des risques est donc initiée au sein même des fonctions opérationnelles, mais cela pose un problème

quant à un challenge réellement efficace entre les lignes de défense. Il est difficile de démontrer que la première ligne de défense soit réellement impliquée dans la gestion des risques, s'il n'existe pas de séparations de fonctions (Zhivitskaya, 2015).

3.4 Rôles et responsabilités

Dans le point précédent, les rôles et les responsabilités des diverses lignes de défense ont été établies, sans toutefois expliciter les fonctions exécutées par les organes de gouvernance, à savoir le Conseil d'Administration et la Direction Générale. Bien que ces derniers se distinguent des trois lignes de défense, la considération des responsabilités de ces organes est primordiale. Ce sont, en effet, les principales parties prenantes auxquelles chacune des trois lignes apportent un soutien.

Le rôle du CA, dans ce cas-ci, établit d'une part les objectifs de l'organisation, et d'autre part les stratégies à adopter pour atteindre ces objectifs. Il doit dès lors encourager la mise en place d'un dispositif robuste de gestion des risques, (AMRAE & IFACI, 2013) en approuvant et en révisant l'appétence et la tolérance pour le risque (Bank for International Settlement [BIS], 2011). Le CA, aussi surnommé le conseil de surveillance, a pour mission de vérifier périodiquement si les fonctions de contrôles au sein des lignes de défense, opèrent correctement. Mais aussi de superviser la Direction Générale pour assurer que les politiques et les procédures sont implémentés à tous niveaux de décisions (BIS, 2011). Afin d'exercer au mieux cette mission, les fonctions de la deuxième ligne peuvent établir un lien direct avec le CA, sans passer par la Direction Générale.

La Direction Générale, ou Senior Management, en anglais, est au cœur du dispositif de maitrise globale de la gestion des risques. Elle met en œuvre les stratégies établies par le Conseil d'Administration à travers des politiques et procédures qui définissent le processus de gestion des risques, et s'en sert comme outil d'aide à la décision (AMRAE & IFACI, 2013). Dans les faits, cette organe de gouvernance supervise les deux premières lignes de défense, tandis que le CA chapeaute les trois lignes de défense.

Il faut néanmoins rappeler que le comité d'audit sert à proprement parler le CA, et n'est pas considéré directement comme un organe de gouvernance.

Ces organes de gouvernance sont les mieux placés pour faire en sorte que le modèle des trois lignes de maîtrise soit pris en compte dans les processus de gestion des risques et de contrôle de l'organisation. Le modèle en sera d'autant plus efficace, tant que les

organes de gouvernance établiront les lignes directrices pour son implémentation. (Mouzas, 2006).

3.5 Critiques du modèle

Concernant la première ligne de défense, le modèle ne met que trop peu l'accent sur cette ligne, or celle-ci semble la plus importante pour une gestion des risques robuste de l'entité (Davies & Zhivitskaya, 2018). Les fonctions opérantes possèdent par ailleurs une responsabilité double et contradictoire. En effet, les managers opérationnels doivent générer des revenus pour leurs entités, mais aussi rester compétent en matière de gestion des risques et de contrôle. Il est dès lors pertinent de se poser la question de l'articulation de cette première ligne de défense autour de ces deux objectifs.

Concernant la deuxième ligne de défense, celle-ci se doit d'être indépendante par rapport à la première. Néanmoins, cela peut paraître paradoxal lorsqu'on sait qu'il existe une étroite collaboration entre ces deux lignes. Les fonctions de gestion peuvent par exemple, développer, implémenter et/ou modifier les contrôles et les processus de risque de l'entité, et peuvent aussi jouer un rôle dans la décision de certaines activités opérationnelles. Dès lors, la notion d'indépendance peut être partiellement remise en question (Anderson & Eubanks, 2015).

Dans le cas où les fonctions de la deuxième ligne sont indépendantes, ces dernières peuvent toutefois manquer de compétences et d'expertises pour contredire efficacement les pratiques et les contrôles effectués par la première ligne. Dans les institutions financières par exemple, il est parfois difficile de valider des modèles complexes ou de fournir des évaluations pertinentes sur l'utilisation de modèles financiers. Toujours dans le secteur bancaire, les rémunérations octroyées posent questions. En effet, celles-ci sont généralement plus élevées au sein de la première ligne que ceux de la deuxième, ceci pouvant donc freiner l'envie d'exercer des fonctions généralement plus qualifiées et plus expérimentées au sein de la deuxième ligne de défense (BIS, 2015).

Concernant le modèle dans son ensemble, la définition donnée par l'IIA restreint la gestion des risques au concept de « surveillance » et de « supervision » de la part du comité de direction, ce qui résonne comme une politique traditionnelle de gestion des risques en silos au sein de l'entité. Ceci est contraire à la vision holistique proposée aujourd'hui par les ERM (Leech & Halon, 2016). La gestion des risques n'est pas non plus une question de défense, mais plutôt d'offense. De la notion de défense découle que la notion de risque est

mauvaise pour l'entité, or, ça ne l'est pas. Le risque peut être positif ou négatif, et il existe généralement une opportunité de changer le potentiel négatif en potentiel positif (Leech & Halon, 2016).

De plus, le modèle offre une approche extrêmement bureaucratique, coûteuse, et démotivante. Pour qu'un business soit parfaitement contrôlé, il faudrait des contrôles à chaque poste de l'entité, mais cela aurait un coût et ne serait pas très agréable à vivre au sein de l'entité. Cela pourrait endommager l'efficacité du business dans son ensemble (Davies & Zhivitskaya, 2018).

Une autre question concerne les parties prenantes définies par le modèle, le comité de direction et le senior management. Selon Lyons (2015), ceux-ci devraient être directement inclus comme ligne de défense, et non juste comme parties prenantes servant le modèle.

Enfin, le modèle ne précise pas les modalités d'attribution et de coordination des tâches nécessaires à la mise en œuvre de la gestion des risques. Les détracteurs du modèle le voient comme un concept ancien, n'offrant que peu en terme d'expérience humaine pratique en organisations complexes et n'est qu'une simplification absurde de la réalité.

4. Effectiveness

4.1 Définition de l'effectiveness

Le concept d'effectiveness est souvent traduit en français par le terme efficacité, pour autant ces deux notions possèdent des définitions de loin opposées.

L'effectiveness représente le « doing the things right », dont le critère est de faire le mieux possible, ce qui exige la meilleure des qualités quant aux connaissances (le savoir), aux techniques (le savoir-faire), aux comportements (le savoir-être) et à la communication (le faire savoir). L'efficience, stricto sensu, est donc très largement imprégnée par la culture » (Renard, 2013, p.38).

L'efficacité est plutôt définie « comme la capacité de faire quelque chose ou de produire quelque chose sans gaspiller du matériel, du temps ou de l'énergie » (Wilson, Wnuk, Silvander & Gorschek, 2018, p.276). Selon Frokjaer et al., l'efficacité se définit comme étant « la relation entre l'exactitude et l'exhaustivité avec laquelle les utilisateurs atteignent leurs goals et les ressources dépensées pour les atteindre » (Wilson & al., 2018, p.277). Les mesures d'efficacité sont souvent reliées, directement et indirectement, au temps et au coût.

Il est intéressant de noter que ces deux concepts sont étroitement liés au concept de gouvernance d'entreprise.

4.2 Effectiveness du modèle des trois lignes de défense

Dans le cadre de ce mémoire, le concept d'effectiveness sera largement utilisé puisqu'il en constitue la base des questions de recherche. Toutefois, les mesures de l'effectiveness sont loin d'être universelles, chaque activité possédant ses propres mesures. La littérature académique offre de nombreuses approches quant à l'effectiveness du contrôle interne, de la gestion des risques ou encore de l'audit interne. Prises isolément, ces mesures ne permettent pas d'établir l'effectiveness du modèle de manière globale.

La question est donc de savoir comment évaluer l'effectiveness du modèle des 3LoD. Théoriquement, l'effectiveness serait « réalisée » si le modèle accomplit ses objectifs prédéfinis, à savoir fournir l'assurance que les processus de gestion des risques et de contrôles fonctionnent de manière adéquate au sein de l'entité.

Puisque le concept d'effectiveness n'est pas fondamentalement relié aux notions de temps ou de coûts, et qu'il n'est à priori pas observable (Power, 1997), il est dès lors vital de déterminer des critères, des facteurs pouvant influencer cet effectiveness.

H. Davies & M. Zhivitskaya (2018), établissent des pratiques permettant d'améliorer l'effectiveness du modèle, de contrer les critiques établies à son encontre. Dans ce cas-ci, ce sont donc un ensemble de facteurs influençant positivement l'effectiveness du modèle des 3LoD.

- Définir clairement l'appétence pour le risque au sein de l'entité, améliorant ainsi le pouvoir de décision des manageurs opérationnels.
- Clarifier quels risques sont couverts par le modèle. Si certains ne sont pas couverts, alors en expliquer et documenter les raisons, et mettre en œuvre une structure alternative.
- Clarifier les limites entre les lignes de défense, que chaque employé puisse respecter son périmètre de travail.
- Equilibrer l'importance des fonctions entre les deux premières lignes de défense, notamment en ce qui concerne les rémunérations.
- Assurer que les fonctions de gestion des risques disposent de ressources suffisantes, et que les membres de la deuxième ligne puissent avoir un accès approprié aux décisions.

A ce jour, il n'existe pas d'autres études établissant l'effectiveness du modèle des 3LoD.

5. Hypothèses

La problématique du mémoire est donc la suivante, *l'effectiveness du modèle des 3LoD.* De par les recherches effectuées ci-avant, il est dorénavant possible de poser deux sous-questions, permettant de préciser l'objet de l'étude.

1. Qu'est-ce qu'un modèle des 3LoD efficace ?

La revue de littérature ne nous permet pas de poser une définition claire et précise de ce qu'est un modèle des 3LoD efficace.

2. Quels sont les facteurs pouvant influencer l'effectiveness du modèle des 3LoD ?

Cette même revue de littérature permet de poser les problématiques suivantes.

- Est-ce que l'interaction entre les lignes de défense influence l'effectiveness du modèle des 3LoD ?
- Une appétence au risque clairement définie par les organes de gouvernance influence-t-elle positivement le modèle des 3LoD ?
- La culture de l'entreprise influence-t-elle l'effectiveness du modèle des 3LoD ?

PARTIE 2 : ANALYSE EMPIRIQUE

1. Méthodologie

Dans le cadre de ce mémoire, la méthode de recherche utilisée consiste en la méthode qualitative. Cette forme de recherche permet de collecter et d'interpréter les données, faisant du chercheur partie intégrante du processus de recherche, tout comme les participants et les données collectées. Les recherches qualitatives sont conçues généralement de manière ouvertes et flexibles, ce qui se heurte à la notion de rigueur tellement importante dans la recherche quantitative. (Corbin & Strauss, 2015).

Il est intéressant de se demander pourquoi la méthode qualitative est préférée à la méthode quantitative dans le cadre de ce mémoire.

Selon Corbin & Strauss (2015), plusieurs raisons peuvent être mises en avant. Cela permet d'explorer les expériences vécues par les participants, d'explorer comment se forment et se transforment les significations, d'explorer des domaines qui n'ont pas encore été soumis aux recherches scientifiques, de découvrir des variables pertinentes qui pourraient être testées dans une étude quantitative, mais aussi d'appréhender l'étude de manière holistique et complète.

De plus, les recherches qualitatives sont considérées comme étant plus fluides, plus dynamiques, ce qui s'oppose à la conception plus structurée de l'approche quantitative. Celles-ci offrent aussi l'opportunité de se connecter avec les participants, et d'aborder le sujet en fonction de leurs points de vue. (Corbin & Strauss, 2015).

Il existe toutefois plusieurs méthodes de recherche qualitative, nous utiliserons dans ce cas-ci, la méthode dite « par théorisation ancrée » (Grounded Theory Method). Cette méthode est unique puisqu'elle permet de produire les concepts, les analyses, sur des données collectées durant le processus de recherche, et non avant le début de la recherche. La recherche analytique et les collections de données sont reliées, et forment un cycle continu à travers le processus de recherche. (Corbin & Strauss, 2015).

2. Méthode de collecte de données et choix de l'échantillon

La méthode de collectes des données s'est effectuée via des entretiens semi-directifs. Cette méthode consiste donc en une interview individuelle avec le participant de la recherche, celle-ci paraissant être la plus efficace dans le cadre de ce mémoire.

L'entretien semi-directif est constitué d'une multitude de thèmes, préalablement établis, mais n'est pas structuré de manière ordonnée. Pour ce, un guide d'entretien a été réalisé au préalable, rassemblant les différentes questions, ou plus largement thématiques abordées au cours de l'interview (voir annexe 10.). L'interviewer peut donc adapter son dialogue en fonction du déroulement de l'interview, tout en gardant à l'esprit les différents thèmes à aborder, ce qui permet un entretien plus confortable et souple. Le chercheur peut aussi ajouter des questions lorsque cela lui semble nécessaire, tel que pour clarifier certains points ou approfondir un sujet. Le participant est aussi libre d'ajouter des éléments qui lui semblent pertinents, une fois l'ensemble des thèmes abordé. (Corbin & Strauss, 2015). L'entretien ne constitue donc pas un interrogatoire privant la liberté d'expression de l'intervenant, ni le développement de ses arguments. (Imbert, 2010).

Ce type d'entretien permet aussi de recueillir des informations de bonne qualité, orienté vers le but poursuivi, et ce dans un laps de temps raisonnable. Généralement, le contenu de l'information est plus dense, et riche, que celui d'un simple questionnaire en ligne. (Imbert, 2010).

Les entretiens réalisés lors de ce mémoire ont donc eu pour objectifs, d'analyser dans un premier temps en quoi un modèle des 3LoD est efficace, lorsque celui-ci est implémenté d'une manière ou d'une autre dans différents types d'entreprises. Certains facteurs pouvant influencer l'effectiveness du modèle ont été préalablement établis, sur bases des différentes recherches littéraires. C'est pourquoi, dans un deuxième temps, il était important d'analyser si ces facteurs pouvaient effectivement influencer, ou non, le modèle des 3LoD. De plus, les questions permettaient à l'interlocuteur de mettre en avant de possibles autres facteurs, non établis préalablement, pouvant influencer cette effectiveness.

L'échantillon utilisé pour les entretiens réalisés, est à la fois varié et complet. En effet, de par premièrement les différents composants qu'abordent mon sujet d'étude, il était important de prendre en considération l'ensemble des acteurs ayant de près ou de loin un rôle dans la gestion des risques de l'entreprise. C'est pourquoi, l'échantillon prend en compte des fonctions opérationnelles, des fonctions de gestion, des fonctions d'audit interne et des fonctions de gouvernance. L'expérience professionnelle n'a pas été un élément restrictif quant au choix des participants.

De plus, différents types d'entreprises ont été consultées, tels que celles du secteur bancaire/assurance, du secteur industriel, du secteur public ou du secteur privé. Ceci dans le but de pouvoir réaliser une étude sur un ensemble d'entreprises, de comprendre le modèle dans sa globalité, et non dans un secteur spécifique, tel que la banque, domaine privilégié pour l'implémentation des trois lignes de défense.

Cette diversité a permis de couvrir un large éventail de pratiques, de mises en place du modèle des 3LoD.

Les différents interviewés sont détaillés ci-après, ils sont au nombre de dix. Ceux-ci ont été trouvés de par le réseau social Linkedin, mais aussi via des relations, des connaissances.

Dans le cas des relations, la méthode de contact utilisée était directe, principalement via le contact téléphonique. La réponse était donc majoritairement positive. Toutefois dans le cas de Linkedin, il n'était pas possible d'obtenir leurs adresses mails ou leurs coordonnées téléphoniques directement, c'est pourquoi il a été plus difficile d'obtenir des réponses positives. Le taux approximatif de réponses positives s'élève en effet à plus ou moins dix pour cents. Toutefois, le délai assez court imposé aux interlocuteurs a aussi pu jouer en défaveur.

Au final, l'échantillon se compose à moitié de personnes contactées via mes connaissances, et à moitié de personnes contactées via le réseau social.

3. Collecte des données

La plupart des participants à l'étude étaient ravis de pouvoir répondre à mes différentes questions, de m'aider à la réalisation de mon mémoire, et en quelque sorte, de faire partie intégrante au processus de recherche. Ils ont tous accepté que l'interview soit enregistrée, me permettant ainsi de garantir une analyse de leurs propos, fidèle et robuste.

L'interview commençait par la présentation du sujet d'étude, à savoir l'explication du modèle des 3LoD, pour ensuite expliquer le terme 'effectiveness', et tenter de leur faire comprendre la direction de ma recherche. Il est toutefois important de noter, que la plupart des intervenants connaissaient ce modèle en long et en large, ce qui facilita la mise en route de l'interview. Dans un deuxième temps, il leur était demandé de se présenter eux-mêmes, d'expliquer quel était leur profession actuelle, leur expérience professionnelle, ou encore leur entreprise. Cette introduction permit principalement de jeter les bases d'une interview sereine et confiante.

Une fois les présentations effectuées, l'interview, comme dit précédemment, se déroule sur base d'un guide d'entretien réalisé au préalable. Ce dernier se compose d'un ensemble de thèmes à aborder, présentés sous la forme de questions ouvertes. Ces dernières sont accompagnées de questions plus précises, dans le but soit de clarifier certains propos, soit de permettre le développement de certains arguments de l'intervenant. L'objectif étant, évidemment, de créer un dialogue limpide avec le participant, lorsque ce dernier abordait un thème préalablement établi, il était nécessaire de rebondir sur celui-ci et d'interagir de manière fluide. Dès lors, il arrivait souvent que la structure mise en place dans le guide d'entretien ne soit pas suivi à la lettre.

Le guide d'entretien se divise principalement en trois parties.

Premièrement, des questions sur la mise en place du modèle des 3LoD au sein de l'entreprise, et sur l'effectiveness du modèle en tant que tel.

Deuxièmement, sur les problématiques établies ci-avant, et dès lors l'influence que ces facteurs prédéfinis auraient sur l'effectiveness du modèle des 3LoD.

Et troisièmement, un ensemble de facteurs pouvant potentiellement influencer l'effectiveness du modèle leur étaient présentés, confrontés, dans le but de savoir si ces

facteurs leur semblaient pertinents ou non. A cela, leur était demandé si selon eux, d'autres facteurs non précités pouvaient influencer cet effectiveness.

4. Présentation des interviewés

	Profil	Type d'entreprise
Interviewé n°1	Le premier interviewé exerce actuellement une fonction de contrôleur interne. Il fut intéressant de l'interviewer pour plusieurs raisons. De par, premièrement, son expérience au sein de ses différentes fonctions exercées dans de la première et de la deuxième ligne de défense. De par, deuxièmement, les entreprises dans lesquelles il a pu travailler. En effet, au sein de la première entreprise, le modèle des 3LoD était relativement bien établi, les fonctions de contrôle existaient en grand nombre, alors qu'au sein de son entreprise actuelle, tout le travail de contrôle interne est à développer.	Secteur de l'assurance
Interviewé n°2	Le deuxième interviewé exerce une fonction d'auditeur interne, indépendant. Ayant une vingtaine d'années d'expérience dans ce domaine, et ayant exercé des fonctions de deuxième ligne de défense, il était donc très intéressant de profiter de son savoir.	Secteur industriel et hospitalier
Interviewé n°3	Le troisième interviewé est responsable de l'audit interne au sein d'une entreprise internationale, cotée en bourse. Ayant une expérience internationale, à la fois en tant qu'auditeur interne et externe, il était donc très intéressant de l'interviewer sans se poser de questions.	Secteur financier

Interviewé n°4	Le quatrième interviewé exerce une fonction de directeur de risque, de compliance et d'audit interne. Cette double casquette qu'exerce ce participant, à savoir l'exercice d'une fonction de la deuxième ligne de défense, et d'une fonction de la troisième ligne de défense, présente des aspects très intéressant pour la rédaction de mon mémoire. De plus, cette fonction étant une fonction de direction, cela rajoute un point de vue quant à l'implémentation des trois lignes de défense dans une grande entreprise publique.	Secteur public, entreprise ferroviaire
Interviewé n°5	La cinquième personne ayant répondu positivement à l'interview, exerce une fonction de responsable d'audit interne. Fort de son expérience de plus de vingt ans dans l'audit interne, l'interviewé a pu développer une vision à la fois large et précise sur les notions de contrôles internes ainsi que de gestion des risques. De plus, l'activité d'une banque privée étant plus spécifique qu'une banque publique, cela ajoute une perspective quant à la compréhension du modèle des 3LoD.	Secteur bancaire
Interviewé n°6	Le sixième interviewé exerce une fonction de responsable d'audit interne. Son expérience professionnelle au sein d'institutions financières aura permis d'établir des comparaisons intéressantes quant à l'implémentation du modèle dans différents types de secteurs.	Secteur public, entreprise de traitement du courrier postal

Interviewé n°7	Le septième interviewé exerce une fonction de responsable d'audit interne. Ce secteur d'activité, dès lors non-financier, permet d'élargir le champ de recherche quant à l'implémentation du modèle.	Entreprise de distribution automobile
Interviewé n°8	Le huitième interviewé exerce une fonction de responsable de la gestion actifs-passifs. Cette fonction faisant partie intégrante de la première ligne de défense, cela ajoute une prise de vue, une position quant au modèle.	Secteur de l'assurance
Interviewé n°9	Le neuvième interviewé exerce une fonction de responsable d'audit interne depuis une dizaine d'années	Secteur bancaire

5. Analyse des interviews

5.1 Interaction entre les lignes de défense

Dans ce premier point, est abordé l'interaction entre les lignes de défense. En effet, il est primordial d'analyser comment les lignes de défense interagissent entre-elles, comment les acteurs de l'entreprise perçoivent cette interaction, quels en sont les différents impacts sur l'effectiveness du modèle, et ce, en fonction du type d'entreprise dans laquelle le modèle est implémenté.

Tout d'abord, il est analysé l'interaction entre les deux premières lignes de défense, à savoir les fonctions opérationnelles et les fonctions de gestion des risques en général. L'analyse est effectuée sur base des modèles décrits par Paul Sweeting (2011), dans le but d'identifier deux thèmes essentiels, qui sont l'indépendance et la collaboration entre les lignes de défense. Pour rappel, les différents types d'interaction définis par Paul Sweeting, se nomment « offense vs defense model », « policy vs policing model », et « partnership model ». Il est néanmoins inutile d'effectuer une analyse transversale sur base du « offense vs defense model », car celui-ci n'a jamais été souligné par l'un des interlocuteurs.

L'observation porte, dans un deuxième temps, sur l'interaction entre la troisième ligne de défense, à savoir l'audit interne, et les deux premières lignes. Dans ce cas-ci, l'analyse est abordée directement à travers les thèmes de l'indépendance et de la collaboration, puisqu'aucun modèle ne permet d'identifier les types d'interaction entre l'audit interne et les autres lignes de défense.

5.1.1 Interaction des deux premières lignes de défense

Le « partnership » modèle

L'interlocuteur n°1 a exercé des postes de première et seconde ligne de défense, en même temps, et au sein de la même entreprise. Selon lui, cela ne pose pas de problèmes particuliers car le système de gestion des risques n'était pas encore mature, il devait se développer au fil des années. Néanmoins, bien que les lignes soient floues, il insiste sur « l'importance de challenger les acteurs de la première ligne », en effectuant des entretiens avec les intervenants pour analyser leurs procédures opérationnelles.

L'interlocuteur n°2 rejoint cet avis, en expliquant que la frontière entre la première ligne et la deuxième ligne n'est certainement pas très bien établie dans certains types

d'entreprises, que ce soit à cause de leur taille, ou à cause de leur secteur d'activités. Selon lui, les responsabilités des deux lignes de défense sont souvent dans les mains d'une même personne. « Dans le département informatique, par exemple, celui-ci est en partie en charge du développement et de la gouvernance, notamment avec le principe de séparation de fonctions, et est en partie en charge de la maintenance opérationnelle ».

Il faut donc un modèle collaboratif, pour qu'un acteur de première ligne puisse aller dans la deuxième ligne, collaborer avec les fonctions de gestion, et ensuite revenir vers la fonction première. Le fait est que, parfois, il semble impossible de séparer les deux lignes.

L'interlocuteur n°8 pense que la collaboration consiste plus en une question de relations interpersonnelles. Selon lui, chaque acteur a un rôle à jouer, il y a une force de proposition et il y a une force d'opinion. Il ajoute, « tant que chacun reconnaît le rôle de l'autre et reste dans sa zone de travail, dans son terrain de jeu, tout se passe correctement ».

L'interviewé n°3 explique aussi que, lorsque le modèle n'a pas encore évolué, les deux premières lignes sont souvent rattachées, elles ne sont pas bien séparées. Historiquement, les fonctions de deuxième ligne de défense se sont détachées de la première ligne, pour occuper le terrain de cette seconde ligne de plus en plus affirmée.

L'interviewé n°5, tout comme l'intervenant n°9, explique, au contraire, « qu'il ne faut surtout pas mélanger les fonctions entre les lignes de défense ». Chacune doit garder son indépendance et ne peut exercer simultanément une autre fonction au sein d'une autre ligne de défense. Si les fonctions sont mélangées, les contrôles sont, par conséquent, annihilés, ce qui pourrait ouvrir la porte à la fraude. Toutefois, si c'est une PME, la question de la séparation de fonctions va être différente, puisque les ressources ne seront généralement pas suffisantes pour créer cette séparation de fonctions.

Le « Policy vs Policing » modèle

Selon l'intervenant n°3, au plus les lignes de défense seront indépendantes, séparées les unes des autres, au plus le modèle sera efficace. Il peut, sinon, « se créer des situations où les acteurs ne savent pas réellement quels sont leurs rôles et leurs responsabilités », ce qui nuit à la gestion des risques dans l'entreprise. En tant qu'auditeur interne, il pousse la deuxième ligne à exercer la fonction de « policy owner », mais aussi la fonction de supervision, de monitoring. En effet, si la seconde ligne parvient à développer et à mettre en place un mécanisme de détection par rapport à des situations non suivies, cela aide la

première ligne à remédier à ses problèmes, et ce, beaucoup plus rapidement que si la troisième ligne effectuait un audit tous les trois ans.

L'interlocuteur n°9 suit ce même raisonnement, en expliquant que la deuxième ligne se doit d'être complétement indépendante, qu'elle n'est pas au front, et qu'elle n'a rien à gagner. Celle-ci émet des critères, mais n'impose pas les contrôles en soi. C'est à la première ligne d'émettre les contrôles qui cadrent avec les critères préétablis. La première ligne est, dès lors, dans l'obligation de suivre ces critères mais peut évidemment les discuter et apporter un point de vue différent.

Par ailleurs, selon lui, il est important de définir ce qu'est la première ligne de défense. Il existe dans cette ligne les fonctions du front office et les fonctions du back office. « Souvent, les gens confondent cette fonction de back office avec la fonction de deuxième ligne de défense, qui est réellement indépendante, pour justement éviter les conflits d'intérêts, il faut donc bien définir cette première ligne de défense. »

L'interlocuteur n°6 insiste sur le fait qu'il doit y avoir un challenge qui s'exerce entre les deux premières lignes de défense. Pour que ce challenge puisse s'effectuer, les deux lignes doivent être totalement indépendantes. Cette affirmation rejoint les dires de l'interlocuteur n°5, qui insiste sur « l'importance de la ségrégation des fonctions entre les lignes de défense ».

Ce challenge pourrait créer de trop grandes disparités d'opinions entre les lignes de défense, toutefois, l'interlocuteur n°8 explique que dans le fonctionnement de l'entreprise, la première ligne présente toujours ses propositions dans un comité, où la seconde ligne est représentée et donne une seconde opinion, avant que le comité puisse valider formellement. Le comité pourrait, dès lors, dévier de la seconde opinion, mais dans les faits, la gestion des risques faisant partie du comité, celui-ci ne vote pas pour une proposition qui n'a pas été validée par sa propre équipe. Ce qui passe dans les comités a déjà été revu et validé.

L'interlocuteur n°1 explique qu'en tant qu'acteur de la deuxième ligne de défense, il est intéressant de varier l'intensité des contrôles. En effet, il définit les fréquences de contrôles en fonction de la maturité des processus mis en place. « Si le dispositif fonctionne correctement et que je remarque qu'après deux contrôles, cela se passe bien,

je diminuerai l'intensité des contrôles. Inversement, je les augmenterai si je constate que ça bloque », ajoute-t-il.

Toutefois, ce dernier explique aussi qu'à partir d'un certain moment, la pertinence de la seconde ligne de défense en tant que superviseur n'a plus réellement d'intérêt. Selon lui, si tout fonctionne dans la première ligne, la plus-value de la deuxième ligne en est impactée. En effet, « si le management de la première ligne de défense suit correctement les contrôles, la deuxième ligne ne sert que pour du pilotage, et ne serait donc pas aussi intrusive que ce qu'on pourrait connaître ».

Pour une entreprise de taille moyenne, dès que l'ensemble des procédures est bien ancré dans la compagnie, la deuxième ligne n'a, à son sens, pas de plus-value. Sauf si, effectivement, il se produit des changements d'outils ou autres dans l'entreprise, alors la deuxième ligne aura son rôle à jouer. Néanmoins, pour les entreprises de plus grandes tailles où il existe des centaines de dispositifs et de procédures, la deuxième ligne de défense peut évidemment apporter de la plus-value à l'entreprise.

Selon l'interlocuteur n°2, lorsqu'on laisse trop de liberté à la deuxième ligne de défense, cela crée des excès qui empêchent finalement l'atteinte des objectifs de l'entreprise. « Si nous prenons l'agence de sécurité alimentaire, par exemple, celle-ci a pour but de protéger le consommateur, ils exercent donc en soi, des rôles dans la deuxième et la troisième lignes de défense, puisqu'ils auditent en fait des restaurants. Mais quelque part ils ont tendance aussi à établir leurs propres normes. Ils ont par exemple interdit la vente de tarte au riz au sein des boulangeries à Verviers, accusant à tort la chaine du froid. »

Il serait donc important de limiter l'indépendance de la seconde ligne de défense dans le but d'éviter des excès de la part de celle-ci. Le challenge est de trouver le juste équilibre entre la procédure qui va sécuriser le process et l'effectiveness du process. De plus, l'interlocuteur n°2 explique qu'une trop forte indépendance risquerait de déboucher sur l'absence de communication et de collaboration entre les individus. C'est aussi une question de mise à disposition des ressources par l'entreprise. S'il y a trop de ressources, trop de fonctions au sein du modèle, il peut exister un détachement trop important entre les deux premières lignes de défense.

L'interviewé n°4 souligne l'importance de la production d'un rapport annuel de la deuxième ligne de défense, expliquant comment, dans leur domaine respectif, ils évaluent

la situation, les actions qui sont en cours et les problèmes qui pourraient se poser. « À la base, cela ne se passait pas, il n'existait qu'une seule fonction qui le faisait. Mais par la suite, nous nous sommes dit qu'il était vraiment important que l'ensemble des fonctions ait un contact direct avec le comité de direction ».

5.1.2 Interaction entre la troisième ligne de défense et les deux premières

Selon l'intervenant n°3, lorsque le modèle est naissant, l'audit interne accumule souvent les rôles, de première et deuxième lignes de défense. C'est lorsque le modèle évolue, lorsqu'il prend de la maturité, que les lignes ont tendance à se distinguer.

L'interlocuteur n°2 explique que la troisième ligne de défense n'est pas forcément obligatoire pour tous les types d'entreprises. Dès lors, lorsque la troisième ligne n'existe pas, la responsabilité qui incombe à celle-ci est diluée au sein de l'entreprise et répartie à l'ensemble des acteurs de l'entreprise. Quand, dans une entreprise, le système de gestion des risques est mature, tout le monde est conscient de ce qu'il a à faire. Par contre, peu d'organisations arrivent à atteindre cette maturité ou, en tout cas, celle-ci est relativement faible.

Il peut arriver, aussi, que l'audit interne ne soit pas totalement intégré au sein de l'entreprise car cette dernière représente une filiale du groupe. L'interlocuteur n°1 explique que cela peut provoquer une méconnaissance de certains aspects de leurs métiers, de certaines spécificités et de certaines entités de la filiale. D'après l'interlocuteur, ceci n'est pas dramatique mais peut poser problème pour l'effectiveness. Ces dires sont confirmés par l'intervenant n°9, qui précise que cela peut également se passer dans le cas d'une grande entreprise, où l'audit interne est implémenté en profondeur. Toutefois selon lui, « au besoin, une personne de l'extérieur ou un consultant peut venir réaliser le travail dans un domaine spécifique ».

Dans le cas de l'intervenant n°6, les deuxièmes et troisièmes lignes sont mélangées dans l'entreprise, ceci s'explique notamment car la gestion des risques n'est pas encore mature dans l'entreprise, cela doit encore évoluer. De plus, ce mélange peut s'expliquer car il existe un ensemble d'outils, tels que les ERM, ERM Gouvernance ou encore des outils de mesures du risque, créant ce qu'il appelle un « risk universe » et un « audit universe ». Cet ensemble d'outils est utilisé par les deux sections à ce jour, ce qui justifie le fait qu'ils travaillent ensemble. Selon lui, le fait de regrouper l'audit et le risk management offre plus d'avantages que de désavantages.

L'interlocuteur n°4 se trouve être dans la même position que l'interviewé n°6. En effet, son poste combine des fonctions de deuxièmes et troisièmes lignes de défense, ce qui pourrait donc créer un conflit d'intérêt ou, en tout cas, une atteinte à l'indépendance de l'audit interne. Selon lui, ces aspects d'indépendance n'ont que peu d'importance pour deux raisons.

Premièrement, vu que sa fonction principale consiste à déclencher la sonnette d'alarme pour avertir le comité de direction en cas de problèmes, que cela provienne des deuxièmes ou troisièmes lignes de défense, cela n'a pas d'importance. Deuxièmement, l'interlocuteur estime que les synergies apportées en contrepartie de cette « fusion » valent, sans doute, la perte d'indépendance. Le fait qu'il gère les risques lui permet de bien comprendre et d'être bien informé sur les risques de l'entreprise, et donc de bien exercer son rôle d'auditeur.

Les intervenants n°4 et n°6 insistent sur le fait que, lorsqu'un audit interne doit être effectué sur l'une de leurs fonctions de deuxième ligne, ils sous-traitent l'audit interne. Cela leur garantit, d'une part, plus d'indépendance et, d'autre part, permet d'apporter plus d'expertise dans certains domaines.

En ce qui concerne la manière dont l'audit interne interagit avec les autres lignes de défense, selon l'intervenant n°3, il existe deux façons de faire de l'audit. Premièrement, comme une fonction « police », généralement perçue négativement par les acteurs de l'entreprise. Deuxièmement, réaliser sa fonction de manière collaborative et développer un partnership avec la première ligne. Au sein de son entreprise, « tous les membres du département audit ont un target de relationship management, par rapport à un business unit ou le projet dont ils sont responsables », ce qui est « très important » selon lui. Il existe par exemple des « target de relationship management », par rapport à un business unit ou un projet dont ils sont responsables. Ils établissent des réunions courtes et informelles, mais régulières et fréquentes. Selon lui, ce partnership est et doit encore être plus poussé avec la seconde ligne de défense, car le but ultime est de s'assurer que la première ligne fait ce qu'elle doit faire.

Avec la seconde ligne qui se développe de plus en plus, la troisième ligne a donc tendance à modifier l'interaction avec la première ligne de défense. C'est-à-dire qu'il y aura une diminution dans l'évaluation de l'effectiveness de la première ligne de défense et, au

contraire, une augmentation de l'évaluation de la deuxième ligne, ou en tout cas ce que fait la deuxième sur la première.

Selon l'interlocuteur n°4, il y a une importance à centraliser tout la connaissance au même endroit, donc dans la deuxième ligne de défense. C'est vraiment plus qu'une collaboration entre les deux lignes de défense, pour autant qu'ils puissent, évidemment, garder leur indépendance. Ceci permet à l'audit de mieux exercer sa fonction.

Il y a une interaction très fréquente et très forte avec la première ligne de défense, puisqu'il existe des meetings une fois par mois avec le CEO mais aussi des statuts réguliers avec chacun des membres du comité de direction. Ceci dans le but de se mettre d'accord sur les différents plans à établir, et d'adopter un positionnement par rapport à cette première ligne de défense.

L'interlocuteur n°5 explique que les lignes de défense sont une source d'information pour effectuer un audit, tout comme les gens du terrain. Les lignes deux et trois vont vraiment se poser la question de savoir si les contrôles sont adéquats, alors que la première ligne va les exécuter.

5.2 L'appétence pour le risque

La littérature scientifique sous-entend que lorsque l'appétence pour le risque est bien définie, il est plus facile de définir les rôles et les responsabilités des trois lignes de défense. Si l'appétence pour le risque a été clairement définie, a été validée par le senior management dans le business et par le comité du risque au nom du conseil d'administration, les managers ont, dès lors, plus d'impact lors des prises de décisions. Il est donc intéressant de savoir si ce facteur prend part dans l'ensemble des entreprises étudié, et si oui, quelle en est la proportion, quel est le degré d'appétence pour le risque qui est nécessaire pour que les rôles soient établis de manière effective ?

De plus, cette appétence pour le risque est définie par les organes de gouvernance de l'entreprise, à savoir le comité de direction et le conseil d'administration. Il est donc intéressant d'analyser l'interaction qui existe entre les acteurs des trois lignes de défense et ces organes de gouvernance.

Selon l'interlocuteur n°3, il n'est pas toujours simple de définir l'appétence au sein d'une entreprise. Comment se matérialise-t-il, comment se traduit-il ? « Ce n'est pas quelque chose qui se définit en une fois », mais, selon lui, cette notion joue évidemment un rôle clé

dans l'effectiveness du modèle des 3LoD. En effet, cela définit, d'une part, qui fait quoi dans les policies et les procédures et, d'autre part, cela reflète le pouvoir discrétionnaire laissé aux différents départements. Le Tone at the Top définit à quel degré l'appétence au risque sera établi dans l'entreprise, ce qui n'est évidemment pas nouveau.

L'interviewé n°3 insiste néanmoins sur le fait que le Tone at the Top doit donner le signal, le message à l'entreprise. « Il faut le support du Top, donc du comité d'audit ou du comité de direction en général, c'est à eux de le mandater, de l'imposer », insiste-t-il. « Si ceci ne passe pas, alors rien ne se passera ». En effet, l'ensemble des acteurs de l'entreprise est occupé par ses propres activités, si ce n'est pas mis comme objectif stratégique, rien ne se passera.

L'interviewé n°9 explique, par ailleurs, que c'est toujours d'en haut que l'exemple vient, le « Tone at the top » est donc très important pour qu'une culture du risque émane au sein de l'entreprise. Selon l'interlocuteur n°2, les entreprises ayant une vision très claire de ce qu'est le risque, et de comment il doit être géré, impacte l'effectiveness du modèle. Par contre, ce dernier ne pense pas qu'il y en ait énormément. Certains secteurs n'ont pas encore défini cette notion de risque.

De plus, les interlocuteurs n°7 et n°8 insistent sur l'importance du comité d'audit dans l'établissement de la culture du risque. Ce dernier doit être demandeur quant à la mise en place des trois lignes de défense et doit mandater, à de nombreuses reprises, les responsables de risques d'évoluer. Le comité d'audit doit aussi organiser des réunions de manière régulière avec les acteurs des deux premières lignes de défense, dans le but de les challenger. Selon lui, ceci explique que le modèle soit arrivé à maturité dans son entreprise et, dès lors, qu'il joue un rôle prépondérant dans l'effectiveness du modèle des 3LoD.

Tout comme l'interlocuteur n°3, l'interviewé n°5 explique que les organes de gouvernance doivent émettre la structure, les limites à respecter quant aux types d'activités, de produits, de leur duration ou de leur montant, au sein de l'entreprise. Néanmoins, il se peut qu'un collaborateur propose une idée au sujet d'un type d'activité, pour ensuite en proposer un cadre de contrôles ou un plan, qui passerait par les différents départements juridiques, de conformités, etc. et qui, au final, remonterait jusqu'au comité de direction pour qu'ensuite, ces derniers valident l'appétence au risque. Le conseil

d'administration va élaborer, sur base des critères et des risques identifiés par le risk management, l'appétence du risque pour l'entreprise, ce que confirme l'interviewé n°9.

Selon l'interviewé n°5, « lorsqu'une nouvelle activité se développe, qu'une appétence au risque se crée autour de ce sujet et que celui-ci est accepté par la direction, cela doit impérativement rentrer dans le dispositif de l'audit interne ». Il faut donc s'assurer que les deux premières lignes de défense puissent encadrer cette nouvelle activité.

Il est donc important de spécifier que, même si ce sont les organes de gouvernance qui doivent donner l'élan quant à la notion de risque dans l'entreprise, les acteurs de premières et secondes lignes font partie du processus de déclenchement de cette notion d'appétence au risque.

Dans le cas de l'interviewé n°6, les rôles des organes de gouvernance ne sont pas encore bien développés au sein de l'entreprise. Il insiste donc, dans ce cas-ci, sur l'importance d'un comité des risques pour la première ligne de défense, au sein duquel la deuxième ligne de défense assisterait. Du fait que les organes de gouvernance ne sont que trop peu présents, l'interlocuteur n°6 met également l'accent sur l'importance de la deuxième ligne de défense et de son rôle à jouer dans l'établissement, c'est-à-dire promouvoir une culture du risque au sein de l'entreprise.

5.3 Autres facteurs

5.3.1 Conscientisation

Au cours des différents entretiens, l'ensemble des participants a, sans exception, affirmé que la conscientisation au risque des acteurs de l'entreprise est un élément fondamental quant au bon fonctionnement du modèle des 3LoD.

Selon l'interlocuteur n°3, il est dès lors impératif que les acteurs de l'entreprise comprennent ce qu'est le modèle, réalisent quels en sont les bénéfices et comprennent vers quoi l'entreprise veut se diriger. Un des facteurs clés du succès du modèle repose sur le fait que les acteurs soient prêts à jouer le jeu ou non en acceptant les recommandations des auditeurs internes par exemple. « Si un membre de la direction est dans une optique de 'push-back', qu'il n'est d'accord sur aucun point, celui-ci n'est, dès lors, pas prêt à jouer le jeu, ce qui peut poser problème », insiste-t-il.

L'interviewé n°6 pense que la conscientisation au risque est une question de responsabilisation des personnes en charge d'endosser leur rôle et une question de

pouvoir aboutir sur un compromis. « Si chacun joue son rôle, que chacun est responsable, parvient à écouter l'autre et à trouver un compromis avec l'autre, alors c'est en bonne voie ». Selon lui, il est très important de se mettre à la place de l'autre et de comprendre pourquoi l'analyse ou l'opinion est sensiblement différente entre les acteurs de l'entreprise. Une fois ce processus réalisé, il est plus facile de justifier les recommandations, ou même, dans le cas où celles-ci ne sont pas justifiées, de pouvoir aisément en discuter, afin d'aboutir à un compromis avec l'interlocuteur.

L'interviewé n°5 parle de la conscientisation au risque comme étant la culture du contrôle au sein de l'entreprise. Cette culture doit, selon cet interviewé, être commune et exister dans l'ensemble des lignes de défense. Le plus important réside dans la valorisation du travail des collaborateurs. Ces derniers doivent y trouver du sens, doivent savoir pourquoi ils font les choses, doivent comprendre pourquoi ces contrôles existent et quels en sont les origines. Selon l'interviewé n°9, à terme, l'entreprise en elle-même doit arriver à une certaine maturité de conscientisation et les acteurs doivent être conscients des risques de chaque action. Il appuie cet argument en expliquant, par ailleurs, que les entreprises les plus pérennes sont, généralement, les entreprises qui mettent en avant cette prise de conscience.

Pour l'interlocuteur n°7, cette notion est réellement importante mais difficile à exécuter. « Il y a plus de 1700 personnes à faire évoluer comme ça, donc ce n'est pas quelque chose qui se fait en 1 an, et ce n'est pas parce qu'on met des organes que les gens vont forcément les suivre ou adhérer ou quoi que ce soit ».

L'interlocuteur n°2 explique que dans le secteur hospitalier, par exemple, « les acteurs de l'entreprise ont tellement le nez dans le guidon, qu'ils ne se posent pas réellement la question du contrôle interne ». Ceux-ci suivent des normes financières et médicales, mais n'ont pas de procédures mises en place. Il n'y a pas d'évaluations ponctuelles du risque et donc pas de prises d'actions par rapport à ce risque-là. Dès lors, l'efficience des trois lignes est nulle. Ils agissent, dans ce cas-ci, de manière active et non proactive. C'est donc toute la différence entre une entreprise qui a pris cette conscience du risque et celle pour qui ce n'est pas le cas.

L'interlocuteur n°5 insiste aussi sur le fait que, de par la petite taille de l'entreprise, l'interaction entre les lignes de défense s'exécute très aisément. Dès lors, tout le monde possède ce réflexe de se dire « tiens, pourquoi est-ce qu'aujourd'hui, j'ai ce document sous

ce format, ... ». L'interlocuteur n°9 rejoint cet avis, en expliquant que la culture de l'entreprise permet ou non d'atteindre une certaine maturité de conscientisation, et que cette culture dépend elle-même du business model et de la taille de l'entreprise.

La conscientisation peut donc être vue à travers deux aspects. Le premier est le fait que chaque acteur puisse adopter ce réflexe contrôle. Le second aspect consiste à ce que chaque acteur comprenne pourquoi il existe un ensemble de contrôles sur les activités qu'il exerce, pourquoi il est soumis, en quelque sorte, à une suite logique de vérifications.

Toutefois, il est intéressant de noter que, selon l'interviewé n°5, il n'est pas nécessaire que l'acteur de la première ligne de défense comprenne l'ensemble du système de contrôle, c'est-à-dire ceux présents dans la deuxième et la troisième ligne de défense. L'existence du contrôle suffit, mais le suivi n'est pas nécessaire.

Formation

Un moyen pour faciliter cette conscientisation au risque réside dans la formation des acteurs de l'entreprise. L'interlocuteur n°5 pense que la formation des agents sur ce qu'ils doivent faire et sur ce qu'ils doivent connaitre au niveau des réglementations joue un rôle essentiel, et ce, pour l'ensemble des fonctions de toutes les lignes de défense.

L'interlocuteur n°9 explique que la formation des acteurs de l'entreprise permet aussi de subvenir aux problèmes d'expertises ou de compétences qui pourraient exister au sein de la deuxième ligne de défense. En effet, si la personne qui est censé effectuer le contrôle de deuxième ligne possède moins d'expertise que l'acteur de la première ligne, cela pose problème. Ce dernier explique, par ailleurs, que les grandes entreprises ont évidemment besoin d'expertises extérieures car tous les domaines ne peuvent être couverts de manière interne.

L'interviewé n°6 soutient les arguments précités car, selon lui, les collaborateurs doivent évidemment savoir de quoi ils parlent, la formation jouant un rôle clé. Toutefois, il ajoute que l'entreprise doit absolument y mettre les moyens nécessaires, les ressources suffisantes. Ainsi, selon les interviewés n°3 et 9, il est idéal de créer un vocabulaire commun dans l'entreprise, une sémantique, une taxonomie, tel qu'un « risk academy », même si cela n'est pas toujours facile. Il est très utile de se créer une même nomenclature sur base des frameworks existants, tels que COSO ou COBIT. En effet, ces cadres permettent aux différentes lignes de défense de parler le même langage, et permet à

chacun d'avoir la même définition d'un risque opérationnel, d'un risque stratégique ou autre.

L'interviewé n°1 appuie l'importance que joue la deuxième ligne dans la conscientisation des acteurs aux risques. « La première phase que j'ai dû faire, ce sont des sessions d'informations, en leur expliquant précisément en quoi consiste le dispositif de première ligne ; à savoir la maîtrise des risques opérationnels, la maîtrise des risques que la première ligne à identifier. » Selon lui, la deuxième ligne doit informer et sensibiliser les acteurs de la première ligne sur ce qu'est la fonction de deuxième ligne, en quoi c'est un contrôle et non un audit interne. Il ajoute que la deuxième ligne est souvent perçue comme une fonction de police, ce qu'il faut évidemment éviter.

Echange de fonctions

Un autre moyen permettant de faciliter la conscientisation des acteurs de l'entreprise aux notions de contrôles et de risques consiste en l'échange de fonctions entre les lignes de défense.

Selon l'interlocuteur n°9, ce changement de fonction ne peut que favoriser la culture du risque au sein de l'entreprise. Attention, on parle bien ici d'un changement de fonction définitif, c'est-à-dire d'une translation définitive d'un acteur d'une ligne de défense vers une autre. Dès lors, le cas d'un auditeur interne qui migre vers l'opérationnel sera profilé comme une personne étant consciente au risque. Plus les gens circulent, pas en même temps bien sûr, et plus la culture du risque sera diffusée dans l'ensemble des départements. « En France, par exemple, un acteur d'une première ligne de défense doit passer par l'inspection financière, une sorte d'audit interne, avant de pouvoir exercer sa fonction en première ligne de défense ».

Selon l'interlocuteur n°5, cet échange de fonction pourrait poser problème à partir du moment où la ligne de défense déforcée ne serait pas renforcée. Mais au contraire, l'expérience acquise au sein d'une fonction permet inévitablement d'apporter de la plus-value dans l'exercice d'une autre fonction, les acteurs en question sont généralement plus sensibles à ce qui est important ou non.

5.3.2 L'existence et le suivi du contrôle

Une analyse qui sous-tend la lecture scientifique réside dans le fait que le modèle des trois lignes des défense serait un modèle trop coûteux et très bureaucratique. Placer, à chaque

risque, un dispositif de contrôle ne serait que très peu efficace et, au final, un nombre excessif de contrôles tuerait le contrôle.

Selon l'interlocuteur n°2, dans certaines administrations, il est courant d'avoir une quantité assez élevée de signatures et d'autorisation dans le cas d'une procédure ou d'un type de contrôle. « Je crois que le maximum que j'ai vu, c'était une dizaine d'approbations, une dizaine de personnes qui signait le cahier général des charges pour l'approuver ». Ceci a pour conséquence une dilution complète du contrôle interne. Plus personne n'est, dès lors, réellement responsable du contrôle interne en tant que tel.

Une solution a été de diminuer drastiquement ce nombre de contrôles et de responsabiliser une seule et même personne, l'efficience en est ainsi que meilleure. Selon lui, il est important de trouver un juste équilibre entre avoir un nombre suffisant de personnes qui contrôlent et veiller à ce que le contrôle ait du sens. L'interlocuteur n°3 confirme cet argument, en expliquant que si les contrôles sont trop nombreux et si trop de personnes sont responsables d'un même contrôle, finalement, plus personne ne le sera.

Selon l'interlocuteur n°1, « l'ensemble de ces fonctions de contrôles servent plus à réaliser du management de CEO » qu'autre chose. Le nombre de contrôles au sein d'une entreprise peuvent, selon lui, clairement impacter l'efficience du business de l'entreprise.

Pour appuyer cet argument, il met en avant deux exemples différents. Le premier, dans une entreprise ne possédant aucun système de contrôles internes, où certains acteurs de deuxième ligne exécutent des rôles de première ligne, ceci dans un but d'efficacité et de pouvoir atteindre pleinement leurs objectifs. Le deuxième, dans une entreprise où la notion de contrôle interne est considérablement intégrée et où, dès lors, plusieurs contrôleurs internes travaillent quotidiennement pour l'entreprise.

Nous pourrions croire que la deuxième entreprise développera, à terme, un business plus efficient, contrairement à la première entreprise. Il n'en est rien, car, selon lui, un surplus de contrôleurs internes ne peut qu'être inefficace pour le business de l'entité. « Parfois je faisais des contrôles pour dire que tout va bien et donc fin du mois, c'était toujours la même chose, c'était tout allait bien. C'est bien beau de dire que tout va bien, mais à partir du moment où c'est mature, je ne trouve pas la plus-value », ajoute-t-il.

Selon l'interlocuteur n°3, les acteurs subissant les contrôles peuvent se plaindre de ceux-ci, ce qui nuit au business de l'entité. Cela est toutefois symptomatique de quelqu'un qui

n'a pas encore compris l'entièreté de son rôle au sein de l'entreprise. Selon lui, l'opérationnel de la première ligne de défense a au moins 10% de contrôle à effectuer dans son travail quotidien. Toutefois, il rappelle que les acteurs de première ligne de défense ne peuvent pas passer tout leur temps en comité de risques et qu'il est donc important de trouver un juste milieu.

Selon l'interlocuteur n°4, il est important de comprendre la notion de « key control », primordiale dans la gestion des contrôles, justement. Il faut essayer de promouvoir le contrôle de manière pertinente. Il cite un exemple qu'il a connu au sein de son entreprise, où il était demandé à une entreprise externe de mettre en place un cadre identifiant l'ensemble des risques et des contrôles, pour ensuite vérifier si ce cadre était appliqué correctement par l'ensemble des départements de l'entreprise. Selon l'interlocuteur n°4, « cette vérification n'est pas faisable, cela coûte trop cher à l'implémentation et personne n'en fait quelque chose de réellement efficace ».

Selon l'interlocuteur n°5, les types de contrôles sont au final, à la fois distincts et complémentaires. D'après lui, les angles de vue pris par chacune des lignes de défense sont totalement divergents, chacun aborde le sujet d'une manière qui lui est propre. Il est donc important d'appréhender le modèle de manière globale, pour comprendre que les contrôles sont efficaces et non redondants. L'ennemi du contrôle, c'est le stakhanovisme du contrôle. Il faut former les acteurs, qu'ils prennent conscience de ce qu'ils font.

L'interlocuteur n°6 met en avant les principes de « four-eyes » et « six-eyes », qui sont des principes assez courants du contrôle interne, et qu'il utilise au sein de son entreprise. Toutefois, le principe du « six-eyes » peut être trop rébarbatif, voire inefficace.

En effet, si la vérification du contrôle n'est pas bien spécifiée, il se peut que la personne en charge de la vérification signe le document, alors que le contrôle n'existe même pas. Selon lui, le plus important consiste en la description du contrôle. Si quelqu'un doit contrôler quelque chose mais qu'il ne sait pas ce qu'il doit faire, évidemment, cela pose un gros problème d'efficacité. Il faut conscientiser les personnes à cette notion de description de contrôles.

Selon l'interlocuteur n°9, un des principes de base consiste à s'assurer que le coût du contrôle n'est pas plus élevé que la recette probable du risque pris. Il est important que le contrôle ait de la valeur ajoutée, qu'il apporte réellement quelque chose. Il faut

constamment prendre en compte ce ratio, afin d'évaluer si le contrôle est efficace ou non. Tout est dans la quantification du risque, qu'est-ce que l'entreprise est prête à (ne pas) accepter ? Indirectement, cela rejoint l'appétence du risque définie par la direction.

5.3.3 Les régulations

Les entreprises consultées durant le processus de recherche sont issues de divers secteurs, que ce soit le secteur bancaire, le secteur de l'assurance, le secteur industriel, ou le secteur étatique. Le modèle des 3LoD est une conséquence indirecte de la crise financière de 2008-2009, qui avait principalement pour but de s'appliquer au secteur bancaire. Toutefois, le modèle a été, par la suite, appliqué à d'autres secteurs, pour finalement devenir une norme générale. Chacune des entreprises consultées est soumise à des normes, plus ou moins poussées, en ce qui concerne la publication des informations de l'entreprise, les contrôles internes et la gestion des risques. Il est donc intéressant d'analyser si la mise en place de normes, de régulations, influencent directement l'effectiveness du modèle des 3LoD.

Selon l'interviewé n°2, le modèle est réactif aux différentes normes. Par exemple, la crise de 2008, suivie des normes de Bâle et de Solvency, ensuite le modèle a été implémenté. « Au niveau de l'U.E, ils ont décidé de passer d'un système de standards à un système de principes, ce qui laisse la liberté d'appliquer ces principes en fonction de leur réalité. Ils font donc le pari de la maturité de l'entreprise ou de la maturité du système de contrôle interne dans l'entreprise. Or, ce système des trois lignes de défense n'est sûrement pas clair dans les petites entreprises ».

L'interlocuteur n°5 explique que, depuis la crise de 2008-2009, les régulateurs bancaires ont insisté sur tout ce qui concerne le contrôle de deuxième niveau, ce qui a donc influencé le développement du modèle dans l'entreprise. Les régulations obligent les banques à adopter le modèle des 3LoD, et ce, d'une manière bien précise. Par exemple, les lignes doivent être totalement indépendantes les unes des autres. Selon lui, les lignes étaient déjà établies mais moins contrôlées.

Le rôle du régulateur est évidemment très important puisqu'ils ont une vue sur l'ensemble des entreprises, pour l'interlocuteur n°6.

Selon l'interlocuteur n°9, les réglementations influencent aussi énormément la conscientisation au risque dans une entreprise puisque celle-ci met un cadre, une

obligation quant à la gestion du risque. Dans le secteur bancaire, en tout cas, cela influence la conscientisation au risque.

5.3.4 Les informations

Selon l'interlocuteur n°2, la qualité de l'information est, assurément, extrêmement importante pour prendre des décisions. Est-ce que le modèle prend en compte la circulation de l'information ? Est-ce que celle-ci est suffisamment fiable ou robuste ? On parle ici de reporting. Le challenge, c'est l'accès à l'information, la qualité des informations ainsi que la temporalité avec laquelle les informations sont diffusées. Le challenge, c'est de définir les informations dont l'entreprise a besoin et, surtout, qu'il y ait une compréhension commune sur ce que contiennent ces informations. Il faut organiser cet accès à l'information.

Selon l'interlocuteur n°3, il existe, comme dans toutes entreprises, des biais d'informations, notamment par le fait que ce sont des humains derrière ces informations. Par exemple, pour la seconde ligne qui n'est, en effet, pas indépendante au sens de la troisième ligne de défense, leur ligne de reporting peut être biaisée.

Selon l'interlocuteur n°4, au plus l'entreprise veut accroitre l'assurance quant à l'information donnée, au plus celle-ci a besoin de contrôler les choses, ce que le « mass data » permet d'obtenir. Par ailleurs, le fait qu'il existe un département indépendant au sein de l'entreprise qui extrait l'ensemble des données permet d'améliorer cette assurance

Selon l'interlocuteur n°5, il existera toujours des biais d'informations au sein de l'entreprise. Il doit donc y avoir un échange d'informations constants et la création d'une boucle d'informations entre les acteurs sur le terrain.

5.3.5 L'histoire de l'entreprise

Selon l'interlocuteur n°9, l'histoire de l'entreprise joue sur la culture de l'entreprise, assurément. Si l'entreprise est familiale, privée ou publique, cela a évidemment un impact sur le contrôle interne et la gestion des risques de l'entreprise.

L'interlocuteur n°7 explique qu'au sein de son entreprise, d'origine familiale, la notion de contrôles et de risques n'était pas réellement présente il y a encore quelques années. « C'est une entreprise familiale de 200 ans, avec un actionnariat majoritaire familial, ça

joue aussi énormément dans l'environnement culturel ». Ce n'est que lorsqu'il y eut un nouvel actionnaire, que cette culture du contrôle s'est propagée au sein de l'entreprise.

Selon l'interlocuteur n°4, la dimension sociale peut aussi impacter la culture de contrôle de l'entreprise. Si l'entreprise est sujette à une dimension sociale plus importante, l'acteur de l'entreprise n'en sera que plus attentif à la réussite du projet. Ce qui passe par une conscientisation plus élevée de la notion de contrôle et de risque, et dès lors, impacte le modèle des 3LoD.

5.4 Modèle en général

Selon l'interviewé n°3, le modèle des 3LoD met du temps pour se mettre en place. Le modèle évolue toujours, avec la maturité de l'entreprise notamment. Il y a énormément d'éléments qui permettent d'expliquer la mise en place du modèle, tels que la complexité de l'entreprise, l'aspect culturel, l'aspect business, etc. Il se veut être la norme aujourd'hui, dans les grandes organisations internationales. Selon l'interlocuteur n°5, en fonction de l'évolution de l'activité de l'entreprise, les deux premières lignes de défense vont se renforcer ou non. C'est l'évolution de la vie de l'entreprise qui conditionne l'évolution du modèle, et donc son effectivité.

Selon l'interlocuteur n°3, la gestion des risques n'est pas une fonction de la première, deuxième ou troisième ligne de défense, mais bien de l'ensemble des personnes dans l'entreprise. L'idée c'est que le modèle, une fois arrivé à une certaine maturité, puisse permettre aux acteurs de l'entreprise de penser au quotidien, à la gestion des risques et à l'évaluation des risques.

Selon l'interlocuteur n°3, l'entreprise doit se donner les moyens pour mener à bien la gestion des risques. C'est-à-dire, se donner les moyens en termes de ressources, de people, de système, de process, etc. dans le but de construire cette deuxième ligne, qui est à son sens, la plus importante. Cette deuxième ligne est extrêmement importante pour que le modèle soit efficace. C'est en effet elle qui, en mettant en place ces propres systèmes de détection, joue le rôle du fait que ça doit vraiment fonctionner.

Selon l'interlocuteur n°4, si le modèle est trop rigide, il ne peut être efficient. Le tout est dans la manière dont le rôle est exercé dans l'entreprise. Par exemple, son prédécesseur dans l'entreprise était perçu comme tellement rigide que plus personne ne lui parlait. Il faut privilégier la collaboration.

Selon l'interlocuteur n°5, le modèle est efficace car lors du développement de nouvelles activités au sein de l'entreprise, les processus de contrôles sont assez bien établis que pour les évaluer de la bonne manière.

Selon l'interlocuteur n°6, le modèle est un système comme les autres, le plus important c'est que les processus soient bien décrits, que l'identification des risques ait bien été réalisée et que celle-ci soit bien gérée. Ce n'est pas le système en soi qui est bon ou mauvais, mais c'est bien la façon dont il est implémenté. Le cadre doit être bien établi, qu'il n'y ait pas de marges de manœuvre concernant l'implémentation, les contrôles, et l'identification des risques.

Selon l'interlocuteur n°9, le modèle sera toujours pérenne, toujours efficace. Il faut, néanmoins, pouvoir effectivement l'actionner et le faire évoluer aussi à l'aune de l'évolution de la société dans sa globalité. Comment rendre le modèle efficace dans ces changements-là ? C'est la question de l'effectivité. Il faut faire tourner le modèle à la lumière des nouvelles technologies, de l'évolution du monde de l'entreprise. Donc, toute la question est de savoir si le modèle répondra aux attentes de demain, concernant, notamment, les nouvelles technologies, les nouveaux métiers robotiques, etc. Est-ce qu'il est suffisamment forward looking ? Comment appliquer ça à des machines ?

6. Discussions

Cette partie du mémoire est dédiée, dans un premier temps, à l'exposition des idées essentielles qui ressortent de l'analyse des interviews, ainsi qu'aux éventuelles recommandations quant à une mise en place effective du modèle des 3LoD dans des entreprises de moyennes et grandes tailles. Ceci aura pour but de confirmer ou infirmer les hypothèses émises suite à l'analyse de la revue de littérature. Dans un deuxième temps, seront exposées les limites de l'analyse des interviews, et du mémoire de manière générale.

À la suite de la revue de littérature, la problématique principale tentait de définir ce qu'est un modèle des 3LoD efficace. Il était cependant difficile d'émettre une définition précise dû au peu de ressources existantes. Grâce aux entretiens réalisés, il m'est maintenant possible d'esquisser une définition quant à un modèle des 3LoD efficace.

Dans un premier temps, un modèle est efficace lorsque chaque acteur de l'entreprise exerçant des fonctions opérationnelles, de gestion ou d'audit pense au quotidien à la gestion des risques et à l'évaluation de ceux-ci. Ce modèle doit privilégier l'aspect collaboratif entre les différentes fonctions. De plus, celui-ci doit permettre la mise en place de contrôles continus, pouvant absorber les probables nouveaux risques inhérents aux nouvelles activités de l'entreprise. Il doit, en outre, évoluer à l'aune de l'évolution de la société dans sa globalité. Le modèle doit pouvoir répondre de manière efficiente à la lumière des nouvelles technologies, doit pouvoir s'adapter à l'évolution du monde de l'entreprise et aux attentes de demain. Un modèle des 3LoD efficace est donc un modèle qui est suffisamment « forward looking ».

La deuxième problématique ciblait les facteurs pouvant influencer l'effectiveness du modèle des 3LoD. La suite de la discussion tente de répondre aux différentes hypothèses émises.

6.1 L'interaction entre les lignes de défense

Il ressort de la revue de littérature deux modèles principaux d'interaction entre les deux premières lignes de défense, à savoir le modèle de « partnership », privilégiant une collaboration extrêmement poussée entre les fonctions, et le modèle de « policy and policing », poussant les fonctions de seconde ligne à émettre des politiques aux fonctions

opérationnelles, pour ensuite en vérifier la bonne application. Le premier modèle, bien qu'il promeuve une prise de responsabilité en matière de gestion des risques au sein de la première ligne de défense, peine à convaincre le régulateur car la séparation de fonction n'est pas clairement établie. Le deuxième modèle, au contraire, prône une réelle séparation des fonctions, indépendante et transparente.

Grâce à l'analyse des interviews, il peut donc être discuté l'influence du type d'interaction entre les lignes de défense sur l'effectiveness du modèle des 3LoD, pour ensuite pouvoir recommander un type d'interaction à privilégier lors de l'implémentation du modèle au sein d'une entreprise quelconque.

D'emblée, on remarque que le type d'interaction existant varie en fonction du type d'entreprise dans laquelle est implémenté le modèle des 3LoD. Il ressort, en effet, que lorsque le modèle n'est pas arrivé à maturité dans l'entreprise, les deux premières lignes de défense ont tendance à se mélanger, ce qui privilégierait l'existence du modèle d'interaction de « partnership ». On remarque par la suite que, lorsque le modèle atteint une certaine maturité au sein de l'entreprise, le type d'interaction demeurant principalement entre les deux premières lignes de défense constituerait le modèle d'interaction « policy and policing ». Il y aurait une tendance, de par l'évolution du modèle, à un détachement progressif de la deuxième ligne par rapport à la première, et donc à une réelle prise d'indépendance.

Il est intéressant, dès lors, de comprendre quels sont les éléments pouvant influencer la maturité du modèle des 3LoD. Est-ce dû, par exemple, à une réelle prise de conscience des organes de gouvernance quant à l'implémentation d'un système de gestion des risques ? Est-ce dû aux régulations plus importantes dans certains secteurs que d'autres, notamment dans le secteur bancaire ? Où, est-ce dû, par exemple, à la culture de l'entreprise ? Ces facteurs influençant la maturité du modèle au sein de l'entreprise sont discutés dans le point suivant.

La conscientisation au risque est véritablement un facteur clé de succès quant à l'efficience du modèle des 3LoD. Il est impératif que les collaborateurs de l'entreprise, tant le comité de direction que les fonctions opérationnelles, soient prêts à jouer le jeu, à prendre conscience des notions de contrôles internes et de gestion des risques. Ceux-ci doivent véritablement adopter un « réflexe risque », et comprendre pourquoi le contrôle

existe. La formation, ainsi que la variation des fonctions au sein de l'entreprise, favorisent cette notion de conscientisation.

Il est donc intéressant de se demander si, d'une part, la conscientisation au risque impacte la maturité du modèle au sein de l'entreprise et si, d'autre part, cela influence l'efficience du modèle. Au vu de l'analyse des interviews, il ressort que la conscientisation au risque n'a pas d'influence sur la maturité du modèle des 3LoD. Que l'indépendance des lignes de défense soit marquée ou non, la conscientisation au risque doit être commune à l'entreprise pour que le modèle soit efficace.

De plus, l'existence de régulations influence clairement la maturité du modèle de 3LoD. On remarque que, lorsque les régulations sont bien établies au sein d'un secteur tel que le secteur bancaire, le modèle aura tendance à être plus mature. Les régulateurs, d'une part, invitent les banques à établir des lignes de défense totalement séparées et, d'autre part, sanctionnent en cas de non-respect de ces normes. Si les ressources mises à disposition par l'entreprise ne sont pas suffisantes, dès lors, un rappel à l'ordre sera effectué par les régulateurs. Forcément, dans les petites entreprises, lorsque les ressources ne peuvent être mises à disposition pour structurer et assigner des rôles et responsabilités distinctes entre les différentes fonctions, la séparation des deux premières lignes de défense ne peut réellement s'effectuer.

Il peut être conclu que le degré de maturité avec lequel le modèle est implémenté et, indirectement, le type d'interaction existant entre les lignes, peut influencer l'effectiveness de ce dernier

Dans un premier temps, dans le cas du modèle d'interaction « partnership », tous les interlocuteurs s'accordent à dire qu'ils sont dans l'obligation d'établir, dans le futur, une séparation distincte et précise entre les deux premières lignes. Bien que, à court terme, ce type d'interaction n'exerce pas d'influence sur l'effectiveness du modèle, cela peut avoir un impact négatif à long terme.

Dans un deuxième temps, le modèle d'interaction « policy and policing » peut, assorti de certaines conditions, influencer positivement l'effectiveness du modèle des 3LoD. Ce détachement de la seconde ligne par rapport à la première permet d'assigner clairement les rôles et les responsabilités aux acteurs de l'entreprise. Toutefois, ce détachement ne

peut être trop important, au risque de causer un déficit de collaboration entre ces différentes fonctions.

En ce qui concerne l'interaction entre la troisième ligne de défense et les deux premières, la manière avec laquelle cette interaction est effectuée influence l'effectiveness du modèle des 3LoD. Il est notamment nécessaire, dans un premier temps, de pousser la collaboration entre l'audit interne et la première ligne de défense et, dans un deuxième temps, de donner de plus en plus de « pouvoir » à la seconde ligne de défense. En ce qui concerne l'indépendance, l'audit interne est, par définition, indépendant des autres organes de l'entreprise. Toutefois, on remarque que, dans certaines entreprises, il existe des fonctions mélangeant des rôles de deuxième et troisième ligne. Encore une fois, cela s'explique soit par le fait que le modèle n'est pas arrivé à maturité au sein de l'entreprise, soit parce que les organes de gouvernance en ont décidé ainsi.

De manière générale, il ressort donc que la deuxième ligne de défense doit impérativement jouer un rôle prépondérant dans le système de gestion des risques. Les fonctions de gestion, de sécurité et de conformité doivent véritablement endosser l'ensemble des responsabilités nécessaire quant à l'exécution d'un système de gestion des risques efficace. Il est vital, pour l'entreprise, que la deuxième ligne de défense possède les fonctions à la fois de « policy owner » et de supervision, dans le but d'améliorer l'efficacité des processus de contrôles internes. De plus, la deuxième ligne de défense doit pouvoir accéder directement aux fonctions de direction pour émettre des suggestions, des recommandations quant à l'efficacité du système de gestion des risques.

6.2 L'appétence pour le risque

Il ressort de la revue de littérature qu'une définition clairement établie de l'appétence au risque de la part des organes de gouvernance permettrait d'assigner précisément les rôles et les responsabilités aux acteurs de l'entreprise. Il en résulterait une prise de risque plus efficiente de la part des managers de l'entreprise. Une réflexion qui ressort notamment de la littérature scientifique consiste à dire que l'appétence au risque ne peut être entièrement définie par les organes de gouvernance. Prenons l'exemple du risque de crédit dans les institutions financières, qui est défini par un organe externe à l'entreprise, à savoir, les agences de notation.

Les questions sont ici de savoir, dans un premier temps, si la définition de l'appétence au risque par les organes de gouvernance peut influencer ou non l'effectiveness du modèle

des 3LoD et, dans un deuxième temps, si le modèle permet de concentrer l'ensemble de l'appétence au risque entre les mains des organes de gouvernance.

De manière générale, l'ensemble des interlocuteurs s'aligne sur le fait qu'une appétence au risque bien définie influence positivement l'effectiveness du modèle des 3LoD. Il est réellement important que le Tone at the Top donne le signal, le support nécessaire quant à l'établissement d'une véritable culture du risque au sein de l'entreprise. En effet, cela aura un impact sur l'ensemble des acteurs des lignes de défense, que ce soit les fonctions opérationnelles pouvant émettre des propositions sur l'établissement d'éventuels cadres de contrôles, ou que ce soit le comité d'audit ayant un rôle dans le challenge des deux premières lignes de défense. De même, il est donc nécessaire de mettre en place des lignes de reporting directes entre certaines fonctions et les organes de gouvernance. Les fonctions de deuxième ligne de défense doivent impérativement rapporter de manière directe à leur comité de direction, pour ensuite agir sur la première ligne de défense.

Néanmoins, dans le cas où les organes de gouvernance ne seraient que trop peu présents et n'établiraient pas de réelle appétence au risque, la deuxième ligne de défense doit, à nouveau, être mise en avant. C'est à elle de prendre le rôle dans l'établissement de la culture du risque au sein de l'entreprise.

6.3 La culture d'entreprise

Par culture d'entreprise, il faut entendre l'ensemble des connaissances, des valeurs et des comportements qui facilite le fonctionnement d'une entreprise en étant partagé par ses membres.

Au vu des interviews réalisées, il ressort que certaines valeurs caractéristiques d'une entreprise auront pour effet d'accentuer la collaboration entre les fonctions, élément essentiel quant à l'efficience du modèle des 3LoD. En effet, il faut impérativement éviter que les acteurs de l'entreprise soient trop rigides et ne partagent aucune valeur commune, il faut favoriser l'entreprise libérée.

L'origine de l'entreprise, qu'elle soit familiale, publique ou privée, aura un impact évident sur l'implémentation de la notion de contrôle au sein de l'entreprise. Il résulte, à la suite de l'analyse des interviews, que dans le cas d'une entreprise à actionnariat familial, la culture du risque n'est pas autant implémentée que dans une entreprise à actionnariat

multiple. En conséquence, la maturité du modèle des 3LoD est plus faible dans ce type d'entreprise.

La dimension sociale de l'entreprise, plus précisément l'objet pour lequel la compagnie existe, peut aussi être un facteur influençant cette notion de contrôle. Il ressort des interviews que lorsque le personnel se sent investi d'une mission sociale, celui-ci sera plus attentif quant à l'exercice de sa fonction.

CONCLUSION

L'objectif principal de la recherche a été d'examiner l'effectiveness du modèle des 3LoD, ainsi que les facteurs pouvant influencer cet effectiveness. Le modèle des trois lignes de défense a été mis en avant à plusieurs reprises comme étant bénéfique pour les entreprises ayant décidé de l'implémenter en leur sein. De plus, la littérature a révélé un ensemble de facteurs pouvant agir positivement sur l'effectivité du modèle des trois lignes de défense. C'est ce qui a été analysé dans ce mémoire.

Lors de la recherche empirique, nous avons défini en premier lieu ce qu'est un modèle des 3LoD efficace. Nous avons ensuite, grâce aux interviewés, démontré qu'une partie des facteurs recensés lors de la revue de littérature, influence positivement l'effectiveness du modèle des 3LoD. Enfin, la partie empirique nous a permis de révéler plusieurs facteurs influençant l'effectiveness du modèle n'étant pas recensés dans la littérature scientifique. Dans le point qui suit, nous exposons les conclusions principales en ce qui concerne les questions de recherche.

Dans un premier temps, l'ensemble des intervenants a été d'accord pour dire que les interactions entre les lignes de défense ont une influence sur l'effectiveness du modèle. Néanmoins, en fonction du type d'interaction exercé au sein de l'entreprise, l'influence sur l'effectiveness varie. L'ensemble des interviewés est d'avis qu'une fois le modèle des 3LoD arrivé à maturité dans l'entreprise, le modèle d'interaction « policy and policing » doit être privilégié. Les deux premières lignes de défense doivent se détacher l'une de l'autre, pour adopter une indépendance totale, tout en collaborant de manière étroite. Toutefois, le modèle d'interaction « partnership », adopté lorsque le modèle des 3LoD n'est pas à maturité au sein de l'entreprise, exerce aussi une influence positive sur l'effectiveness du modèle, à condition qu'un challenge intensif s'exerce entre les deux premières lignes.

Dans un deuxième temps, nous pouvons observer que l'ensemble des interviewés s'aligne sur le fait que l'appétence au risque influence positivement l'effectiveness du modèle des 3LoD. L'échantillon nous a permis d'affirmer qu'une appétence au risque clairement définie par les organes de gouvernance favorise l'assignation des rôles et des responsabilités aux acteurs des différentes lignes de défense. Plus précisément, ceux-ci

ont, dès lors, une plus grande marge de manœuvre quant à l'exécution de leurs fonctions, qu'elles soient opérationnelles ou de gestion. En outre, la gouvernance de l'entreprise, à savoir le Tone at the Top, doit émettre un signal fort quant à une véritable création d'une culture du risque au sein de l'entreprise.

Dans un troisième temps, la culture d'entreprise a aussi un impact quant à l'effectiveness du modèle des 3LoD. Que ce soit l'origine de l'entreprise, l'objet de celle-ci ou les valeurs partagées en son sein, cela influence la manière dont la culture du contrôle est implémentée au sein de telle ou telle entreprise.

Limites et recommandations

Durant la réalisation de ce mémoire, plusieurs limites ont été rencontrées. Celles-ci sont exposées au point suivant. De plus, des recommandations sont émises pour chaque limite, afin d'éviter que celles-ci n'apparaissent dans des recherches futures.

Premièrement, la revue de littérature n'a pas pu mettre en exergue une suffisance d'informations quant à l'effectiveness du modèle des 3LoD, et quels éléments pourraient influencer cet effectiveness. Cela s'explique notamment par le fait que le modèle ait été développé que très récemment. Il existe en effet un bon nombre de ressources, émanant principalement d'organismes et d'entreprises internationales, détaillant ce qu'est le modèle des 3LoD, et comment celui s'implémente dans les entreprises.

Deuxièmement, le modèle des 3LoD a été développé de base pour répondre à la crise financière de 2008-2009, et a donc été implémenté de manière obligatoire dans les banques et les assurances. Toutefois, en ce qui concerne les autres entreprises situées dans d'autres domaines d'activités, il n'a pas été obligatoire d'utiliser ce modèle. C'est pourquoi, il a été difficile, d'une part, de trouver des entreprises issues de domaines non financiers, ayant implémenté le modèle de manière complète, et donc d'autre part, de pouvoir étudier à part égale, l'effectiveness du modèle des 3LoD.

Il pourrait être intéressant, pour de futures recherches de réaliser une étude au sein d'un même secteur, tel que le secteur bancaire.

Troisièmement, toujours concernant la collecte des données, la taille de l'échantillon ne représente que 9 entreprises différentes, ce qui peut représenter des failles quant aux conclusions tirées. De plus, même si l'ensemble des interviewés connaisse le modèle des

3LoD, il a parfois été difficile d'établir un sens exact quant à l'objet de l'étude. Enfin, le modèle regroupant des fonctions hétérogènes, les questions posées pour les uns, n'étaient pas forcément pertinentes pour les autres. Bien que cela ait provoqué une divergence d'informations, dans certains cas, cela a pu limité le développement des réponses de la part des interviewés. Il n'a pas non plus pu être interviewé un Chief Operational Officer, ce qui aurait pu augmenter la qualité des réponses.

BIBLIOGRAPHIE

Agbejule, A., & Jokipii, A. (2009). Strategy, control activities, monitoring and effectiveness. *Managerial Auditing Journal, 24*(6), 500-522. Retrieved from: https://doi.org/10.1108/02686900910966503

Arndorfer, I., & Minto, A. (2015). The “four lines of defence model” for financial institutions. Financial Stability Institute (BIS), Occasional Paper N°11. Retrieved from https://www.bis.org/fsi/fsipapers11.pdf

Anderson, D., & Eubanks G. (2015). Leveraging COSO across the three lines of defense. The Institue of Internal Auditors. Retrieved from https://www.coso.org/Documents/COSO-2015-3LOD.pdf

Arwinge, O. (2013). *Internal control: A study of concept and themes*. Berlin : Springer. DOI: 10.1007/978-3-7908-2882-5

BIS. (2011). Bank for International Settlements: Principles for the Sound Management of Operational Risk. Retrieved from https://www.bis.org/publ/bcbs195.htm

BIS. (2015). The "four lines of defence model" for financial institutions. Retrieved from https://www.bis.org/fsi/fsipapers11.pdf

Banque Nationale de Belgique. (2018). Circulaire Coupole Système de Gouvernance. Retrieved from https://www.nbb.be/fr/supervision-financiere/controle-prudentiel/domaines-de-controle/entreprises-dassurance-et-de-6

Beasley, M., Hermanson, D., & Viscelli, T. (2017). The Integration of ERM and Strategy: Implications for Corporate Governance. *Accounting Horizons, 31*(2), 69-82. DOI: 10.2308/acch-51692

Bouquin, H. (2005). Herméneutiques du contrôle. Comptabilité et Connaissances. Retrieved from https://halshs.archives-ouvertes.fr/halshs-00581134

Bouquin, H. (2004). *Le contrôle de gestion (6è éd.).* Paris : Presses Universitaires de France

Bowling, D., & Rieger, L. (2005). Making Sense of COSO's New Framework for Enterprise Risk Management. *Bank & Accounting Finance, 18*(2), 29-34. Retrieved from https://www.superbessaywriters.com/wp-content/uploads/2017/01/week_2_article.pdf

Cappelletti, L. (2006). Vers une institutionnalisation de la fonction contrôle interne ?. *Comptabilité – Contrôle – Audit, 12*(1), 27-43. DOI : 10.3917/cca.121.0027

Casualty Actuarial Society. (2003). Overview of Enterprise Risk Management. Retrieved from https://www.casact.org/area/erm/overview.pdf

Committe of Sponsoring Organizations of the Treadway Commission. (2004). Enterprise Risk Management - Integrated Framework : Executive Summary. Retrieved from https://www.coso.org/Documents/COSO-ERM-Executive-Summary.pdf

Committe of sponsoring Organizations of the Treadway Commission. (2013). Internal Control - Integrated Framework : Executive Summary. Retrieved from https://na.theiia.org/standards-guidance/topics/Documents/Executive_Summary.pdf

Corbin, J., & Strauss, A. (2015). Basics of Qualitative Research: Techniques and Procedures for Developping Grounded Theory (4è éd.). USA : SAGE

Curkovic, S., Scannell, T., & Wagner, B. (2013). ISO 31000:2009 Enterprise and Supply Chain Risk Management: A Longitudinal Study. *American Journal of Industrial and Business Management, 3*, 614-630. Retrived from http://dx.doi.org/10.4236/ajibm.2013.37072

Davies, H. & Zhivitskaya, M. (2018). Three Lines of Defence: A Robust Organising Framework, or Just Lines in the Sand ?. *Global Policy, 9* (1), 34-42. doi: 10.1111/1758-5899.12568

Decaux, L. (2017). Risk Management, Internal Control and Auditing. Syllabus, Louvain School of Management.

Dickinson, G. (2001). Enterprise Risk Management: Its Origins and Conceptual Foundation. *The Geneva Papers on Risk and Insurance, 26*(3), 360-366. Retrieved from https://search-proquest-com.proxy.bib.ucl.ac.be:2443/docview/902458611?pq-origsite=summon

Dugan, M., Heier, J., & Sayers, D. (2005). A century of debate for internal controls and their assessment: a study of reactive evolution. *Accounting History, 10*(3), 39-70. Retrieved from https://doi-org.proxy.bib.ucl.ac.be:2443/10.1177/103237320501000303

Ebondo Wa Mandzila, E., (2004). *La contribution du contrôle interne et de l'audit au gouvernement d'entreprise (Doctoral dissertation)*. Université Paris XII Val de Marne, Paris. Retrieved from http://halshs.archives-ouvertes.fr/tel-01202572

Ebondo, E., & Pigé, B. (2002). L'arbitrage entreprise/marché : Le rôle du contrôle interne, outil de réduction des coûts de transaction. *Comptabilité - Contrôle - Audit, 8*, 51-67. DOI: 10.3917/cca.082.0051

ECIIA, & FERMA. (2011). Guidance on the 8th EU company law directive, article 41. En ligne : http://www.ferma.eu/sites/default/files/inline-files/eciia-ferma-guidance-on-the-8th-eu-company- law-directive.pdf

ECIIA, & FERMA. (2011). Guidance on the 8th EU company law directive, article 41: Part 2. En ligne: http://www.eciia.eu/wp-content/uploads/2013/09/Blog-4.4-Avoid-reg-part-2.pdf

Eklund, T., Jokipii, A., & Lansiluoto, A. (2016). Internal control effectiveness - a clustering approach. *Managerial Auditing Journal, 31*(1), 5-34. DOI: 10.1108/MAJ-08-2013-0910

Ernst & Young. (2013). Maximizing value from your lines of defense. Insights on governance, risk and compliance. Retrieved from http://www.ey.com/Publication/vwLUAssets/EY-Maximizing-value-from-your- lines-of-defense/$File/EY-Maximizing-value-from-your-lines-of-defense.pdf

Financial Reporting Council. (2016). The UK Corporate Governance Code.

Gordon, L., Loeb, M., & Tseng, C-Y. (2009). Enterprise risk management and firm performance: A contingency perspective. *Journal Accounting and Public Policy, 28*(4), 301-327. DOI: 10.1016/j.jaccpubpol.2009.06.2006

Gumb, B., & Noël-Lemaître, C. (2007). Le rapport des dirigeants sur le contrôle interne à l'épreuve de l'analyse de discours. *Comptabilité – Contrôle – Audit, 13*(2), 97-126. DOI : 10.3917/cca.132.0097

Gumb, B., & Noël-Lemaître, C. (2006). Le contrôle interne au travers des représentations que s'en font les dirigeants de groupes du CAC40 : Une étude exploratoire.

Grose, V-L. (n.d). Five Weaknesses of Enterprise Risk Management. Omega Systems Group Incorporated. Retrieved from https://www.prweb.com/releases/2013/3/prweb10569791.htm

Hwang, B-G., Pheng Low, S., & Zhao, X. (2015). *Enterprise risk management in international construction operations*. Singapour : Springer. DOI: 10.1007/978-981-287-549-5

IIA. (2013). Prise de position de l'IIA : Les trois lignes de maîtrise pour une gestion des risques et un contrôle efficaces. Retrieved from https://na.theiia.org/translations/PublicDocuments/PP%20The%20Three%20Lines%20of%20Defense

Imbert, G. (2010). L'entretien semi-directif : à la frontière de la santé publique et de l'anthropologie. *Recherche en soins infirmiers, 3*(102), 23-34. En ligne : https://www.cairn.info/revue-recherche-en-soins-infirmiers-2010-3-page-23.html?contenu=article

Kinney, W. (2000). Research Opportunities in Internal Control Quality and Quality Assurance. *Auditing*, 83-90.

Khter R., & Othman, M. (2013). Cobit Framework As a Guideline of Effective IT Governance In Higher Educaton : A Review. *International Journal of Information Technology Convergence and Services, 3*(1), 21-29. DOI: 10.5121/ijitcs.2013.3102

Klotz, M. (2015). Implementing corporate governance with the "lines of defense model". Trends in the World Economy, 7 Real Economy and Financial Sector in the Company World (pp. 53-68). En ligne: http://wneiz.pl/nauka_wneiz/twe/7-2015/twe-7-53.pdf

Krishnan, J. (2005). Audit Committee Quality and Internal Control: An Empirical Analysis. *The Accounting Review, 80*(2), 649-675. Retrieved from http://www.jstor.org/stable/4093072

Lalonde, C., & Boiral, O. (2012). Managing risks through ISO 31000: A critical analysis. *Risk Management, 14*(4), 272-300. Retrieved from https://www.jstor.org/stable/23351513

Leech, T., J., & Hanlon, L., C. (2016). *Three lines of defense versus five lines of assurance: Elevating the role of the board and CEO in risk governance*. Canada: John Wiley & Sons. Retrieved from http://riskoversightsolutions.com/wp-content/uploads/2011/03/3LoDvs5LoA-Elevating-the-Role-of-the-Board-and-CEO-Final-TLeech- LHanlon.pdf

Liebenberg, A., & Hoyt, R. (2003). The Determinants of Enterprise Risk Management: Evidence From the Appointment of Chief Risk Officers. *Risk Management and Insurance Review, 6*(1), 37-52. Retrieved from https://search-proquest-com.proxy.bib.ucl.ac.be:2443/docview/209605386/fulltextPDF/C6163725748B4ED8PQ/1?accountid=12156

Lyons, S. (2015). Entreprise risk management and the five lines of corporate defense. *The Journal of Enterprise Risk Management, 1*(1). Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2711229

McCrae, M., & Balthazor, L. (2000). Integrating Risk Management into Corporate Governance: The Turnbull Guidance. *Risk Management, 2*(3), 35-45. Retrieved from https://www.jstor.org/stable/3867838

Maijoor, S. (2000). The Internal Control Explosion. *International Journal of Auditing, 4*(1), 101-109. DOI: 10.1111/1099-1123.00305

Mouzas, S. (2006). Efficiency versus effectiveness in business networks. Journal of Business Research, 59, 1124-132. DOI 10.1016/j.jburses.2006.09.018

Renard, J. (2013). *Théorie et pratique de l'audit interne* (8è éd.). Paris : Eyrolles

Seago, J. (2015). Defense in depth: Organizations that have adopted the three lines model experience collaborative opportunities to address risk. Internal Auditor. Retrieved from https://www.iia.nl/SiteFiles/IA/ia201510-dl2.pdf

Sébéloué, S., & Zanvit, C. (2015). Les métiers de conformité dans la banque. Les études de l'Observatoire. Retrieved from : www.observatoire-metiers-banque.fr/f/etudes/sf/plus/s/metiers_conformite

Spira, L., & Page, M. (2010). Regulation by disclosure: the case of internal control. *Journal of Management and Gouvernance, 14*(4), 409-433. DOI: 10.1007/s10997-009-9106-9

Spira, L., & Page, M. (2003). Risk Management: The reinvention of internal control and the changing role of internal audit. *Accounting, Auditing & Accountability Journal, 16*(4), 640-661. Retrieved from http://www.emeraldinsight.com/0951-3574.htm

Van de Poel, K., & Vanstraelen, A. (2011). Management Reporting on Internal Control and Accruals Quality: Insights from a "Comply-or-Explain" Internal Control Regime. *Auditing: A Journal of Practice & Theory, 30*(3), 181-209. DOI: 10.2308/ajpt-10052

Whitman, A. (2015). Is ERM Legally Required? Yes for Financial and Governmental Institutions, No for Private Enterprise. *Risk Management and Insurance Review, 18*(2), 161-197. DOI: 10.1111/rmir.12045

Wilson, M., Wnuk, K., Silvander, J., & Gorschek, T. (2018). A Literature Review on the Effectiveness and Efficiency of Business Modeling. *E-Informatica Software Engineering Journal, 12*(1), 265-302. DOI: 10.5277/e-Inf180111

Zhivitskaya, M. (2015). The practice of risk oversight since the global financial crisis: closing the stable door? PhD thesis, The London School of Economics and Political Science (LSE)

de Zwaan, L., Stewart, J., & Subramaniam, N. (2009). Internal audit involvement in enterprise risk management. *Managerial Auditing Journal, 26*(7), 586-604. DOI: 10.1108/02686901111151323