

ANNEXES

1. Annexe 1 : Interview n°1

2. Explication du sujet du mémoire

3. Présentation de l'interviewé, de son parcours, de son rôle dans son entreprise et de son entreprise

Dans mon entreprise, je suis responsable du contrôle interne. Donc ça veut dire qu'avant, préalablement il n'y avait pas de contrôles. En fait ils avaient juste ce qu'on appelle des dispositifs de première ligne.

Des dispositifs de première ligne qui, j'ai envie de dire c'est assez classique à partir de moment où l'environnement de contrôle n'était pas encore mature, donc je suis en train d'essayer de développer cette maturité, c'est qu'au fait les contrôles n'étaient pas toujours faits en temps ou en heure, ou ce genre de chose, par un manque de temps. Parce que en plus de ça on vient changer d'outil, en 2016, je suis arrivé en 2017, mais en 2016, ils ont décidé pour des raisons économiques, ils n'ont pas eu le choix, ils ont dû s'adapter à un nouvel outil assez rapidement.

Donc du fait qu'on passe d'un ancien outil à un autre, ils ont du travailler sur tout un moment sur deux outils, l'ancien et le nouveau. Du coup, l'ancien outil au niveau des contrôles était super bien développé, mais donc dès qu'on passe sur le nouveau, ça prend du temps pour l'analyse, etc... Il n'y avait pas vraiment non plus une fonction contrôle interne au sein de l'entreprise.

Cette fonction là est reliée à une équipe finance, dont je fais partie, mais c'était lié à tout ce qui est "reserving". C'est-à-dire qu'au fait, normalement le secteur de l'assurance, impose un cadre de contrôle, Solvabilité 2, et donc dans ce cadre à toutes les entités du groupe, sont imposées à toutes ces entités, un cadre de contrôle interne.

Dans ce cadre de la finance, donc une personne de la finance qui était mon responsable d'équipe de l'époque, faisait tous des contrôles sur tout ce qui était vraiment le test de notre solvabilité. Donc on l'appelle "contrôleur interne". Mais il n'y avait que, entre guillemets, que des contrôles sur l'aspect Solvency 2, qui était contrôlé, parce que lui c'est vraiment de la seconde ligne de défense sur la Solvency 2. Mais il n'y avait pas vraiment de contrôle interne sur tous les autres aspects business.

Il y avait les contrôles de dispositifs de première ligne, niveau de tout ce qui était souscription, au niveau achats de produits, d'assurance, de conseils, de respect des procédures, si jamais il faut faire quelque chose à la demande d'un client, suivi des projets IT, suivi des ressources humaines, ... Il y avait des dispositifs de première ligne, mais de par la faible taille de l'entreprise, parce que tout le monde pense que notre entreprise est grande, mais il ne faut pas oublier que c'est scindé. Il y a le pôle assistance, le pôle "club" et le pôle "assurance", qui n'est uniquement responsable de la branche auto, moto, et habitation. Du coup, du fait de par cette disparité, mais c'est voulu en fait, c'est que le groupe a racheté notre filiale pour avoir ces disparités, puisque nous on est "direct". De par cette disparité, le groupe s'est dit "très bien, on sait qu'on va acheter une compagnie de direct, si jamais nos clients parce que, c'est vrai qu'évidemment, on est moins cher, on espère qu'il va retourner chez nous".

Moi je suis donc responsable de tout ce qui est 2ème ligne de défense en effet.

4. Comment analysez-vous justement l'interaction avec la première ligne de défense ?

Donc là c'est ce qui serait intéressant pour votre mémoire je pense, moi je viens d'une entreprise qui avait un framework de contrôle interne très mature, où je suis arrivé en quelque chose, quand je parle de première ligne, de seconde ligne, à un dispositif de second ligne qui était quasi inexistant, sauf ce qui était Solvabilité.

Donc là bas, je suis arrivé et ... "Bonjour est ce que le contrôle interne ?". Et donc la ça fait bientôt deux ans que j'y suis donc j'ai encore beaucoup de travail...

Donc la première chose que j'ai dû faire au niveau des premières lignes c'est déjà leur expliquer qu'un dispositif de deuxième ligne n'était pas un audit. Parce que tout le monde et même dans leur typologie de contrôle, il disait "on fait un audit" mais évidemment ce n'est pas la même chose.

Du coup la première phase que j'ai dû faire, ce sont des sessions d'informations, en disant : le dispositif de première ligne c'est vraiment la maîtrise des risques opérationnels, la maîtrise des risques que la première ligne à identifier ; la seconde ligne de défense, donc pour le reporting de contrôle interne, c'est s'assurer que les contrôles sont fait en temps et en heure, qui couvrent bien le risque, qui sont correctement effectués, et éventuellement s'il y a des choses qui ne sont pas identifiées ou contrôlées, de renforcer la première ligne pour faire du pilotage ; l'auditeur interne lui vient, il a une mission et s'il y a des aspects de contrôle interne qui veut vérifier, là il s'adressent à moi.

En effet tout le monde pense qu'un auditeur va tout regarder, mais non, il va regarder ce qui est en fonction de sa mission, sur un périmètre spécifique, si c'est juste pour vérifier la sécurité physique, tous les aspects contrôle interne business, il ne va même pas regarder.

Donc ça a été la première phase, donc vraiment information et sensibilisation, faire comprendre à la première ligne de défense que c'est important d'avoir un pilotage, de leurs propres contrôles, et que ça doit être chez eux.

La deuxième phase, évidemment, c'est toute une phase d'analyse, donc alors on passe en revue tous les contrôles et on s'assure que ça couvre un risque, que ça couvre le risque

identifié et donc du coup, mais encore une fois il y avait des manuels, mais pas vraiment des procédures internes.

Donc du coup bah là encore une fois là par manque de temps, c'est moi qui l'ai fait pour eux. J'ai fait beaucoup de premières lignes dans un premier temps, je pense qu'on n'avait pas le choix. Donc en tant que première ligne, j'écris les procédures, donc ça veut dire vraiment pour tous les dispositifs opérationnels, dans un premier temps, je me tenais à côté, je disais "Comment tu fais tel processus ?", et on écrit.

Juste rappeler, vous voyez vraiment, la première ligne, on a ce risque qui est couvert par un processus la seconde vous ne trouvez pas indépendance évidemment derrière si on veut de la troisième.

Du coup là je leur ai expliqué les avantages d'avoir une procédure opérationnelle. Mais donc comment je l'ai fait : il y a un petit fichier excel.

Ce n'est pas une vraie procédure, ça c'est parce qu'à l'époque, j'étais arrivé et ça faisait à peine deux mois que c'était là. Je connaissais pratiquement aucun processus, voilà donc du coup j'en ai écrit une comme exemple, en leur disant que tiens voilà ce que ça pourrait être. Donc en fait à mon sens pour avoir une procédure, déjà il faut dire ça couvre quel processus, une petite description juste assez rapide en disant voilà ce que ça fait, un historique pour éventuellement si jamais il y a des adaptations, ... et c'est parce que parfois ça peut arriver, dans un process, il y a un changement, une adaptation, un nouveau déploiement d'informatiser, du coup, les choses qu'on doit plus faire.

C'est informatisé alors on décide d'un autre mode de fonctionnement. Mais avoir l'historique c'est toujours utile parce que parfois, quand on a un audit, on sait retomber dessus. Et puis là, on a vraiment la description du contrôle, on part du principe que c'est une ligne. Donc normalement dans un flux, il y a toujours des moments où ça fait

comme ça, par exemple le client nous contacte, hop ils appellent pour une offre, très bien, on continue l'offre, puis en plein milieu de son offre, il a une question sur une autre chose, hop ça redescend.

Du coup c'est là où on a mis en place des extensions. Donc ça veut dire, ici le client, il n'appelle pas pour une offre, il appelle pour autre chose, qu'est-ce que doit faire l'agent ?

Dans cette procédure, on peut déjà, mais bon ce n'est pas évidemment indispensable, si oui ou non, on peut déjà mentionner là s'il y a un contrôle opérationnel, ou et si c'est oui ou non un contrôle de premier niveau. Le but par la suite, j'ai réussi à mettre en place sur tous les contrôles de premier niveau encore une fois...

En fait pour chaque contrôle qu'est-ce qu'ils disent, le contrôle on le fait une fois par an, deux fois par an, une fois par an, une fois par moi, ... Qui le contrôle, qui réalise l'activité de contrôle, qui contrôle, ça c'est juste pour prouver que celui qui fait le process n'est pas celui qui contrôle.

Clairement, évidemment, quand c'est au sein des opérations, c'est le team leader qui contrôle ces gens. Si c'est un expert, un expert dit "bon ok c'est moi, agent expert, qui vais contrôler mon agent". On dit quel risque on couvre, on dit vite en deux mots en quoi consiste le contrôle, ça c'est juste en termes d'audit ou pour moi pour comprendre si jamais. Et là on rentre un peu plus dans le détail, en disant vraiment qu'est ce qu'on fait, donc c'est à dire qu'est ce qu'on doit produire pour faire le contrôle, et si jamais on a trouvé des erreurs, comment est-ce qu'on les corrige. Donc là au moins, normalement il est vraiment dit où se trouve le lieu des évidences du contrôle et donc pour moi, en seconde ligne, qu'est-ce que je fais, je vais directement dans les évidences, et je m'assure que tout ça a été produit. Donc ça c'est vraiment tout ce que j'ai montré là, c'est la première ligne.

Moi en tant que deuxième ligne de défense, j'ai mes propres procédures, donc là c'est vraiment, on a un processus, on a le risque, on a un dispositif, ça reprend le récapitulatif du fameux fichier word, et voilà comment moi je le contrôle. En général comment je définis les fréquences de contrôle, c'est en fonction encore une fois, vu que c'est du pilotage, de la maturité du dispositif.

Donc si je veux faire un contrôle, à fréquence trimestrielles et que je vois, que deux fois, des choses qui n'ont vraiment pas, là je vais le faire plus souvent. Si par contre je le fais deux fois et que les deux fois, il va être super, je vais peut-être encore éventuellement le faire une fois en trimestre, mais l'année suivante, je le fais une fois tous les deux ans. Donc c'est en fonction de la maturité du processus.

Clairement, c'est ça qui est bien, comparé à mon ancienne entreprise, eux ils voulaient qu'on fasse des contrôles quoi qu'il arrive. Les fréquences étaient définies et on n'en sortait pas. 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. Moi j'allais trouver mon big boss en disant "Moi je sers à quoi ici, à part dire que tout va 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.

Ici l'avantage, encore une fois c'est l'avantage de quelqu'un qui débute, enfin quand on engage quelqu'un pour le faire, c'est qu'on crée comme on veut, et donc du coup moi c'est comme ça que je le fais. Quand ça va bien, on ne me voit pas, mais quand ça va mal, là je suis un peu plus intrusif et je contrôle plus fréquemment.

Et donc je dis là qu'est ce que je dois avoir comme sources documentaires, donc qu'est ce que la première de défense doit me fournir, et comment moi je le contrôle, et j'essaie toujours "Existence et suivi". Donc là c'est vraiment le compte rendu. Donc "existence", là ça fait sous forme de question maintenant c'est parfois aussi operating, c'est-à-dire, niveau "existence", qu'est-ce qu'ils ont dit qu'ils devaient faire qu'il le font, par exemple ici là ça pour le suivi des paiements, donc ok est ce qu'ils ont fait leur extraction, est-ce

que ça a été transmis au responsable équipe, est-ce qu'ils l'ont bien fait sous la fréquence définie, trois petites questions oui oui ok tout va bien.

Alors là c'est moi qui prends un échantillon et qui teste, et je dis déjà à l'avance, mais ils peuvent savoir, ce n'est pas un problème, et je dis ce que je fais. Il y a un rating angle et à la fin, voilà ici là je dis, et si j'ai quelque chose, je mets un compte rendu. Je peux vous montrer si vous voulez, un exemple de toute la chaîne.

Donc moi c'est pas au fait, typiquement on a deux outils, on a un outil qui s'occupe de tout la gestion des contrats et on a un autre outil, malheureusement les deux outils sont pas liés entre eux, qui sont les outils de paiement. À partir du moment, où les clients nous fournissent ce qu'on appelle une domiciliation SEPA, quand le gestionnaire est en train d'encoder, quand il a fini, s'il manque un SEPA, il doit aller dans la pratique dans la plateforme de paiement pour encoder le compte bancaire et créer le SEPA. Et donc ce que moi j'avais identifié à l'époque, c'était que souvent les clients transmettaient les domiciliations SEPA, et qu'on les encodait pas. Alors tout en soit le processus n'est pas trop grave parce qu'il y a un courrier qui envoyait en automatique à partir du moment où on n'a pas reçu le paiement. Mais pour le client, clairement, c'est ennuyant. Il se dit moi j'ai donné une domiciliation, je ne m'attends pas à réencoder manuellement les paiements tous les mois. Et donc ça crée de la frustration chez les clients.

Le fait c'est qu'encore une fois on a vu qu'on était dans le cas d'un nouvel outil c'était mal fait. Donc du coup qu'est-ce que j'ai implémenté, parce que là ça c'est vraiment moi qu'il ait fait, d'A à Z, c'est un reporting qui dit tous les mois, mais tiens voilà toutes les offres, qui basculent en contrat, où il y a un paiement mensuel à réclamer, et où il n'y a pas de domiciliations SEPA, dans l'outil de paiement.

Donc du coup, une fois par mois maintenant il y a un rapport qui sort. Donc moi qu'est-ce que je leur dis au niveau des documents, qu'est-ce que je dois avoir, mais je dois avoir les extractions mensuel, qui en plus de ça sont générés, par une équipe de reporting, donc ça

veut dire que c'est eux qui font tout le reporting financier, donc toute l'équipe qui doit produire, c'est une équipe spécifique qui le fait, et ça c'est top pour moi parce que c'est vraiment pas les équipes business qui doivent le faire.

C'est directement une équipe spécifique et en plus c'est automatisé, ils ont un programme qui s'appelle SQL, le programme sort normalement tous les mois.

Donc avantage pour la première ligne, c'est est-ce que les extractions ont été produites, ce sera toujours oui. Est-ce que oui ou non, est-ce qu'on a analysé le fichier, est ce qu'on est rentré dedans, est-ce qu'on a été regardé si oui ou non on a reçu la domiciliation, est-ce qu'on a pris les actions qu'il fallait. Donc moi, des contrôles de l'existence, je m'assure que si oui ou non, ils ont bien ouvert le fichier, que si oui ou non ils ont bien fait le suivi. Quand on prend le compte rendu : voilà donc là je leur rappelle qu'au départ c'était moi qui le faisais, cela c'était quand j'ai identifié le problème, et la direction m'a dit très bien, merci d'avoir identifié le problème et on est dans un cadre ou en train de former nos agents, etc...

Et puis après, un moment où le virement faut que ça soit repris par la première ligne de défense. Donc là du coup depuis avril, on a pris la décision avec la direction, maintenant c'est fait par eux directement. Donc là c'est vraiment une seconde ligne de défense, comme contrôle, donc là ce que je me suis rendu compte, c'est qu'ils avaient fait des actions dans l'outil, qu'ils les avaient pas documentés. Donc ils ont pas juste mis dans leur fichier, bon ok ça on a adapté, ça on n'a pas dû faire, j'ai aucune ce qu'on appelle, piste d'audit. C'est la raison pour laquelle pour moi l'existence, elle est pas trop mal parce qu'il y a quand même eu un exercice, d'aller vérifier, etc... mais il n'y a pas de suivi. Donc voilà c'est fait, mais comme c'est la première fois qu'ils le faisaient aussi, on n'allait pas rentrer dans les détails.

Et au niveau du suivi est donc là vraiment je leur fais un détail, en leur disant voilà, il y avait 94 cas, ici ok ça c'est top ça a été bien fait, ils ont correctement remplis les mandats

etc... Il y en a 21 ans que j'ai identifiés où ils ont rien fait, donc il y a eu, il y a eu un gros bang été transmis par le client mais il n'a pas été encodé. "Car Security", donc là ce parce qu'on a un partenaire qui s'appelle "car security", donc en fait si vous achetez une toyota demain, on va vous faire un contrat assurance en notre nom. Ça c'est ce qu'on appelle un produit B2B, donc c'est-à-dire qu'en fait, vous pensez que vous êtes assurés chez toyota ou chez renault et en fait c'est chez nous que vous êtes assurés.

Donc là on l'envoie directement aux partenaires qui font ces actifs, il y a quand même un truc où on a encodé un mauvais compte, et donc là il y en a un ou là c'est le client qui a mal transmis son mandat, voilà donc la pas de chance pour l'agent, il devait prendre contact avec le client. Donc voilà, donc ça je transmets ça aux responsables d'équipes et au manager de l'équipe en charge et après je les challenge sur la mise en place d'un plan d'action.

5. Justement y-a-t-il une troisième ligne de défense au sein de l'entreprise ? Est-ce que l'audit interne est présent ?

Alors oui, donc nous, comme on est une petite boîte, 180 personnes, on n'a pas vraiment de service d'audit interne. Mais c'était la même chose dans ma précédente entreprise, on était 80. Donc au fait qu'est ce qui se passe dans ce genre de cas, c'est vu qu'on fait partie d'un groupe, nous on a délégué notre audit interne au groupe.

Donc c'est le groupe qui vient chez nous auditer, et ils viennent. Donc oui on a une troisième ligne de défense mais encore une fois comment ça se passe ; l'aspect gouvernance, les auditeurs définissent chaque année leur plan d'audit, validé par le groupe, qui valide le plan de contrôle, et dedans leurs plans d'audit des entités qui font partie du groupe. Il y a nous, et encore d'autres entités.

Donc derrière, sur cette base, les auditeurs viennent chez nous. C'est bien parce que, on est audité tous de la même manière. Ce qui est moins bien, mais ce n'est pas grave, c'est pour ça que je suis arrivé, c'est que clairement les auditeurs n'ont pas la connaissance de toutes les entités et de toutes leurs spécificités.

Donc voilà il y a à boire et à manger, mais nous on ne voyait pas l'objectif de mettre l'audit à 180 personnes. Nous sommes une petite structure, qui, il ne faut pas oublier aussi, qu'on utilise énormément d'outils, du groupe dans son ensemble, et on remonte énormément de chose au groupe.

Tout ce qui est calculs de solvabilité, c'est consolidé au niveau du groupe.

Donc voilà c'est normal qu'on n'ait pas pris sa décision d'avoir un morne. Maintenant clairement voilà ils viennent quand ils sont sur base d'une mission. Pour exemple, l'année prochaine on ne le verra pas. Parce qu'ils sont tellement venus durant ces premières années qu'ils ont tout couverts.

6. Comment se passe l'interaction avec les organes de gouvernance justement ?

On a évidemment un comité d'audit, il faut savoir qu'au niveau de la banque nationale belge, on nous impose d'avoir des organes de contrôle, donc impose donc c'est d'ailleurs pour ça qu'ils m'ont engagé, dans le but d'avoir un contrôleur interne indépendant, d'avoir un comité d'audit. Donc on a ce qu'on appelle le board, où on a les administrateurs, les auditeurs et le comité de direction qui se réunissent quatre fois par an. Le comité a pour responsabilité de valider nos process,

Donc chaque année Solvency 2, c'est très long comme process, nous impose de revoir une procédure de remettre à jour, la législation de fonctionnement, les groupes les guidelines

du groupe, chaque fois qu'on fait une modification, on doit leur soumettre nos procédures et le board doit valider. Chaque année, il y a ce qu'on appelle un rapport du compliance officer, qui doit produire beaucoup de documents également, donc le comité d'audit est quand même souvent là. Et on a également des réviseurs externes, qui viennent évidemment comme toute entreprise certifier les comptes. Et également, ils viennent une fois par an, qualifié le dispositif de contrôle. Une fois par an on a quand même l'audit externe qui vient.

6.1 Vous la verrez comme une ligne de défense qui pourrait être intégrée au modèle ?

À prendre en compte, un auditeur externe est là pour certifier les comptes, et donc il est juste là pour identifier le seuil de matérialité identifié, s'assurer que oui ou non on est solvable. Donc on est obligé de l'avoir, parce que la banque nationale belge nous l'impose. C'est normal qu'il soit là mais on comprend qu'ils n'ont pas le temps de rentrer vraiment dans le vif du sujet.

Et pour vous dire que, ce n'est pas qu'ils n'ont pas de plus-value, loin de là, chaque fois qu'ils détectent des choses au niveau comptable pur, ils ont énormément aidé. Maintenant sur pure dispositif de contrôle, avant vu qu'ils n'étaient pas là, il venait tester le contrôle interne, ils ont vu l'ampleur des dégâts, mais le fait qu'il n'y avait pas de seconde ligne de défense, le fait qu'il savait tout ça, on n'a jamais reçu de recommandations d'un auditeur externe, donc en disant il faut mettre en place les contrôles, il faut mettre en place des dispositifs de renforcement. Eux ils basent plus ça sur un entretien.

C'est vraiment parce que la première année ou moi, j'ai eu à faire à un auditeur externe chez PWC, il n'y avait pas de seconde ligne de défense, j'étais seulement en train de renforcer la première ligne, j'avais quelques petits contrôles au sein de la seconde ligne

de défense mais rien d'extraordinaire, ils sont arrivés ça faisait peine 6 mois que j'étais là. Et sur base de l'entretien, on leur a expliqué et ben qu'est-ce qu'on allait mettre en place, quelque un plan d'action, pourquoi, comment, etc... donc on leur effectue une réunion préalable, en leur expliquant notre contexte, donc j'ai envie de dire, eux, ils valident ou pas, mais ce n'est pas leur rôle de nous challenger.

Ca, c'est le rôle de l'audit interne, qui justement, eux, sont missionnés pour un audit de souscription. Ils ont vu tout ce qui a été fait au niveau seconde ligne de défense, ils ont vu tout ce qui a été fait au niveau de la première ligne, et ils ont mis des recommandations sur ces sujets. C'est normal en soit, un auditeur externe est juste là pour certifier des comptes, certifiés un mode de fonctionnement éventuel, éventuellement identifier les dysfonctionnements mais ce n'est pas lui qui va dire "Vous ne respectez pas telles ou telles règles, ..." ce genre de choses avec les mandats SEPA, ce n'est pas leur travail.

A mon sens vraiment les réviseurs externes, ils sont vraiment là pour, même si encore une fois ils sont arrivés et on leur a expliqué tout ce que nous, on avait identifié comme problème dans notre outil, ce qu'on allait mettre en place comme plan d'action, et derrière eux ils valident le plan d'action mais ils ne vont pas nous challenger. Ils vont revenir l'année d'après et demander ce qu'on a fait. On va leur dire ce qu'on a fait et ce qui a été fait ou pas fait, sur cette base-là, ils vont faire leurs audits.

Donc en audit interne, j'ai une recommandation, niveau low, medium ou high, et fonction de celle-ci je devrai agir rapidement ou non. Ce qui est plus intrusif.

Cela permet vraiment au CEO, et c'est le but, de le rassurer. Même si au bout du compte, toutes ces fonctions de contrôle, d'audits, de contrôle interne, d'auditeur externe, servait plus à faire du management de signaux qu'autre chose. En effet, un CEO ça rassure, un conseil d'administration ce n'est pas leur job.

7. Pensez-vous que trop de contrôles tuent le contrôle ?

Moi je suis entièrement d'accord. Parce que, par exemple, auparavant j'étais responsable d'équipe. Clairement dans ma précédente boîte, on était une petite boîte, on est né en 2008. Au début on fonctionnait vraiment comme des cowboys entre guillemets, sans vraiment de contrôles. Parfois quand il fallait passer une opération qui respectait pas vraiment les procédures, on allait vite trouver l'IT, qui débloquent l'accès pour passer l'opération puis le re-bloquait. Parfois pour aller plus vite, pour plus vite répondre aux clients, on ne respectait pas toujours les bonnes procédures, les bonnes manières de faire.

Donc quand on a commencé à installer le cadre de contrôles dans cette entreprise, clairement tout le monde a vu ça comme quelque chose d'intrusif, parce qu'il existait trop de contrôleurs internes par rapport au nombre d'employés. On avait vraiment un contrôleur interne par équipe, parfois deux, et ils venaient vraiment de manière très intrusive, en disant que ce n'est pas fait, etc... D'ailleurs que s'ils mettaient des rapports, etc... là c'était trop.

Voilà exactement la situation dans laquelle on se disait que trop de contrôles tuait le contrôle. Ce n'est pas évident à mettre en place et il faut du temps et il faut avoir à mettre en place pas mal de choses pour que ça roule et que ça fonctionne. Quand je dis "le contrôle tue le contrôle", c'est clairement ce fait selon moi ces première et deuxième lignes de défense, mais voilà ça dépend où est-ce qu'on veut mettre la barre. Si on veut juste quelqu'un qui lisent les contrôles, c'est fait, c'est fini, ça peut aller très vite. Maintenant à voir comment on veut challenger la chose.

A mon sens il y a un moment où la seconde ligne de défense, si tout roule dans la première ligne je ne vois pas trop où sont les plus-values. Dans ma précédente entreprise, tellement que tout roulait bien, comme je l'ai dit, j'avais 80 ou 90 contrôles par mois, tous étant super satisfaisant. Donc d'un point de vue de la première ligne, on est vu comme

quelqu'un qui est juste là pour dire que tout va bien. Donc où se trouve la plus value ? Donc pour le contrôleur ce n'est pas intéressant, mais pour la première ligne aussi.

Maintenant je comprends aussi le fait que si on n'a pas les gens derrière au niveau de responsabilité d'équipes, qui suivent leur contrôle, ça ne va pas. A mon sens si c'est suivi au niveau gouvernance, la première ligne, si le management de la première ligne est présent, alors la deuxième ligne, ce n'est pas qu'elle n'a pas de raisons d'être, mais à mon sens c'est quelque chose qui doit être juste du pilotage.

Maintenant tout dépend du contexte, si on a une petite boîte avec peu de dispositifs je comprends, maintenant si on est un gros groupe avec des milliers d'employés, je peux comprendre les dispositifs multiples. Pour une petite boîte à mon sens où ce genre de choses ça n'a pas beaucoup de plus values. Si, à partir du moment à l'implémentation, dès que ça roule, sauf s'il y a changement d'outil, sauf si il y a changement de fonctionnement, à mon sens ça n'a pas pu la nuire.

Pour des grosses entreprises qui pilotent des milliers de salariés, où il y a des centaines de dispositif, là je peux comprendre.

Clairement, notre entreprise a développé un cadre de contrôle interne, encore heureux nous n'y sommes pas soumis. Mais j'ai regardé un petit peu ce qu'ils demandent, je vais vous donner un bel exemple, les contrôles sur la fonction "conformité, officer", un de leur contrôle c'est "est-ce qu'un compliance officer a été nommé conformément aux règles de la banque nationale belge ?". Ca veut dire, est-ce que oui ou non, l'audit interne, le comité de direction, oui ou non à valider sa nomination. Nous on est une petite entité, le compliance officer, est là depuis 8 ans. Il n'y a donc pas de plus value de contrôle dans notre filiale, mais clairement dans notre groupe c'est important.

Tout dépend donc de la taille ,du contexte de l'entreprise et la complexité des process.

8. Selon vous, existe-t'il d'autres facteurs pouvant influencer positivement ou négativement l'effectiveness du modèle des trois lignes de défense ?

A mon sens vraiment, tout dépend encore une fois de la manière dont cela est perçu au niveau de la gouvernance, et à tous les niveaux. Et donc ça a été vraiment encore une fois, très difficile pour moi d'un environnement très structuré à un environnement peu développé, c'est qu'il faut du temps faire comprendre dans un premier temps la plus value. Et donc clairement quand il ya son propre CEO qui vous dit "c'est quoi un contrôle de deuxième ligne de défense?", là il y a du boulot. Même pendant l'audit, où elle comprenait pas vraiment la plus-value de mettre une deuxième ligne de défense,... voilà donc il y a quand même au niveau de la gouvernance voir comment c'est perçu.

À partir du moment où c'est perçu comme il faut quelqu'un pour le faire, est-ce qu'elle va réussir à avoir une plus-value, non. Si le management part du principe, que ça ne sert à rien, que c'est juste là parce que c'est rébarbatif et qu'il faut le faire.

Si voilà finalement on va dans un mode constructif, en se disant, on veut arriver à un objectif, où nos contrôles sont pertinents, ça aussi il faut essayer de mettre en place quelque chose de pertinent. Il faut aller plus dans le fond des choses, mais cela demande beaucoup d'énergies et beaucoup de temps. Mais tout ça ne se fait pas d'un claquement de doigt, et le désavantage c'est qu'il faut des outils pour. Pour le moment c'est moi j'ai tout fait à ma manière, mais il y a des outils de contrôle qui peuvent être là aussi, des outils de reporting, ...

2. Annexe 2 : Interview n°2

1. Explication du sujet du mémoire

2. Présentation de l'interviewé, de son parcours, de son rôle dans son entreprise et de son entreprise

Donc moi je suis indépendant et j'ai fondé ma société en 2016, en tout cas j'ai commencé mes activités d'indépendant en 2016, j'ai un passé d'auditeur interne, donc j'ai été consultant chez "Arthur & Densen" et puis j'ai fait aussi pas mal d'autres sociétés dans l'audit interne, dans la gouvernance, l'optimisation des processus et autres. Et donc ma volonté c'est d'apporter ce type de services à des organisations ou des entreprises qui n'ont pas des services d'audit interne, internalisé. Ou bien de venir en support des départements d'audit interne, ou encore d'assister le management dans le renforcement des systèmes de contrôle interne qui vont de l'optimisation des procédures jusqu'à dans la définition des contrôles internes dans certains processus. Parallèlement à ça, je donne également via une autre société de consultance des formations justement à la commission européenne sur tout ce qui risk management, contrôle interne et on parle de tout des trois lignes de défense à la commission européenne.

2.1 Vous avez donc exercé des postes dans les trois lignes de défense au final ?

En tout cas j'étais auditeur interne, qui est la troisième ligne de défense, j'ai fait des missions dans l'établissement des procédures, la deuxième ligne, et comme j'ai été longtemps consultant, la première ligne, disons pour moi elle est assez assez claire et je n'ai pas forcément appliqué ce genre de chose, quoique tout le monde finalement est concerné par cette partie du modèle.

3. En tant qu'auditeur interne, ou ex-auditeur interne, comment est-ce que tu pourrais identifier l'interaction qui existe entre la première et la deuxième ligne de défense ?

Je crois que c'est important d'abord de définir ce que chaque ligne fait.

Pour moi la première ligne de défense, c'est les personnes qui appliquent quelque part toutes les normes et qui font en sorte que le contrôle interne et les normes en matière de contrôle soient appliquées, telles qu'elles ont été établies par la seconde ligne, en tout cas c'est comme ça que je comprends le modèle, qui est finalement une espèce de supports transversal, qui définit qui doit faire quoi à quel moment, que ça soit au niveau financier, que ça sera au nouveau opérationnel, mais également au niveau IT.

Puisque pour moi la gouvernance IT, fait partie de cette deuxième ligne de défense, qui définit les systèmes de protection des données, d'accessibilité, ce genre de choses. Et la troisième ligne de défense, qui est l'audit interne, tous les organes de contrôle, audit interne, audit externe et éventuellement des auditeurs qualité pour tout ce qui concerne la qualité.

L'audit interne est censé contrôler la bonne application des normes de contrôle interne par la première ligne de défense, mais aussi vérifier que les normes qui ont été établies adressent bien tous les risques qui ont été identifiés et qu'il y a une efficacité dans le niveau de contrôle qui est bien en place. Et donc pour moi l'audit interne intervient souvent sur les deux autres, évalue si tu veux, les deux autres lignes et apporte des conseils et des recommandations sur l'amélioration des systèmes de contrôle interne, ou sur l'application des systèmes de contrôle interne.

3.1 Est-ce que cela a un impact sur la compagnie en elle-même, dans le contrôle des processus et la gestion des risques ? Est-ce que le système de gestion des risques peut être moins bien établi ?

Mais en fait le fait d'avoir un audit interne au sein de l'entreprise permet quelque part de systématiser la revue des processus, et la revue du système de contrôle interne. Quand il n'y a pas de audit interne, en fait, cette responsabilité est un peu répartie, chez tout le monde. Alors quand on a une entreprise relativement mature en termes de gestion de risque, tout le monde est conscient plus ou moins de ce qu'il doit faire, par contre, moi je constate que le niveau de maturité de ces organisations, de ces entreprises, parfois elle est relativement faible.

Je te prends l'exemple des hôpitaux que je connais assez bien parce que je travaille je fais des missions dans des hôpitaux. Il y a très très peu d'hôpitaux en wallonie qui ont un service d'audit interne. Et en fait ce que je constate, c'est qu'ils sont tellement le nez dans le guidon, qu'ils ne se posent pas forcément beaucoup la question sur le contrôle interne. Il y a des normes des normes médicales, il y a des normes financières, mais il n'y a pas une revue de processus qui est faite de manière structurée.

J'ai fait un audit dans un hôpital sur le processus achat par exemple. La demande partait du fait qu'ils avaient failli payer des factures à des escrocs, parce que le système d'autorisation, de modification des coordonnées des fournisseurs n'étaient pas bien définies, ce qui fait qu'ils ont reçu une demande d'un soi-disant fournisseur, qui avait changé de numéro de compte, qui disait de ne plus payer en belgique, mais en espagne, en pologne, un truc comme ça. Et la personne a failli le faire parce qu'elle a changé les coordonnées bancaires, ils ont réussi à arrêter le paiement juste avant qu'il parte, en se disant "C'est quand même un peu bizarre ce truc,...", ils se sont renseignés avec la banque et tout.

Cela veut dire qu'il n'y a pas d'évaluation, si tu veux, du risque à certains moments et donc il n'y a pas de prise d'actions par rapport à ce risque là. Ce qui fait que l'efficience de ces trois lignes en fait, n'est pas là, de manière globale, de manière structurée. Alors ils font un peu des trucs à droite et à gauche, mais c'est plus au niveau réactif qu'au niveau proactif. Ils se rendent compte d'un problème, qu'il faut modifier, qu'il faut renforcer la procédure ou le contrôle, etc... Mais de manière proactive il n'y a pas ce genre d'approche

en fait. Et c'est vraiment toute la différence entre une entreprise qui a pris conscience de ces risques et qui se dit "Oui, ok, il faut faire quelque chose de structuré" et ceux qui sont réactifs où ils fonctionnent un peu en fonction des événements qui surviennent.

4 À l'inverse, n'y a-t-il pas dans les entreprises trop de fonctions de risque, trop de contrôles, est-ce que cette tendance à établir trop de contrôles peut "tuer" le contrôle ?

Oui je vais te donner un exemple. J'ai été intérim manager, en 2009 et 2010. J'étais en charge de toute la gestion des marchés publics, dans lequel tu as un cahier spécial des charges, que tu envoies différents fournisseurs et puis tu as les réponses et puis il faut attribuer au marché.

Dans le cahier général des charges, en fait avant que ce cahier ne soit envoyé à toute une série de personnes il fallait qu'il y ait une quantité assez impressionnante de signature et d'autorisation d'approbation sur ce cahier général des charges. Je crois que le maximum que j'ai vu, c'était des dizaines d'approbations, une dizaine de personnes qui signait le cahier général des charges pour l'approuver. Et en fait ça dilue complètement le contrôle interne parce que le premier ou la première qui doit signer le cahier, se dit "Bon ok il y en a neuf derrière moi qui vont signer, et je vais le regarder mais voilà je signe j'ai pas le temps". Celui qui est au milieu se dit "Bon il y en a déjà quatre qui ont signé et il y en a encore cinq qui doivent venir derrière, je signe et quelqu'un d'autre fera mon boulot". Et le dernier s'est dit "bon il y en a neuf qui ont signés, pourquoi est-ce que moi je refusais le truc".

Et donc en fait on se rend compte qu'il y a une espèce de dilution du contrôle interne et plus personne n'est vraiment responsable du contrôle interne en tant que tel. Et donc une de mes actions, ça a été aussi de réduire drastiquement le nombre de personnes, parce que ça fait gagner en temps et ça améliore si tu veux la responsabilisation des gens. Il y a

ça dans énormément de grosses administrations, où tout le monde finalement veut mettre son grain de sel dans le contrôle mais plus personne ne l'est vraiment, du contrôle.

Je trouve que c'est simplement un challenge, c'est de trouver le juste équilibre entre avoir un nombre suffisant de personnes qui vérifient une action, tout en regardant l'efficacité et tout en faisant en sorte que le contrôle interne ait un sens.

5 Donc c'est ça un des rôles de l'audit interne, par exemple, c'est de vérifier justement cet équilibre au sein de l'entreprise ou peut-être pas du tout ?

Je pense de plus en plus que oui le rôle de l'audit interne a évolué et ça ne date pas d'hier, ça vient depuis pas mal de temps. Entre le fait de se dire "Oui, le contrôle interne tel qu'il a été défini, a bien été mis en place et oui le contrôle interne tel qu'il a été défini non seulement a bien mis en place mais efficace et efficient également". Et donc le rôle de l'audit interne, c'est aussi pour moi de dire "Vous avez trop de contrôles, donc ça grippe quelque part la machine par rapport au niveau de risque que vous avez". Je ne sais pas si tu as déjà vu cette matrice de risque "likelihood et impact", et de dire "Bon, ok, mes risques élevés se trouvent là. Après la question c'est dire quel est mon niveau de contrôle par rapport à ces risques-là ?"

Et donc c'est le rôle de l'audit interne d'attirer l'attention sur le fait qu'il y a une exagération ou trop de contrôles et de dire aussi si ces contrôles sont pas appliqués adéquatement en fait.

6. Par rapport aux organes de gouvernance, quel est le lien entre l'audit interne et l'organe de gouvernance ?

Alors en fait déjà l'audit interne, à priori, il doit être attaché au plus haut niveau fonctionnellement de la hiérarchie, pour avoir accès directement à ce plus haut niveau sans qu'il y ait de filtres. Tu peux difficilement rattacher l'audit interne au directeur financier, par -exemple, parce que s'il y a des recommandations sur la finance,

évidemment le directeur financier est en première ligne, et risque, entre guillemets, de bloquer certaines recommandations.

Déjà il faut que cet audit soit rattaché au plus haut niveau, généralement au secrétaire général, soit la direction générale. Après quand il y a un comité d'audit, l'audit interne doit rapporter régulièrement au comité d'audit qui est composée dans les "best practices" avec une ou deux personnes en interne mais également des gens extérieurs, qui ont une connaissance des principes de risques, qui ont une connaissance sur le principe de gouvernance, et des connaissances financières aussi. Puisque le rôle du comité d'audit, c'est pas seulement de revoir le travail l'auditeur interne mais aussi de voir aussi le travail de l'auditeur externe et les recommandations qui sont établies par l'auditeur externe.

Donc effectivement tu as un rattachement qui est double, mais il n'y a pas toujours de comités d'audit dans des entreprises. Il faut savoir qu'en Wallonie, maintenant, il y a eu le décret gouvernance, qui a été établi en avril 2018, qui impose à chaque organisme d'intérêt public et chaque intercommunale d'avoir un comité d'audit et qu'il y ait un rapport d'un auditeur interne, que celui-ci soit un employé de l'intercommunale, à ce comité d'audit de manière régulière.

Donc si tu veux il y a une double ligne en fait en matière de reporting.

6 Justement, le lien avec l'audit externe, est-ce qu'intégrer l'audit externe au modèle des trois lignes de défense, permettrait d'améliorer l'efficacité du modèle ?

En fait, pour moi l'audit externe fait aussi partie de la troisième de défense, puisqu'il contrôle finalement la bonne application des normes comptables. Normes comptables qui ont été définis par la deuxième ligne de défense ou par un organe externe, en général tout ce qui est principes comptables internes à l'entreprise sont définies dans le rapport annuel. Ces normes sont appliquées par la première ligne de défense qui est toute la structure financière de l'entreprise.

Donc les auditeurs externes finalement vérifient aussi la bonne application de ces normes là. Donc en soit, ils font partie de la troisième ligne de défense.

Par exemple au niveau des institutions européennes, tu as ce qu'ils appellent la cour des auditeurs, qui est chargé de certifier les comptes de tous les entités européennes et qui est intégrée dans la troisième ligne de défense selon le modèle de la commission européenne.

C'est un organe de la commission européenne. Comme tu as la cour des comptes en Belgique qui est aussi chargé de revoir les comptes de normalement tous les entités publiques belges, que ce soit au parlement, que ça soit le FOREM qui a été concerné par la cour des comptes. Tu as des inspecteurs des finances qui rapportent je pense à la cour des comptes. Donc eux font partie de la troisième ligne de défense, puisqu'ils font une évaluation sur le reste.

7 D'un point de vue de la première et de la deuxième ligne de défense, de ce que j'ai lu dans la recherche que j'aie effectuées, il pourrait parfois avoir un problème d'indépendance donc c'est à dire que les fonctions de deuxième ligne de défense pourraient avoir au final trop d'importance dans la première ligne de défense. Pourrais-tu me dire si cela a un impact sur l'effectiveness du modèle ?

Parfois la ligne n'est pas tout à fait claire. Par exemple l'informatique qui en fait définit, non seulement des processus de travail, des processus ou des principes de séparation de fonction, ce qu'on appelle le "four eyes principles", "segregation of duties", ce genre de choses, qui sont intégrées dans les systèmes. Mais en même temps ils font en sorte que la facturation, par exemple, ou les processus qui génèrent des revenus fonctionnent efficacement, et sont parties au fonctionnement. Donc souvent on a dans ces départements informatiques, on a une partie plus développement et gouvernance, et une de maintenance opérationnelle, c'est-à-dire, d'une maintenance des systèmes.

Est-ce que ça a un impact en termes d'indépendance et sur la génération ? Comme ça je n'ai pas d'exemples qui me viennent, mais c'est clair de par mon expérience, gérer l'informatique et discuter avec l'informatique, parfois c'est un peu la problématique, je ne dirais pas mais on parle à deux niveaux. On parle de la gouvernance et de la mise en place et la mise en œuvre des processus en fait.

8 Est-ce que l'information qui circule entre les lignes de défense, au sens propre, peut influencer l'effectiveness du modèle des trois lignes de défense ?

Tout est une question de l'efficacité de cette circulation d'informations, ça c'est une chose, et de la qualité des informations qui circulent. Si tu n'as pas une bonne information qui circule, il est clair que tu vas prendre des mauvaises décisions. Tout le reporting d'une entreprise est basée finalement sur la qualité des informations C'est pour ça qu'il y a d'énormes projets de business intelligence, et que les informations sont tellement nombreuses, tellement importantes, et parfois tellement complexes, qu'il faut pouvoir les organiser de manière à ce que tu aies la bonne information. Je te prends un exemple, si tu commences à réfléchir sur le fait d'augmenter ta marge dans tes activités mais que tu n'as pas une bonne définition de ta marge, et que les informations financières ne permettent pas de définir correctement ta marge, forcément tu risques de prendre des mauvaises décisions sur certaines lignes de produits ou sur certains types de service qui font que voilà tu étais complètement à côté de la plaque. Donc effectivement le challenge, c'est l'accès à l'information, la qualité des informations et la temporalité à laquelle tu obtiens à ces informations.

Mais je crois que vraiment le challenge c'est de définir les informations dont on a besoin et surtout qui ait une compréhension commune sur ce que ces informations, sur ce que contiennent ces informations. C'est vraiment pour moi, un point à point clé, c'est de savoir de quoi de quoi on parle, quel est quel est l'objectif qui est souvent définit par la direction ou par la première ligne de défense, qui finalement va vers la seconde ligne pour organiser aussi cet accès à l'information. Mais il y a une question de définition et de compréhension de ces informations. En fait maintenant, tu sais plus gérer les

informations, c'est les datas en fait, sont tellement importante et il y en a tellement, que c'est le challenge, c'est de pouvoir les gérer de manière correcte.

9. Quelle est la limite entre la collaboration et l'indépendance des fonctions ?

Je crois qu'il y a une collaboration qui est nécessaire, tu ne peux pas avoir des services ou des lignes de défense, qui fonctionnent de manière complètement indépendante les unes des autres, parce que sinon on n'est pas dans le même monde.

Tu vas avoir au niveau au niveau IT, ou au niveau sécurité "health and safety", des gens qui vont vouloir, parce que c'est la tendance à tout sécuriser, c'est leur objectif, et puis à côté de ça tu as des gens qui ont besoin que ça tourne de manière correcte, enfin que voilà ils puissent travailler.

Et donc il faut un moment donné, que cette collaboration se passe sur base d'une évaluation des risques qui est commune et qu'après chacun puisse définir clairement ses besoins et trouver le dénominateur commun par rapport à ça.

Si tu prends l'AFSCA par exemple, l'agence de sécurité alimentaire, tu peux te dire que l'AFSCA, son but de protéger le consommateur, et donc en soi, ils sont dans la deuxième ligne de défense et la troisième puisqu'ils auditent en fait des restaurants. Mais quelque part ils ont tendance aussi à établir leurs propres normes. Je ne sais pas si tu as entendu ces problèmes de tarte au riz à Verviers ? En fait l'AFSCA à un moment donné, a débarqué chez un ou deux boulangers, en leur interdisant de vendre de la tarte au riz, parce que soi disant, la chaîne du froid n'était pas établie de manière de manière correcte. Mais en fait c'est un principe global, la chaîne du froid doit être maintenu, mais là ils ont poussé les raisonnements tellement loin, que finalement ils ont interdit de vendre de la tarte au riz. Ce qui a fait un tollé, enfin moi j'ai été biberonné à la tarte au riz, j'ai 47 ans ça va j'en suis pas mort.

Donc on voit à certains moments, qu'il y a une espèce de, quand on laisse trop de liberté à la deuxième ligne, on va dans des excès qui empêchent finalement l'atteinte des objectifs de la société en soit, puisqu'on veut tout sécuriser. L'objectif est de trouver le juste milieu entre les risques effectifs, l'impact et la probabilité, en prenant ces deux composants et le fonctionnement effectif d'une entreprise, ou d'une organisation. Et je pense que c'est vraiment à l'heure actuelle le challenge de trouver le juste équilibre entre la procédure qui va sécuriser le process et l'effectivité du process, qu'il va pas prendre trop de temps ou qui va être trop cher à mettre à mettre en place, parce qu'on a mis trop de contrôles.

10. Quelle est l'influence des régulations sur le modèle des trois lignes de défense ?

Alors moi je ne suis pas du tout un spécialiste du secteur financier, je suis plutôt un industriel et dans les institutions mais pas dans le secteur financier. Je pense moi d'après ce que je vois que c'est un modèle qui fonctionne par action, réaction, dans le sens où Bâle & Solvency ont été établis après la crise financière de 2008, et qui ont eu une tendance à renforcer la capacité financière des institutions financières pour éviter des problèmes comme il y a eu en 2008 et 2009.

Sauf qu'on est déjà à Solvency 2 donc ça veut dire que le Solvency 1 n'était pas suffisamment établi par rapport à l'évolution du marché. Bâle je sais pas à combien ils sont, tu vois c'est chaque fois des "releases" du truc ce qui veut dire que le modèle tente de cadrer les activités.

Mais pour moi, c'est un principe humain, tu as les règles, tu essaies de jouer dedans, donc pour moi les règles elles sont à certains moments on n'est plus dans un principe de réaction donc forcément il y aura toujours quelqu'un qui aura une mauvaise idée en plus, ce qui va obliger de renforcer les règles.

Par contre ce que je constate, c'est que dans les institutions européennes, ils sont passés, donc dans le modèle de contrôle interne et de risk management au niveau des institutions européennes, est passée en 2008 d'un système de standards, c'est-à-dire qu'ils avaient

des standards de contrôle interne qui étaient applicable à l'ensemble des institutions depuis la grande direction générale, jusque la plus petite agence. Et ils sont passés vers un système de principes. Ca veut dire que tu as des principes de contrôle interne, c'est à chaque entité à appliquer ces principes de contrôle selon leur réalité, leurs besoins, et leurs spécificités et qu'on n'est pas forcément dans un système de compliance mais plutôt d'adaptation du modèle pour respecter les principes.

Ce qui veut dire qu'ils font le pari de la maturité des institutions en matière de contrôle interne et aussi de laisser à chaque direction la possibilité de dire "bon ok on doit avoir un système de ségrégation of duties, sauf qu'on n'a pas forcément toutes les personnes pour l'appliquer d'une manière standard, donc on va essayer de trouver des systèmes alternatifs pour mettre en place ce principe de séparation fonctions.

Mais je crois que ce concept de ligne de défense est pas clair dans des organismes plus petits, ou dans des entreprises plus petites, elle est certainement très clair dans des institutions européennes, elles l'est certainement dans le secteur financier, dans des plus grosses entreprises qui ont pris conscience de ça oui.

Je pense que la frontière notamment entre la première et la deuxième ligne est pas tout à fait établi tout le temps. Par exemple, le département informatique est en même temps seconde ligne parce qu'ils établissent des normes et des contrôles, mais en même temps sont parties prenantes à la vie de l'entreprise. Il n'y a pas cette frontière qui est établit de manière stricte tout le temps. Donc je crois qu'effectivement ce qui est important, c'est de bien définir qui fait quoi. Et puis il y a des entreprises de plus petite taille où tu sais pas établir ce modèle de manière aussi strict parce que t'as pas forcément la surface nécessaire pour les établir.

11. Ce n'est pas en fonction de la maturité de la gestion des risques, c'est plus en fonction la taille de l'entreprise ?

Je pense que tu vas aller parler à un hôpital où tout le monde est le nez dans le guidon, où ce sont des concepts qui vont être un peu abscons, un peu flou, et pas forcément très praticable. Par exemple je commence un audit dans un hôpital où la directrice opérationnelle est en même temps dans la gestion de sa zone et en même temps essaye d'établir les normes. Donc parfois les responsabilités de ces deux lignes sont dans les mains de la même personne.

Donc il faut un modèle collaboratif ou, un moment donné tu sors de ton rôle de première ligne pour aller dans la deuxième, et tu dois collaborer par exemple avec l'IT ou avec la finance pour définir les normes, et puis après revenir dans ton rôle de première ligne.

Je pense que c'est normal que ça ne soit pas établi de manière aussi claire parce que c'est pas possible effectivement.

12. En fonction de la taille et la complexité de même de l'entreprise, le modèle va-t-il s'identifier de manière différente ?

Clairement, je pense que oui. Dans les institutions publiques où il y a peut être plus de ressources, quoi qu'on en dise, oui tu auras des gens qui vont faire du process, d'autres qui vont faire de la norme et d'autres qui les appliqueront. Le risque c'est évidemment que ces gens ne se parlent pas, et qu'on fasse du process et puis qu'on applique de manière un peu aveugle le process ou qu'on fasse appliquer manière aveugle le process, sans avoir posé la question "Est-ce qu'on atteint bien tous les objectifs, et est ce qu'in finé c'est vivable pour pour la personne ?".

13. Donc les ressources constituent aussi un point très important dans l'entreprise ?

Oui. Je crois que dans certaines organisations à taille plus réduite, ces deux rôles se confondent, ce qui n'est pas mal en soit. Ils ont une sorte de référence implicite à ce genre

de situation, en se disant "Il faut mettre une procédure en place, parce que ça ne tombe pas dans mon département". On met la ressource en place, après on la fait appliquer aussi nous-mêmes tel qu'on l'a établi.

A certains moments certainement oui, dans des entreprises qui ont une vision très claire de ce qu'est le risque et de comment il doit être géré, oui. Par contre, je ne suis pas sûr qu'il y en ait énormément.

Certainement dans le secteur financier mais je te dis je suis pas un spécialiste du domaine. A mon avis dans des entreprises type énergétiques, oui, certainement. Parce que là on est déjà dans la chimie et et autres, parce que là forcément ils gèrent des risques dès le début et la notion de risque, elle est vraiment liée à leurs activités. Après cette notion, elle percolle dans d'autres départements, dans d'autres secteurs de l'entreprise, qui ne sont pas liées forcément à l'activité première. Par contre, moi pour avoir discuté avec différents directeurs financiers, des directeurs généraux, dans des hôpitaux, même si la notion de risque est très présente au niveau médical, dans les hôpitaux il n'y a pas encore cette notion très claire de ce qu'est un risque en fait.

Ils ont pas mis le doigt dessus, ils ont pas mis définition sur ces risques.

3. Annexe 3 : Interview n°3

1. Explication du sujet du mémoire

2. Présentation de l'interviewé, de son parcours, de son rôle dans son entreprise et de son entreprise

Je suis responsable de l'audit interne, et donc je suis en charge par tout ce qui est hors US, International Market, pour l'Asie, le Moyen-Orient, l'Europe et l'Amérique du sud. J'ai évidemment des collègues aux Etats-Unis qui s'occupent aussi d'autres parties, IT,...

Donc moi je suis ce qu'on appelle en tant qu'audit interne, la fameuse troisième ligne. Par rapport on a aussi un modèle des trois lignes de défense, que l'entreprise a aussi implémenté il y a 4, 5, 6 ans. Donc voilà ça prend du temps pour que les choses se mettent en place, mais je pense qu'au jour d'aujourd'hui, on peut dire que ça fonctionne assez bien et donc moi en tant qu'audit interne, voilà je joue dans ce rôle, la troisième ligne avec évidemment beaucoup d'interaction sur la deuxième ligne et sur la première ligne, de manière générale, je dirais, faire évoluer, faire maturer le modèle de manière à ce que ce soit le plus efficace possible.

C'est un peu le rôle de l'audit interne dans beaucoup de boîtes américaines, c'est donner de l'assurance aux boards, mais en plus de ça il y a vraiment évolué le thinking global niveau risk management et donc le modèle de trois lignes de défense.

3. Comment analysez-vous justement l'interaction avec la première ligne de défense ?

Alors donc, ce modèle des trois lignes de défense a été a été implémenté il y a 5-6 ans. Je pense que c'est assez répandu au jour d'aujourd'hui, certainement dans les secteurs financiers, mais aussi dans la plupart des grosses boîtes américaines en tout cas.

Dans mon ancienne entreprise, on avait le même modèle également. C'est un peu on va dire, un peu comme COSO ou COBIT, c'est un peu le modèle qui se veut un peu la norme

aujourd'hui pour ce genre d'organisations multinationales. Cela implique évidemment toutes les fonctions risques.

Nous on a ce qu'on appelle ERM, Enterprise Risk Management, on a ORM, Operations Risk Management, qui eux sont vraiment charge, si tu veux, d'avoir défini, implémenté, le modèle. Moi en tant qu'audit, au quotidien, je dirais la façon dont j'interagis avec la première et la deuxième ligne de défense, en fait on continue en fait à nous à faire des missions d'audit, donc essentiellement donner de l'assurance, par rapport à que fait la première ligne, mais aussi de plus en plus que ce que fait la seconde ligne.

Parce qu'historiquement et même avant qu'on ait le modèle des trois lignes de défense en place, la majorité de ce qu'on faisait c'était en fait auditer ou revoir des activités qui vraiment faisaient partie de la première ligne. Avec la mise en place du modèle, et donc le rôle maintenant de plus en plus important dévolu à la seconde ligne, donc la seconde ligne chez nous c'est tout ce qui est Risk Functions, tout ce qui aussi Policy Owner, tout ce qui Compliance Functions, les fonctions SOX etc...

Il y a vraiment un rôle que joue cette seconde ligne de défense, pour elle-même implémenter différents contrôles pour que la première ligne suive, et donc avec la seconde ligne qui se développe de plus en plus, nous on a aussi tendance si tu veux à déplacer aussi notre type d'interaction.

Historiquement principalement sur la première ligne, on le fait toujours, mais de plus en plus on regarde nous, à évaluer l'effectivness aussi de la seconde ligne par rapport à ce qu'elle est censée faire sur la première ligne.

4. Comment définiriez-vous l'interaction avec les organes de gouvernance ?

Donc en fait nous, en audit interne, c'est le cas dans la plupart des boîtes américaines, des grosses boîtes américaines, nous rapportons en fait directement à l'audit committee, qui est l'un des trois comités du board. Ma bosse en fait donc la Chief Audit, elle rapporte directement au Chairman de l'audit committee. Elle a aussi un "dotted" vers la CFO groupe, tout ce qui est administratif, ... Mais clairement l'audit committee est l'organe si tu veux suprême ultime qui lui est en charge de s'assurer que tout ce qui est gouvernance,

en ce compris l'audit interne, en ce compris des fonctions risque, en ce compris l'audit externe, interagissent et délivrent ce qu'ils sont censés délivrer.

Donc clairement, nous prenons nos missions, nos ordres on va dire, de l'audit committee et l'audit committee est clairement très impliqué et très demandeur en terme, disons, justement de mise en place du modèle des trois lignes, en termes de risque thinking, pour tout le monde, 1st, 2nd line.

Parce que comme tu le sais, le risk management, ce n'est pas une fonction de la 2nd ou de la 3rd ligne de défense, c'est tout le monde qui au quotidien, fait sa partie de Risk Management.

Donc l'Audit Committee, notre organe directeur, est très très impliqué et à de nombreuses reprises, mandate si tu veux, ma bosse mais aussi les fonctions risques, d'évoluer et de maturer.

On a quelques exemples concrets qui sont passés récemment, qui à nouveau, sont en ligne avec l'évolution, si tu veux de la maturation du modèle. Ce qu'on fait aujourd'hui, est vraiment beaucoup plus sophistiqué par rapport avec qu'on faisait, il y a 4-5 ans.

5. Quels seraient les facteurs influençant l'effectiveness du modèle ?

Donc la complexité de l'entreprise, l'aspect culturel, l'aspect business, il y a énormément d'éléments qui je pense rentrent en ligne de compte pour expliquer, pour qualifier la mise en place du modèle.

Mais clairement quand on a commencé, quand le board a commencé, à émettre cette idée, à donner les mandats il y a 4-5 ans, ça ne se passe pas du jour au lendemain. Il faut que les gens, je dirais d'abord, un comprennent c'est quoi ce modèle, quel est le bénéfice, vers quoi est-ce qu'on va.

Des éléments simples, par exemple en termes de sémantique, s'assurer aussi que tout le monde parle le même langage. En termes de définition des risques, les différents types de risques, on a développé ce qu'on appelle une taxonomie, de manière à avoir un langage commun, comment est-ce qu'on qualifie les risques, quelles sont les catégories de

risques (stratégique, regulatory financial, legal) il y a une matrice, tout ça. Simplement le point départ le fait de parler le même langage est quelque chose qui prend du temps.

Donc à nouveau on est maintenant cinq six ans derrière elle et les premiers débuts le modèle qu'on a aujourd'hui je pense, est robuste et efficace, maintenant dire qu'il est parfait non. Il évolue toujours avec l'évolution et la maturation je te dirais, ou maturité je pense, justement de ces rôles et responsabilités que l'on attend non seulement de la première ligne mais aussi de la seconde ligne.

6. Que pensez-vous du fait que « trop de contrôles tuent le contrôle » ?

C'est un point tout à fait correct, et bon si on peut un peu schématiser, donc la première ligne, en fait on va dire c'est les business manager, c'est un responsable marketing,...

Peut-être une parenthèse, pour expliquer les trois lignes défense, on a quelquefois, utiliser l'analogie avec un match de football. Où tu vois la première ligne c'est vraiment ce qu'ils sont, ils attaquent, la deuxième ligne c'est milieux terrain, défense et la troisième c'est le goalkeeper.

L'analogie, la première ligne, donc ceux qui se prennent en gros les business decisions ,... eux ils ont ils ont un job au quotidien, ils doivent signer des contrats, ils doivent délivrer on va dire par rapport à aux objectifs opérationnels. Un discours qu'on entend souvent quand on parle à la première ligne, en fonction à nouveau de cet état de maturité, c'est "on fait trop de contrôles, on fait trop de risques, laissez-moi faire mon job".

Donc ça au niveau c'est symptomatique peut-être aussi de quelqu'un qui n'a pas encore non plus intégrer le fait 90% le business et puis on fait 10% à côté du risque et de contrôle. L'idée c'est que tout soit vraiment intégré.

Au quotidien, quand on prend des décisions, en principe, dans un modèle bien mature, une décision c'est aussi le résultat d'un risk assessment, du risk management que l'on gère au quotidien, on fait du risk management en fait sans s'en rendre compte. C'est juste maintenant qu'on le formalise qu'on met un nom sur certaines choses mais en principe, si les gens appliquent le thinking nécessaire par rapport à ce qu'ils doivent faire

dans leurs objectifs opérationnels, la partie risk assesment doit être complètement intégré dedans.

Donc oui voilà si on te dit "ouais on fait trop de risk management, risk committee, risk dashboard, ça me parle pas à quoi ça sert..." oui donc voilà, cette fois une réaction négative parce que je pense que le modèle n'est pas encore intégré. Si c'est intégré on ne se pose peut-être même plus la question.

Maintenant à côté de ça c'est vrai que il y a parfois, on l'a eu aussi, on essaie un peu de l'harmoniser maintenant, parfois c'est un peu une pléthore de comité de risque,... Parfois, il faut aussi leur donner le crédit du fait que voilà, ils ont aussi un job à faire et on peut pas non plus prendre 50% de leur temps sur des risques committees ...

Donc parfois en effet trop est aussi nocif, parce que alors le fait d'en avoir trop va plutôt conduire un comportement de réaction de rejet.

7. Comment définiriez-vous l'interaction entre les deux premières lignes de défense ? Doivent-elles être totalement indépendantes l'une de l'autre ?

Clairement ce qu'on appelle l'indépendance, est surtout applicable bas à l'audit interne, la troisième ligne est par définition indépendante et objective, elle rapporte au board donc qu'elle rapporte pas au management. Première ligne et deuxième ligne sont plutôt ce que nous on appelle le management. La seconde ligne, c'est plus des fonctions risques, c'est plus des fonctions de contrôle, c'est plus des fonctions on va dire de policy owner, mais ça reste quand même le management, que ce soit financier, opérationnel, marketing, ...

Donc la définition d'indépendance au sens où on l'applique à l'audit interne est unique à l'audit interne, l'indépendance au niveau des deux premières lignes ne rentre pas dans cette définition là.

Alors ce qu'on a parfois, à nouveau je pense que c'est certainement en fonction de la maturité du modèle, tu n'as pas du jour au lendemain, quelqu'un qui décrète il faut mettre en place le modèle des trois lignes et elle se met automatiquement en place.

Non, historiquement si tu veux je pense ce qu'il s'est passé, c'est que les fonctions de seconde ligne se sont détachées, de ce qu'elle jouait avant en première ligne, pour en effet occuper le terrain de cette seconde ligne de manière de plus en plus affirmée.

Alors ce que tu as au début c'est quand la première et deuxième ligne ne sont pas bien séparées, je pense que c'est essentiellement lié au fait que le modèle n'a pas encore suffisamment évolué.

D'ailleurs même souvent dans certaines boîtes je pense en discutant avec des confrères, avec des collègues, souvent ce qui se passe c'est que c'est l'audit interne qui reçoit la mission de l'audit committee, qui prend son stick de pèlerin, et qui essaye en effet de mettre en place les contrôles internes, risk management,...

Dans un modèle qui est naissant, qui n'est pas très évolué, tu as souvent en fait l'audit interne qui quelque part cumule, parfois, en tout cas afin pas à pas la première, risques et contrôles. Avec cette évolution, cette maturation du modèle à nouveau, c'est là que tu as les trois lignes qui commence à bien prendre leurs marques, à bien se différencier et à nouveau, à se caractériser comme vraiment indépendantes les unes des autres, certainement pour la troisième ligne mais aussi la première par rapport à la deuxième.

8. Est-ce que cela a un impact sur la gestion des risques dans l'entreprise ?

Je pense qu'en effet au mieux les trois lignes sont définies au mieux l'effectiveness va se manifester également. Parce que sinon tu risques d'avoir des situations à nouveau un peu de "c'est pas clair, qui fait quoi". Il y a des choses qui risquent de ne pas donner le résultat escompté.

9. Y-a-t-il un équilibre à adopter entre la collaboration et l'indépendance ?

Nous en tout cas pour l'audit interne, ça revient un peu plus sur le rôle de l'audit que vraiment sur le modèle des trois lignes, mais en fait pour le schématiser un peu de manière simpliste en fait, tu as un peu deux façons de faire de l'audit.

Historiquement l'audit était souvent perçu comme le policier, qui attrapait le voleur. Tu es dans ta tour d'ivoire, tu débarques une fois tous les trois quatre ans pour faire une

mission, tu passes les trois quarts de ton planning à simplement comprendre le business, tu fais deux trois tests basiques de compliance puis te reviens 3 ans plus tard. Ca c'est un peu le stéréotype extrême, de l'audit tel qu'il faut pas le faire.

Nous ce qu'on fait de plus en plus, et à nouveau j'avais cette approche dans mon ancienne entreprise, c'est vraiment de faire notre métier de manière vraiment collaborative et de développer ce partnership avec le business. Parce que ce que je te décrivais juste avant ne fonctionne pas. Tu ne construis pas une relation de confiance, une relation de continuité, les gens vont toujours se considérer comme le mal nécessaire. En tout cas on a vraiment développé un modèle relationnel très poussé. Pas rien qu'à mon niveau, mais tous les gens de mon équipe, tous les gens du pôle audit team ont un "target" de relationship management, par rapport à un business unit ou le projet dont ils sont responsables.

En effet, de manière à ce qu'on développe cette relation de manière continue et de manière que cette relation soit une relation à deux sens. On reçoit de l'info le fait d'être en relation permanente avec le business, ça nous permet d'avoir de l'info, de se dire "tiens qu'est-ce qui se passe, quels sont les développements, quels sont les nouveaux risques qui se passent" et ça nous permet aussi de donner de l'information en retour. On partage aussi ce qu'on va en termes de "global think", des problèmes que j'ai vus, je peux aussi partager ça avec l'europe pour dire "tiens, ce qu'on voit là-bas, c'est pour vous, assurez-vous aussi peut-être que ce qu'on a vu en Asie n'est pas prévalant chez vous, et n'attendez pas un audit avant de commencer à vous, mettre en place des actions correctives".

Donc ce Relationship est surtout vraiment super important pour nous et ça fait vraiment partie de notre ADN. Donc moi j'ai essentiellement, donc par rapport à la couverture géographique, j'ai une personne qui s'occupe de l'Europe, une personne qui s'occupe de l'Asie, ... Chacune de ces quatre régions donc pour laquelle j'ai un lead au niveau de mon team a vraiment des réunions régulières et fréquentes, ne fût-ce qu'un catch-up une demi-heure. Simplement se tenir au courant et donc ça si tu veux c'est le point de départ par rapport au fait qu'on le vire quotidien.

Quand on est amené à faire des missions d'audit, on est évidemment tout à fait indépendant donc si notre conclusion, notre autre audit et très mauvais en termes de substance de ce qu'on voit, la CFO ne pourra rien dire, on sort notre rapport pour dire ce qu'on a vu.

La relation de partnership, de collaboration, va faire qu'on essaye aussi d'avoir un dialogue constructif, d'expliquer aussi le pourquoi, de pas seulement émettre un rapport rouge, mais dire pourquoi on estime que c'est rouge et voilà, non seulement les problèmes mais aussi les "routes causes". Et donner aussi des suggestions d'améliorations, donc quand tu donnes un message positif c'est toujours plus facile, quand tu donnes un message plus dur, plus négatif c'est plus difficile.

Mais il y a certainement moyen de le faire de manière constructive, et tu me croiras ou pas, mais même quand on sort des rapports qui ne sont pas bons en termes de substance, les gens nous remercient. Par rapport à la façon dont on a tenu notre mission, par rapport au fait à la façon dont nous les avons tenus au courant, engagé pendant le déroulement de la mission. De manière aussi à ce que le rapport ne soit pas une surprise. Si c'est mauvais, on peut ressentir assez rapidement, on le confirme et on sort le rapport qui ne doit pas être une surprise. On a ce dialogue, cette relation. Donc ça c'est vraiment par rapport à l'audit interne le partnership.

On travaille de manière générale avec un partnership équivalent, voire même encore plus poussée avec les fonctions seconde ligne. Parce que le but ultime, si tu veux c'est surtout de s'assurer que la première ligne fait ce qu'elle doit faire. On va être clair, on est tous première ligne, moi aussi je suis première ligne par rapport à mon rôle de people manager. Donner un exemple concret, c'est comment j'approuve l'expense report de mon team, même si je suis audit, je fais un rôle de première ligne, je dois m'assurer que mon team remplisse un rôle par rapport à ce que je lui demande. S'il y a quelque chose qui n'est pas correct, c'est moi qui le remballe à mon team member, en disant ça c'est pas correct.

Donc ça c'est ce qu'on appelle un contrôler un peu basique mais illustratif.

C'est quoi un rôle de la première ligne, c'est exécuté en fait les contrôles qui sont définis par rapport à certaines parties. Et pourquoi est-ce qu'on exécute les contrôles, c'est en

ligne avec les contrôles et procédures qui sont finalement quelque part la réflexion de risk appetite en fait. C'est un peu simplifié mais c'est un peu ça. Pourquoi est-ce qu'on a une politique, de dire ça c'est ok ça ce n'est pas ok, c'est quelque part la traduction de risk appetite qui a été décidé pour ce sujet-là.

Et donc chacun, dans son rôle de premier league doit respecter, disons les règles établies par rapport à ça. On a surtout une relation très collaborative extrêmement poussée avec la seconde ligne parce que quelque part troisième ligne et deuxième ligne, on travaille avec le même objectif de s'assurer, que la première ligne fait son rôle de première ligne. Mais l'objectif si tu veux est vraiment partagé.

Deuxième ligne, les fonctions risks , nous on définit aussi en deuxième ligne tout ce qui est policy owner, donc celui qui définit la policy "sales/deal", est en charge de définir la policy, de l'expliquer clairement, d'organiser les trainings, les formations, de manière à ce que les personnes qui sont censés suivre la policy, comprennent et aussi développer les mécanismes de monitoring. C'est une fonction aussi que nous poussons de plus en plus pour la seconde ligne. "Ok, vous êtes la policy owner, vous avez écrit votre papier c'est bien, mais vous devez en tant aussi que seconde ligne, l'implémentation est effective. C'est à vous de définir vos mécanismes de monitoring, de detectives controls, de manière à ce que vous, seconde ligne, puissiez voir que dans l'ensemble on suit ce que vous avez demandé".

C'est pas, oui nous on va faire un audit pour voir si de temps en temps c'est fait, mais on fait un audit d'une fois tous les x années, c'est vous la seconde ligne, qui devez mettre en place, construire cet élément aussi de monitoring, ...

10. Est-ce que la surveillance de la deuxième ligne de défense sur la première n'impacte pas l'effectivité de la première ligne ?

Je ne pense pas, parce que justement si la seconde ligne parvient à développer et à mettre en place un mécanisme de détection par rapport à quelles sont les situations c'est pas suivi, ça aide la première ligne à justement remédier à ses problèmes, beaucoup plus rapidement que si un audit vient détecter ces problèmes tous les trois ans.

11. Est-ce qu'une appétence au risque bien définie par les organes de gouvernance, influence positivement l'effectiveness du modèle ?

Pour moi oui la réponse est 100% oui. Même si la définition de risk appetite est pas forcément toujours facile. C'est quoi le risque appetite, comment se matérialise, comment est-ce qu'il se traduit, c'est pas, à nouveau, un truc qui se passe en une fois, il faut du temps ci pour arriver à ça.

Mais je dirais oui, 100% oui, parce que c'est ça qui va te définir en effet qui peut faire quoi. Donc par la traduction dans les policies, dans les procédures, souvent dans les grosses boîtes aussi où tu as le HQ, ici dans mon cas c'est New-York, puis tu as une assez grande autonomie, qui est laissée aux régions donc à nouveau l'Asie, le Middle East, l'Europe,... chacune de ces régions ayant aussi ses organes de gouvernance, avec un président, avec un CFO,... ça reflète aussi finalement quelle est l'autonomie de décision laissée aux régions, laissées aux managers du département et ça si tu veux c'est un peu à nouveau le Tone At the Top qui te dit "Voilà on est ok que ça c'est votre autonomie de décision, tout ce qui est supérieur à tel montant, vous n'avez pas notre délégation d'autorité pour le signer vous mêmes".

Ce sont des choses qui doivent remonter à l'échelon au-dessus. Chaque société définit souvent ces niveaux de gouvernance, on va dire, mais c'est souvent comme ça que ça se passe. On approuve la matrix, une policy, c'est quelque part tout ça c'est un peu le reflet aussi de de risk appetite qui est décidé au niveau de l'organe de gouvernance.

12. Quel est le rôle selon vous de l'audit externe dans le modèle ? Pourquoi, selon vous, l'on pourrait qualifier l'audit externe de quatrième ligne de défense ?

Ecoute moi j'ai fait de l'audit externe il y a bien longtemps, donc j'ai commencé ma carrière chez Price, en audit externe, puis j'ai fait autre chose, j'ai fait du conseil, j'ai occupé des fonctions de seconde ligne dans d'autres sociétés et puis l'audit interne.

J'ai eu moi ma propre expérience par rapport à que fait l'audit interne que fait l'audit externe, moi ça fait 20 ans que je bosse pour des grosses boites américaines, donc à nouveau tout ce qui est SOX, ... c'est assez élevé en termes d'exigences.

L'audit externe que l'on qualifie parfois en effet de quatrième ligne, a un rôle vraiment différent, déjà ils sont externes. Clairement au jour d'aujourd'hui en tout cas, ils viennent une voire deux fois par an. En général ils font des intérim, puis ils font le final pour en effet donner le sign off sur les financials, sur les SOX, ... leur rôle je pense est assez différent en tant que 4ème ligne si tu veux être assez différent de la dynamique interne de l'entreprise. Est-ce qu'il pourrait être mieux intégré dans le modèle des trois lignes directement, j'ai du mal à voir comment.

Si ce n'est alors marcher sur nos plates-bandes à nous, l'audit interne, ils ne peuvent clairement pas faire des fonctions de deuxième et première ligne, encore moins que nous évidemment, donc en termes d'intégration de la 4ème ligne sur le modèle trois lignes, à moins de quelque part faire ce que nous faisons je ne vois pas trop comment. Il ne faut pas non plus oublier quelles sont les missions de chacune de ces deux parties.

Nous l'audit interne même si on est indépendant, que nous reportons au board, mais quelque part notre mission reste sur la société. Le rôle de levier externe, il ne travaille pas vraiment pour compte de la société, il travaille pour compte des actionnaires. L'audit externe, quelque part, même s'ils sont engagés par la société pour faire un rapport, une mission, leur client final ce n'est pas la société, c'est vraiment les actionnaires.

Alors par rapport à ça aussi, les régulateurs avec lesquelles j'interagis moi aussi de plus en plus, par rapport au business de l'entreprise, eux quelque part aussi sont intéressés par une forme d'assurance, et on interagit avec eux tout comme j'interagis avec l'audit externe, mais les régulateurs leur stakeholder principal, ce n'est pas la société, c'est par définition on va dire le marché, mais ce n'est pas la société.

Par rapport aux modèles de troisième je pense ce qui unit les premières deuxièmes troisièmes lignes, c'est que c'est ça fait partie du microcosme interne de la société. Les auditeurs externes vont plutôt faire une mission dans l'intérêt des actionnaires ou du

grand public par rapport à la cotation de la société. Les régulateurs eux ont une mission plus de de protection ou de demandes d'assurance par rapport à l'état général du marché. Il y a vraiment une grosse, pour moi ,séparation entre les trois lignes, et puis 4ème 5ème, et cette séparation c'est vraiment pour moi la société elle-même. Les trois premières travaillent tous dans le meilleur intérêt de la société.

13. Est-ce que l'information qui circule entre les lignes de défense, au sens propre, peut influencer l'effectiveness du modèle des trois lignes de défense ?

Tu reviens un peu sur ce que tu discutes en termes de l'indépendance, est ce que le risque qu'on a une seconde ligne qui soit ne pas tout à fait indépendante peu en fait, parce que sinon je t'aurais dit toutes informations, par définition, tu peux la considérer comme biaisée.

Une information c'est souvent une personne qui communique à une autre personne, l'information la communication a toujours son niveau de bruit. La façon dont la première personne à l'expose à la seconde personne b, n'est pas forcément la même que si c'est une personne "c" qui parle à une personne "d", même si c'est la même information.

Comme toi et moi on se parle, si deux autres personnes qui parlent exactement de la même chose, ce ne serait pas exactement la même chose. Principes théoriques, toute information a un côté de bruit, de biais. Mais ça mise à part, si la question est vraiment sur la partie indépendance, oui clairement la seconde ligne ce n'est pas la troisième ligne, la seconde ligne ce n'est pas l'audit interne et donc il y a je pense dans toute société même avec toutes les meilleures intentions, un risque on va dire, de biais, de non indépendance, qui n'est pas nulle. Même avec l'audit interne à voir la pureté 100% objectivité, c'est jamais le cas, on est tous des êtres humains, on interagit tous avec nos qualités, nos défauts. Même si on fait son possible évidemment pour que l'information soit aussi objective que possible, le fait que ce sont des humains qui sont derrière ça, amène toujours son côté subjectif.

Pour la seconde ligne en effet, comme in fine, tu as un reporting line qui n'est pas indépendant comme nous mais qui est un niveau de management, tu as peut-être des

risques en effet d'interférences de biais, qui peuvent se jouer et donc ce qui fait à nouveau le succès du modèle, c'est est-ce que les acteurs clés sont prêts à jouer le jeu.

Donc moi quand j'interagis sur des missions d'audit, sur des pré-rapports, des rapports, des conclusions, je sens directement si le CFO joue son rôle ou pas. Par rapport à nous, est ce qu'il fait "push-back, push-back" ou est-ce qu'il est plus neutre en disant "oui ça c'est incroyable je comprends pas,..." ou parfois "tiens, là je comprends pas bien pourquoi,..." pour moi ça c'est une interaction qui est balancée, qui est équilibrée. J'ai eu des types d'interactions où sur chaque point le CFO n'était pas d'accord, ça pour moi ce n'est pas une relation équilibrée. Même chose avec les conclusions, les rapports, les résultats si tu veux des activités de 2ème ligne, tu vois directement si le CFO va prendre ça en compte de manière équilibrée ou pas.

14. Auriez-vous d'autres facteurs en tête qui pourrait influencer ce modèle ?

Donc les succès facteurs, c'est souvent ceux qu'on cite dans beaucoup d'autres exemples. Il faut le Tone at The Top. Il faut le support du top, ici c'est le board, c'est l'audit committee qui le mandate, qui l'impose. Si tu n'as pas ce signal, ce message, du Top, rien ne va se passer, mais parce qu'à nouveau, on a tous des choses à faire et si ça n'est pas émis comme vraiment objectif stratégique, primordial à mettre en place, il y a rien qui se passe.

Deuxième élément, c'est je pense en termes de succès, c'est que l'organisation parvienne en effet à se donner les moyens pour que le modèle fonctionne, et c'est en effet donner les moyens en terme de ressources, de people, de système, de process, que sais-je... pour en effet construire cette seconde ligne. Sans la seconde ligne, c'est un modèle bancaire, où l'audit fait aussi le rôle de la seconde ligne sur la première ligne.

Donc le vrai modèle, il doit avoir cette seconde ligne qui est extrêmement importante pour l'efficacité du modèle. Si t'as pas cette seconde ligne, le modèle ne fonctionne pas.

Comme on dit tantôt là quelque part la seconde ligne est amené à un peu comme l'audit, à évaluer que la première ligne fait ce qu'il doit faire, mais doit pouvoir aussi construire ça de manière permanente. Nous on va faire une mission, on va regarder, même si on a

audit period d'un an passé, realtim, mais on regarde ça une fois tous les 2-3-4 ans, c'est ponctuel, on peut avoir un coverage de 100%. C'est la seconde ligne à nouveau, qui en mettant en place ses propres systèmes de détection, vraiment joue le rôle du fait que ça fonctionne comme ça doit fonctionner.

Le troisième élément par rapport à ça, c'est peut-être simplement la culture générale de l'entreprise qui doit être je pense tout en ayant ce mandat tout en se donnant les moyens, donc 1er et 2eme point, parvient à développer une culture dans laquelle le modèle, le risk management,... ça fait vraiment partie de quelque chose qui est sain, qui doit être permanent, qui doit être proactive, constructif, on apprend tous des erreurs, on travaille ensemble, donc de la culture aussi, de l'aspect collaboratif que tu expliquais, pour moi je dirais, ça se sont déjà trois keys success factors.

A nouveau, il faut réaliser que cela n'a pas été construit en un jour, ça se passe pas du jour au lendemain, ça prend du temps. C'est quelque chose qu'il faudra évoluer, avec en effet une partie culture d'entreprise.

Un modèle tel qu'on a chez nous, le même modèle, avec les mêmes fonctions, les mêmes rôles et responsabilités, tu peux pas faire un copie paste, sur notre boîte, c'est important que le modèle puisse aussi s'adapter à la culture, à la dynamique propre de chaque boîte, qui est différente. Je peux même imaginer que si tu prends Belfius, KBC, ING, ça va même être des déclinaisons différentes du modèle. Le modèle est le même mais en pratique même, il y a des cultures, des dynamiques différentes.

Ce modèle, il est théorique, il est le même, mais son implémentation, sa mise en place, doit et c'est normal prendre des déclinaisons différentes en fonction justement de la taille, de la complexité, de la culture de l'entreprise. Il doit s'adapter, tu n'as pas comme souvent, enfin c'est le cas tous les modèles, leur mise en place, c'est pas une solution one fit all, le modèle théorique, OK, et puis la façon aussi dont tu le mets en place va par définition être main très, un peu, sensiblement très différents en fonction des boîtes.

4. Annexe 4 : Interview n°4

1. Explication du sujet du mémoire

2. Présentation de l'interviewé, de son parcours, de son rôle dans son entreprise et de son entreprise

Donc au niveau du positionnement, c'est clair que l'entreprise est cotée en bourse, ce qui a un impact important par rapport à cette problématique là, parce qu'on doit faire du reporting et du disclosure, notamment des risques par exemple mais également dès qu'il y a des problèmes importants, on doit être à même directement, de manière transparente de les donner au marché. Donc dans ce type de sociétés, tu as une obligation supplémentaire de vraiment t'outiller pour être au courant des choses qui se passent, des problèmes et les éventuels risques auxquels tu es soumis, pour pouvoir les rapporter aux analystes financiers.

Donc ça c'est une chose. Donc on a des activités un peu partout maintenant, donc c'est des activités internationales, on est structuré autour de trois grosses business units, tu dois t'imaginer tout le business traditionnel de l'entreprise comme on l'entend, comme beaucoup de gens l'entendent encore, c'était le métier autour des lettres, mais pas uniquement les lettres, tout ce qu'on faisait dans les bureaux, l'activité bancaire tout ça, qu'on appelle "Mail Retail", ça c'est une grosse business unit.

Il y a un deuxième business unit, qui s'occupe de tout ce qui est la croissance en matière de paquets donc on a un métier qui décroît au niveau des lettres, mais on a un métier qui a une forte croissance avec les paquets et qui est fortement lié à tout ce qui est e-commerce. Donc on a côté de ce métier de distribution de paquets, pris un positionnement de se développer en matière de logistique, les e-commerces. À partir d'un moment où tu as cliqué sur un achat on-line, nous on s'occupe de tout, les stocks, la commande, même le contact center. On peut gérer les services de fraude autour de paiement, on peut gérer surtout l'acheminement aussi du paquet, services complets de logistique. L'entreprise se

situé dans un environnement qui bouge tout le temps, il y a aussi quelque part, et c'est important par rapport à ce qui nous occupe.

Chez nous tu as le board, et donc le CEO qui apporte au Board, qui est un comité de direction classique, qui est structurée avec trois 'business unit' comme je te l'ai dit. Il y a les services supports classiques dont moi je fais partie, finance, HR, IT,...

Pourquoi ce que je dis ça mais parce qu'au niveau du board, chez nous ils ont également décidé séparer en trois sous board, qui sont d'une part l'audit comité, mais il y a aussi un stratégique comité et il y a un rémunération comité. Rémunération Comité, c'est toutes les parties approbation des politiques de rémunérations, les bonus, la rémunération du CEO,... Stratégie Comité ça c'est vraiment un board qui regarde plus les acquisitions qu'on veut faire où certains gros mouvements stratégiques. Et alors l'audit comités qui est vraiment celui qui a la compétence pour tout ce qui est validation des chiffres qui sortent. Il n'y a pas un chiffre financier qui peut sortir la société, sans que le comité d'audit puisse les valider, mais également tout ce qui est environnement général de contrôle.

Et donc je rapporte ici à au président du comité d'audit et aussi au CEO. Donc c'est les deux personnes, j'ai deux lignes hiérarchiques, mais ma ligne "hard" c'est celle là. Donc moi je suis un peu en dehors de, ce qui en termes de gouvernance est assez fort, parce que j'ai un accès direct à des administrateurs, qui ne font pas partie de ça.

Pourquoi est-ce qu'on parle de ça mais parce que donc ces gens là, en tout cas dans le comité d'audit, c'est un comité d'audit qui est assez actif ici, donc on se réunit cinq fois par an minimum, mais c'est un comité avec des gens vraiment assez pointu, assez spécialisés.

Donc ils sont vraiment en train de challenger tout le temps, de poser des questions et donc de jouer un rôle de contre pouvoir par rapport à ce qui se passe. Et donc qu'ils sont aussi demandeurs d'avoir beaucoup d'informations sur les problèmes, les audits ça les intéresse, mais également tout ce qu'on fait du mode analyse des risques. Donc il y a quelque part un environnement où il y a de plus en plus de pressions sur des départements comme les miens, sur comment tu t'organises,... et nous on a une perspective sur le groupe.

A la base de tout, nous on a choisi de se doter du fameux modèle des trois lignes de défense comme beaucoup, qui est soutenu par un département qui peut avoir les moyens de réaliser ce dont le modèle exige. Ceci ici ça explique dans les grandes lignes comment fonctionne au niveau de trois lignes de défense. C'est assez classique comme modèle, il n'y a pas de "rocket science" là dedans, donc le principe des trois lignes de défense, tout le monde est bien d'accord, mais la question va toujours être, comment est-ce qu'on fonctionne, est-ce que ceci va jouer suffisamment son rôle pour ne pas obliger à ceux-ci de devoir faire trop de choses importantes, ou faire faire à celui-là des choses qui sont en partie l'activité ici.

Une définition un petit peu de comment on répartit les rôles, de nouveau rien de challenging, si ce n'est qu'au niveau des lignes de défense, tu auras quelque part... Ici c'était spécifiquement la définition de ce que fait le risk management chez moi. C'est un peu particulier parce que moi je combine la deuxième et la troisième ligne de défense, je vais expliquer pourquoi. Mais donc moi j'ai quelque part une double casquette qui a priori n'est pas permis, dans certains secteurs, mais qu'on voit de plus en plus se développer.

Moi j'ai un rôle dans la deuxième et un rôle dans la troisième, normalement tu ne peux pas combiner ses rôles, dans le domaine bancaire c'est strictement interdit. Par contre, tu vas voir mon homologue chez Proximus, il a également certains aspects de Compliance et de Risk Management dans son champ.

3. Cela n'impacte-t-il pas là le modèle en tant que tel ?

Alors c'est ça c'est vraiment des discussions sémantiques, peut-être pas pour les théoriciens,... La seule chose que moi je peux dire, c'est que moi le comité de direction ils m'ont dit "Toi tu es là, pour tirer la sonnette d'alarme quand il faut". C'est de manière très résumée ici ce qu'on me demande de faire. Donc je peux la tirer avec la deuxième, la troisième ou la quatrième, ça leur est égal, du moment que l'on tire la sonnette d'alarmes quand il faut que ça soit tiré.

Sur les aspects d'indépendance, ça je trouve vraiment que ça n'a pas d'importance. À partir du moment où moi ma ligne de reporting, elle est sur l'administrateur et sur le CEO, l'indépendance,...

Tout dépend de la latitude dont on va te donner pour exercer la fonction, est-ce que le comité de direction va être collaboratif, est-ce que CEO, qui est quand même mon supérieur hiérarchique, est-ce qu'il va être ouvert ou pas avec moi en termes d'information, est-ce qu'il va me donner de la pression par rapport à certaines choses,... Si on est dans ce cas de figure là alors, c'est à toi de réagir et aller voir ton board member, et lui dire "écoute ici j'ai un problème".

Ça c'est vraiment personnel dans ta manière, dans ta déontologie à toi de fonctionner. Je pense qu'au-delà de tous ces modèles, c'est comme ça que ça doit être, parce que tu peux faire les plus beaux modèles que tu veux, après tout dépend de la manière dont les gens vont remplir les fonctions. Et ici c'est vraiment impactant, parce que tu dois pouvoir de temps en temps, soit taper sur la table, même si ça déplaît au CEO, soit être un peu plus compréhensif et dire là "je vais aider sur certains aspects" parce qu'il faut quand même faire avancer la boîte.

4. Quel est le rôle des organes de gouvernance dans l'implémentation du modèle ?

Je pense même les gens qui occupent les fonctions, et vraiment les personnes qui vont se cacher derrière les différents types de fonctions.

Je dépends du comité d'audit, j'ai vraiment cette faculté d'appeler le président du comité d'audit et lui dire "nous avons un problème".

Moi j'ai quand même bien scindé par rapport à la problématique des premières et deuxièmes lignes de défense. Tout ce qui est métier d'audit, où je dois donner de l'assurance, là je sers le comité d'audit vraiment en priorité, avec un objectif de donner

une assurance, sur ça fonctionne correctement, on n'a pas trop de problème à rapporter. On a toute une approche de l'audit du groupe, c'est tout le groupe. Il y a une équipe qui est basée aux USA maintenant avec trois personnes, il y a une équipe ici à Bruxelles.

On a deux types d'audit : audit général (process, projet,...) et audit de nature opérationnelle, dans les sites opérationnels, dans les bureaux de poste, sur les gros sites, comme les centres de tri, qui sont beaucoup plus du black and white, qui vise principalement à se donner une idée sur le fonctionnement des opérations (est ce qu'elles ont respecté toutes les règles en matière de sécurité, en matière de safety, au niveau de la gestion du personnel,...) Ici c'est une boîte où tu gères du personnel, il y a toutes les lois sociales, c'est important que dans le terrain, que tout ça soit correctement organiser. Tout ça c'est vérifié au niveau de l'audit.

Au niveau du risk management, on en a parlé donc il y a vraiment une identification donc avec le comité de direction, c'est plutôt du second line donc, de la vie du conseil, de l'animation, c'est ce genre de choses. Ici l'objectif principal c'est dérouler un ERM paddle qu'on a, avec trois échelons, les risques stratégiques, ... avec un but de dire voilà on a une liste des risques stratégiques de la boîte, qu'on monitor avec le comité de direction, avec le comité d'audit et qu'on met à jour régulièrement et sur lesquels on fait du reporting quand il faut le faire. Il y a un département de fraude, ce sont les gens, des détectives privés qui investissent sur des cas de fraude interne qui sont placés en deuxième ligne. Ils sont ici dans l'exécution pures, ce sont des gens qui vont analyser des cas de fraude. L'audit peut se poser la question, "qu'est ce que l'organisation fait quand il y a des fraudes?", ils vont donc auditer cette activité là.

5. Est-ce que, en tant que deuxième ligne de défense, émettent-ils des recommandations, des procédures à la première ligne ?

Ils peuvent, on l'a fait dans certains cas. Par exemple on a eu un gros cas de vol, dans notre activité transport, donc c'est un chauffeur qui a détourné beaucoup de marchandises dans des centres de tri et les bureaux distributeurs.

Donc on l'a repéré, dans ce cadre là, comme c'était tellement important, l'audit à regarder le cas aussi et a émis des recommandations pour résoudre le problème. C'est pas eux en tant que tel, c'est un auditeur qui est venu "Ok, le cas est tellement important, je le revois aussi, je comprends ce qui dysfonctionne dans les processus, j'émet des recommandations, ..."

Compliance, c'est un métier qui est venu s'ajouter, parce qu'alors tu combines vraiment tout ce qui tourne autour du respect des risques, tout est assez liés parce que quand moi je m'interroge ici sur les principaux risques la boîte, c'est un Input très important pour savoir où ils doivent aller auditer.

Il y vraiment un intérêt à centraliser tous ce knowledge au même endroit, c'est plus qu'une collaboration, parce qu'on devient vraiment des bons spécialistes des risques et ça permet à l'audit de mieux exercer son rôle, pour autant qu'ils puissent à tout moment quand même garder leur indépendance.

Moi je pense qu'avec une seule ligne sur le président et le comité d'audit, tu es tranquille.

Pour terminer dans compliance, il y a deux activités principales, c'est pas tout c'est uniquement tout ce qui est relatif aux règlements en matière de blanchiment des capitaux.

C'est une activité assez importante qu'on trouve dans plusieurs filiales, donc ça vaut la peine de les mettre à niveau corporate. Ici c'est tout ce qu'est GDPR, typiquement ce genre de thèmes sont des thèmes qu'on pourrait rajouter, si ils ont un intérêt pour la totalité du groupe.

Comment est-ce que moi je m'en suis sorti, tout d'abord sur le plan d'audit, on audit une de mes activités, et bien j'ai utilisé un externe (pas une fonction d'audit externe, mais bien interne) pour le faire.

On a ici des contrats de co-sourcing, donc ce sont des contrats qu'on peut appeler dans des domaines où on cherche de l'expertise qu'on a pas. Pour le cas du GDPR, on a demandé

à quelqu'un de le faire pour auditer cette partie là. Ce qui garantit plus d'indépendance quelque part. C'est du co-sourcing d'audit interne.

Donc ça c'est un exemple qui montre qu'on peut trouver les moyens dans ce genre de cas, où 2ème et 3ème ligne sont exercées par la même personne.

Dans l'audit de l'IT, même chose, on va aller les chercher parce qu'ils ont l'expertise et tu peux au travers de ça, arriver, à garder plus d'indépendance que si tu devais le faire en interne.

Peut-être, encore juste pour la forme, on a ici un centre de compétences autour de tout ce qui est data analytics, masse data, pourquoi, parce qu'on est dans des domaines ici où plus tu veux accroître l'assurance que tu vas donner, au plus tu as besoin de contrôler les choses, et le mass data c'est vraiment le rêve maintenant, parce que tu peux downloader, toutes les opérations sur des périodes et faire des check. Donc on a deux spécialistes qui servent en fait tous les métiers, parce que ici quand on cherche des fraudes, c'est aussi bien de download toutes sortes de choses. Les gens reviennent chez eux et disent "voilà notre problème" et ils savent où sont les bases de données et ils transmettent vraiment l'information les lignes. Enfin c'est uniquement en interne chez nous.

Par contre je ne sais pas de nouveau dans le cas de la fameuse fraude qu'on avait trouvé, un moment donné, ça au travers de routine d'analyses qui ont été développées ici, et après on a développé ces routines analyses, on les a données à la première ligne de défense, aux gens de l'opérationnel, pour qu'ils puissent mettre en place un reporting avec ces outils là, parce que c'est à eux à faire tourner ça régulièrement. Ce n'est pas à nous de le faire.

Donc ça c'est important, à un moment donné, pour analyser la situation, et qu'on trouve que c'est des bonnes choses, on donne les choses la première défense voire la deuxième de défense, pour qu'elles les réalisent.

6. Comment analysez-vous justement l'interaction avec la première ligne de défense ?

Donc les dans les interactions qu'on a c'est à tous les niveaux en fait. L'audit dit c'est la première et la deuxième ligne de défense, donc là, s'ils tombent dans le plan, on a des interactions.

Mes interactions, c'est d'une part, je dois gérer tout ce qui se passe au niveau du Board et du comité d'audit, donc là qu'est ce que je fais, j'ai cinq meetings par an avec le comité d'audit, j'ai des one to one avec le président du comité d'audits, la même chose avec président du board, qui me demande de me voir. C'est aussi une ligne que j'ai de reporting qui est importante, bien évidemment.

De manière générale l'importance est grande d'avoir un accès full à toutes les informations, donc moi j'ai accès j'ai le même accès que tous les administrateurs à l'information. On a une plateforme qui est une plateforme informatique sur laquelle sont mis tous les documents qui vont comité direction, tous les documents qui vont au comité d'audit, tous les documents du comité stratégique, tout au board, et moi j'ai accès à ça et je suis le seul à avoir cet accès total. Les gens du comité de direction n'ont pas un accès full à la plateforme. Parce que j'ai le droit de tout voir, dans ma liberté, de mon autonomie. Donc ça veut dire aussi que j'ai un certain devoir de confidentialité.

Et alors j'ai un accès à tout ce qui est audit externe, évidemment des rapports réguliers avec l'audit externe, parce que d'abord on se met d'accord sur l'approche d'audit, lui il va utiliser une partie de nos conclusions pour voir le niveau de détails, d'analyses, qu'il va faire dans le cas de nos audits externes des chiffres. Donc on se voit souvent.

Et alors ici donc au niveau de tout ce qui est contacts avec la première ligne si tu veux, je vois évidemment le CEO régulièrement, minimum une fois par mois, je fais des statuts réguliers avec chacun des membres du comité de direction, pour leur partie pour les audits qui a dans leur domaine, donc je les vois régulièrement aussi, pour qu'on se mette d'accord sur comment on doit ajuster le plan à ces choses là,...

Je participe à deux processus importants de la société, qui sont l'établissement du budget et tout ce qu'ils montrent le monitoring qu'on appelle "quartering reviews", et où tous les trimestres chaque membre du comité de direction, vient expliquer au CEO, où est-ce qu'il en est par rapport à ces objectifs, qu'est ce qui fonctionne et ce qui ne fonctionne pas, quels sont les chiffres financiers. Donc là moi j'assiste aussi, c'est pour moi très important parce que ça me permet d'avoir un positionnement par rapport à la première ligne de défense.

Je pense que pour bien exercer ce métier là tu dois être vraiment être capable d'abord de comprendre toutes les activités, et au delà d'être capable de suivre un peu comme fait le CEO, les différentes problématiques, parce que pour savoir s'il y a pas des risques induits ou des choses à proposer. Donc je fais régulièrement avec les membres du comité de direction aussi, des réunions plus formelles tous les trimestres et alors, tous les gens qu'il y a en dessous du comité de direction, régulièrement des meetings, en ce compris évidemment tous ceux qui gèrent les seconds line, puisque ça c'est évidemment pour moi des gens importants qui peuvent donner des informations.

Ce que nous, on appelle des secondes lignes de défense, de nature "corporate", parce que tu peux avoir, ça il faut bien comprendre, dans la boîte tu as les business units, ayant chacun leur P&L, leur Bottom Line, ce sont des métiers à part entière. Ils ont les coûts et les revenus de leurs activités et ils sont en profits ou en pertes, ils ont leurs objectifs opérationnels de leur organisation. À côté de ça, il y a des fonctions de support HR, IT, Finance, ...

Il y a tout ce qui est mon département, corporate, audit, risk. Alors ces fonctions de seconde ligne sont de nature différente de celle là parce que celles là elles ont vraiment une vocation à servir les 3 business units.

En principe je pense la plus facile, c'est "legal", c'est typiquement une fonction de deuxième ligne, c'est le département juridiques ici, les experts juridiques qui vont donner des avis juridiques. Ils sortent chaque année, ils appellent ça "le rapport des risques

légaux" qu'on a, donc tous les process, tous les problématiques liés à la concurrence déloyale, il y a une liste de risques assez conséquent, qu'on a chez nous mais "legal" gère tout ça, à travers tout le groupe.

Si je prends le cas de HR, j'ai une fonction safety, qui gère tout ce qui est prévention, c'est vraiment typiquement de nouveau une fonction de seconde ligne qui va vérifier dans les opérations si sur notre site, je ne sais pas lequel, le centre de tri, on fait ce qu'il faut en matière de prévention pour limiter les accidents de travail. Si on respecte toutes les lois, la loi sur le bien-être, ces gens-là qui vont monitorer ça.

Par contre tu peux très bien avoir aussi, on va prendre le cas des vols, il y a ici une fonction au sein de métier de quelqu'un qui gère pour tout ce qui est, incidents de nature frauduleuse. C'est vraiment la personne au sein de cette entité-là qui va aider essayer de monitorer la situation en matière de vol au sein de cette entité-là. Une fois qu'il y a un gros incident, il à venir contacter les gens chez moi, les trois détectives privés, en disant "ici j'ai un gros incident, il faut votre support pour analyser le cas". C'est une fonction de seconde ligne défense qu'on appelle les correspondants de "spock" dans les business units. C'est plus flagrant encore si l'on prend tout ce qui est activités financières, donc en matière de finances, tu as par définition besoin d'avoir des deuxièmes lignes qui vérifient de temps en- temps, comment se sont déroulées les opérations. Ici, personne ne sait ça mais on gère des comptes bancaires qui sont tous les comptes des ministères. En fait nous gérons tous les comptes de l'état, c'est une activité que personne ne connaît. Mais donc chaque process, tous les paiements de l'état, c'est les factures de l'état.

Donc tous les jours on donne à l'état une vue consolidée de tous ses comptes banques si tu veux qu'elle a, et on donne ça à la trésorerie de l'état, nous on gère la trésorerie de l'état de manière opérationnelle.

Sur les flux, qu'est-ce que c'est, un ministère nous donne des fichiers de paiements que nous on va processor, quand on va s'assurer qu'ils sont bien exécutés et autres et on va

faire du reporting tout ça, dans tout ce flux là, c'est un flux opérationnel qui se déroule ici, à travers ce flux là ils ont envie de monter un moment donné quelques fonctions de contrôle pour s'assurer, il y a un reporting surtout ce qui est user access.

Sur des process pareils tu dois quelque part avoir quelqu'un qui n'est pas impliqué dans ce process, donc une séparation de fonction. C'est tous les processus où tu crées des séparations de fonctions, donc tu as besoin de séparation de fonction quoi parce que là ça va te permettre d'avoir quelqu'un qui va avoir regarder si quelqu'un n'est pas en train de commettre des fraudes. Tu as ça dans comptabilité aussi où des gens qui gèrent les master data, typiquement des fournisseurs, donc dans la comptabilité des gens qui ont inscrit qui avaient une société intel avec son compte en banque, s'il y a des changements sur le numéro de compte en banque, il y a quelqu'un d'autre qui va être prévenue. C'est typiquement des endroits où tu organises des niveaux de contrôle et ça c'est la deuxième ligne par définition.

La première ligne est responsable de ces procédures auxquelles elle va dire moi même que j'organise le processus comme ça et à cet endroit là je pense c'est important d'avoir un contrôle,... La première ligne est "owner de ça.

Ici on a des correspondants de deuxième ligne un peu partout et alors il y a des métiers plus rentrer au ça c'est plutôt celle là dans business business control est aussi quelque part une deuxième ligne de défense, parce que tout ce qui risk manager, tout ce qui est contrôle interne, tout ce qui est "integrity", "safety",... Tout ça ce sont des fonctions qui ont cette volonté de contrôler.

7. Est-ce que, à contrario, quand il y a trop fonctions de contrôle, cela peut tuer entre guillemets le contrôle dans l'entreprise ?

Oui ça c'est clair, ça évidemment c'est à éviter. C'est pour ça qu'il y a la notion du "key control", dont il faut essayer de promouvoir les choses.

Il y a ici un résumé de la manière dont on va définir un plan d'audit, ou la définition de comment est-ce qu'on va donner du confort au comité d'audit, que les choses ont l'air de fonctionner correctement.

Voilà, tu pars d'un univers d'audit qui comprend la totalité du groupe, donc tu dois essayer de les cataloguer, et donc des ensembles qui sont cohérents, pour moment où tu choisis d'évaluer une entité, tu évalues l'entité de manière cohérente.

Parfois on va retenir une filiale, parfois un projet, parfois on va retenir un processus, un département. Ce qui fait du sens, comment tu découpes tout ton groupe. Ensuite, tu te poses la question de savoir, quels sont ceux qui m'intéresse d'aller regarder ou comment est-ce que je vais contrôler tout ça. Tu as fondamentalement deux possibilités, tu peux choisir sur base d'une analyse des risques de ce que tu fais, ou bien sur base, comme je l'expliqué, sur base plutôt d'un coverage des opérations. Ici on fait les deux.

C'est assez puissant parce qu'on peut rassurer sur un bon fonctionnement au jour le jour, de ce qui se passe dans l'entreprise, quel est le processus de collecte dans les boîtes rouges, que les processus de tri sont organisés correctement et à côté de ça on va essayer d'aller choisir, suivant une méthodologie qui est expliqué ici, les items ce qui sont plutôt dans notre matrice où le niveau de contrôle est évalué plutôt bas et les risques sont plutôt important.

Donc ça c'est l'approche de base si tu veux qu'on a scindé, et ça ici c'est du coverage, donc on va établir la fréquence à laquelle on va auditer nos business units.

Tout ça a été catalogué, et en fonction de ça, ils vont être plus ou moins visités, donc ici à la fin on voit tout. Il pourrait très bien que des activités ne soient pas audités.

A côté de ça, il y a peut-être aussi des endroits, quand on a pointé toutes nos activités, pour lesquelles on veut quand même avoir d'autres types d'approches parce que c'était autre chose. Donc l'IT c'est clairement devenu tellement important que tu es mieux quand

même d'avoir une réflexion, donc nous on suit le modèle COBIT, donc tu as des moyens spécifiques parce que c'est tellement spécifique que tu dois rassurer le comité d'audit. Ils font partie de cette analyse générale mais tu as un programme quand même bien particulier que tu dois bien pouvoir être expliqué.

La banque même chose, la banque c'est tellement autre chose, là on a un département d'audit interne, spécifique, c'est une filiale à 50%, ils sont indépendants de la manière dont ils s'évaluent, mais on a du reporting avec eux, ils font des missions conjointes et tout ça, mais donc c'est autre chose. Donc autre chose autre programme.

Tout ce qui risque de compliance, un moment donné on s'est dit que ça valait la peine de les cartographier, de savoir l'approche sur les 5 ans. Même chose pour les filiales ici, maintenant avec toutes les acquisitions qui a eu, pas mal de filiales, c'est bien de les visiter régulièrement. Certainement quand tu es la maison mère.

Il y a ça ici, ça c'est intéressant, parce que au niveau des liens des trois lignes de contrôles, on fait ce qu'on appelle des "contrôles effectiveness combined with masse datas analytics" dans certains domaines. Quand tu es dans un domaine où tu as a priori des risques importants, mais un contrôle important. Le comité d'audit m'a dit "c'est très bien d'aller chercher pour celui là (high - important) mais qu'est ce que vous faites pour celui là (high - pas important).

Les risques sont tellement importants, par exemple les processus de paiement d'états, c'est tellement important de voir rassurés par le fait que ça fonctionne bien, qu'on veut que vous fassiez régulièrement des missions.

Ce sont des missions dans laquelle on a d'abord, comme l'environnement de contrôle est élevé, ils ont eux-mêmes réfléchi à leurs risques, ils ont fait eux-mêmes réfléchi aux contrôles qui sont mis en place pour gérer ces risques, et donc on arrive dans un environnement où ils ont très bonne vue tant de le risque de leur contrôle.

Première chose que l'audit fait, elle valide la liste des risques et la liste des keys controls.

Ce qu'est ce que vous avez déterminé, vous, première ligne comme key control, est-ce ça fonctionne bien. Une fois qu'on a validée, on teste l'effectiveness du contrôle.

Comment est-ce qu'il est documenté, comment est-ce que vous pouvez nous prouver que le contrôle a été effectué et qu'il avait été bien réalisé et on en refait nous même de manière indépendante.

Là tu as vraiment la combinaison complète entre la première ligne qui a fait son travail, quels sont mes risques, quels sont mes contrôles, les contrôles qui sont effectués probablement par des deuxièmes de défense ou de première ligne, ça dépend du type de contrôle, et la troisième ligne qui vient valider.

Donc ça on fait beaucoup dans des domaines qui sont par exemple le paiement des rémunérations, donc chaque mois quand on a payé les personnes de l'entreprise, c'était un processus important parce qu'il y a un peu de millions qui vont partir sur les salaires des gens. Et donc il y a une série de contrôles pour s'assurer que l'information que tu vas donner, que le paiement va bien s'effectuer et tout ça. Typiquement, un domaine qui est très risqué et sur lesquels on a beaucoup de contrôles et beaucoup de maturité, mais on veut s'assurer que ça fonctionne bien.

Tout ce qui est paiement des factures fournisseurs, tout ce qui est suivi des paiements, tout ce qui est clôture de la comptabilité, typiquement des reportings,... A travers de ça, alors après tu peux encore utiliser d'autres types d'informations qui sont, par exemple, des selfs assessments que le business va faire, des résultats d'audit externe ou bien tu as aussi maintenant, des certificats qui sont donnés.

Donc et nous on nous on demande aussi de plus en plus de remplir des questionnaires,...

Aux états unis par exemple, dans notre filiale aux états-unis, ils nous demandent chaque année, nous envoie toutes sortes de report.

Donc ça c'est tout le système. On a aussi ici institué donc annuellement, un certain nombre de lignes de défense corporate produit un rapport annuel, en expliquant comment dans leur domaine respectif, ils évaluent la situation, les actions qui sont en cours et les problèmes qui pourraient se poser. On oblige les lignes de défense a rapporté ça au minimum une fois par an comité de direction, et éventuellement comité d'audit. Risk management le fait, Integrity le fait, Compliance le fait.

Donc ils ont vraiment un contact direct avec les comités de direction. Ca ne se passait pas donc c'est parce qu'on a réfléchi un peu comment fonctionne le système de défense, il y avait que lui qui le faisait. Lui il avait institué mais les autres ne faisaient pas, ce qui ne va pas. On a mis ça en place, il faut que le responsable intel rapporte telle chose... une fois par an. Exemple, "safety" avec tout ce qui touche aux accidents de travail, ou "security" avec tout ce qui touche à la sécurité des centres de tris.

A un moment donné, il faut que le comité de direction soit informé de ça et qu'il puisse éventuellement dire ce qui doit être mis en place. Donc à côté de ça donc on a un accès full à toutes les infos et on a les business review. Tout ça fait un ensemble cohérent qui permet à ici dans un troisième ligne de défense nous dit de bien fonctionner.

Ici, dans le risk management, donc de nouveau tu as le modèle, qu'est ce qu'il dit: tu as des risques stratégiques, tu as des risques de nature opérationnelles, tu as ici vraiment des risques au niveau d'un processus, d'un produit, d'un projet de plus bas niveau. Tu as une espèce de pyramide des risques dans la société, et entre des risques stratégiques et opérationnelles, la frontière n'est pas toujours claire parce que ici, un risque opérationnel est tellement important, par exemple on doit démarrer le nouveau centre de tri pour les paquets, c'est un projet de quatre ans, avec un risque opérationnel très important car si il ne démarre pas, on ne sait plus travail, il est tellement critique qu'il peut devenir stratégique.

Typiquement on dit que ceci est dirigé au niveau du board, et du comité de direction (stratégique), ceci va être géré au niveau des business units elles-mêmes parce que ce sont leurs risques (opérationnels), ils sont censés gérer le risque. Le boulot d'un manager, c'est gérer des risques et des opportunités.

Donc par exemple, notre département Risk Management, on travaille principalement à produire cette liste là, pour compte du conseil d'administration et du comité de direction, donc on est en train de faire l'exercice en ce moment, donc on voit plein de gens dans la société pour discuter des risques, on consolide, on voit chaque membre du comité de direction puis on anime un workshop au niveau du comité de direction, en disant voilà est-ce que ça c'est bien la liste, et on donne le framework, etc.. Parce qu'après on amène ça au board, mais tout ça on donne au CEO, qui va les expliquer, c'est "l'owner" de ça. On est vraiment une sorte de conseillers externes qui le fait.

Ici même chose, à ce niveau là à l'intérieur d'une business unit, il y a des endroits où il y a des risk manager, qui vont réfléchir à ça.

Donc ici tu as typiquement, si quelqu'un a un produit ou un process, a réfléchi à ces risques, ici c'est projet important, ça peut devenir un risque opérationnel important et donc tu as comme ça une cascade.

Ici, c'est là le positionnement des trois lignes de défense qui évidemment s'intéressent aux risques.

Donc ici tu es un peu des explications sur comment tout ça fonctionne, comment elle est organisée, comment on fait une révision des risques stratégiques, comment est-ce qu'on organise le monitoring...

Quand on se focalise uniquement sur les risques, comment est-ce qu'on les définit donc ce n'est que des incertitudes, ou bien des opportunités qui sont tellement importantes qu'il pourrait avoir un impact significatif. Dans ce cas-ci c'est un impact sur le compte de total plus de 20 millions d'euros, ce qui est beaucoup. Et alors on a créé trois catégories, mais ça c'est vraiment pour pouvoir faciliter le dialogue parce les risques, c'est tellement

fou parfois, on les a catégorisé pour faciliter les discussions. Quel va être l'environnement réglementaire qu'on va devoir garantir, c'est vraiment très spécifiques et c'est très impactant. Est-ce qu'on peut augmenter les prix,... ça c'est des choses qui se gèrent ici.

Il y a on appelle ça, des stratégies business risk, c'est tout ce qui peut se passer en dehors de l'entreprise sur lesquelles on n'a pas de prise, mais qui vont impacter la manière dont nos stratégies sont effectuées. Si notre concurrent décider de s'implémenter en Belgique, on a un problème. Ils l'ont pas fait, mais ils travaillent en collaboration avec nous. C'est ce genre de choses qui sont ici pointées.

Alors ici les critical operationnal risks, ça c'est des choses qui sont en principe gérées en interne mais elles sont tellement importantes, qu'on préfère quand même leur donner un spotlight.

Donc ici c'est IT security par exemple, c'est la réalisation de très gros projets. Ici on c'est le framework qu'on utilise avec les montants, donc les fusions supérieurs à tel montant, où on met ce qui est spécifique chez nous, ici c'est que dans l'évaluation du curve control on a mis la probabilité, d'habitude tu vois pas ça ici.

Ici tu évalues à la fois la probabilité de risque et ta capacité à le contrer. C'est un peu la cartographie qu'on a.

8. Est-ce qu'il existe, selon vous, certains facteurs pouvant influencer les modèle des trois lignes de défense ?

Comme dans tout modèle, si c'est trop rigide, ça ne va pas. Voilà nous ici on a pris une liberté de mixer des fonctions de la troisième ligne avec les fonctions de la deuxième ligne, on n'est pas une petite boîte ici, donc le comité d'audit a jugé que c'était possible. Il y a eu des discussions du comité d'audit en disant "ça ne va pas, vous avez combiné ces points là,..." mais on a répondu, en disant que les synergies créées sont gagnantes.

Le fait que je gère aussi ces aspects là, je ne gère pas les risques pour autant, mais je suis bien informé et j'aide le business à bien comprendre les risques, et ça me permet aussi de bien comprendre les risques pour faire mon métier d'auditeur.

Le gros risque de tout ces modèles, si tu les appliques mal,... d'ailleurs il y a aussi, je répète, beaucoup dans la manière d'exercer les différents rôles, parce que mon prédécesseur ici un moment donné il était tellement perçu comme rigide par le reste de l'organisation, que plus personne ne lui parlait.

Si la troisième de défense est sur son île déserte, tu n'auras pas la même intensité de discussion que si les responsables d'un comité de direction te font confiance, et sont là pour vraiment te parler ouvertement de leurs inquiétudes.

9. Pensez-vous que le modèle soit arrivé à maturité au sein de l'entreprise ?

On a fait ça au moment de la mise en bourse de l'entreprise, parce qu'au moment où la boîte est cotée en bourse, là tu dois être tout à fait précis sur toute une série de choses et donc ça fait partie. Si tu prends le rapport annuel de l'entreprise, des statements de gouvernance très précis que tu dois respecter.

Maintenant, c'est assez logique de structurer de cette manière là, avec le problème que si tu mets trop de contrôles partout, ça tue le contrôle. Dans certains cas, tes deuxièmes lignes sont vraiment calquées sur des obligations légales, ça me semble le minimum, mais dans d'autres cas, il faut que tu les mette, parce que tu en as besoin parce que c'est trop sensible.

C'est plutôt liée la séparation des fonctions, qui est naturelle et qui doit être bien orchestrée dans ton organisation parce que si tu ne le fais pas, il peut avoir des fraudes. Ici, il y a eu des fraudes dans la comptabilité, si tu n'as pas monitorer ça, et que tu n'as pas une liste d'exceptions qui te dit quelles sont les choses à faire, tu es mal parti.

Donc tu as besoin de ça, c'est une absolue nécessité. Voilà donc je pense c'est aussi beaucoup de théories pour finir, des principes qui sont tout à fait logique.

On a fait ici un moment donné, avec la mise en bourse, on a demandé à Deloitte, de mettre en place tout un framework, les risques, les contrôles... donc ils allaient voir tous les mois, dans tous les départements, plein de gens pour demander où est-ce que vous en êtes,... c'est pas possible, ça coûte des millions en implémentation, personne ne fait rien de ce truc. Après ça devient un tic de box, "oui oui c'est bon c'est bon" et tout le monde s'en fout.

5. Annexe 5 : Interview n°5

1. Explication du sujet du mémoire

2. Présentation de l'interviewé, de son parcours, de son rôle dans son entreprise et de son entreprise

Nous travaillons dans le département d'audit et nous effectuons principalement des missions d'audit.

3. En quoi, selon vous, est-il nécessaire d'implémenter un dispositif de gestion des risques tel que le modèle des trois lignes de défense ?

En fait, simplement, un dispositif où une organisation humaine d'une manière générale a toujours ses failles et donc c'est important qu'il y ait quelqu'un qui fasse, quelqu'un qui contrôle, quelqu'un qui ait un petit peu plus de recul pour qu'il contrôle et la troisième ligne qui est l'audit en l'occurrence qui est une vue d'ensemble, qui est indépendante, ça permet d'effectuer également des contrôles, mais aussi d'avoir du recul et de s'assurer que tous les risques sont bien maîtrisés.

4. Quel est votre interaction avec la première et la deuxième de défense ? Comment qualifieriez l'interaction avec ces lignes de défense ?

C'est une question compliquée, dans le sens où il y a tellement de cas particuliers. Mais de manière générale, je peux vous répondre, elle est bonne. Elle est collaborative. C'est à dire que quand on fait nous une mission sur une activité ou un sujet ou une entité, on va s'assurer que ces deux lignes de défense fonctionnent adéquatement. Et on va collaborer avec elle, pour avoir des informations, des des reportings, ... par ailleurs surtout la deuxième ligne, peut être la première également, il peut nous arriver quand on fait une mission sur autre chose, d'aller consulter pour faire des parallèles. Par exemple entre une

entité ici et une à l'étranger sur un sujet qui serait similaire, voir un peu les procédés de contrôle qui sont mis en place de reporting de gouvernance, ... Donc on utilise les informations, et on s'assure que les deux lignes de défense fonctionnent adéquatement mais aussi on collabore avec elle pour avoir des infos, ou leur en donner d'ailleurs des fois, en disant voilà on a remarqué ça, est-ce que ça vous semble normal.

Ils sont audités mais en même temps parfois on collabore avec eux.

5. Y-a-t-il un juste équilibre à adopter entre l'indépendance des fonctions et la collaboration ?

Nous on est indépendant, en tant qu'auditeur interne, ça s'est vécu, c'est expérimenté, il y a des tractations dans ce qu'on écrit, ... c'est donc à nous d'équilibrer les informations en fonction de qui on les reçoit. C'est-à-dire que ce soit l'audité, que ce soit une ligne de contrôle numéro un, numéro deux, ou même un avocat à l'extérieur qu'on consulterait ou le juriste de l'établissement qu'on consulterait, c'est à nous de faire un équilibre entre tout ça, et d'essayer de voir où est le risque et est-ce qu'il est adéquatement maîtrisé.

Donc c'est une source d'information, les lignes de défense, mais d'ailleurs il n'y a pas que les lignes de défense, mais aussi les gens du terrain, qui sont une énorme source d'information pour faire un audit. Et on rassemble toutes ces infos, mais certaines ne sont pas prépondérantes par rapport à d'autres.

6. Pensez-vous de manière générale que le modèle peut varier en fonction de la taille et de la complexité de l'entreprise ?

Il existe certainement une proportionnalité, quand on prend les très grands établissements, par exemple, les auditeurs, sont obligés d'être spécialisés sur des sujets, parce que ça devient tellement volumineux comme activité et peut-être complexe. La plupart des grandes banques sont structurées de cette manière. Lorsque tu es auditeur, par exemple, dans une grande banque, tu audites toujours la même chose, alors que nous,

on est généraliste. La seule fonction spécialisée, c'est celle de l'IT, mais sinon sur le reste on monte en puissance, en compétences, en accompagnant juniors et des seniors, mais on monte en puissance. On a des soutiens aussi, on a des formations, on a un programme de travail, etc... Et collaboration entre auditeurs, ça c'est essentiel.

Et de nouveau, consultation des lignes, consultation de ce que le régulateur peut indiquer, comme soucis ou préoccupations qui puissent avoir sur un sujet. Consultation sur la réglementation, sur des incidents qui auraient pu avoir lieu dans la banque, donc par exemple on allait voir les services qui gèrent les incidents comptables, ... un ensemble d'indicateurs en fait.

7. Est-ce que le modèle a besoin d'une certaine maturité pour arriver à être effectif dans l'entreprise ?

Moi je suis arrivé il y a neuf ans dans cette entreprise, c'était déjà en place l'année d'avant, ma responsable est arrivée l'année d'avant, et quand elle est arrivée, il y avait déjà une équipe en place depuis plusieurs années.

En fonction de l'évolution des activités, il y a des lignes de défense 1 et 2 qui sont renforcées ou voilà c'est l'évolution de la vie d'entreprise je dirais.

Non ça c'est en place depuis quand même un petit temps, et même j'ai une expérience dans les banques en France, c'était en place aussi avant. Mais en effet ça a été renforcé par la crise surement, c'est juste que les réglementations ont été formalisées. Je pense que la crise a amené principalement que le régulateur insiste très fortement sur tout ce qui est contrôle de deuxième niveau, sur tout ce qui risk banking, donc sur les fonds propres, ratio, liquidités, ces sujets là aussi, produits, ce qu'on peut vendre aux clients, ... Tout ce qui est 1ère et 2ème ligne, a été fortement renforcée et du coup les contrôles des régulateurs ont été renforcés.

Par contre, l'existence d'une troisième ligne d'audit et puis des deux autres, avant ça existait largement. Le régulateur a peut-être précisé dans des lois aussi que l'audit, il y a une circulaire qui précise, que l'audit à ça et ça comme fonction et surtout qu'elle a accès à tous les documents, ... ça a été renforcé depuis la crise. Le régulateur l'a reformulé, mais la loi bancaire existe déjà depuis le début des années 2000. L'audit était déjà positionné comme ça sans aucun souci, y compris dans l'indépendance, y compris dans l'accès aux documents.

Nous on n'a jamais refusé des documents ou des informations, car la loi nous oblige à le faire.

La troisième ligne, enfin les lignes étaient déjà en place, par contre on sent maintenant, que le régulateur vérifie beaucoup plus qu'elles sont effectives, et ça je pense que c'est depuis 2008.

8. Quelle est l'importance des organes de gouvernance dans le modèle des trois lignes de défense ?

Je crois qu'il ne faut pas confondre l'appétit de risque que peut décider d'avoir un établissement bancaire au niveau de son comité de direction et de son conseil d'administration, qui finalement définit des grandes stratégies du type, on a fait tel type d'activité, ça peut aller sur un produit complexe par exemple, ou structuré. Dans les structurés, pour prendre cet exemple-là, il y en a qui sont très peu risqués, qui était très peu risqués en et qui n'ont pas amené des pertes et puis il y en a qui ont été catastrophiques.

Donc le comité, enfin la gouvernance, va effectivement définir des grands appétits du risque, du genre, effectivement on va sur tel type de produits, on accepte tel type de duration, on va définir des montants, définir des volumes, on va définir des notations par exemple, on n'ira jamais en dessous d'une certaine notation. Donc il y a une définition des grandes activités que la banque peut accepter.

Régulièrement dans un établissement bancaire, quelqu'un va avoir une idée, va proposer une nouvelle activité. Sur les produits complexes, pour reprendre cet exemple là, et en proposant un cadre, on n'irait pas en dessous de ça, derrière le sous jacent ce serait ça,... il y a tout un plan qui sera proposé à ce moment là, qui passe par les différents départements clés, juridique, compliance,... et ça finit au comité de directions et là on va valider cet appétit de risque là.

Cette activité là, est-ce qu'on a envie de prendre ce risque là, ou pas ? Ca c'est le premier élément.

Après si c'est juste la création d'un nouveau produit, dans l'organisation de la banque, les services de contrôle existent déjà. C'est à dire que mon opérationnel qui s'occupe d'encoder les produits par exemple, et de vérifier que tout est juste, que le client a bien acheté 20, qu'il a bien l'argent portefeuille, qu'il est couvert, qu'il répond au descriptif qu'on a dit pour ce type de client,... tout ça existe déjà, il le fait pour d'autres produits, on lui dit juste, rajoute celui-là.

La deuxième ligne qui est le risk management par exemple, puisqu'on parle ici d'un produit, qui va dire moi je contrôle tous les produits, etc... voilà ça va être dedans, ils vont vérifier tout avec le recul, comme le nombre de clients, le temps de détention des produits, le client il a un minimum dans son portefeuille pour accéder à ce genre de produits, d'autres services vérifient que le client est bien mis en place, ... Tout le dispositif, il existe déjà.

Donc il y a la stratégie, c'est-à-dire la gouvernance de la banque va décider un ensemble d'éléments pour l'entreprise. Et en dessous ça change rien au niveau de l'organisation, sauf si effectivement on faisait pas de crédit et on se met à faire, là je suis d'accord il faudra mettre les deux lignes en place.

Les trois lignes de défense, c'est surtout une obligation réglementaire maintenant. Peu importe, l'appétit de risque du comité de direction, ils n'ont pas vraiment le choix.

Je dirais, il est immuable, il est partout. Même la commande de revue publicitaire, il y a quelqu'un qui commande, ensuite il y a un premier niveau de contrôle et il y a un deuxième niveau de contrôle. Et puis si nous, on faisait l'audit de l'activité imprimerie qui commande des revues ou marketing, et bien il y aurait un troisième niveau de contrôle. Donc il est systématique et il est immuable.

Par contre quand il y a de l'appétit de risque qui se développe sur un sujet et qui est accepté par la direction, le conseil administration de la banque, ça rentre dans notre dispositif et il faut s'assurer que ça rentre dans notre dispositif, dans les flux habituels qui sont contrôlés de façon adéquate. Et notamment ça c'est le genre de questions que nous on va se poser au troisième niveau, quand il y a une nouvelle activité très souvent, on fait un audit dans l'année pour aller voir si tout est bien pris en compte, et s'il y a bien les deux lignes au-dessus.

Effectivement si le comité de direction, qui a lancé un produit ou quelque chose, c'est le choix du comité de direction et du conseil d'administration. Nous notre rôle c'est pas d'aller à l'encontre du comité de direction, de leur choix, c'est leur choix. Après nous, ce qu'on doit faire c'est contrôlé qu'il y a des contrôles en place,...

Il faut qu'effectivement le comité de direction, quand il a dit de mettre ça ou ça en place, il faut qu'ils aient conscience des risques derrière.

9. Faut-il conscientiser les acteurs de l'entreprise à cette notion de risque ?

Je pense que ça dépend de la culture d'entreprise. Est-ce qu'un acteur de la première ligne de défense doit connaître tout le dispositif des trois lignes de défense, je ne suis pas sur. Il est en première ligne, il doit s'assurer que son contrôle il est bon, après savoir ce que nous on fait, et ce que le risk management fait, je ne suis pas sur que ce soit nécessaire.

Alors "le mieux est l'ennemi du bien", c'est-à-dire que quelqu'un qui est au premier niveau de contrôle ne doit pas connaître tous les dispositifs de contrôle qui sont au-dessus, sinon il pourrait les "bypasser". Je parle ici surtout de la deuxième ligne en fait. Ce qui est

important, c'est de valoriser le travail des gens, en leur donnant le sens en fait. Il faut qu'ils comprennent. C'est une force de notre établissement qui est petit, mais c'est une force du coup, car les gens ont une interaction, ont des réflexes de contrôle parce qu'ils se disent, "tiens je sais très bien que derrière, ça va dans tel département, c'est bizarre qu'aujourd'hui, j'ai quelque chose qui soit sous ce format-là alors qu'il devrait être sous un autre format..."

En plus, plus le contrôle est tôt, donc première ligne, mieux c'est en fait, la réaction est plus rapide, etc... Donc au contraire, oui, la culture de contrôle doit d'abord être "commune" et pas que dans les départements de contrôles, ligne 1, 2 ou 3. En plus effectivement, s'ils savent pourquoi ils font les choses c'est quand même beaucoup plus intéressant.

J'avais eu le cas, en private banking, où la cellule qui faisait les contrôles au private banking, on avait beaucoup discuté des lois, et ils ne savaient pas d'où venaient les contrôles, quelles étaient leurs origines. On en a rediscuté, et si on arrivait à leur faire comprendre quel était l'origine du contrôle et pourquoi il existait, c'était tout de suite plus intéressant. Cela leur donnait de la hauteur de vue, c'est plus impliquant et c'est parfois plus clair.

Il y a deux choses différentes, soit, ce dont toi tu parles, c'est-à-dire que chaque acteur doit comprendre son contrôle et pourquoi il le fait. Par contre, si l'acteur doit comprendre tout le système des trois lignes défense, ça je ne pense pas. Evidemment, si tu veux bien faire un contrôle faut le comprendre, le contrôle on doit le comprendre, et pourquoi on le fait. Mais effectivement, il ne faut pas connaître l'ensemble. Il faut savoir qu'il y a d'autres niveaux de contrôle qui vont intervenir, ce qu'il met un petit peu de pression sur celui qui contrôle au premier niveau ou au deuxième niveau. L'existence suffit.

10. Pensez-vous, de manière générale, que le modèle pourrait être trop bureaucratique, trop coûteux ? Que l'implémentation d'une multitude de contrôles nuirait au modèle ?

Moi je ne pense pas parce qu'on ne fait pas du tout les mêmes types de contrôles. La première ligne de défense, elle est dans l'opérationnel, la deuxième ligne de défense, elle fait des "samplings" sur ce qui a déjà été fait, donc du contrôle de second niveau, c'est vraiment différent. La deuxième ligne est beaucoup plus spécialisée sur leurs risques, leurs départements. Et nous, en tant que troisième ligne, on ne fait pas du tout les mêmes contrôles que les lignes précédentes. On est vraiment dans un aspect beaucoup plus global, moi je pense que justement c'est assez efficace parce que c'est pas du tout redondant.

On n'a pas les mêmes angles de vue. On ne regarde pas les choses de la même façon. À notre niveau par exemple, on ne va pas s'installer à côté d'un opérateur pour voir s'il vérifie ce qui a sur sa feuille, et que c'est bien effectué, encodé, ce n'est pas ça qu'on va regarder. Nous on va vraiment chasser, en disant, déjà est-ce qu'on est sûr que toutes les feuilles sont bien traitées et arrivent bien dans le bon département. Est-ce qu'il n'y a pas une instruction qui arriverait ailleurs ? On va vraiment essayer de vérifier le respect de la réglementation, le fait qu'il n'y ait pas de tentatives, de possibilités de fraudes, d'erreurs, ... c'est vraiment très différent.

Nous on regarde aussi l'organisation du département, est-ce qu'il est bien organisé, son interaction avec les autres départements, est-ce que les tâches sont bien définies, est-ce que c'est clair, ... il y a plein de sujets que nous on aborde, que les autres n'abordent pas du tout.

Les lignes sont complémentaires, il faut ça, on ne regarde finalement pas la même chose. Aucune des trois lignes ne regarde la même chose.

On va dire d'avoir une assurance, une probabilité élevée que tout est en ordre, c'est ça qu'on cherche, on ne cherche pas à mettre l'autre en défaut, on cherche surtout à être sûr que tout est bon. Si on mélange les deux lignes, ben on annihile un des deux niveaux de contrôle, en tout cas je pense que c'est pour ça qu'en banque c'est vraiment possible, on ouvre la porte à une fraude en fait. Il ne faut pas que les deux contrôleurs soient une seule et même personne.

C'est surtout que la deuxième ligne par exemple, elle va vérifier aussi, comme la 3ème va vérifier, les contrôles de la ligne inférieure. Donc est ce que les contrôles sont adéquats, alors que la première ligne ne va pas vraiment se poser la question est ce que ces contrôles sont adéquats, elle va exécuter. En fait les lignes deux et trois vont vraiment se poser la question est ce que ces contrôles adéquats. On regarde les contrôles, on regarde si, déjà c'est efficace, on va les tester aussi. C'est pour ça que la ségrégation est super importante entre 1, 2 et 3.

Si on faisait nous par exemple des contrôles de troisième ligne, comment après on pourrait se dire qu'ils sont bons. On aurait la tête dans le guidon, on serait en train de les faire. Chaque ligne doit avoir du recul par rapport à l'autre.

Surtout, dans les banques notamment, tout ce qui est opérationnel et notamment le cash, tout ce qu'est virement, on ne peut pas avoir la même personne qui vérifie, qui prépare le virement, qui l'encode et puis qu'il le vérifie. Ou qui au deuxième rang, vérifie que tout à fait correctement dans les deux étapes précédentes que je viens de décrire. A ce moment là on en situation où on est en train de donner à quelqu'un la clé du coffre. Les contrôles doivent être indépendant pour avoir d'abord l'assurance qu'ils sont bien faits et puis, ne pas les déstructurer.

Maintenant, attention, d'un point de vue de la proportionnalité, je peux comprendre qu'il se trouve que dans les PME, le comptable fait ses vérifications bancaires, parce qu'il n'y a pas les moyens. (Est-ce que les moyens mis à disposition par l'entreprise peuvent influencer l'effectiveness du modèle? Comparaison PME vs Grande entreprise)

Ça doit être proportionnée au risque, une pme qui fait un chiffre d'affaires de quoi payer une personne par an, ils ne vont pas fermer l'entreprise.

11. Quel est le rôle selon vous de l'audit externe dans le modèle ? Pourquoi, selon vous, l'on pourrait qualifier l'audit externe de quatrième ligne de défense ?

Alors la quatrième ligne, elle existe, c'est le régulateur, dans les faits. C'est à dire qu'on est régulièrement audité nous par la FSM, la Banque Nationale ou la BCE, sur le terrain avec les opérations, les lignes de défense, ... Donc il existe ce modèle.

Souvent l'audit externe est concentré sur ce qui est financier, il insiste aussi. C'est à dire que de nouveaux notre auditeur externe financiers ou notre réviseur en fait, regarde quand même nos comptes. Regarde de nouveau sous un angle différent et donne une assurance importante, non seulement sur les chiffres de la banque des chiffres de la banque, mais en plus sur les risques, parce qu'il y a les provisions, il y a plein de choses.

Dans les faits cette quatrième ligne, elle existe déjà. C'est un jugement indépendant qui est rapporté au comité d'audit, qui est rapporté au conseil d'administration. Il y a un flux tout à fait indépendant qui est très important. Mais là par contre on parle d'un angle de vue qui est lié d'abord aux chiffres, donc financier, d'audit comptable, et puis qui va parfois plus loin, mais c'est pas un audit d'activité, qui vient vérifier ceci ou cela. Maintenant ça arrive aussi, en ce moment nous on a un quality audit assessment. Notre département est actuellement audité par un auditeur externe, on voit la qualité de ce qu'on fait, si elle correspond et ça sera rapportée aux organes de gouvernance.

12. Est-ce que l'information qui circule entre les lignes de défense, au sens propre, peut influencer l'effectiveness du modèle des trois lignes de défense ?

De par l'humain, de par l'organisation, on peut toujours avoir une info qui est biaisée. C'est à nous notamment de nous assurer que quand on va, nous, regarder ce que fait la première ligne, on va s'assurer d'abord qui a d'abord toujours une première ligne

pour toutes les activités, qu'il y a des procédures qui leur "ok vous devez faire ça comme ça le contrôle, etc... et leur apporter de telle manière. Ensuite il faut pas oublier que la deuxième ligne fait des contrôles, normalement, non pas en prenant ceux de la première ligne mais en faisant leur propre contrôle, donc logiquement, il devrait en tout cas pas dépendre, des résultats du travail de la première ligne et donc pas être biaisée de cette façon là.

Donc nous on va vérifier que qu'ils travaillent correctement, première et deuxième ligne, mais effectivement, on en rencontre forcément il y a des cas où, il y a des éléments qui ont mal été compris, mal pris en compte, pas encore pris en compte, mal procéduré,... et ne pas oublier que le management, normalement à accepter et connaît sa stratégie, a quand même des éléments, pour se dire "tiens c'est curieux, je reçois pas d'infos là dessus, où ça est curieux,..." j'ai déjà connu ici dans cette bande, où dans une base de suivi d'incidents, pour citer un exemple, tout d'un il y en avait plus. Ils se sont dit "tiens c'est curieux quand même que l'on n'est plus du tout, il y a toujours quand même un client qui râle ou quelque chose". Mais le management doitn comme ils ont l'habitude aussi de recevoir des infos, le jour où ils n'en reçoivent plus, il y a un manque de cohérence, il y a aussi une interaction.

Donc oui l'humain et l'organisation, la mise en place de choses, il y aura toujours des biais, et en fait, on travaille à ce qu'il y en ait plus, ou le moins possible. Nous et le management, parce qu'il y a aussi le responsable du département, parce que lui il le sait qui a une nouvelle activité, lui aussi il voit les rapports de contrôles de première et deuxième ligne.

Il faut que rien nous échappe.

13. Existe-t-il, selon vous, des facteurs pouvant influencer l'effectiveness du modèle en général ?

La culture de contrôle, l'implication des gens, le support du management aussi. Les ressources mises à disposition, c'est tout de façon une obligation. Si au niveau d'une ligne ou l'autre, c'est nettement insuffisant (les ressources), le régulateur va le dire.

Alors on fait la boucle, parce qu'il faut des processus clairs, avec des stratégies définies et qui mettent en place l'organisation puis les contrôles clairs et puis un reporting clair, et ça tourne en fait. Le terrain, puis l'opérationnel et puis le management, du département ou carrément des directions dans les administrations, il doit y avoir comme ça des échanges d'informations sur ce que vous voulez faire, comment vous voulez faire, ou ce que vous voulez adapter, et les reporting de risques etc ... qui permettent un petit peu de faire des itérations. Il y a des échanges, et la communication est très importante.

Donc, la collaboration, la communication, le développement de la culture du contrôle, la formation des agents sur ce qu'ils doivent faire, connaissance de la réglementation. Et ce, pour l'ensemble des fonctions, de toutes les lignes de défense. Parce que si on veut que les gens aient une valeur ajoutée autre, deux c'est vraiment "pourquoi je le fais, ou tiens ça ça me semble bizarre par rapport à ce que normalement je vais faire". Au final des bonnes interactions.

Il faut que les gens puissent se poser les questions en fait. Donc l'ennemi du contrôle, c'est le stakhanovisme du contrôle, je fais ça mais je sais pas ce qui se passe derrière, ça ne va pas. Il faut former les acteurs et puis effectivement si quelqu'un en a marre de faire une fonction, il faut changer, il faut éviter l'ennui.

14. Est-ce que selon vous ça poserait un problème, que quelqu'un qui exerce une fonction de première ligne de défense, soit transféré dans une fonction de deuxième ligne de défense ? Ou inversement ?

Oui à partir du moment, où la première ligne est renforcée, et que la personne change de fonctions perdent ces accès de la première ligne. Au contraire, si l'entreprise peut profiter de son expérience, très bien. De même qu'il y a des gens d'audit, qu'ils partent parfois dans des fonctions de contrôle, ou de terrain. Ça s'enrichit, c'est à dire que l'on a d'anciens collègues dans d'autres départements, qui du coup sont sensibles, qu'ils savent que c'est important, qui en plus quand ils ont des questions, l'interaction est super bonne.

15. Est-ce que la rémunération des acteurs peut influencer l'effectiveness du modèle ?

D'accord, modifier son discours au profit de sa carrière. Ca serait applicable à n'importe qui, je travaille à la salle des marchés et je veux après passer au private banking, ou je travaille à l'audit et après je veux passer à la salle des marchés, on peut me dire je vais avoir finalement un conflit d'intérêt, c'est à dire modifier mon discours. Dans tous les cas je pense, il y a un responsable du service. Nous par exemple, j'imagine le cas, où je veux aller à la salle des marchés l'année prochaine, je fais un rapport justement sur la salle des marchés et je vais être vraiment super sympa dans mon rapport. Ma responsable, elle relit le rapport, elle va me dire "je comprend pas là, il y a un risque énorme, pourquoi tu mets un low risque, et pourquoi ci,..." et puis je suis pas sûr que j'impressionne le management de la salle des marchés si je commence à faire aussi un truc qui est pas très cohérent. C'est vrai pour n'importe quel niveau de contrôle, c'est vrai pour n'importe quel employé en fait.

En plus concrètement j'ai vu des collègues qui sont passé après dans des activités alors qu'avant ils les avaient audité, et ils avaient dit ce qu'il y avait à dire.

Après il y a la formulation, pas obliger d'avoir un ton assassin, dans tous les cas il faut rester correct. Mais par rapport à la deuxième de défense, je pense que l'accent doit être mis sur le Chief Compliance Officer, et le Chief Risk Officer, parce que c'est qui du coup vont relire tous les rapports. Donc l'accent, il doit être mis vraiment sur eux, ce sont des personnes clés.

Tu peux toujours avoir un conflit d'intérêt, donc l'accent il doit être mis sur la personne que tu embauches, et au dessus, un responsable de département, ou le comité d'audit.

Rendre un contrôle en disant que les choses vont alors qu'elles ne vont pas, c'est un risque énorme, car le risque peut se concrétiser, et la perte serait énorme. C'est une question d'intelligence, celui qui a envie de le faire peut essayer, mais je pense vraiment, ce n'est pas une vision à moyen ou long terme, ou à court terme.

Du biais, il peut y en avoir dans tout, c'est l'idée justement de mettre des contrôles, c'est d'essayer d'éviter d'avoir du biais, ça peut exister mais en général c'est pas intelligent.

Maintenant, il faut voir peut-être dans les très grandes entreprises de nouveau, ou dans les petites PME. Dans une petite PME, on dépend du grand patron, et si le grand patron a envie de voir la chose d'une certaine manière, c'est peut-être plus difficile de lui résister. De toute façon l'humain va tenter de mettre du biais, et c'est aux organisations de désigner les contrôles.

Il faut bien voir une chose, c'est tout ce qui est bancaire est extrêmement réglementée et depuis très longtemps, et donc on n'a pas du tout le même type d'organisation que de l'industrie par exemple en audit.

16. Est-ce que la réglementation influence l'effectiveness du modèle ?

C'est beaucoup plus lourd depuis beaucoup plus longtemps (impact sur la maturité du modèle?)

Le risk management et la compliance qui sont des grands éléments de deuxième ligne, c'est un place aussi depuis au moins avant les années 2000.

Donc Compliance, c'est répondre à la réglementation. Un des grands thèmes, c'est lutte contre le blanchiment d'argent, dans les années 90', c'était déjà en place.

Risk Management, c'est à dire gestion des risques notamment par exemple dans une salle des marchés, voir les engagements qu'on prend par rapport aux fonds propres de la banque, ne pas accepter des dépassements de temps,... pour faire simple, on peut vendre certains produits qui nous engage pour mille fois plus, les options. Faut maîtriser le monsieur qui est dans la salle des marchés et qui s'occupe de ça. Il faut faire du Risk Management sur ça, et être sûr que les actions prises ne dépassent pas les limites émises en interne.

Les trois lignes de défense, ça va être difficile de les comparer dans une pme ou comparé à un circuit de grande surface,... Les métiers sont différents.

Dès qu'on mélange les lignes en fait, on annihile un des deux contrôles.

6. Annexe 6 : Interview n°6

1. Explication du sujet du mémoire

2. Présentation de l'interviewé, de son parcours, de son rôle dans son entreprise et de son entreprise

Mon rôle se trouve dans les deux lignes de défense, donc ça c'est déjà quelque chose qui n'est pas tout à fait, comment dirais-je, normal, ça doit être une exception. Pour le moment, dans le département, on gère le risque de façon deuxième ligne de défense, donc on établit un Enterprise Risk Management. De l'autre côté, il y a aussi tout ce qui est audit dans le département. J'ai donc un rôle un dans les deux lignes de défense. Et donc selon les règles, parce que donc c'est plutôt pour l'audit que ça peut poser un problème, mais donc les règles de l'Institute of Internal Auditor, avec lesquels on travaille, dit qu'on peut faire ça pendant une période limitée, et qu'alors les services de la deuxième ligne sont audités, par un partenaire externe. Mais normalement ça doit être scindé, ça je suis tout à fait d'accord.

3. Pourquoi est-ce que justement dans l'entreprise vous avez mélangé les deux lignes de défense ?

C'est parce que la gestion des risques, dans notre entreprise, a encore un certain chemin à parcourir et donc pour le moment, les rôles sont chez la même personne. Mais ce n'est pas une exception, il y a encore d'autres sociétés où c'est encore organisé comme ça. C'est parce qu'il y a encore beaucoup de travail à faire et certainement aussi, donc les ERM, ERM gouvernance mais aussi, la mesure des risques par exemple, créent un "audit universe" et un "risk universe", pour moi, les deux doivent utiliser les mêmes outils. Et c'est pour ça que c'est bien maintenant qu'on travaille ensemble pour utiliser ces outils à travers les lignes de défense.

4. Est-ce que justement, cela n'impacte pas sur la gestion des risques dans l'entreprise, vu que les fonctions sont mélangées et qu'il n'y a pas l'indépendance des fonctions ?

Comme je dis, donc moi je suis responsable pour les deux, donc Chief Audit Officer, mais il y a quelqu'un qui est "Head of Audit", et une autre personne qui est "Head of Risk", donc il y a encore deux personnes entre moi et le reste des risques quoi.

Quel pourrait être le risque, je pense que pour le moment il y a plus d'avantages que de défauts. Et quand on regarde les trois lignes de défense, la deuxième ligne crée le "canvas", dans lequel la première ligne doit travailler, la troisième ligne regarde si tout est bien organisé entre la deuxième et la première ligne. Maintenant comme je t'ai dit que la deuxième ligne n'est pas encore très développée, pour moi pour le moment ça ne me pose pas de problèmes. Donc comme j'ai dit, il y a plus d'avantages mais à un certain moment il va devoir scinder. C'est pour ça qu'il y a déjà ces deux départements là et ils doivent tous les deux croître, et à un certain moment, il y n'y aura plus un seul responsable, mais il n'y a que "Head of Audit" et "Head of Risk".

5. Depuis combien de temps utilisez-vous ce modèle ?

Donc à moi je suis ici depuis avril, mais avant c'était déjà le cas. Le pôle Risk Management est ici depuis quelques années seulement, il y a donc une gouvernance, mais ça n'a pas encore été vraiment opérationnaliser. La deuxième ligne donc a fait un document de base, dans lequel pour moi, le plus important, est la façon dont on mesure les risques. Et la 3ème ligne utilise ça, ce qui est fait aussi, c'est tous les six mois, un inventaire des risques qui ont été identifiés par le business, discuté et on voit comment ce risque est adressée, est mitigé. Mais c'est un peu tout, donc il n'y a pas de proactif Risk Management vraiment. C'est plutôt un état des lieux pour le moment.

6. Est-ce que la taille de l'entreprise ou la complexité de l'entreprise aura un impact sur l'effectiveness du modèle ?

Pas pour moi parce qu'il est très important de bien scinder l'entreprise dans des départements, dans des processus de description, et que sur base de cette description, on

identifie les risques, et alors les contrôles alors pour mitiger ces risques. Bien évidemment dans une entreprise plus large, le travail est plus difficile et plus complexe, mais de l'autre côté le fait que ce travail est fait, donne quand même la possibilité de gérer les risques d'une manière proactive. Donc pour moi la taille de l'entreprise n'est pas très importante. De l'autre côté si c'est une entreprise de 50 personnes, on peut se demander, est-ce qu'il faut vraiment avoir scindé risques, et mettre des lignes de défense ensemble.

7. Comment se passe l'interaction avec la première ligne de défense ?

Comme j'ai dit, donc l'interaction avec la première ligne de défense, c'est donc tous les six mois qu'on demande, tiens voilà ça ce sont les grands risques que vous identifié, est-ce qu'ils sont toujours les mêmes, comment est-ce qu'ils ont évolué et vous aurez des nouvelles. C'est comme ça que c'est ici, dans la banque c'est tout à fait différent, mais ici c'est comme ça donc vu le fait que tout doit encore se développer.

8. Y-a-t-il une collaboration continue avec la première ligne de défense ?

Pas continue, parce que donc c'est tous les six mois qu'on demande. Et pour le reste il n'y a pas encore cette interaction-là. A la banque, c'était bien comme ça, et à la banque, on avait même le "first line defence / offence risk management", qui aidait le business a gérer ses risques, mais qui était du côté du business. Et là, la deuxième ligne travaillait ensemble avec la première. Ce sont deux extrêmes, la façon dont les trois lignes de défense sont implémentées dans une banque et la façon dont c'est implémenté dans notre entreprise. Mais je n'ai pas encore vu mais il se peut donc que dans des sociétés étatiques, c'est tout à fait différent.

9. Est-ce que l'indépendance des fonctions est primordial pour que le modèle soit effectif ?

Ça je trouve bien à la fin, oui quand même, parce que si le Risk Management est bien implémenté, c'est la première ligne de défense qui est le mieux placé pour identifier les risques et les mitiger. Là je suis convaincu. Donc quand il y a un nouveau produit, un nouveau process, ou un nouveau projet on fait donc un "product risk assessment" ou

"un project risk assessment", et c'est la première ligne de défense qui est responsable pour identifier tous les risques liés à ce produit, ce processus, ce projet et définir les "mitigances".

Dans ces réunions, la deuxième ligne est présente d'une manière indépendante, pour challenger le business. Pour dire, voilà nous avons défini le canvas dans lequel vous pouvez travailler. On a établi les risques ou le seuil de risque que l'entreprise devait prendre, donc là vous allez trop loin, donc vous vous dites que c'est "medium", mais selon notre Risk Manuel, ce n'est pas correct, nous on pense que c'est plutôt "High" au lieu du "Medium". Donc ce challenge doit se faire et pour ça il faut que les deux soient indépendant.

Alors la troisième ligne n'est pas présente à ce moment là parce qu'elle vient par après, elle donne l'assurance aux organes de gouvernance. Donc elle peut faire ça dans le design ou dans le design et l'effectiveness.

Donc l'audit peut venir immédiatement après tout ce qui a tout ce qui a été implémenté même lors de l'implémentation, un certain moment, pour voir si le design est bon, même quand le design est définit, l'audit peut déjà venir et regarder si l'identification des risques a bien eu lieu, si l'audit ne voit pas de risque, qui n'ont pas été identifiés, et aussi si les "metican?" sont bien décrits. Et la façon dont ils seront implémentés et exécutés sur papier, c'est bien fait. Et donc là c'est un audit design qui peut se faire encore même quand on est en train d'élaborer le tout.

9.1 Donc c'est important d'avoir un challenge entre les lignes de défense, de challenger les lignes de défense ?

Oui, ça c'est la tâche de la deuxième ligne, la troisième ligne donne de l'assurance.

10. Alors quel est le rôle des comités de direction ou des organes de gouvernance dans tout ce qui est établissement de la culture du risque dans l'entreprise ?

Ici, le rôle n'est pas encore très développé. Il faut qu'il y ait un Risk Committee, et déjà un Risk Committee dans la première ligne de défense, et pas un comité qui émane du CA mais vraiment un comité dans la deuxième ligne de défense, du business dans lequel la deuxième ligne assiste aussi. Donc à la banque on avait tous les trois mois, il y

avait un comité de risques, et là, l'état des lieux pour tous les départements, pour tous les types de risques étaient donnés, discutés, et s'il y avait des mesures à prendre, ils étaient discutés à ce moment-là.

Dans la présence du executif committee, il y a le risk officer et le business ensemble. Mais dans lequel le risk officer avait le dernier mot.

11. Donc c'est important qu'il y ait vraiment cette culture du contrôle du risque qui soit implémentée pour que les lignes défense soient effective ?

Les tâches doivent être bien établie et toujours la seconde ligne de défense a le pouvoir du dernier mot.

12. Que pensez-vous du fait que « trop de contrôles tuent le contrôle » ?

Tout à fait donc là tu parles du principe de "for-eyes" or "six-eyes", ça veut dire chaque fois qu'on tient quelque chose, ou qu'il y a un contrôle à faire, normalement le contrôle est fait par une personne, en tout cas si c'est un contrôle manuel et non effectué par le système, une personne qui fait le contrôle. Par exemple pour des paiements jusqu'à 10000 euros, une personne fait le contrôler c'est suffisant. Mais à partir d'un million on dit quand même il vaut mieux qu'il y ait deux personnes qui font.

Donc une personne c'est le "4 eyes principle", la personne qui fait la manipulation ou tout ce qui est à faire, et une deuxième personne qui contrôle si ce qui a été fait a été bien fait ça. Tu as le "6 eyes", c'est à dire il y a deux personnes qui vérifient donc tu as trois personnes au total. Il y a toujours moyen que même si c'est "6 eyes principle", qu'il y ait des problèmes de vérification au final. Mais ces deux principes sont assez courant.

Mais je pense que ce qui est plus important, comme tu dis cela peut créer une illusion de contrôle, mais le plus important, c'est que l'audit doit vérifier, intel doit vérifier, mais qui n'est pas bien spécifier comment et quand, alors la personne qui doit vérifier signe, et parfois, alors qu'il n'y a même rien, parce que le contrôle n'existe pas, la personne signe. Donc à ce moment-là, il y a un grand problème, donc pour moi bien évidemment quand il y a trop de personnes, ce n'est pas très efficace mais ce n'est pas très efficient non plus, ça

coûte beaucoup. Mais ce qui est plus important c'est que quand la personne doit faire un contrôle, il faut que le contrôle soit bien décrit. Ça pour moi c'est le plus important. Quand on dit, celui-là il va le contrôler mais que l'autre il ne sait pas ce qu'il doit faire, là il y a un problème et ça c'est quelque chose qu'on voit quand même souvent.

Il faut conscientiser les acteurs de l'entreprise, conscientiser que les contrôles soient bien décrits.

13. Pensez-vous que le modèle soit trop bureaucratique ?

Comme je dis, dans une petite entreprise, oui, mais à partir d'une certaine taille je pense que le modèle de défense est vraiment important. Et dans la banque il y a eu beaucoup de discussions, est-ce que c'est vraiment nécessaire, est-ce qu'on ne peut pas mettre la première ligne et la deuxième ligne ensemble, ...

L'objectif est de gérer les risques et tu mets quelque chose en place et si c'est bien organisé, c'est ok. Il y a sans doute encore d'autres moyens de gérer les risques ou d'arriver aux mêmes conclusions, ou d'arriver à la même risk confort.

C'est un système comme les autres, mais le plus important, c'est qu'il y a des processus qui sont bien décrits, l'identification des risques a été bien fait et que l'identification des risques est bien gérée. Ce n'est pas le système en soi, qui est mauvais, c'est la façon dont il est implémenté. Quand il n'y a pas de description du processus, alors comment tu peux identifier les risques. Quelqu'un qui connaît bien donc le processus peut dire "voilà ok moi je veux ça ça et ça", mais les autres qui ne connaissent pas ne vont pas pouvoir ajouter leur sagesse dans le processus, donc pour moi ça c'est très important .

14. Est-ce que l'interaction entre les deux lignes de défense pourrait au final avoir un impact sur la prise de décision ?

La de nouveau, quand quelqu'un dans la deuxième ligne de défense, quand un processus n'est pas bien décrit, pas bien compris par tout le monde, alors il se peut qu'il y ait ce malentendu entre les deux, et que la personne du business qui connaît bien son processus

dit que c'est suffisant et l'autre qui pense que c'est tout à fait différent parce que c'est pas bien décrit, qu'il y a ce malentendu, mais c'est pour ça que c'est si important d'avoir cette description de ce processus, que tout le monde parle ou parle de l'identification des risques et de la gravité des risques, parle du même concept et du processus. Donc c'est ça qui est le plus important. Donc il se peut bien évidemment qu'il y ait ces malentendus qu'on les moyens ne sont pas là. Et ça prend beaucoup de temps d'établir un ERM.

15. Donc les ressources qui sont mises à disposition sont très importantes pour que le modèle soit effectif ?

Le processus bien décrit et bien évidemment les gens doivent savoir de quoi ils parlent et certainement quand tu as le Risk Manager lui il doit quand même être bien formé, pour avoir ce "réflexe risque". Et alors la personne doit aussi pouvoir remettre le risque qu'on voit dans le contexte de la société, et relativiser vis à vis d'autres risques qui existent dans l'entreprise.

16. Comment définiriez-vous votre interaction avec l'audit externe ?

Quand je regarde l'auditeur externe, il est souvent là pour regarder les chiffres, est-ce que le bilan représente bien les chiffres et les résultats de la société.

Tu vois beaucoup moins que l'auditeur externe fait une analyse approfondie des risques non financiers. Et donc la gestion des risques non financiers ça pour moi, et donc là ça c'est le boulot de l'audit interne et du risk management. Et donc bien évidemment il doit y avoir une conversation et ce qui est important pour l'auditeur externe fait quand même un évaluation de la qualité de l'audit interne pour savoir s'il peut compter sur la qualité du travail de la troisième ligne de défense. Je pense que ça c'est important. Et à la banque j'avais des réunions trimestrielles avec l'auditeur externe ou je donnais mon état des lieux et qu'ils disaient "voilà donc nous on a vu ça ça et ça" et donc il y avait cette conversation là.

Il y a un échange et il doit être réel. Maintenant c'est un peu différent parce que c'est le cour des comptes qui fait des audits, mais donc il donne quand même aussi des

recommandations sur des points non financiers, mais là je donc je veux avoir cette conversation, ce dialogue avec la 4ème ligne de défense.

17. Pensez-vous que les régulations, les normes présentes dans le secteur, influencent l'effectiveness du modèle des 3LoD ?

Je pense que le rôle de la banque nationale par exemple est très importante parce qu'ils ont la vue sur toutes les banques. Comme les banques sont des entreprises financiers, s'il n'y a pas ces régulateurs, comme il y a un règlement pour les chemins de fer aussi, s'il y aurait pas ça, il se pourrait qu'une banque aille trop loin et on l'a déjà vu en 2008, tout le monde était là et tout le monde a vu. Mais donc c'est important qu'il y ait quand même une source externe de l'industrie, si je peux le dire, qui dans des industries, des activités, qui peuvent avoir un grand impact sur la société, qu'il y ait un régulateur qui dit voilà, vous allez le faire comme ça, et moi je vais veiller à ce que vous le faites comme ça.

Donc ça c'est le rôle très important, mais je dirais pour des activités qui ont ou pouvaient avoir un grand impact sur la société.

Le risque le plus important dans notre entreprise, c'est le risque de la sécurité du personnel, et celui des passagers. Donc il y a beaucoup de règles sur la façon dont le transport est réglé, sur la régulation donc des transports, donc le temps entre deux trains et aussi quels types de railles,... Tout ça pour éviter qu'il y ait des problèmes de sécurité.

18. Selon vous, existe-t-il d'autres facteurs pouvant influencer l'effectiveness du modèle des 3LoD ?

C'est la qualité des gens bien évidemment ça s'est très important et que le cadre est bien établi, et ne laissent pas, pour des choses importantes, de marge de manœuvre concernant l'implémentation et des contrôles et l'identification des risques. Donc la culture des risques, tout le monde peut apporter quelque chose.

19. Pensez-vous que la différence de rémunération entre les deux premières lignes de défense peut influencer l'effectiveness du modèle des trois lignes de défense ?

Oui, il y a toujours des gens qui peuvent penser comme ça. C'est une question de personnes, mais quand le Risk Manager voit qu'un de ses collaborateurs est même constamment plus généreux, ou que tous ces mediums doivent devenir des "high".

Il est même stimulé que des gens de première ligne aillent dans la deuxième ligne pour alors retourner dans la première ligne.

20. Justement, qu'en est-il de cet mobilité des fonctions au sein de l'entreprise ?

Si c'est bien géré, de nouveau, ça c'est la tâche du manager, comme c'est la tâche du manager dans la première ligne de défense, si quelqu'un doit exécuter une tâche, il regarde si la tâche est bien exécutée, ça c'est son devoir. Si c'est pour faire des voitures alors les voitures doivent être bien, si c'est pour gérer le risque et bien il y a aussi un autre output qui peut être regardé.

De nouveau c'est le cadre dans lequel tout ça se fait, si tout est bien établi, est bien réglé et bien décrit, c'est ok. Quand le risque est moins important, ça peut arriver. On est des humains, il peut y avoir des problèmes. La gouvernance est très importante.

Il est nécessaire de l'implémenter parce que chaque ligne a sa responsabilité et ses tâches, et ça ne doit pas être mélangé. Il doit bien y avoir quelqu'un, c'est comme dans le football, tu as l'équipe de football, et ils vont jouer contre une autre équipe. Qu'est-ce que l'équipe de football fait ? La première ligne de défense regarde le jeu des autres et il voit des opportunités et il voit des dangers donc comme ça il met sur place un jeu pour gagner.

Alors il y a le FIFA, ou les référés, qui font en sorte qu'il y ait un cadre dans lequel tout le monde doit jouer, et qu'il y ait quelqu'un qui fait en sorte que ce cadre est bien respecté, et alors il y a la troisième ligne de défense qui sont les commentateurs de football qui regarde les gens qui disent "ah oui ben là celui-là il n'aurait pas du faire ça, ça et ça, et le referee là il n'a pas bien pris une bonne décision", tu as ta troisième ligne de défense. Et donc si tout ça est bien décrit, c'est nécessaire, donc tu le vois partout, les trois lignes de défense maintenant ça existe dans tous types d'entreprises.

Bon comme je dis, dans une petite entreprise, c'est différent. Il faut quand même être conscient des risques, parce que faire quelque chose demande d'écouter beaucoup.

Le plus important c'est qu'il y ait une bonne description, je reviens toujours toujours vers lui. Ce n'est pas les trois lignes de défense en soi, qui font que ça va bien, les trois lignes de défense doivent être bien implémentées. La qualité dépend quand même aussi delà de la description des processus et donc de tout ce qui fait en sorte que l'identification des risques et la médication se fait bien. Les trois lignes de défense en soit ne valent pas grand chose si le reste n'est pas là.

7. Annexe 7 : Interview n°7

1. Explication du sujet du mémoire

2. Présentation de l'interviewé, de son parcours, de son rôle dans son entreprise et de son entreprise

Moi je suis responsable de l'audit interne. Notre entreprise est présente sur le marché de l'automobile, plus précisément dans le retail. Il faut savoir aussi qu'auparavant, j'étais auditeur interne dans une banque, ce qui change énormément au niveau des réglementations. Mon expérience a par ailleurs débuté au sein d'une des « big four ».

3. Est-ce que vous avez déjà entendu parlé du modèle de trois lignes de défense ? Est-ce que vous l'utilisez dans l'entreprise ?

Quand on a mis en place le département audit, cela fait maintenant trois ans maintenant que ce département audit existe vraiment, on a instauré vraiment une claire différence entre la troisième ligne et le business. Maintenant entre la première ligne et la deuxième ligne, oui ça existe, il y a des fonctions opérationnelles et des fonctions plutôt de support mais c'est pas non plus vraiment bien défini comme des audits de conformité ou autres qui ont vraiment des rôles de contrôle, ce n'est pas vraiment à ce point développé. Voilà ça existe, les gens le savent, ou du moins ils en ont eu connaissance, mais ce n'est pas fixé.

4. Quelle est votre interaction justement avec la première ou la deuxième ligne de défense ?

Moi c'est le cas dans des audits en fait, donc quand on fait des audits on va vérifier si les contrôles et les processus sont bien mis en applications et ensuite dans le cadre du suivi des recommandations qu'on a faites.

5. Pensez-vous que cette division, finalement peu implémentée au sein de votre entreprise, impacte la gestion des risques de l'entreprise ?

Non, selon moi, pas directement. À ce stade, les deux premières lignes ne sont pas indépendantes, mais la troisième oui. Comme c'est en phase d'implémentation pour beaucoup de choses, j'ai pas encore suffisamment de recul pour dire "est-ce que c'est plus ou moins de risque par rapport à telle ou telle ou chose", donc c'est en construction. Pour l'instant je ne pourrais pas évaluer ça.

Cela fait trois ans que le département audit existe, mais après l'idée des trois lignes de défense en tant que telle n'a jamais été formellement faite, mais ça existait dans l'entreprise d'une manière ou d'une autre. Mais vraiment avoir une troisième ligne de défense, avoir des contrôles et procédures, c'est depuis trois ans qu'on met ça en place.

6. Y-a-t-il une collaboration qui s'effectue entre la première et la deuxième ligne de défense ?

Oui oui c'est organisé parfois au sein du même département, donc des personnes qui sont plus dédiées à ça et d'autres à ça ou alors c'est une autre rotation.

Il peut donc avoir un mélange de fonctions, des acteurs dans les fonctions opérationnelles qui se retrouvent dans des fonctions plus de gestion, de conformité, ...

7. Mais cela ne pose-t-il pas un conflit d'intérêt entre ceux qui émettent les politiques et les procédures de contrôle, après qu'ils doivent effectuer des opérations pour le business en tant que tel ?

Non parce que ça se fait dès fois plus tôt, enfin s'il y a un souci à un contrôle ça se fait avec la troisième ligne, et donc entre la première et la deuxième, c'est plus du quotidien, ce n'est pas vraiment des structures indépendantes qui sont en charge de la conformité ou autre. Oui, il y a le département légal par exemple, donc si cela représente une fonction de deuxième ligne, oui là c'est séparé, il y a une hiérarchie séparée. Il y a peut-être certains départements qui ont une identité propre en deuxième ligne, mais non au sein d'un département business on va avoir des gens qui font aussi bien l'implémentation que du contrôle de par exemple d'un encodage, ou le contrôle d'un encodage, ... et puis, il va y avoir quelques fonctions qui va assurer pour certaines questions spécifiques, mais sinon ça se passe avec l'expérience et l'expertise de la première ligne en fait.

8. Est-ce qu'il y a une culture du contrôle qui a été clairement établie de la part des organes de gouvernance ?

Cela commence, ce n'est pas dans la nature de l'entreprise. Mais ça commence à s'établir dans l'entreprise petit à petit, c'est pour ça qu'on a différents organes qui se mettent en place, mais ça se construit.

Cela se construit parce que l'actionnariat, le corporate, les actionnaires et administrateurs ont demandé d'avoir des structures un peu plus en place, parce qu'il y a cinq ans d'ici, un nouvel actionnaire majoritaire est arrivé, et celui-ci en venant d'un secteur bancaire, il a souhaité d'avoir un peu plus de normes, comme on pouvait l'avoir dans le secteur bancaire, mais qui n'existait pas dans l'industrie.

9. Votre secteur n'est donc pas soumis à des normes spécifiques ?

Non parce qu'ici, nous ne sommes pas dans la construction, on est dans du retail donc il n'y a pas de spécificités.

10. Comment se passe l'interaction avec l'audit externe ?

Ils viennent me voir deux à trois fois par an, quand ils viennent faire des audits, financiers ou intérim, et donc pour me demander quels sont les rapports, qu'est ce que j'ai fait, si j'ai des points d'attention,... et puis je les rencontre quatre fois par an comité d'audit parce qu'ils sont présents, quand je présente mes conclusions et qu'eux présentent les leurs.

11. Ont-ils un impact dans la gestion des risques de l'entreprise ?

J'ai aménagé un peu mais ça dépend mon programme d'audit, en ne focalisant pas sur certains aspects financiers, parce que c'est eux qui font l'audit financier, mais on ne va pas refaire la même chose. Eux, en tout cas s'appuient sur peut-être mes rapports, mais moi je ne m'appuie pas sur le leur.

12. Selon vous, trop de contrôles tuent-ils le contrôle ?

Oui je pense, mais nous ne sommes clairement pas encore à ce stade ci dans notre entreprise. Donc oui, d'un point de vue personnel je pense que oui, j'essaie de ne pas forcément implémenter ça, mais on n'est pas dans ce cadre de figure ici. On est plutôt dans l'autre cas de figure, où il n'y en a pas encore assez.

13. Pensez-vous que la taille ou la complexité de l'entreprise puisse influencer l'effectiveness du modèle des 3LoD ?

Entre une PME et une grosse boîte, oui. Maintenant, à partir d'une certaine taille, pour moi, c'est des choses qui doivent exister. Donc je ne sais pas si c'est vraiment lié à la taille, mais plus qu'une PME, pour moi oui. Maintenant, entre une grosse, une très grosse et une très très très grosse, je ne vois pas la différence. Il faut que ça existe en tout cas.

14. Dès lors, si le modèle des 3LoD n'était pas implémenté auparavant, comme les risques étaient gérés ?

Personnellement, je suis en fait venu dans la boîte à partir du moment où une gestion des risques a été imposée par les actionnaires, donc avant je ne sais pas comment ça se gérait. Mais sans doute, on réagissait par rapport à un fait passé ou par rapport à l'expérience du terrain, des gens et donc il n'y avait pas vraiment une culture du risque et des contrôles comme on veut l'instaurer maintenant. Donc je sais pas, il n'y avait pas.

15. Comme vous êtes au début de l'implémentation d'un système de contrôle, quel est votre but à terme ? Voulez-vous implémentez le modèle des 3LoD de manière stricte ?

L'idée est d'aller vers plus de structures et de contrôles, mais c'est un changement de culture, c'est un changement d'approche, donc ça met du temps en fait. Donc oui c'est la volonté du management d'aller dans cette direction là, mais 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, ça doit être aussi actif quoi.

Il faut conscientiser les acteurs de l'entreprise en fait, c'est ce travail que je fais en partie dans le cadre de l'audit. Mais pour l'instant, on n'a pas encore de résultats, on a commencé à implémenter il y a deux ans une cellule qui rédige les procédures. Mais elle rédige les procédures, elle ne s'assure pas de la mise en application de ces procédures. Donc on construit des cellules pour arriver à ça, mais on n'a pas vraiment, comme je disais, cette définition, cette séparation entre quelqu'un fait, quelqu'un va vérifier et puis la troisième ligne. Pour l'instant c'est moi qui viens vérifier, on implémente des choses et on s'attend que la première ligne le fasse.

Mais on n'a pas encore eu le temps en trois ans de vérifier que tout était bien fait, et que chacun était indépendant dans les commentaires qu'il donnait.

16. Pensez-vous de manière générale, peut-être de votre expérience dans le passé, si déjà vous avez utilisé ce modèle dans d'autres entreprises, à d'autr ?

Quand je travaillais dans une banque avant, c'était clair, mais c'est le secteur bancaire qui est comme ça, ici c'est le secteur industriel-retail. À la base, il n'y a déjà pas forcément de normes ou autre qui sont obligatoires d'être suivie, que la loi le code civil ou le code de société, il y a beaucoup moins de restrictions enfin d'imposition à faire ça. Donc ça dépend un peu du bon vouloir, mais aussi du bas du management qui gère sa boîte, et qui donne les lignes directrices.

17. Pensez-vous que la rémunération peut influencer l'effectiveness du modèle des 3LoD?

Oui enfin, pour moi, la rémunération peut influencer n'importe quoi. Ce n'est pas forcément les lignes de défense, ça dépend des personnes. Pour moi ce n'est pas propre aux lignes de défense et ce n'est pas propre au modèle. C'est propre à la personne. C'est une situation, qu'on soit dans la même ligne, ou dans telle ou telle ligne de défense, ou on veut changer de départements, on va aussi bosser différemment.

Pour moi oui c'est un facteur, mais comme il pourrait intervenir à n'importe quel niveau et dans n'importe quelle situation, pas forcément par rapport à une ligne de défense.

18. Auriez-vous d'autres facteurs pouvant influencer positivement ou négativement l'effectiveness du modèle des 3LoD ?

Par exemple ici, le fait de ne pas avoir justement cette séparation aussi poussée, ça a ses avantages et ses inconvénients. C'est à dire que l'avantage, c'est justement, il n'y a pas trop de lenteur à contrôler, et à avoir des personnes différentes, et il y a une conscientisation et une prise de responsabilité plus forte de la première ligne.

Le désavantage par contre c'est qu'effectivement, les gens sont un peu "owner" de faire, pas ce qu'ils veulent quand ils le veulent, mais ils sont plutôt assez libres, et donc ça peut amener des déviances ou des gens qui vont être moins ouverts, moins concernés par le risque. Parce que ce n'est pas leur job, parce qu'ils n'ont pas le temps de penser à ça. Et donc ils n'ont pas un regard externe ou high level pour leur dire attention à ça, puisqu'ils sont full time occupés.

Voilà ça a ses avantages parce que c'est un regard externe, c'est un avantage parce que ça déresponsabilise un peu les gens dans leurs applications d'un rôle.

Après voilà, l'entreprise est dans un contexte particulier, c'est une entreprise familiale de 200 ans, c'est des entrepreneurs, c'est une entreprise belge avec un actionnariat majoritaire familial, ça joue aussi énormément dans l'environnement culturel. J'ai été aussi surprise en arrivant ici, venant d'un des big four et puis de milieux bancaires, c'est un peu le jour et la nuit pour moi. C'est assez particulier, c'est pas forcément représentatif d'une industrie ou l'autre, mais il faut tenir compte du contexte managérial et de l'historique de l'entreprise.

L'environnement joue énormément dans cet aspect là, ce n'est pas juste les secteurs qui entourent ça et l'historique de la boîte qui entourent aussi ce changement.

8. Annexe 8 : Interview n°8

1. Explication du sujet du mémoire

2. Présentation de l'interviewé, de son parcours, de son rôle dans son entreprise et de son entreprise

Je suis le « Head of ALM », c'est à dire que lorsqu'on a des contrats d'assurance, il y a des engagements qui sont définis avec les clients. Donc pour tout ce qui est assurance P&C, les engagements ils sont d'être là en cas de sinistre, accompagner le client, des démarches aussi dans son indemnisation, on essaie d'élargir de plus en plus notre intervention. Et pour passer de payeurs à partenaires, c'est la direction dans laquelle l'entreprise veut aller. Et puis, on a les clients en assurance vie, où là il y a un volet financier dans la plupart des contrats. Mon rôle c'est de s'assurer qu'au niveau, avec les investissements qu'on fait on est capable de premièrement arrivé à servir nos engagements et nos engagements financiers, donc des taux d'intérêt à servir sur des contrats. Et de l'autre côté qu'on rémunère aussi l'actionnaire pour le risque qu'il prend. Quand l'actionnaire nous donne un euro de capital, on doit le rémunérer suffisamment pour qu'il soit heureux d'investir chez nous, de l'autre côté le client doit être satisfait de ce qu'il obtient chez nous. Tout ça dans des enveloppes de risque qui sont bien déterminés, parce que le shareholder va jamais me dire "voilà je vous donne un euro, vous pouvez le perdre à la fin de l'année", donc on doit mesurer qu'est ce qu'on pourrait perdre et rester dans des limites qui sont acceptables pour l'actionnaire. Donc mon rôle là dedans c'est au niveau des investissements, donc à chaque produit correspond un portefeuille d'investissement. Dans les investissements, quel est le meilleur mix d'actifs qui va répondre à toutes ces contraintes. Je définirais donc mon rôle comme étant un rôle de première ligne de défense.

3. En quoi pensez-vous que votre fonction influence l'effectiveness du modèle ?

En tant que première ligne, on est là pour montrer, pour limiter les risques selon notre vue, donc dans chaque opinion qu'on va donner, la deuxième ligne de défense va aussi

revoir comment on a construit notre opinion, ils vont nous challenger là dessus et puis vont me dire "Tout est ok, on valide" ou "On pense que cette partie là de votre opinion pourrait être backé par plus d'analyses, ou par une analyse différente, ou vous pourriez enrichir cette analyse. Voilà donc c'est le type de recommandations que la deuxième ligne va donner à la première. Donc dans le fonctionnement de l'entreprise, donc la première ligne va présenter toujours ses propositions dans un comité, où la seconde ligne est représentée et donne sa seconde opinion, avant que le comité puisse valider formellement. Donc la seconde opinion n'est pas contraignante, le comité pourrait dévier de la seconde opinion, mais dans les faits, le risk management faisant partie du comité, il va pas voter pour une proposition qui n'a pas été validée par sa propre équipe. Donc essentiellement ce qui passe dans les comités, a déjà été revu, et validé.

4. Quelle est l'importance des organes de gouvernance dans le modèle des 3LoD ?

Le comité de direction est attentif à ce que le l'audit interne, donc la troisième ligne de défense revoie les processus de manière régulière. Le bien fondé de ça c'est qu'il y a un regard extérieur, parfois pas du tout expert sur la matière, qui vient juste constater comment ça se passe et qui donne un avis qui sont des recommandations faites, et qui sont contraignantes. On doit apporter des réponses à ces recommandations. Il y a plusieurs niveaux, soit la recommandation est urgente, très importante et donc des moyens seront alloués pour les résoudre. Normalement donc on a tout un panel de recommandations et dans un certain temps, on doit répondre avec des actions concrètes.

5. Quelle est l'importance des ressources octroyées par les organes de gouvernance ?

Bien sûr, s'il n'y a pas de ressources, on va être limiter dans les réponses qu'on va apporter. Voilà c'est toujours la même chose dans une entreprise, c'est une question de priorité et le comité de direction met des priorités importantes sur les recommandations de l'audit. Ces sont des choses sur lesquelles il y a une pression importante, donc si on doit choisir entre réaliser une étude stratégique qui fait partie de mon "BAU", mais qui n'est pas, voilà qui peut être reporté de quelques mois ça ne changera rien. Si une recommandation d'audit est importante sur la table, on commencera à travailler sur celle

là. Donc c'est une question de ressources bien sur, mais de priorisation aussi dans les tâches.

6. Que pensez-vous du fait que « trop de contrôles tuent le contrôle » ?

Je pense que tout le monde est responsabilisé, il y a une culture du risque qui est très présente dans l'entreprise, donc il y a un risque management qui est un rôle important, qui est un vrai poids de seconde opinion, donc comme j'ai déjà expliqué, si la seconde opinion n'est pas favorable, il est quasi certain que la proposition de la première ligne ne passera pas, donc c'est quelque chose qu'on intègre. On sait qu'on ne peut pas dévier d'un certain appétit au risque, et donc on intègre ça. Il y a vraiment une prise en compte des risques, il y a un framework qui est établi. Il y a en tout cas, pour la partie investissement, il y a une connaissance dans les équipes de première ligne de quel est le framework, donc quel est l'espace de risque dans lequel on peut jouer, quelles sont nos contraintes et on essaie de tenir compte de ça dans nos propositions. Et au niveau de la troisième ligne de défense, donc le département audit, il a un rôle qui est important, qui est reconnu par le management committee, et pour lequel il y a aussi des priorités, une pression assez importante. Je pense que chacun joue son rôle et l'importance du rôle est reconnue par tout le monde et donc in fine, tout le monde intègre cette culture du risque.

On ne va pas chercher des éléments d'analyse de la deuxième ligne de défense, on va chercher là une approbation de ce qu'on a fait. Il y a une direction Risk Management qui est identifiée, il y a une direction audit qui est identifiée, ce sont deux directions qui sont indépendantes, de toutes les autres directions, de tous les autres départements qui représentent la première ligne de défense.

7. Y-a-t-il un juste équilibre à adopter entre l'indépendance des fonctions et la collaboration ?

Non la collaboration je dirais que c'est plutôt une question de relations interpersonnelles et chacun a un rôle à jouer, il y a une force de proposition et il y a une force d'opinions.

Chacun joue son rôle et voilà. 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.

C'est une question de responsabilisation des personnes en charge de jouer leur rôle et une question de pouvoir aboutir sur un compromis. Donc c'est plus question de relations interpersonnelles et d'être sûr que chacun joue bien son rôle plutôt. C'est une question des responsabilités par rapport au contenu de sa fonction. Si chacun joue son rôle et que chacun responsable et parvient à écouter l'autre et trouver un compromis avec l'autre. Je pense qu'un truc qui est super important, c'est qu'on puisse se mettre à la place de l'autre et comprendre pourquoi il y a une certaine opinion ou pourquoi il a une certaine analyse et une fois qu'on fait ça, on se dit "bah ouais si j'étais à sa place j'aurais sans doute les mêmes remarques, c'est justifié ou alors je n'aurai pas les mêmes remarques c'est pas justifié, mais j'en discute et j'essaie de convaincre mon interlocuteur".

Donc voilà parce que quand tout le monde est responsable, quand tout le monde veut faire fonctionner la boîte, quand tout le monde est conscient que la culture de risque c'est quelque chose d'important voilà.

8. Pensez-vous que les différences de rémunération entre les deux premières lignes de défense peuvent influencer leur effectiveness ?

Je ne sais pas si ça se vérifie, j'ai aucune idée des différences de rémunération et première et deuxième ligne. Je sais qu'il y a un framework de rémunération, de définition de fonctions qui est assez standardisé, donc dans le schéma qu'on vit tous les jours dans notre entreprise, il y a un poids de fonction qui est défini, qui définit un midpoint de rémunération et un minimum et un maximum autour de ce midpoint. Ça fonctionne partout de la même façon, je pense qu'il y a une différence quand on est dans la seconde ligne de défense, c'est que s'il y a une partie variable, cette partie variable ne peut pas être liée aux résultats de l'entreprise, ce qui est sain. Je suis même pas sûr que c'est comme ça que ça fonctionne, mais je pense que c'est comme ça que ça fonctionne et dans cette situation, c'est sain parce que la seconde ligne n'a pas à s'inquiéter du résultat de la compagnie pour pouvoir produire ses opinions, et ça donne de l'indépendance.

De l'autre côté si bien sûr, il y a moins de salaire variable, j'imagine que quelque part ça doit être reconnue aussi. Il y a peut-être une variable qui n'est pas basé en tout cas sur les résultats de l'entreprise, donc peut-être il a calculé différemment. Je crois que le lien avec le résultat de l'entreprise est complètement coupé pour la deuxième ligne de défense, mais après est-ce qu'il y a des différences importantes entre les rémunérations des uns et des autres, je ne crois pas parce qu'on observe des mouvements horizontaux dans les équipes, où quelqu'un qui est dans la première ligne, peut faire un move dans la seconde ligne et inversement, des gens qui étaient dans la seconde ligne rejoignent la première.

Quand quelqu'un qui est à la première ligne va à la seconde, en effet il a une conscience de ce qui se passe à la première ligne, donc forcément il a des sensibilités, et voilà il a déjà un know-how.

C'est une obligation de s'adapter, donc on doit répondre à certains standards, c'est une contrainte qui s'impose à nous.

Le modèle il va rester le même, il y aura toujours les trois lignes de défense. Si la première ne s'adapte pas aux nouvelles contraintes, on aura des remarques de la deuxième, et de la troisième, parce que l'audit interne joue aussi un rôle sur la première ligne, on est audité régulièrement sur ce qu'on fait. Donc en effet, il y a une vérification que les contraintes Solvency 2 sont bien respectées.

9. Quels sont, selon vous, les autres facteurs influençant l'effectiveness du modèle ?

Oui si la collaboration ne fonctionne pas bien entre la personne qui font partie des trois lignes, mais en tout cas ce sont des points de blocage qui vont apparaître dans la gestion de l'entreprise, parce que la troisième la deuxième et la première ligne doivent trouver un consensus sur est-ce qu'on travaille bien, ou est-ce qu'on travaille pas bien. La première va penser qu'on ne travaille pas bien et la troisième aura un avis contraire, la deuxième va être au milieu.

Si les personnes ne s'entendent pas, je pense que le modèle peut être effectif mais il va jouer un rôle bloquant leur même dans la gestion d'entreprise

Peut-être la conscientisation au risque, c'est quelque chose qui pourrait jouer. Si tout le monde considère que les auditeurs de la troisième ligne n'ont aucun rôle à jouer quand on est dans la première ligne. C'est important que tout le monde soit conscient que les risques dont on doit tenir compte et qu'on doit couvrir c'est quelque chose qui joue sur la survie de l'entreprise.

Donc l'awareness au risque, c'est quelque chose qui est important. Si c'est dans la culture, s'il est soutenu par le management, si c'est mis comme une priorité dans l'entreprise ça joue un rôle par rapport à une entreprise où ce ne serait pas le cas. Je pense que l'effectiveness du modèle va être influencé par ça aussi.

Est ce que la direction donne justement cette direction de dire "voilà les risques c'est ma priorité, je veux que mon entreprise survive à telle crise et je veux que tous les acteurs de cette gestion de risque puisse jouer leur rôle".

Donc les relations interpersonnelles, la culture.

9. Annexe 9 : Interview n°9

1. Explication du sujet du mémoire

2. Présentation de l'interviewé, de son parcours, de son rôle dans son entreprise et de son entreprise

Je fais partie effectivement de l'équipe risk management, je suis la personne de contact de l'audit interne pour le CEO, donc en l'occurrence les trois lignes de défense, ça me parle, puisque c'est quelque chose que je revois, j'évalue constamment dans mes audits.

Moi mon but, c'est de revoir un ensemble de processus et un ensemble de business y compris la première et la deuxième ligne de défense. Je ne peux pas passer à côté d'un problème en disant, "c'est la deuxième qui devrait le faire ce n'est pas moi". Je suis obligé de donner si tu veux une assurance complète, une assurance raisonnable mais sur un business complet. Après j'é mets la recommandation, front office peut venir avec un plan d'actions ou autres. A moi de décider que la solution qu'il me propose permet d'atténuer les risques pour la ramener à niveau résiduel acceptable.

3. Comment le modèle est-il appliqué au sein de votre entreprise ?

Ici dans la banque, si tu veux c'est un modèle exigé la European Central Bank, et plus précisément EBA, European Bank Authority qui sort, pas mal de papiers sur le modèle des trois lignes de défense. Il y a une imposition de plus en plus vers un modèle comme ça, de trois lignes, voir de quatre lignes si tu mets les régulateurs à l'intérieur. Le principe, ce modèle est ce qu'il est appliqué dans la banque, oui. Il y a des obligations. Il y a un front office en 1ère ligne, la 2ème c'est le risk management, la troisième l'audit interne, et la quatrième l'audit externe.

Le principe, c'est d'abord, la séparation des fonctions, s'assurer qu'il y a une vraie muraille de chine entre la fois, ceux qui font le front et ceux qui sont censés les contrôler. La deuxième ligne va proposer des critères, donc on est dans une banque, tu prends on fait du crédit d'investissement, le principe c'est de dire "ok je mets en place des critères à

suivre, tu ne peux pas racheter autant, tu ne peux pas investir dans tel type de choses, tu ne peux pas traiter avec tel type de personnes, par exemple.

Le front doit appliquer ces critères qui ont été soumis par le risk management, et validés par le conseil d'administration. Le conseil d'administration, sur base des critères et des risques identifiés par le risk management, va élaborer ce qu'on appelle le risk appetite d'une banque. Quels sont les risques on est prêt à prendre, ou pas, quels sont ceux ce qu'on pourrait prendre moyennant certaines accommodations (les contrôles donc que je mets en place).

Une fois qu'on a identifié ces risques-là, toujours par le risk management, on va quantifier ces risques. Par exemple on a identifié qu'on avait un risque de crédit, on va le quantifier, il nous coûterait combien ? Pour le risque de crédit, qui doit mettre quoi du capital, qu'en est-il du buffer ? La question c'est de savoir effectivement chaque fois que tu prêtes de l'argent je dois mettre un buffer derrière au cas où. Donc je le quantifie pour donner effectivement une quantification sur ce risque-là.

Une fois que je l'ai quantifié, j'apporte une réponse aux risques, parce que c'est extrêmement important, cela fait partie des principes du risk management. Donc j'identifie mes risques, je les quantifie, une fois que je les quantifie je peux apporter une réponse.

Mais quelle réponse ? Est-ce je garde ce risque, est-ce que je le transfère en prenant une assurance, est-ce que je l'évite ? Comme toute société commerciale, une banque vit aussi sur des risques.

Une fois qu'on a fait ça on va élaborer ce qu'on appelle le risk appetite. C'est toujours un truc très high level, que le conseil va définir. Là va se décliner si tu veux les limites, les setups à mettre en place dans les différents business units, qu'eux doivent suivre ça. Et puis on a un quatrième principe du risk management, c'est de pouvoir monitorer tout ça, "m'assurer que ce que je t'ai demandé de suivre comme critères, tu les suis bien", c'est ça le rôle de la deuxième ligne.

La première ligne fait son activité de première ligne, elle est au front, elle vend,... La deuxième ligne y met des gardes fous. "Voici mes limites et tu dois les respecter". Mais je

dois faire aussi un monitoring, parce que je dois rapporter, ça c'est le cinquième principe du risk management. Il faut le rapport au management, au dessus, que ce que je t'ai demandé de faire et ce qu'ont validé les administrateurs, c'est bien qu'on suit en front. Intervient avant la troisième ligne, mon rôle à moi, c'est de m'assurer que la deuxième ligne a fait son travail de deuxième ligne, et qu'elle l'a effectivement monitoré. Donc alors qu'elle a bien mis des critères tels que définis plus haut, que la première ligne a bien respecté ce que la deuxième ligne a demandé de faire, que la deuxième ligne a bien monitoré, donc les rapports sont bien partis vers le haut, et enfin, mon seul objectif c'est d'apporter ce qu'on appelle de l'assurance raisonnable aux administrateurs

La quatrième ligne, si moi je prends des régulateurs, ce sont eux qui font une inspection au sein de la banque, ils vont aussi vérifier ce que j'ai fait. Regarder si la troisième ligne a bien fait son travail, en rapport avec la 1ère et la 2ème ligne. Moi je peux aussi faire des recommandations à la première ligne par exemple. Il y a des textes extrêmement précis sur les modèles et au sein de la banque, effectivement, on a bien installé ce côté première deuxième ligne et troisième ligne. C'est en soi une obligation. Il existe EBA et BIS qui réglementent, cadrent parfaitement ces modèles.

Pour moi c'est un des principes de base, quand tu mets en place des contrôles tu dois toujours te poser le principe, la question suivante, "est-ce que mon contrôle ne coûte pas plus cher que le risque que je prends ?". Le cost/income du contrôle finalement. Par exemple je prends un risque, quelle est la probabilité que mon risque arrive, et quand il arrive, quel est son impact potentiel, et donc je dois pouvoir chiffrer l'impact.

Par exemple, si je fais ça, ça risque de me coûter 100 euros, par contre si je mets le contrôle en place et qu'au final ça me coûte 400/500 euros, alors je ne le prends pas. C'est ça la quantification, qu'est-ce que je suis prêt à prendre, qu'est-ce que je suis prêt à accepter, qu'est-ce que je vais absolument pas accepter, ... et donc du coup quand tu vas mettre en place des contrôles, c'est une question que tu vas poser en permanence, mais en permanence.

Est-ce que le modèle est bureaucratique ou pas, tout dépend de ce que tu fais de ton modèle.

Est-ce que l'indépendance est une obligation ? Oui, sinon ça ne sert à rien en fait. Si tu n'as pas une indépendance et une séparation de fonction, qui est un principe de base, autant ne pas le faire, mais après tout dépend effectivement de la société. Si tu as une petite PME, tu ne vas pas imposer un modèle. Un patron et trois ouvriers, on va pas commencer à faire des séparations dans tous les sens. Par contre, dès que tu commences à avoir un certain nombre de personnes, tu as bien intérêt à distinguer les fonctions. Sinon tu peux avoir aussi fatalement de la fraude. Si la personne qui fait à la fois le recrutement, à la fois des paiements, à la fois le contrôle des paiements plus la comptabilisation de paiements, quels contrôles tu as ? Comment est-ce que tu t'assures que quelqu'un n'est pas en train de tricher ?

4. Y-a-t-il un juste équilibre à adopter entre l'indépendance des fonctions et la collaboration ?

La limite si tu veux c'est peut-être une limite humaine. Imaginons qu'une première d'une de défense ne s'entend absolument pas avec sa deuxième ligne parce que elle estime qu'ils sont venus pour la faire chier et que la deuxième ne s'entende surtout pas avec la troisième qui sont venus juste là pour m'emmerder, ... C'est une culture en fait, la culture de risque au sein de l'entreprise. Est-ce-que ton entreprise que tu vas aller visiter a une certaine maturité au niveau de la conscientisation par rapport au risque ou pas ?

Si tu as visé une banque, oui la culture du risque est peut être plus présente parce que les banques se sont cassés la gueule, parce que des failles arrivent, parce que des fraudes sont là, parce que le monde digital est là, parce que les cybers attaques sont là,... Il y a une conscientisation, que ce soit au front, etc... Le front dit "j'ai besoin d'avoir des gardes fous en haut", et puis en haut il dit "c'est bien d'avoir encore un autre garde fou".

C'est le cas dans les banques, ou dans d'autres entreprises plus matures, que tu trouveras tête dans une entreprise plus petite, nouvelle, si tu prends une startup tu vas pas avoir cette notion là. Je compare toujours, tu n'as pas d'enfants, quand ils sont tout petits, ils sautent dans tous les sens, ... puis vers 10 ans, tu les vois que les mecs ils prennent conscience que sauter de ce fauteuil, il risque de lui casser une jambe donc il le ferait peut-

être moins. On a une autre perception par rapport aux risques. Tu prends une conscience en fait de tes propres limites et donc des risques.

Et donc si tu prends une start up qui commence, en général il y a trois gus sur cette startup, ça bosse énormément, ils ne vont pas commencer à se poser la question des séparations des quatre lignes,... plus la startup avance, plus elle se construit en entreprise en petites pme etc, elle va commencer à réfléchir. On commence à avoir de l'argent faire tourner, une trésorerie et du cash etc... On peut penser à demain, il faut remettre de l'argent... et puis l'entreprise est beaucoup plus grande ou une entreprise qui existe depuis des années, enfin elle arrive une certaine maturité de conscientisation de tous, et garder cette culture, et te dire-attention.

La culture du risque ce n'est pas juste une question de deuxième ligne, de troisième ligne, de première ligne,... c'est l'ensemble des collaborateurs de l'entreprise qui doivent se dire "avant de faire un truc, on réfléchit".

Dans une banque, beaucoup plus important, puisque on travaille d'abord avec l'argent des gens, qu'on a une certaine intégrité à démontrer. Le jour où ton banquier ne fait pas bien son travail, tu ne lui feras plus confiance.

Donc fatalement oui, il doit y avoir une conscientisation de qu'est ce que je fais avec l'argent des gens. Je dois démontrer quand même une certaine crédibilité, une certaine intégrité.

Et puis attention, c'est une banque, avec des systèmes, de la cyber, des contrôles, c'est la fraude, tout le monde doit être conscient à se poser ces questions de bon sens finalement. C'est ce que j'appelle la conscientisation du risque. Tu n'as pas le même niveau de responsabilité aujourd'hui que tu ne l'avais il y a quinze ans.

5. Cette conscientisation émane-t-elle de la culture du risque ?

Exact, la culture du risque c'est quoi, c'est la culture d'entreprise. Est-ce que ton entreprise est une entreprise qui effectivement dilue un peu et fait passer ce message, en disant attention. Ou est-ce que c'est une entreprise qui n'est pas très risqué mince; ça peut être le cas. Mais encore une fois tout dépend de la maturité dans l'entreprise, du

business model de l'entreprise et il est clair que tu n'attendras pas d'une start up, le même niveau de confiance ou de risques awareness d'une entreprise pharmaceutique par exemple. Un exemple très important, l'entreprise pharmaceutique, c'est potentiellement du poison pour des gens. Ou si tu prends de l'agroalimentaire c'est aussi quelque chose d'extrêmement important, quality check, ... Encore une fois c'est en fonction de ton business, de ce que tu fais comme business, mais en même temps tu vas le voir que les entreprises de plus pérennes, c'est des entreprises qui ont cette conscience effectivement, de s'assurer en bon père de famille.

6. Est-ce que c'est la régulation ou la culture du risque qui influence cette conscientisation ?

Les deux, parce que quand tu regardes les nouveaux modèles de défense, c'est assez neuf, surtout après la crise. Mais oui mais la culture joue aussi, est-ce que la culture est influencé par la réglementation ou l'inverse ? Je dirais les deux.

Si tu as une banque qui est très risk minded, en général elle s'en sort. Tout ça parce qu'il y a une culture, si tu avais pas les gens avec cette culture de risque, de conscientisation du risque, je ne suis pas persuadé que tu peux faire la même chose.

Donc oui les deux. Si tu as un management, c'est ce qu'on appelle en anglais "tone of the top", c'est toujours d'en haut que l'exemple vient. Si en haut, ils s'en foutent complètement, fatalement la culture derrière ne vas pas suivre nécessairement. Mais je pense que oui, je pense que, j'allais dire les deux surtout influencent, les réglementations certainement. Les réglementations, ce qui est intéressant, elle met un cadre, alors tout le monde maintenant suit ça.

Parce que le risque c'est que si tu prends donc dans le monde financier, la personne qui prend qui sera le plus "risk averse" peut-être, passerait à côté de certains marchés, que d'autres qui seraient peut-être moins "risk averse" prendraient. Mais maintenant la réglementation, ce qui est intéressant avec la réglementation, c'est comme elle l'impose à tout le monde, au moins on part sur les mêmes bases.

7. Que pensez-vous de l'audit externe, pourquoi est-elle considérée comme quatrième ligne de défense ?

Moi quand je dis interne parce que ton réviseur te donne de l'assurance sur tes chiffres. Il dit en fait que ce que tu as mis dans ton bilan, que ce que tu as mis dans ton compte de résultat reflète l'image de la société. Donc pour le management d'abord, c'est de dire qu'on a bien fait le travail mais pour l'extérieur surtout. Si toi tu veux faire du business avec nous, et tu as vu que notre bilan a été validé par un réviseur externe, qui est complètement indépendant, même si tu le payes, il est indépendant, en plus il engage sa crédibilité. Mais pour pouvoir faire ça il fait aussi qu'un appelle processus en alterne, comment est-ce qu'on a fait, jusqu'à l'élaboration de... il va beaucoup plus loin.

Donc il apporte à la fois au management cette assurance supplémentaire, mais aussi pour l'extérieur c'est extrêmement important. C'est pour ça qu'on peut considérer comme une quatrième parce qu'il intervient quand même d'une manière ou d'une autre en interne. L'interaction, elle est là, moi je suis en interaction avec les réviseurs externes qui peuvent se baser sur mes travaux, comme moi je peux aussi me baser sur leurs travaux. Le risk management peut être aussi en collaboration avec des réviseurs puisque les réviseurs peuvent venir en disant "tiens vous avez pris des provisions mais on estime que d'autres provisions sont nécessaires,..." donc il y a de l'interaction, donc on peut pas dire qu'ils soient complètement en externe en fait. Ils sont en externe, parce qu'ils donnent cette certification de manière indépendante sur les comptes de résultats mais pour pouvoir faire ça, ils viennent aussi en interne, pour justement s'assurer que... et donc il y a une interaction entre la deuxième et eux, et entre la troisième et eux, parfois même la première et eux.

C'est extrêmement important, c'est pour ça qu'on appelle dans le modèle, tu vois parfois dans les modèles qu'il est considéré comme une quatrième puisque c'est aussi un pilier important. Si lui constate un risque important, il ne va pas le laisser comme ça, il a le droit et d'ailleurs quand tu regardes dans une banque, l'organe de conseil d'administration nomme deux organes importants, qui sont ces adviseurs, le comité d'audit et le comité des risques. Le comité d'audit, c'est lui qui engage les réviseurs, qui viennent lui apporter ses résultats, au même titre que l'auditeur interne.

Donc oui c'est quand même extrêmement important, donc je ne dirais pas qu'il est juste un acteur externe, tu te bases sur les travaux de l'entreprise, tu es obligé d'interagir avec des gens internes. Les gens en interne, oui, tu es auditeur, donc tu parles le même langage, on a la même indépendance, puisque moi e, tant qu'une troisième ligne je suis complètement indépendant du management. Mon patron c'est le comité d'audit avant tout.

8. Est-il important de développer un vocabulaire dans l'entreprise, une sorte de sémantique pour vraiment créer cette notion de gestion des risques ?

L'idéal oui, c'est pas toujours aussi facile, mais l'idéal oui. C'est ce qu'on appelle effectivement une espèce de risk academy. Ce serait l'idéal pouvoir justement parler la même langue, etc... Ce qui se fait souvent en fait dans les entreprises, c'est qu'on crée effectivement une même nomenclature, une façon de décrire un risque, sur bases de par exemple de frameworks existants, ici en l'occurrence, on va prendre du COSO, ou du COBIT pour tout ce qu'est IT.

Il est clair qu'on prend effectivement une nomenclature et un framework de contrôles qui parlent à tout le monde pour que les différentes lignes puissent parler le même langage. Les différentes fonctions de contrôles puissent parler le même langage, risk & compliance, legal, audit,... Pour avoir justement quand on dit par exemple un risque opérationnel on sait de quoi on parle, quand on dit un business risk, on sait ce qu'est un business risk, c'est quoi le strategic risk,... En audit interne, on se base parfaitement sur ceux-ci pour les process, tout comme la deuxième ligne de défense.

9. Comment analysez-vous justement l'interaction avec la première ligne de défense ?

Alors il faut d'abord aussi définir qu'est-ce que c'est que c'est la première ligne. Souvent les gens nous disent "Front office c'est la première, et le back c'est la deuxième". Non, le back office c'est toujours considéré comme étant première ligne de défense, c'est très important pour tes recherches. Par exemple la personne qui est au front et qui va vendre, et puis il y a un gars qui va faire de l'administration. Souvent dans des entreprises on

considère que ça c'est une deuxième. Or une deuxième pour moi, elle doit être aussi complètement indépendante, pour justement éviter ce que tu dis.

Un risk management est complètement indépendant, il n'a rien gagné, il n'est pas au front. Il travaille pour une seule boîte et donc son souci, c'est dire qu'il faut que la boîte se porte bien. Donc je vais mettre des contrôles que les gars doit mettre en place et puis moi je vais vous voir. A la limite, il n'imposerait pas le contrôle, il dit voilà "ce sont les critères que tu dois suivre". C'est plutôt la première, elle peut choisir les contrôles et peut-être pragmatique; de dire quel type de contrôle je mets en place pour assurer que ces critères sont respectés. Si toi demain, tu gères un front office, avec des mecs qui vont faire des ventes. Tu es leur manager, il est clair que tu as besoin de mettre des contrôles, parce que tu peux pas te permettre de les laisser aller à leurs trucs, donc tu devras mettre des objectifs précis, etc... et donc tu as besoin de gens qui te mettent des critères en disant "jusqu'où je peux aller par exemple, quel type de prix je peux émettre,..."

Mais toi déjà en tant que manager, la première ligne, tu as besoin d'avoir ça, c'était les premiers contrôles. Les gars des premiers contrôles c'est la première ligne, c'est eux qui sont au charbon en fait. La deuxième va émettre que des critères à mettre en place mais la manière dont tu vas les mettre, ça c'est toi qui décide.

Moi quand je viens je peux par exemple t'aider à dire "tu sais tu mets ça comme type de contrôles, mais franchement ceci serait plus pragmatique, plus efficient"

Il faut que les contrôles comme tu dis, t'apportent quelque chose, qu'ils soient added value, qu'ils t'apportent vraiment quelque chose, sinon c'est juste pour imprimer un papier et signer derrière, et juste dire que j'ai bien signé, ça ne veut rien dire. Le contrôle doit permettre effectivement d'apporter une valeur ajoutée.

Le contrôle il ne faut pas le voir aussi comme un espèce de soupçon, qu'on aurait sur quelqu'un parce qu'il va tricher. Non c'est aussi parce que tu aimerais bien que quelqu'un derrière revoie un peu ce que tu as fait tu as fait quoi. Ne serait-ce pour être sur.

Deux têtes en valent toujours mieux qu'une. Il ne faut pas voir le contrôle comme un frein. Il faut voir un contrôle, et là où tu as raison, c'est de dire il ne faut pas qu'il soient

bureaucratique, il ne faut pas qu'il ne serve à rien. Le rôle d'un troisième c'est aussi de regarder ça, de se poser les bonnes questions finalement, soyons pragmatique.

Un moment ça ne sert plus à rien et puis les gens ne comprennent plus et là du coup tu risques d'avoir le côté inverse. Comme on s'en fout complètement, ça ne va plus.

10. Selon vous, le modèle est-il effectif au sein de l'entreprise ?

Oui je pense que oui quand même on arrive à quelque chose, je dirais oui comme ça. Après c'est peut-être subjectif, c'est mon entreprise. Mais bon après est-ce qu'il y a des éléments objectifs qui peuvent sous-tendre ça, c'est effectivement une entreprise qui fonctionne, on n'a pas de remontrances des régulateurs qui nous disent "vous êtes complètement à côté de la plaque". Moi je dirais que dans notre entreprise ici, le modèle fonctionne. Est-ce qu'il fonctionne toujours bien, oui. Est-ce qu'il y a des améliorations possibles, certainement, toujours. Puisque le monde change, le monde avance, donc le modèle doit changer.

Dis-toi une chose, on ne fait plus le même business bancaire qu'on le faisait il y a dix ans, quinze ans. Par exemple, avec la robotique, avec la digitalisation, c'est un autre risque, c'est d'autres contrôles, c'est une autre vision. Tu vois aujourd'hui les frontières sont assez poreuses en fait, tout est digitalisé, tout est sur des systèmes IT,... il faut pouvoir mettre des contrôles, la séparation du modèle, tu dois le mettre aussi dans des systèmes. Il y a des systèmes aussi qui existent, donc le modèle en soit, il est bien mais le modèle il faut aussi le faire tourner à la lumière des nouvelles technologies, de l'évolution, du monde de l'entreprise.

Effectivement on est plus banquier comme on l'était il y a cinq ans. Ce n'est plus la même chose. La digitalisation a appelé autre chose, d'abord un, la vitesse. Un client aujourd'hui qui te demande un prêt via une application bancaire, il ne va pas attendre trois semaines. Tu fais tes achats online, tes achats, tu n'as pas envie de te dire que ce que tu viens d'acheter, tu l'auras dans trois semaines. Non, tu le veux directement. Le consommateur aujourd'hui veut, quand il fait une demande de prêt à la fin quand il a terminé, et pas avec 15 questions, il doit pouvoir le faire avec trois questions oui non et voilà vous avez votre crédit.

Le modèle est-ce qu'il va fonctionner comme il a fonctionné sur un principe de base qui était, tu venais à l'agence, tu faisais ta demande, etc... Tu suivais tout un processus prédéfini, classique. Donc la, effectivement, le modèle fonctionne. Aujourd'hui, tu dois aller rapidement, donc le modèle doit fonctionner, tu dois mettre des principes aussi IT, qui puissent générer effectivement et t'assurer effectivement toujours de cette séparation des différents niveaux de fonction pour être sûr qu'il n'y a pas eu de fraudes, pas eu de problèmes,... et qu'on a pas laissé passer un client qui était complètement insolvable et qui passe quand même. Ajoute à ça tout à la réglementation, vie privée, les données, etc... Il y a toute une série de choses. Le monde change il est en perpétuelle évolution. -Voilà donc est ce que ton modèle, le principe pour moi, il sera toujours péren, toujours effectif. Il faut pouvoir effectivement l'actionner et le faire évoluer aussi à l'aune de l'évolution de la société dans sa globalité.

11. Le modèle permet-il cette flexibilité ?

Il devrait, je ne sais pas s'il l'est. Ce serait peut-être une question que tu pourrais te poser. En tout cas comme finalité de ton mémoire, est-ce qu'il suffisamment flexible que pour pouvoir justement être suffisamment "forward looking" pour demain, ça c'est intéressant. Parce que le modèle de base est là, le principe et là, c'est un principe de bon sens.

Comment est-ce que demain ce modèle vivra ? Dans l'ère de la robotique, c'est une série de robots qui vont prendre cette décision. Comment est ce que tu fais, comment est-ce que tu t'assures ? Tu as toute une question. De plus en plus des robots prennent des décisions sur pas mal de choses Comment est-ce que tu appliques ce modèle là sur la robotique, sur cette évolution. Fatalement, tu fais évoluer les principes. La question d'effectivité, c'est comment est-ce que tu le rends effectif dans ces changements là ?

Il existe, il est là comment est-ce qu'il évolue, comment est-ce qu'il évoluera, comment ce qu'il évoluera en prenant en considération justement la robotique, le marché online, sur l'intelligence artificielle, toutes ces choses là effectivement. Comment est-ce que tu appliques ça à des machines?

Mais attention, dans d'autres entreprises c'est pas aussi facile. Une petite entreprise, le mec il fait un peu de tout quoi, il va pas commencer à engager deux personnes pour checker. Donc ça dépend de la taille effectivement et de la complexité de ton business.

Mais en même temps, attention, c'est aussi une arme de gestion, c'est de la bonne gestion aussi. Quand bien même effectivement, tu avais un business où tu produis des boulons, c'est quand même intéressant d'avoir une vraie séparation sinon tu perds de l'argent aussi.

Ca doit être permanent, cette notion de cost/income, qu'est-ce que ça me coûte par rapport à ce que ça me rapporte, ça doit être permanent. Sinon tu ne mets pas en place un modèle qui tienne la route, sans tenir compte de cette notion de coût. Ce n'est pas un truc théorique, c'est pas un truc pour faire joli, il faut que ça rapporte. Il ne faut pas oublier que t'es dans une société commerciale, mon but c'est d'apporter de l'argent.

Donc c'est extrêmement important de se dire, qu'est-ce que ça me coûte et de considérer que les contrôles que tu mets doivent être aussi des contrôles opportunistes, qui vont te rapporter mieux. C'est en mettant ces contrôles que tu vas avoir beaucoup plus.

Par exemple, j'ai une petite entreprise qui fabrique des boulons. Tu as un comptable, un autre qui fait un peu d'administration, HR, etc, et puis tu as un gars qui s'occupe de ton atelier, et un gars qui va s'occuper voilà de circuler, donc ton commercial. Tu vas donc instaurer un système de contrôle. L'administrateur vérifie que le commerce a bien fait ce qu'il a rentré, le comptable va vérifier que c'est bien la facture de monsieur x, et puis ton chef d'atelier, il va produire certainement, il va quand même vérifier que le bon de commandes que le commercial a reçu, que c'est bien ce bon de commande là qui correspond à monsieur x et à la fin le comptable il va vérifier, à la fois la production, qu'est-ce qui a été produit pour monsieur x, c'est bien ce que le commercial avait demandé et c'est bien que l'administrateur.

Imagine que tu n'as personne qui vérifie tout le bazar, tu perds de l'argent. Pourtant tu as une entreprise de cinq personnes, mais si tu n'as pas mis en place des contrôles strictes, tu t'en sors pas.

Alors la question si j'avais mis des contrôles, oui ce serait peut-être un peu lourd, mais c'est important. Et ce qui fait la pérennité d'une entreprise, peu importe l'entreprise, cette

notion de coût tu dois l'avoir en permanence. Et à chaque fois que tu mets de nouveaux contrôles, tu dois te poser question.

12. Est-ce que l'information qui circule entre les lignes de défense, au sens propre, peut influencer l'effectiveness du modèle des trois lignes de défense ?

Peut-être si tu n'as pas les contrôles nécessaires, mais on revient toujours à ces contrôles. Imaginons, tu parles de base de données, mais les bases de données, il y a aussi des risques informatiques, car les informations ont été introduites par une main humaine, obligatoirement. Est-ce qu'il y a des contrôles à l'intérieur de la machine ? Vérifier qu'il n'y a pas de duplicate, de double entrée,... donc il y a des contrôles dans la machine. Et comment est-ce que l'information sort ? C'est toujours ce principe de "input - processing - output". Tu as des contrôles à chaque étape, parce que à chaque étape, tu as des risques spécifiques, un risque à l'input n'est pas le même que le risque à l'output

C'est tout une question, de quel est le type de contrôles, que tu mets en place et donc quel est le degré de confiance que tu mets dans ces contrôles. Si je prends le cas d'une banque, quand je vérifie ce que la première et la deuxième font, je me dois de vérifier aussi que l'information de base est bien la bonne. Et pour pouvoir faire ça je vérifie que les contrôles sur ces systèmes IT, sont bien en place, sont effective. Le principal en audit interne, on a deux principes. Est-ce que le design du contrôle est bien, est-ce que le contrôle est adéquat, est-ce qu'il existe ? Et deuxième chose est-ce qu'il est effectif ?

Donc oui ce principe de base effectivement, sur toute l'agrégation des données, ta gestion des data c'est extrêmement important. On parlait de la digitalisation du monde qui change, c'est le nerf de la guerre aujourd'hui.

Les entreprises qui investissent des millions, parfois des milliards sur le data mining ,... ça vaut de l'argent pour eux. Dans une entreprise c'est extrêmement important, tu n'imagines même pas dans une banque, les datas c'est tout ce qu'on a, c'est notre capital.

13. Pensez-vous que l'interaction entre les deux premières lignes de défense peut-être biaisée dû à un manque de compétences de la deuxième ligne ?

Oui ça c'est possible, ça c'est le danger exactement. Imaginons que tu es un front officer qui ait beaucoup plus de connaissances et d'expertises, que la personne qui est censé le contrôler, c'est fortement possible. D'où la question effectivement de la formation, de l'expertise, et puis expertise externe aussi. Tu vas effectivement que les boîtes de conseil, de consultance explose, justement pour ça.

Reprenons l'entreprise de boulons, tu as besoin de quelqu'un pour faire un peu de la cyber security parce que tu dis "ok, je vends beaucoup sur le net,... je vais pas engager une personne pour ça". D'abord pas possible de trouver sur le marché mais c'est impayable et puis on n'a pas besoin 24/24. Tu vas faire appel à une société de contrôle, de conseil, il va t'apporter un gars qui va t'aider sur trois mois.

Ce n'est pas parce que t'es une grande entreprise, que tu as toutes les expertises. Non tu vas te faire aider, mais le danger, tu as raison, c'est qu'effectivement tu risques d'avoir des gens, mieux formés dans une ligne, première ou deuxième, d'où l'importance de mettre des critères extrêmement aux strictes peut-être aussi.

Donc la première ligne est bien obligé de suivre ces critères mais qui peut effectivement aussi discuté ces critères, parce qu'ils peuvent apporter aussi leur point de vue. C'est pas parce qu'ils sont la première ligne, qu'ils n'ont pas leur mot à dire.

La culture du risque et la culture de ce modèle, c'est un partage en fait. Mais ça restera toujours un danger, comme un peu le danger de la troisième ligne qui n'est peut-être pas suffisamment experte. Parce que le troisième ligne ne doit pas rentrer dans une expertise, elle doit comprendre les choses, mais quand même, je le vois moi-même, effectivement le monde change. Je m'occupe du risk management, ça va du marché aux crédits en passant par le risk opérationnel, et donc voilà il faut maîtriser mathématiquement, maîtriser aussi des produits derrière, et donc maîtriser les crédits,...

Il faut aussi maîtriser toute la partie statistiques et probabilités, mais aussi des modèles et comprendre des modèles, de la génération des modèles, la manière dont on monte les modèles, la manière dont calibre, en code aussi.

Est-ce que tu as tout ça ? Non, mais tu as une bonne notion et puis quand au besoin je peux apprendre d'un gars de l'extérieur, d'un consultant, qui ponctuellement va m'aider sur un sujet bien précis.

Voilà donc oui je dirais c'est le danger, mais en même temps c'est un danger qu'on vivra au fur et à mesure. Si tu n'es fait rien pendant 10 ans, c'est le danger.

C'est ça que tu dois prendre en considération dans ta vision, c'est de dire que le changement est tellement rapide, c'est de dire qu'elle est la capacité qu'ont les entreprises justement de mettre en place et de pouvoir rendre son modèle aussi flexible que d'évolutions.

14. Pensez-vous de la mobilité des fonctions entre les lignes de défense puisse influencer l'effectiveness du modèle des 3LoD ?

Oui je pense que ça valorise en tout cas la culture du risque parce qu'imaginons surtout l'inverse, imaginons tu passes à l'audit interne, puis tu retournes à la salle des marchés.

Tu es déjà profilé comme un "risk minded" beaucoup plus important, donc plus des gens effectivement circulent, pas en même temps bien sur, mais plus la culture du risque est un peu diluée dans l'ensemble des départements. Par exemple si tu prends le cas français, je sais qu'en France voilà, pour certains postes, il te demande de passer par l'inspection financière, qui est une espèce d'audit interne d'une entreprise. Ça c'est une chose

Je sais qu'effectivement on a pas mal de turnover. Par exemple, tous les auditeurs qui nous quittent, parce que ça tourne beaucoup, et bien beaucoup de gens de chez nous vont au risk management. Il y a des gens du risk management qui vont aux salles de marché, ou dans un front office. Beaucoup de managers ont suivi des cursus un peu comme ça.

Donc oui il y a quand même une culture qui s'installe en fait et que du coup en fait, quand tu as travaillé dans un modèle, ou dans un département plutôt "risk minded", tu le prendras toujours avec toi. Si ça te forge d'une manière ou d'une autre, si tu veux oui ou non, ça te forge avec toi.

Ce qui ne veut pas dire qu'il faut être complètement fermé, il y a cette notion de pragmatisme, de se dire "restons pragmatique", et qui a aidé la valeur ajoutée que j'apporte.

A ce modèle effectivement pour moi je le lierais à la culture et effectivement le fait qu'il y ait des échanges en terme humains, en termes de capacité. Si je fais par exemple un audit sur un sujet bien particulier, je vais prendre mon téléphone, je vais appeler un gars de la salle des marchés. Je vais utiliser son expertise. Après moi je me fais mon opinion mais je vais utiliser son expertise.

Comme lui par exemple s'il est en face d'une situation, et qu'il n'est pas sûr de qu'il est en train de faire, il va m'appeler.

Donc l'échange, il est là. Ca après tu installes dans une entreprise, c'est une mentalité, c'est connaître des gens... c'est la confiance, du partage, ça c'est important. Mais ça d'une entreprise à l'autre, c'est en fonction aussi de la culture de l'entreprise.

Nous on est dans une entreprise où effectivement il y a ce côté un peu on se connaît bien... Et puis l'histoire aussi je pense qui réunit aussi des gens.

Tout le monde se challenge si tu veux, tout le monde se connaît bien, en tout cas le management, la culture d'entreprise, par exemple je te tutoie directement... Avec une dimension effectivement social,... ça crée effectivement un climat de confiance et de partage. Est-ce que tout est bien ? Non, mais au moins moi c'est assez clair, si je ne suis pas d'accord avec toi je vais te le dire. Je vais émettre une recommandation, et qu'il me dit qu'il ne va pas le faire, à lui de me prouver que c'était peut-être pas nécessaire, et si en effet ça ne l'est pas, OK pas de problèmes, on continue.

Attention cette collaboration n'est pas toujours facile. Voilà j'ai eu d'autres expériences dans d'autres entreprises, c'est pas toujours évident. Mais peut-être que l'histoire, ou un passé commun, permet certainement à l'entreprise de mieux fonctionner.

Je suis persuadé que cette dimension sociale fait qu'on peut pas se permettre de jouer. Est-ce que la culture d'entreprise et la culture du risque sont liés, et donc est-ce que le modèle est effectif ? Je pense oui, je pense que c'est un tout.

10. Annexe 10 : Guide d'entretien

- 1. Explication du sujet du mémoire, rappeler le modèle des 3LoD ainsi qu'expliquer le terme effectiveness.**
- 2. Présentation de l'interviewé, de son parcours, de son rôle dans son entreprise et de son entreprise.**
- 3. Comment définiriez-vous un modèle des 3LoD efficace ?**
- 4. Pensez-vous que le modèle des 3LoD est efficace au sein de votre entreprise ?**
- 5. Comment analyseriez-vous l'interaction entre les deux premières lignes de défense ?**
- 6. Comment analyseriez-vous l'interaction entre la troisième ligne de défense et les deux premières ?**
- 7. Y-a-t-il un juste équilibre à adopter entre l'indépendance des fonctions et la collaboration ?**
- 8. Comment définiriez-vous l'interaction avec les organes de gouvernance ?**
- 9. Est-ce qu'une appétence au risque bien définie par les organes de gouvernance, influence positivement l'effectiveness du modèle ?**
- 10. Pensez-vous que la culture de l'entreprise puisse influencer l'effectiveness du modèle des 3LoD ?**
- 11. Selon vous, existent-ils d'autres facteurs pouvant influencer positivement ou négativement l'effectiveness du modèle ?**
- 12. Que pensez-vous du fait que « trop de contrôles tuent le contrôle » ? Est-ce que le modèle des 3LoD est trop bureaucratique ?**
- 13. Est-ce que l'information qui circule entre les lignes de défense, au sens propre, peut influencer l'effectiveness du modèle des trois lignes de défense ?**
- 14. Pensez-vous que les différences de rémunération entre les deux premières lignes de défense peuvent influencer leur effectiveness ?**
- 15. Quel est le rôle selon vous de l'audit externe dans le modèle ? Pourquoi, selon vous, l'on pourrait qualifier l'audit externe de quatrième ligne de défense ?**