Annexes

Liste des annexes :

Annexe 1 : Gestion du risque selon le COSO II ……..140
Annexe 2 : Comment communiquer de manière transparente ……...146
Annexe 3 : La veille réglementaire ……147
Annexe 4 : Le triangle de la fraude ……148
Annexe 5 : Grille à impact ……149
Annexe 6 : Cartographie des risques ……..149
Annexe 7 : Une communication de l'éthique efficace ……150
Annexe 8 : Étude de comparaison sectorielle des performances extra-financières ……151
Annexe 9 : Les différentes mesures éthiques et responsables pour les institutions financières …….152
Annexe 10 : Matrice RepTrak® ……153
Annexe 11 : Information complémentaire sur le risque réputationnel ……..153
Annexe 12 : Exemples d'indicateurs pour certains groupes de parties prenantes ……156
Annexe 13 : Dimensions, Sous-dimensions & Indicateurs RSE du Global Risk Initiative (GRI) …158
Annexe 14 : Équation de mesure du risque social ……159
Annexe 15 : Aspects de la communication menant à du Greenwashing ……159
Annexe 16 : Lignes directrices non contraignantes de l'EU ……160
Annexe 17 : Questionnaires vierges soumis aux différents intervenants ……..162
Annexe 18 : Résumé des interviews ……..170

Annexe 1 : Gestion des risques selon le COSO II

Modèles de Risk Management

Gardons néanmoins à l'esprit que même les managers les plus expérimentés ne sont pas conscients de tous les risques liés à l'activité de leur département respectif. C'est alors qu'adopter un modèle de risk management prend tout son sens. Dès lors, il s'agit de choisir le modèle le plus approprié à l'entreprise. (Andersen & Winther Schrøder, 2010)

Il existe une multitude de modèles de par le monde :

- En **Australie** et **Nouvelle-Zélande**: AS/NZS 4360 1994/1999/2004
- Au **Royaume-Uni**: AIRMIC / ALARM / IRM 2002
- Aux Etats-Unis et à l'international: COSO ERM 2004 (Guardians of Governance, 2014)

C'est en 2009, grâce au travail d'un groupe de conseillers techniques issus de 18 pays différents, que le standard ISO 31000: 2009 vit le jour. Le but de cette démarche était de mettre sur pied un modèle pouvant être utilisé par un grand nombre d'entreprises de taille et complexité variée et actives dans des pays et marchés différents. Cette norme donne aux décideurs un meilleur aperçu des risques pouvant compromettre l'atteinte des objectifs et leur permet de mieux évaluer l'efficacité des contrôles déjà mis en place. (Musweu, s.d.; ISO, 2018)

Bien que le modèle ISO et COSO soient très similaires, nous allons davantage nous intéresser aux modèles issus du COSO et plus particulièrement celui du COSO II - Enterprise Risk Management (ERM) car ce dernier est plus spécifique et intègre mieux la notion de Risk Appetite et de gouvernance dans son processus.

COSO I - Internal Control

Afin de mieux comprendre le COSO II - Enterprise Risk Management Framework, penchons-nous d'abord sur le COSO I - Internal Control. Une première version du COSO I - Internal Control (IC) vit le jour en 1992 et fut, ensuite, mise à jour en 2013 afin d'intégrer les changements au niveau des opérations et de l'environnement économique des 20 dernières années. Par exemple, ces changements prennent en compte la globalisation des marchés, les concepts liés à la gouvernance, les nouveaux business models (avec l'inclusion de parties tierces), les nouvelles lois et régulations en termes de protection des parties-prenantes et de reporting externe, les nouvelles compétences et responsabilités du personnel dues à la complexité grandissante des entreprises, les technologies de systèmes d'informations ou encore la considération accrue des risques de fraude dans la fonction de risk management. (KPMG, 2013)

En revanche, les 5 composantes du contrôle interne de 1992 restent identiques à celles de 2013 (Contrôle de l'environnement, Évaluation des risques, Activités de contrôle, Information et communication, Pilotage[1]). Cependant, nous ne nous attarderons pas davantage sur les composantes du COSO I - Internal Control puisque ces composantes se retrouvent en intégralité dans le COSO II - Enterprise Risk Management (ERM), modèle que nous allons analyser en détails ci-après. (KPMG, 2013)

(Catillo, 2017) (Opgenorth, 2017)

COSO II - Enterprise Risk Management (ERM)

Comme visible sur les graphiques ci-dessus, les modèles de COSO I - Internal Control et de COSO II - Enterprise Risk Management Integrated Framework sont très similaires. Nous pouvons, cependant, remarquer deux changements majeurs entre les deux modèles. Le premier est qu'en plus des trois catégories d'objectifs déjà présents dans le COSO I (*Operations, Reporting, Compliance*) une quatrième catégorie d'objectifs vient s'insérer dans le COSO II, un objectif Stratégique. Le deuxième changement, est que la partie *Risk Assessment* du COSO I est détaillée en quatre sections dans le COSO II, à savoir : *Objectives setting*, *Event Identification*, *Risk Assessment* et *Risk Response*. Ainsi, nous pouvons dire que l'Enterprise *Risk Management* englobe l'*Internal Control* mais l'ERM porte une plus grande attention au Risk Management. Notons également que l'ERM étend l'objectif de Reporting pour y intégrer l'Internal Reporting. Finalement, l'ERM introduit la notion d'appétit aux risques et de tolérance aux risques que nous développerons ci-après. (Protiviti Inc., 2006)

[1] Monitoring Activities

3.4.1 Objectifs de l'ERM

Toute entreprise se doit d'avoir une mission, une vision globale qui régira la façon dont le top-management établit la stratégie de l'entreprise et définit des objectifs stratégiques pour l'ensemble de la firme. Ces objectifs se déclinent en quatre catégories distinctes : Stratégiques, Opérations, Reporting et Compliance. Bien entendu, ces objectifs s'entre croisent et peuvent être la responsabilité de plusieurs cadres d'entreprise. (Everson, Martens, Nottingham & Steinberg, 2004)

a) Objectifs Stratégiques

Nous l'avons vu, avec l'Enterprise Risk Management, stratégie et gestion des risques sont étroitement liés. Ces objectifs doivent être ambitieux et alignés avec la mission globale.

Tout le monde dans l'entreprise a une responsabilité vis-à-vis du risque. Dans le but de guider chacun et plus particulièrement les Risk owners (*la personne qui, en fin de compte, sera tenue pour responsable d'assurer que les risques liés à ses activités soient gérés de façon appropriée* (Stanford, s.d.)) dans leur gestion du risque, l'entreprise est tenue de définir sa Risk Culture. La culture de risque est déclinée en plusieurs types de décisions. C'est elle qui établit la nature du système de récompenses, le niveau de formalisation qui règne dans l'entreprise ou encore l'ambiguïté des objectifs. A titre d'exemple, une culture moins averse au risque se reflète par une tendance du top-management de faire davantage confiance en leurs employés. (Bozeman & Kingsley, 1998; Everson, Martens, Nottingham & Steinberg, 2004; Nagumo, 2005)

b) Objectifs Opérationnels

Les objectifs opérationnels, quant à eux, visent à consommer les ressources à la fois de manière efficace et efficiente. (Everson, Martens, Nottingham & Steinberg, 2004)

c) Objectifs de Reporting

Concernant les objectifs de reporting, le management doit s'assurer d'établir un système de reporting fiable. (Everson, Martens, Nottingham & Steinberg, 2004)

d) Objectifs de Compliance

Finalement, en ce qui concerne les objectifs de compliance, le management doit s'assurer que les activités de l'entreprise soient en règle avec les lois et régulations en vigueur. (Everson, Martens, Nottingham & Steinberg, 2004)

3.4.2 Composantes de l'ERM

L'Enterprise Risk Management Framework comporte huit composantes corrélées les unes aux autres et découlant directement de la stratégie et de la culture de l'entreprise. Ce sont ces composantes qui

régissent le processus de management de l'entreprise. Bien que ces composantes soient présentées dans un certain ordre, il est important de garder à l'esprit que chacune de ces composantes interagit avec les autres et non uniquement avec la suivante. (Everson, Martens, Nottingham & Steinberg, 2004)

a) Contrôle de l'environnement

Cette composante décrit la voie à suivre que le top management indique au reste de l'entreprise en termes de philosophie de risk management, d'appétit aux risques (définit la propension d'une entreprise à tolérer un certain niveau de risque ou non), d'attribution d'autorité et de responsabilités, de l'engagement du conseil d'administration envers les valeurs éthiques, de formation et développement des compétences des employés. (Everson, Martens, Nottingham & Steinberg, 2004; Pritchard, 2015; Protiviti Inc., 2006)

Par ailleurs, l'entreprise ne peut pas se limiter au contrôle de son propre environnement. Il est crucial d'également contrôler l'environnement des clients et fournisseurs de l'entreprise puisque tantôt la culture risque du client remplacera celle de l'entreprise, tantôt la culture risque de l'entreprise remplacera celle des fournisseurs. (Pritchard, 2015)

b) Détermination des objectifs

Le top-management établit des objectifs stratégiques qui fourniront, ensuite, un contexte pour les objectifs opérationnels, de reporting ainsi que de compliance. L'ERM assure que le top-management ait un processus pour déterminer ces objectifs et cherche à aligner les processus de contrôle du risque avec la stratégie. D'ailleurs, ceux-ci doivent être établis en lien avec le Risk Appetite de l'entreprise qui déterminera la tolérance face au risque pour les différents niveaux de l'entreprise et établira les bases pour l'identification, l'évaluation et la réponse aux risques. (Everson, Martens, Nottingham & Steinberg, 2004; Protiviti Inc., 2006)

Afin que les objectifs du risk management soient constamment alignés avec la stratégie, il faut que le responsable du risk management ne soit pas juste un exécutant mais aussi un partenaire stratégique. En d'autres termes, il doit avoir un contact privilégié avec le top-management afin d'adapter les objectifs en fonction des nouveaux risques détectés. (Thel & Manwah, 2015; Chatterjee & Milam, 2007)

c) Identification des risques

A ce stade, le management identifie les événements internes et externes pouvant impacter négativement mais également positivement la capacité de l'entreprise à implémenter sa stratégie ainsi que l'atteinte de ses objectifs et de ses performances. C'est à ce stade que le management doit pouvoir distinguer les risques des opportunités. D'un côté, les risques identifiés feront l'objet d'une évaluation (*Risk Assessment*) et devront être adressés de façon appropriée (*Risk Response*). De l'autre, les opportunités

devront être intégrées en amont pour influencer la stratégie et la détermination des objectifs. Chaque département ou entité dans l'entreprise est chargé d'identifier et gérer les risques opérationnels et de conformité. (Everson, Martens, Nottingham & Steinberg, 2004; Nagumo, 2005; Protiviti Inc., 2006)

Il existe de nombreuses méthodes d'identification du risque utilisées en entreprise. Les équipes de gestion du risque sont très regardantes sur l'identification des risques, à cause de la tendance naturelle à ne voir que les choses négatives, mais le sont légèrement moins quant à l'identification des opportunités. Il est donc important d'utiliser des méthodes permettant d'identifier facilement les risques comme les diagrammes de cause à effet, des systèmes dynamiques ou encore des diagrammes d'influences. Mais aussi des techniques permettant de pousser les responsables à aller au-delà des risques négatifs afin de capter des opportunités tels que les techniques de l'identification SWOT[2], l'analyse des contraintes et hypothèses[3] ou encore l'analyse des rapports de force[4]. Notons que dans le secteur bancaire, le risque est généralement classé en trois catégories : les risques de marché, les risques de crédit et les risques opérationnels. (Hillson, 2002; Nagumo, 2005)

d) Évaluation des risques

Le stade suivant consiste en l'élaboration de scénarios par le biais d'une évaluation quantitative des risques, permettant de connaître l'impact potentiel des risques en fonction de modèle mathématique intégrant différentes variables (le coût, la durée, les ressources nécessaires, …) avec des modèles comme des analyses sensitives[5], des arbres de décisions[6] (decision Trees) ou encore l'analyse Monte Carlo[7]. L'analyse doit se faire aussi par le biais d'une évaluation qualitative permettant d'analyser la probabilité et les impacts potentiels par l'intermédiaire d'une analyse Probabilité-impact. Une technique efficace permettant de capter les risques ainsi que les opportunités est de représenter les deux dans une matrice à impact comme le montre le graphique ci-dessous. (Hillson, 2002; Nagumo, 2005)

---

[2] Analyse en premier lieu des forces de l'organisation ainsi que les opportunitées des objectifs et en second lieu identifier les faiblesses de l'organisation et les menaces des objectifs.

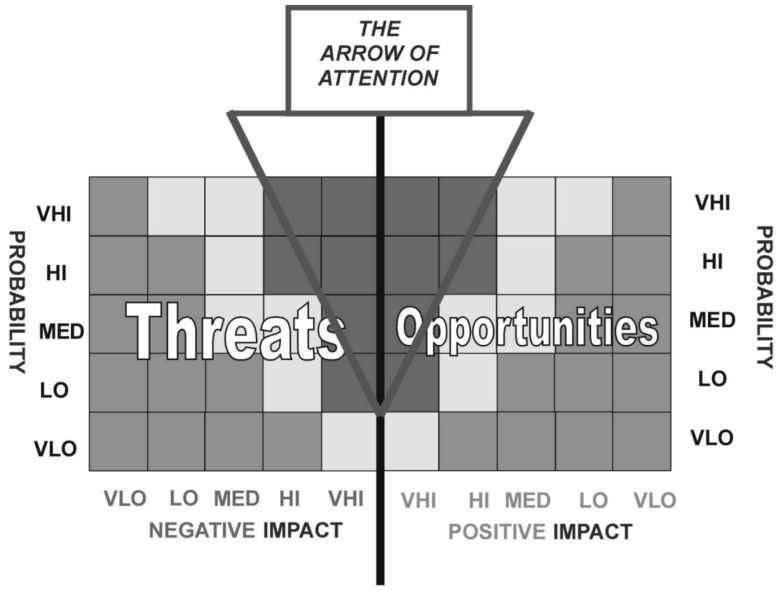
[3] Technique faisant appel à des hypothèses pour émettre des prédictions et ainsi essayer de connaître les possibles futures opportunitées tout en établissant les contraintes.

[4] Technique permettant d'identifier les éléments pouvant faciliter ou s'opposer à l'atteinte des objectifs.

[5] Analyse par le biais d'un modèle mathématique comment une variable influence une autre variable indépendante

[6] Modèle sous forme d'arbre représentant la probabilité d'occurrence, l'utilisations de ressources ainsi que l'utilité finale.

[7] Simulation de la probabilité d'occurrence de différents événements difficilement anticipables à cause de la présence de variables aléatoires



Une des spécificités de l'ERM est qu'il ne se concentre pas seulement sur un département en particulier mais prend en compte l'ensemble des risques de l'ensemble de l'entreprise afin de comprendre les interconnections des risques entre les départements et ainsi mettre un place un contrôle permettant d'intégrer plusieurs risques. Ceci permet ainsi de réduire les coûts du management des risques ainsi qu'un gain en efficacité. C'est à partir de ces scénarios que le management déterminera comment répondre aux risques en fonction de la probabilité et de l'impact potentiel. Un risque avec une haute probabilité et un important impact doit être traité de manière prioritaire (Everson, Martens, Nottingham & Steinberg, 2004; Nagumo, 2005; Protiviti Inc., 2006)

A) Réponse aux risques

Après l'identification et l'évaluation des risques, vient la réponse à ces risques. Le management va décider de la meilleure façon de gérer le risque selon une logique coûts/bénéfices. Le management peut soit choisir d'éviter, de réduire, de partager ou d'accepter le risque. La réponse optimale est sélectionnée selon le degré de tolérance et d'appétit aux risques de l'entreprise. En effet, le but de la démarche est de réduire le risque en-dessous du niveau de tolérance au risque fixé par l'entreprise. (Everson, Martens, Nottingham & Steinberg, 2004; Nagumo, 2005; Protiviti Inc., 2006)

e) Activités de contrôle

Par la suite, le management doit mettre en place des politiques et procédures à tous les niveaux de l'entreprise pour s'assurer que les réponses aux risques soient exécutées efficacement. (Everson, Martens, Nottingham & Steinberg, 2004; Nagumo, 2005; Protiviti Inc., 2006)

Il est important de noter qu'il ne faut pas implémenter des processus de contrôle d'activités trop lourd pour n'importe quel type de risque. Cela a pour résultat de frustrer l'employé ainsi qu'une difficulté plus

grande à capter les opportunités car le délai de réactivité est également plus long. (Chatterjee & Milam, 2007)

f) Information, communication & reporting

Par ailleurs, pour s'assurer que les employés de l'entreprise puissent tenir leurs responsabilités, l'entreprise doit identifier, récolter et communiquer les informations pertinentes provenant à la fois de sources internes et externes à l'entreprise. De plus, ces informations doivent être communiquées à tous les niveaux de l'organisation (aussi bien en amont qu'en aval). D'ailleurs, certains outils, comme le *Balanced Scored Card*, peuvent faciliter la transmission et la communication des informations stratégiques. (Everson, Martens, Nottingham & Steinberg, 2004; Nagumo, 2005; Protiviti Inc., 2006)

g) Pilotage

Finalement, le pilotage est une étape aussi importante que les précédentes puisqu'elle permet d'évaluer le fonctionnement des différentes composantes de l'ERM ainsi que leurs performances respectives au fil du temps. Il est également à souligner que le pilotage est généralement la responsabilité de deux entités : les managers et les auditeurs internes. D'une part, les managers contrôlent les performances des différents départements ou unités par le biais d'évaluations continues et/ou d'évaluations ponctuelles. L'implémentation d'un système IT reprenant automatiquement les pertes et la liste des événements est un aspect non négligeable afin d'éviter les pertes d'informations qui peuvent être essentielles dans cette phase. D'autre part, les auditeurs internes mesurent l'efficacité du risk management au sein de chaque département/unité organisationnelle mais ils évaluent aussi si la relation stratégie - risk management est bien établie. (Chatterjee & Milam, 2007; Everson, Martens, Nottingham & Steinberg, 2004; Nagumo, 2005; Protiviti Inc., 2006

Annexe n°2 : Comment communiquer de manière transparente.

Selon Rawlins (2008), ces dernières années ont vu apparaître une nouvelle forme de communication nommée la « la communication transparente » permettant de générer une certaine confiance et crédibilité auprès de ces parties prenantes. Cette communication transparente comporte 3 aspects : les informations fournies, la participation et la responsabilité.

Premièrement, il faut rendre toutes les informations jugées importantes par les parties prenantes disponible, qu'elles soient positive ou négative à l'image de la société. (Rawlins, 2008) Par l'intermédiaire de cette communication, l'entreprise essaye de fournir des informations utiles aux parties prenantes pour comprendre la situation actuelle de l'entreprise. Les informations fournies ne doivent

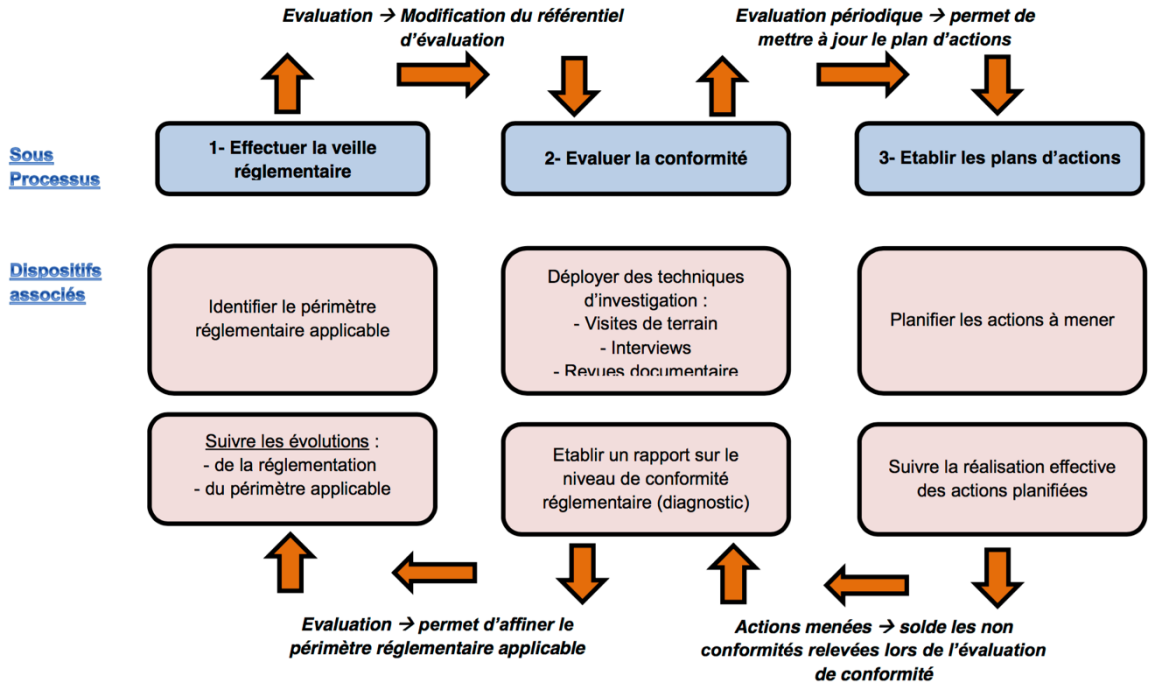
pas être divulguée dans l'intérêt de l'émetteur mais bien en fonction des besoins du receveur. (Linjuan Rita, 2014)

Ensuite, lorsque nous parlons de participation, cela implique une démarche de recherche auprès des parties prenantes permettant d'identifier quelles informations sont requises pour leur processus de décision. Les entreprises ont besoin d'inclure les besoins des parties prenantes à savoir quelle information est vraiment nécessaire, quelle quantité, quelle niveau de précision. Comment l'entreprise arrive à répondre à ce besoin déterminera le niveau de transparence de l'organisation (Rawlins, 2008).

Enfin, être transparent signifie que l'entreprise communicante est responsable des informations fournies et qu'elle est ouverte aux jugements et critiques du public cible. Nier ou omettre certaines informations exposant des problèmes ou des faiblesses de l'entreprise est contraire à ce principe de responsabilité. (Rawlins, 2008) Si une entreprise assume sa responsabilité et ses faiblesses et par conséquent ouverte aux critiques, montre une ouverture d'esprit des dirigeants ainsi qu'une volonté d'aller au-delà de ces problèmes. Cette démarche permet de montrer une certaine présence de l'éthique au sein de l'entreprise. (Linjuan Rita, 2014)

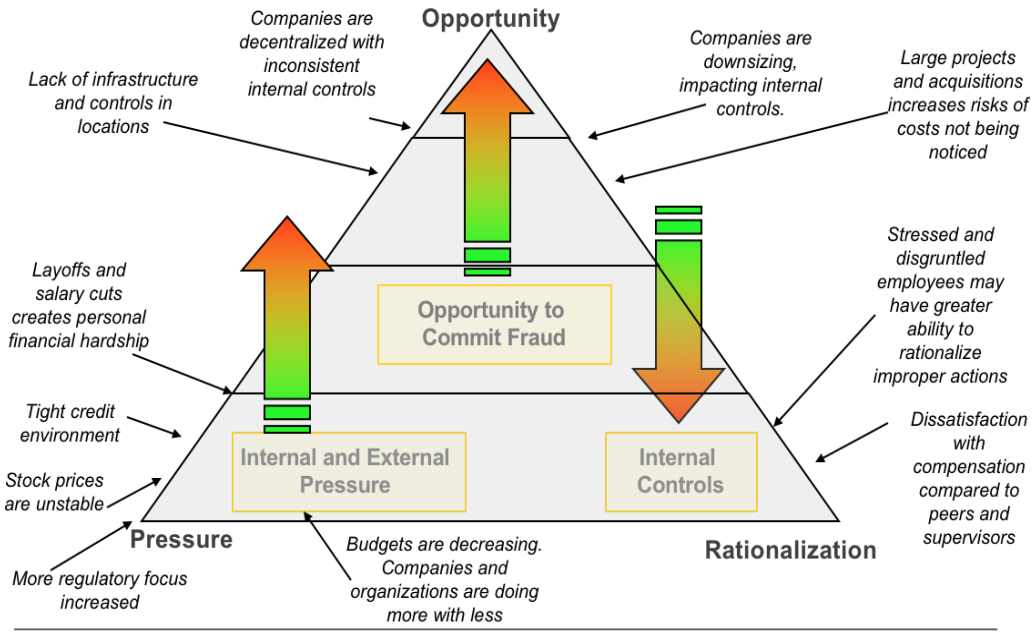
Annexe n°3 : Veille réglementaire

(Wogue, 2016)



Annexe n°4 : Le triangle de la fraude

("Fraud Risk - Houston IIA 2015 Government Auditing Conference", 2015)



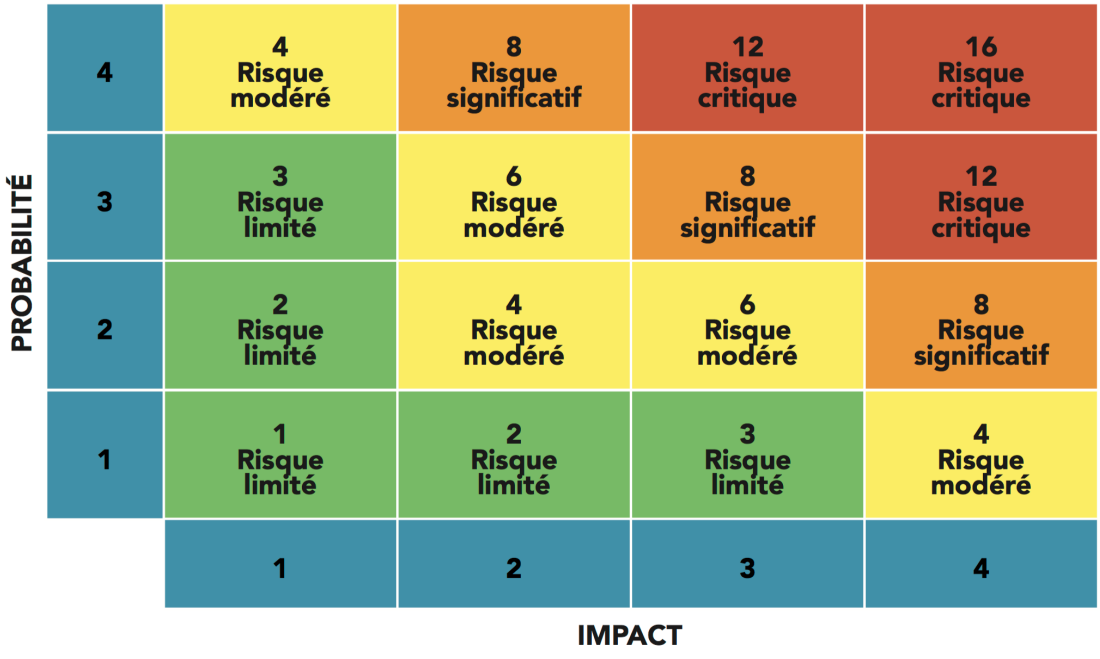
Annexe n°5 : Grille à impacts

(Wogue, 2016)

Niveau	Impact Sanction Financière / litiges clientèle	Impact image / Réputation	Impact administratif / disciplinaire / judiciaire
4. Critique	> à 1 000 K€	Diffusion dans les médias internationaux Et/ou impact sur la cotation du titre	Condamnation devant un tribunal/sanction administrative prononcée
3. Fort	500 K€ à 1 000 K€	Diffusion dans les médias nationaux Et/ou impact sur la cotation du titre	Ouverture d'une procédure de sanction
2. Moyen	50 K€ à 500 K€	Diffusion dans les médias spécialisés	Mise en demeure par un régulateur
1. Faible	< à 50 K€	Pas de diffusion dans les médias	Pas de mise en cause

Annexe n°6 : Cartographie des risques

(Pécriaux, 2017)



Annexe n°7: Une communication de l'éthique efficace

La communication est un élément crucial permettant d'évaluer la performance d'un programme de compliance. (Jane, 2016) La qualité de la communication aux collaborateurs est un des facteurs clés de succès dans l'implémentation d'une culture éthique et de la compliance (Jane, 2016). Ceci est également confirmé par l'étude menée par Kaptein (2011), qui mentionne que la qualité de la communication est un élément entrant en compte dans la corrélation entre l'efficacité du code de conduite et la diminution des comportements non éthiques.

La transmission des valeurs et de l'éthique commence avec l'établissement d'un code de conduite. Ce code doit être efficace, reprenant ainsi des mesures disciplinaires pour les comportements déviants mais également des récompenses et incitations promouvant les comportements éthiques, (Di Florio, 2011 ; Hireche, 2004) mais également communiquer de manière adéquate à tous les employés. Comme mentionné précédemment il ne suffit pas simplement de le publier mais il faut également engager les collaborateurs. (Toti & Moulin, 2017). Il faut clairement communiquer les comportements éthiques attendus à tous les niveaux de l'entreprise mais également les conséquences des actes non-éthiques. Si un acte non-éthique est relevé au sein de l'organisation, il ne faut pas hésiter à le communiquer, sous couvert d'anonymat, à l'ensemble des collaborateurs pour les conscientiser aux sanctions possibles. (Andreisovà, 2016)

Selon une étude menée par PWC auprès de plus de 800 personnes (Falcione, 2016), il en ressort que 98% des entreprises utilisent le code de conduite comme moyen de communications des valeurs mais seulement dans 3% des cas, les employés signent de manière individuelle ces codes pour marquer leur approbation. Pourtant il est important de sensibiliser les employés à ce code de conduite afin qu'ils puissent y adhérer et appliquer ces valeurs dans leur tâche quotidienne. Il pourrait également faire une évaluation de ce code de conduite d'améliorer ce sentiment d'appartenance aux valeurs partagées au sein de l'entreprise. (Andreisovà, 2016)

Annexe n°8 : **Étude de comparaison sectorielle des performances extra-financières**

La première colonne du Tableau n°1 reprend l'ensemble des secteurs[8] et régions analysés. Le reste des colonnes reprennent les différentes dimensions liées à la RSE (Reporting, Business ethics & products responsibility, Labor issues, Environment, Community relations et Corporate governance). Le critère de performance pour ces différents facteurs est classé sur une échelle de 0 à 1, où 0 signifie que le facteur n'est pas du tout intégré et où 1 signifie que le facteur est totalement intégré. (Diaz, Schwegler & Weber, 2012)

Sector	Reporting	Bus. ethics & prod. resp.	Labor issues	Environment	Community relations	Corporate governance	Total
Utilities	0.52	0.72	0.48	0.46	0.54	0.72	0.57
Materials	0.48	0.73	0.47	0.46	0.44	0.69	0.55
Energy	0.43	0.75	0.45	0.34	0.44	0.78	0.53
Consumer staples	0.46	0.68	0.46	0.39	0.44	0.69	0.52
Telecommunication	0.47	0.68	0.44	0.33	0.42	0.72	0.51
Industrials	0.39	0.70	0.44	0.43	0.40	0.67	0.50
Information Technology	0.33	0.74	0.42	0.41	0.38	0.70	0.50
Health care	0.33	0.70	0.42	0.37	0.41	0.71	0.49
Consumer discretionary	0.36	0.69	0.44	0.37	0.39	0.68	0.49
Financials	0.34**	0.66**	0.39**	0.40	0.43	0.69	0.48**
Asia-Pacific	0.42**	0.68**	0.43**	0.45**	0.41**	0.53**	0.49**
Europe	0.45**	0.66**	0.46**	0.44**	0.45**	0.68**	0.52**
North America	0.32**	0.70**	0.43**	0.40**	0.42**	0.69**	0.51**
Average without financials	0.40	0.71	0.44	0.40	0.42	0.69	0.51
Total average	0.39	0.70	0.43	0.40	0.42	0.69	0.51

Table 1. CSR averages of the different sectors
**Significant difference between financials and other sectors or between the regions.

(Diaz, Schwegler & Weber, 2012)

En observant la colonne "total" nous obtenons déjà un premier élément de réponse puisque le secteur financier a le moins bon score total (0,48) parmi tous les secteurs. Cela s'explique par le fait que le secteur financier a des performances significativement moins bonnes dans les domaines de reporting, de business ethics et de labor issues. (Diaz, Schwegler & Weber, 2012)

Dans le Tableau n°2, le secteur financier est utilisé comme référence et est comparé aux autres secteurs. Ainsi, la colonne "B-weight sustainability performance" indique la différence de performance entre le secteur financier et les autres. Si nous observons un chiffre positif, cela signifie que le secteur en question a de meilleures performances que le secteur financier et plus le chiffre est grand, plus grand est l'écart de performances. Nous constatons alors que le secteur financier a des performances extra-financières significativement moins bonnes que les secteurs des biens de grandes consommation (3.874), de l'énergie (5.486), des matériaux de construction (6.359), des services publiques (8.343). (Diaz, Schwegler & Weber, 2012)

[8] Les secteurs sont classés selon les standards GICS - Global Industry Classification Standard

Sector	*B*-weight sustainability performance	*p*	*B*-weight dummy Europe	*p*	*B*-weight dummy North America	*p*
Energy	5.486	<0.001	−0.062	0.866	1.486	<0.001
Materials	6.359	<0.001	−0.441	0.055	−0.205	0.380
Industrials	2.089	<0.001	0.078	0.674	−0.123	0.539
Consumer discretionary	0.405	0.626	−0.152	0.450	0.185	0.356
Consumer staples	3.874	<0.001	−0.124	0.644	0.399	0.124
Health care	0.367	0.735	0.413	0.160	1.033	0.000
Information technology	1.612	0.103	−0.589	0.022	0.546	0.015
Telecommunication services	2.246	0.141	0.550	0.192	0.565	0.193
Utilities	8.343	<0.001	0.116	0.710	0.663	0.030

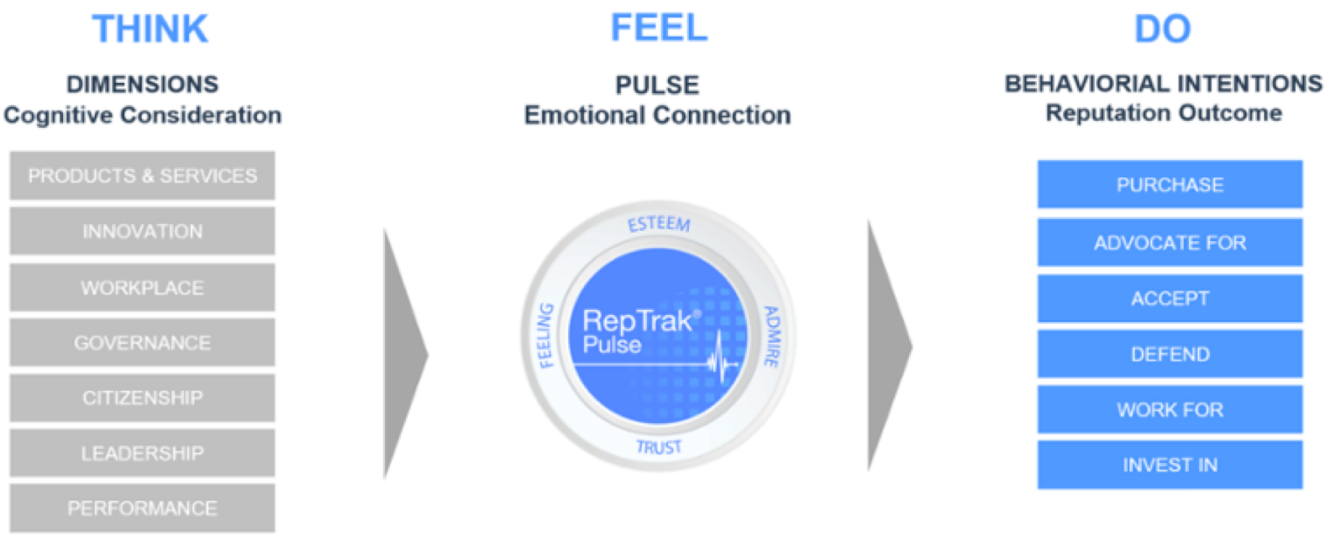
Table 2. Results of the multinomial logistic regression analysis with the financial sector as reference category

Annexe n°9 : Les différentes mesures éthiques et responsable à prendre en tant qu'institution financière

1. Réaliser des Investissements Socialement Responsables (ISR). C'est-à-dire, prendre en compte des critère Environnementaux, Sociaux et de Gouvernance (ESG) pour accorder leur prêts et financement. Il s'agit de soutenir uniquement des activités socialement responsables et contribuer à la protection de l'environnement en refusant de prêter ou d'investir dans les industries polluantes.
2. Maintenir la confiance envers le système financier en fournissant des garanties aux déposants pour protéger leurs dépôts
3. Utiliser l'argent reçu en dépôt de manière responsable
4. Revoir leurs marges à la baisse pour que de plus petits agents économiques puissent bénéficier de financements à plus faibles coûts pour leur business.
5. Opérer en toute transparence en expliquant en détails à leurs clients toute la complexité des produits financiers qu'elles proposent ainsi ce qu'ils doivent payer en contractant un emprunt (il se peut que les banques tirent avantages de ce manque de compréhension des clients pour prêter à leurs clients à des coûts supérieurs)
6. Etablir une politique interne de management éthique pour éviter de se retrouver dans les prémices de la crise de 2008 où les managers s'étaient vus accorder des bonus faramineux
7. Intégrer des clauses sociales et environnementales dans les contrats passés avec les fournisseurs (Andrada, 2015 ; Diaz, Schwegler & Weber, 2012)

Annexe n°10 : Matrice RepTrak®

(Reputation Institute, 2017)



Annexe n°11 : Information complémentaire sur le risque réputationnel

Le Risque Réputationnel

Au fil du temps, la perception de la nature des risques a considérablement évolué. En effet, les risques sont interdépendants et multidimensionnels, c'est-à-dire que les risques comme les risques climatiques, éthiques, géopolitiques, sociétaux, réputationnels, technologiques, etc. sont globaux et interagissent. Cela signifie qu'il faut adopter une approche plus systémique des risques et comprendre les relations qu'il existe entre ceux-ci. (Richer, 2016)

L'un des dénominateurs communs de ces risques est sans nul doute la réputation de l'entreprise. En effet, la réputation est comparative entre firmes et est basée sur la perception que l'ensemble des parties prenantes ont de l'entreprise et de ses activités. Ainsi, chaque partie prenante développe sa propre impression de la compagnie sur base de facteurs tels que la culture d'entreprise, l'image de marque ou encore le pays d'origine et la construit à travers une multitude de canaux comme les médias, les interactions avec les employés, l'expérience personnelle du produit ou service, etc. (voir tableau ci-dessous)

Table I Reputational risk factors from a market perspective

Reputational dimension	Offering (products, services)	Communication (Promotion, public relations)
Corporate image	Offering products and services that are associated with illegal activities, damaging the environment, low quality, and symbolising social class differences	Openly denying publicly available claims, reports, facts, opinions that are relevant for consumers of the products and users of the service
Product/ service class image	Offering a product range that cannot be recycled or reused Offering services with single-use products and/or materials	Highlighting customer's benefits that are disproportionately low to the burden of factory workers and to the harm of the society at large for manufacturing the goods and delivering the service
Image of country of origin	Sourcing materials and/or product parts from countries that do not comply with human rights and/or fight against religious beliefs and/or defeat political views and/or suppress freedom of opinion	Promoting products, services, partnerships, suppliers, associations from countries that do not comply with human rights, etc Highlighting the profits generated by sourcing in low-cost countries
Brand users image	Offering products and services that used to be fashionable (to traditional market segments), but are now associated with unsocial, unsustainable, etc., aspects	Placing users of the products and services in an unsocial light in advertisements, marketing material, etc.
Corporate culture/ personality	Manufacturing parts, final goods, and delivering services by treating employees unfairly Having a product-oriented culture that does not understand the needs and interests of consumers (nor having the appreciation why this may be relevant)	Emphasising exclusively the product and service benefits and ignoring (and/or not understanding) the customer benefits when using the products and services Pointing out the high working standards and pro-social behaviour within the workforce and actually not fulfilling those claims
Brand image	Offering a range of products that have toxic ingredients Offering services that ham the environment	Making branded gifts to public figures that are negatively perceived by the public
Experience	Offering products and services that do not work or do not fulfil the expectations or promises	Emphasising false claims of products and services (including environmental or social aspects, "greenwash") leading to mistrust

La réputation de l'entreprise est donc l'impression collective, généralement stable, de toutes ces expériences personnelles. Se construire une réputation solide est primordial pour l'entreprise car elle est génératrice de confiance. En effet, c'est elle qui encourage le bouche-à-oreille positif et donc l'achat des

produits et services, c'est la bonne réputation qui incite les travailleurs qualifiés à rejoindre l'entreprise et à y rester, c'est encore elle qui attire les investisseurs potentiels. A l'inverse, une mauvaise gestion de la réputation représente un réel risque pour l'entreprise et peut potentiellement se solder par un boycott des produits et services par les clients, par une désertion des travailleurs qualifiés et des investisseurs, par une perte de parts de marchés ou encore par une augmentation du coût du capital. (Lemke & Petersen, 2013 ; Reputation Institute, 2017 ; Reputation Institute, s.d.; Walter, 2016)

Naturellement, une réputation positive prend du temps à être développée et peut être facilement endommagée. Toute entreprise influence la perception des parties prenantes à son égard par le biais de ses actions, de ses offres, de sa communication et construit sa réputation autour de six éléments principaux : les performances financières, la qualité du personnel, l'innovation, la qualité des biens et services fournis, la qualité du management, les performances extra financières liées à responsabilité sociale et environnementale. (Bebbington, Larrinaga & Moneva, 2008; Reputation Institute, 2017)

<u>Annexe n° 12:</u> Exemples d'indicateurs pour certains groupes de parties prenantes

Table II Company internal aspects and indicators

Aspects	*Indicators*
Worker representation	Existence and function of safety committee and other committees comprising worker representatives
Non-discrimination	Equal benefits and salaries Discrimination-related litigations
Employments and layoffs	Existence of employee contracts Procedures related to the employment and layoff processes, including terms of notice
Stability of employees	Seniority Ratio of absence due to illness
. . . in total 23 aspects	. . . in total 55 indicators

Table III Aspects and indicators regarding suppliers and sub-contractors

Aspects	*Indicators*
Explicit requirements	Expression of any social-related requirements Evaluation of the supplier's ability to meet the requirements Supplier written commitments to meet the requirements
Bribery and corruption	Policy, procedures and compliance mechanisms regarding bribery and corruption If the audited company has been sued by any suppliers/subcontractors, the number and reasons for each litigation and if any pending cases remain
. . . in total four aspects	. . . in total nine indicators

Table IV Aspects and indicators regarding customers (products/services)

Aspects	*Indicators*
Lawsuits	Has the audited company been sued for any reasons related to their products or services, the number and reasons why, and remaining open questions
Complaints and remediation procedures	Procedures and compliance mechanisms related to ensure correct product information and labeling Number and frequency of complaints and the major reasons why Procedures/management systems and compliance mechanisms to solve and meet customer complaints Means to measure how satisfied or dissatisfied customers are with the provided products and services
In total two aspects	In total five indicators

Table V Aspects/indicators regarding national and international surroundings

Aspects	*Indicators*
Unethical activities and products	Direct or indirect involvement of the audited company in manufacturing or selling firearms, GMOs, nuclear installations or addictive products Test on animals/clinical trials and countries where the trials are performed/conflicts, threats, vandalism or litigations related to the operation of the audited company
Outside judgements of reputation	Interest groups' groups and opinion leaders' judgements of the reputation of the audited company
Social investment companies	Unwillingness to engage in the audited company or other companies within the same branch
Handling of the media … etc.	Existence of procedures and compliance mechanisms describing how to advertise and handle contact with and response to journalists … etc.
In total five aspects	In total 11 indicators

<u>Annexe n°13:</u> Dimensions, Sous-dimensions & Indicateurs RSE du Global Risk Initiative (GRI)

(Calabrese, Costa & Rosati, 2015)

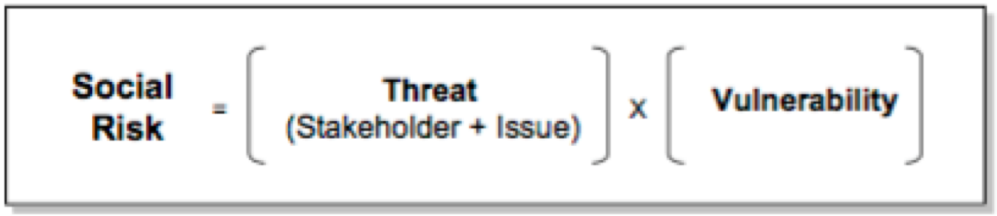
Table 1
GRI structured framework: CSR dimensions, sub-dimensions and items.

CSR dimension	CSR sub-dimension	CSR items
Economic	–	Direct economic value (EC1) Financial implications due to climate change (EC2) Organization's benefit plan obligations (EC3) Financial assistance received from a government (EC4) Market presence (EC5 + EC6 + EC7) Indirect economic impacts (EC8 + EC9)
Environmental	–	Materials (EN1 + EN2) Energy (EN3 + EN4 + EN5 + EN6 + EN7) Water (EN8 + EN9 + EN10) Biodiversity (EN11 + EN12 + EN13 + EN14 + EN15) Emissions (EN16 + EN17 + EN18 + EN19 + EN20) Effluents and spills (EN21 + EN23 + EN25) Waste (EN22 + EN24) Products and services (EN26 + EN27) Compliance with environmental laws and regulations (EN28) Transport (EN29) Overall (EN30)
Social	Labour Practices and Decent Work (LA)	Employment (LA1 + LA2 + LA3 + LA15) Labour/management relations (LA4 + LA5) Occupational health and safety (LA6 + LA7 + LA8 + LA9) Training and education (LA10 + LA11 + LA12) Diversity and equal opportunity (LA13 + LA14)
	Human Rights (HR)	Investment and procurement practices (HR1 + HR2 + HR3) Non-discrimination (HR4) Freedom of association and collective bargaining (HR5) Child labour (HR6) Forced and compulsory labour (HR7) Security practices (HR8) Indigenous rights (HR9) Remediation (HR10) Assessment (HR11)
	Society (SO)	Local communities (SO1 + SO9 + SO10) Corruption (SO2 + SO3 + SO4) Public Policy (SO5 + SO6) Anti-competitive behaviour (SO7) Compliance with laws and regulations related to accounting fraud, workplace discrimination and corruption (SO8)
	Product Responsibility (PR)	Customer health and safety (PR1 + PR2) Product and service labelling (PR3 + PR4 + PR5) Marketing communications (PR6 + PR7) Customer privacy (PR8) Compliance with laws and regulations concerning provision and use of products and services (PR9)

Annexe n° 14: Équation de mesure du risque social

(Kytle & Ruggie, 2005)

Figure 4: Social Risk Equation



Annexe n°15 : Aspects de la communication menant à du Greenwashing

(Futerra, s.d.)

Greenwashing (éco-blanchiment) : Une entreprise doit éviter de communiquer sur un produit écologique si ses actions ou ses discours ne sont pas cohérents. Par exemple, si elle :

- Se comporte d'une façon non responsable
- Adopte un langage édulcoré (environmentally-friendly)
- Utilise des images suggestives du développement durable qui n'ont rien en commun avec le produit
- Promeut un aspect non significatif du produit
- Compare avantageusement le produit sur un attribut à peine amélioré
- Promeut un produit dangereux (pour la santé par exemple) comme étant écologique
- Utilise un langage scientifique hermétique
- Produit une autodéclaration environnementale qui donne l'illusion d'être endossée par une tierce partie
- Manque de preuves pour étayer un attribut soi-disant durable
- Utilise de fausses données, déclarations

<u>Annexe n°16:</u> Lignes directrices non contraignantes de l'EU

Sources European Commission (2014)

Liste non exhaustive des aspects thématiques que les sociétés devraient prendre en compte lorsqu'elles publient des informations non financières :

a) Questions environnementales

- Informations significatives sur la prévention et le contrôle de la pollution
- Incidence de la consommation d'énergie sur l'environnement
- Émissions atmosphériques directes et indirectes
- Utilisation et de la protection des ressources naturelles (par exemple l'eau, les sols) et de la protection de la biodiversité dans ce contexte
- Gestion des déchets
- Incidences environnementales des transports
- Mise au point de produits et services écologiques.

b) Questions sociales et de personnel

- Mises en œuvre des conventions fondamentales de l'Organisation internationale du travail
- Questions de diversité, comme par exemple la diversité de genre et l'égalité de traitement en matière d'emploi et de travail (incluant l'âge, le genre, l'orientation sexuelle, la religion, l'handicap, l'origine ethnique et d'autres aspects pertinents)
- Questions d'emploi, notamment la consultation et/ou la participation des employés, les conditions d'emploi et de travail
- Relations syndicales, notamment le respect des droits syndicaux
- Gestion du capital humain, notamment la gestion des restructurations, la gestion des carrières et l'employabilité, le système de rémunération, la formation
- Santé et la sécurité au travail
- Relations avec les consommateurs, notamment la satisfaction des consommateurs, l'accessibilité, les produits ayant un effet potentiel sur la santé et la sécurité des consommateurs
- Incidences sur les consommateurs vulnérables
- Relations avec la collectivité, notamment le développement social et économique des communautés locales.

c) Questions sur le respect des droits de l'Homme

Une société peut envisager de publier des informations significatives et des ICP concernant :

- Les cas d'incidences graves sur les droits de l'homme liées à ses activités ou décisions
- La procédure de réception et de traitement des plaintes, l'atténuation et la réparation des violations des droits de l'homme
- Les activités et les fournisseurs présentant un risque significatif de violation des droits de l'homme
- Les procédures et les mesures de prévention de la traite des êtres humains, pour toutes les formes d'exploitation, de travail forcé ou contraint et de travail des enfants, pour le travail précaire ou les conditions de travail dangereuses, notamment en ce qui concerne les zones géographiques à haut risque d'abus
- Le degré d'accessibilité de leurs locaux, documents et sites internet pour les personnes handicapées
- Le respect de la liberté d'association
- L'interaction avec les parties prenantes concernées

d) Questions sur la lutte contre la corruption

Une société peut envisager de communiquer des informations significatives et des ICP concernant des aspects tels que :

- Les politiques, procédures et normes anti-corruption
- Les critères utilisés dans l'évaluation des risques liés à la corruption
- Les procédures de contrôle interne et les ressources consacrées à la prévention de la corruption
- La formation appropriée des salariés
- L'utilisation de mécanismes de lancement d'alerte
- Le nombre d'actions en justice en cours ou terminées concernant des comportements anticoncurrentiels.

e) Questions sur la chaine d'approvisionnement

Si une société estime que la publication d'informations détaillées concernant des évolutions imminentes ou des affaires en cours de négociation pourrait lui nuire gravement, elle peut se conformer à l'objectif général de transparence en publiant des informations synthétisées qui ne lui portent pas tort.

Une société peut envisager de communiquer des informations significatives et des ICP sur des aspects tels que le contrôle des fournisseurs concernant :

- Les pratiques de travail, notamment le travail des enfants et le travail forcé, le travail précaire, les salaires, les conditions de travail dangereuses (y compris la sécurité des bâtiments, les équipements de protection, la santé des travailleurs)
- La traite des êtres humains et d'autres questions relatives aux droits de l'homme

- Les émissions de gaz à effet de serre et autres types de pollution de l'eau et de l'environnement
- La déforestation et autres risques pour la biodiversité et le suivi de l'incidence de la société sur les fournisseurs, par exemple ses conditions de paiement et ses délais moyens de paiement

Annexe n°17: Questionnaires vierges soumis aux différents intervenants

a) Questionnaire soumis auprès du risk manager

Introduction

1) Quel type de framework du Coso utilisez-vous?
    a. COSO 1 – internal Control
    b. COSO 2 – Entreprise risk management

Liens avec la compliance

Selon le FSMA et la BNB, la fonction de compliance doit être indépendante des autres fonctions de l'entreprise. Cependant, il existe dans certain cas une collaboration entre la fonction de compliance et le risk management de l'entreprise dans la gestion des risques.

1) Pouvez-vous nous expliquer si ce genre de collaboration existe auprès de votre organisation ?
2) Au niveau du reporting, est-ce que vous incluez des KRI Compliance dans votre rapport de risk que vous transmettez au conseil d'administration ?
    a. Quelles sont les types de KRI utilisés ?
    b. Pensez-vous que cette intégration/non-intégration permettrait d'avoir une meilleure vision globale des risques ainsi qu'une meilleure influence de la compliance sur la stratégie ?
3) Le risk management et la fonction de compliance traitent de risques parfois similaires mais étant abordés de manières différentes dans les deux fonctions.
    Prenons l'exemple des risques opérationnels comme les erreurs humaines et de fraudes qui sont gérés par votre fonction de risk management. Par l'intermédiaire de procédures, vous allez mitiger ce risque. Cependant, le département compliance s'attaquera aussi à ce type de risque mais d'une autre manière par l'implémentation de règle de conduite afin de pousser les employés à agir de manière éthique et responsable.

    a. Existe-t'il une certaine collaboration sur l'implémentation de procédure de contrôle d'activité afin d'éviter les doublons ?

i. OUI, jugez-vous cette collaboration efficace et permettant de couvrir les risques dans les deux fonctions de la même manière que si vous le faisiez de manière distincte ?
ii. NON, Pourquoi ne pas collaborer sur l'élaboration contrôle d'activité permettant de mitiger un risque présent dans les deux fonctions et ainsi avoir une vision plus globale de la gestion des risques ?

4) A l'avenir, pensez-vous que la fonction de compliance restera indépendante ou qu'un possible rapprochement entre les fonctions de risk management et de compliance soit à nouveau possible afin d'avoir une vision plus globale des risques d'une entreprise ? Quelles seraient les raisons qui pousseraient les deux départements à collaborer de manière plus étroite sur certains risques

Liens entre le risk management et la RSE

1) Quel est la coopération actuelle avec le département RSE?
2) Gérez-vous les risques liés au risque réputationnel?
3) Gérez-vous les opportunités liés aux actions RSE ?
    a. Pourquoi ne pas les intégrés au vu des mêmes méthodes d'analyse (risk based approach vs matérialité ?)
4) Au niveau du reporting, utilisez-vous des KRI liés à la RSE ?
    a. Pensez-vous que cette intégration permettrait une plus grande influence de la RSE sur la stratégie d'entreprise ?
5) Collaborez-vous sur certains contrôle mis en place afin de tacler un même risque ?

La gestion des risques

1) Quels sont vos KRI ? (Qu'est-ce qui vous empêche de dormir la nuit)
2) Pour chacun, comprendre leur méthode de fonctionnement
    a. Identification, comment avez-identité ce risk, à quel endroit ?
    b. Pourquoi est-il un Key risk ?
    c. Quelles sont les procédures de contrôles ?
        i. Y-a-t'il une concertation sur ces contrôles avec la compliance/Brand manager/CSR ? Afin de tacler en même temps un risque de compliance/ réputationnel/opportunité
    d. Comment ces risques sont-ils communiqués ?
        i. Newsletter

ii. Training
iii. Documentation de processus
iv. Communique-vous aussi les risques de compliance dans s'ils entrent aussi dans votre processus ?
v. Intégrez-vous ces KR dans votre reporting ?

e. Comment ces risques sont-ils monitorer/testing ?
i. Par qui ?
ii. A quelle fréquence ?
iii. Faites-vous aussi un audit des risk RSE/reputationnel avec votre audit risk ?

f. Comment le risk appetite influence vos décisions

Conclusion

1) Pensez-vous qu'intégrer les risques compliance à vos processus/communication/reporting et monitoring permettraient :
   a. D'influencer la stratégie
   b. Une meilleure maîtrise des risques avec des processus de contrôle plus complet ainsi qu'une meilleure conscientisation des risks owner's ?
2) Pensez-vous qu'une intégration du management des risk et opportunités de la RSE par votre département permettrait une meilleure maîtrise des risques/opportunités lié à la RSe ?

A) Questionnaire soumis auprès du Chief Compliance Officer

Introduction

1) Selon vous, a quoi sert un programme de compliance au sein d'une entreprise ?
2) Dans quelle mesure trouvez-vous que votre entreprise soit Éthique et compliant?

La compliance

1) Selon-vous quelle est la différence entre compliance et la RSE ? Existe-t'il un lien entre ces deux notions ?
2) Selon vous, quelle est le scope de la compliance ? De quel sujet traite-t'il ?

Risk management et compliance

Selon le FSMA et la BNB, la fonction de compliance doit être indépendante des autres fonctions de l'entreprise. Cependant, il existe dans certain cas une collaboration entre la fonction de compliance et le risk management de l'entreprise dans la gestion des risques.

1) Pouvez-vous nous expliquer si ce genre de collaboration existe auprès de AXA Banque ?
2) Au niveau du reporting, est-ce que le risk management utilise vos KRI de compliance dans son rapport de risk qu'il transmet au conseil d'administration ?
    a. OUI
        i. Quels types de KRI sont utilisés ?
        ii. Pensez-vous que cette démarche ait un meilleur impact auprès du conseil d'administration ainsi qu'un plus grand impact sur la culture d'entreprise que votre propre rapport de reporting ?
    b. NON
        i. Selon vous, pourquoi le risk management ne prends pas en compte vos KRI dans son rapport ?
        ii. Pensez-vous que votre reporting ait une influence sur le conseil d'administration dans leur prise de décision ainsi que sur la culture d'entreprise ?
        iii. Pensez-vous qu'une intégration des KRI de compliance dans le reporting du risk management aurait un plus grand impact sur le conseil d'administration ?

3) Le risk management et la fonction de compliance traitent de risques parfois similaires mais étant abordés de manières différentes dans les deux fonctions.
   Prenons l'exemple d'un cas du risque éthique qui est traité par la fonction de compliance. Par l'intermédiaire de procédures et de règles de conduites, vous allez influencer les parties prenantes à agir de manière plus responsable et évitant ainsi les déviations de comportements. En faisant de la sorte, vous allez également agir sur un risque opérationnel qui est traité par le risk management qui sont les erreurs humaines ainsi que sur l'exposition à la fraude.

    a. Existe-t'il une certaine collaboration sur l'implémentation de procédures de contrôles d'activités afin d'éviter les doublons ?

        i. OUI, jugez-vous cette collaboration efficace et permettant de couvrir les risques dans les deux fonctions de la même manière que si vous le faisiez de manière distincte ?

ii. NON, Pourquoi ne pas collaborer sur l'élaboration contrôle d'activité permettant de mitiger un risque présent dans les deux fonctions et ainsi avoir une vision plus globale de la gestion des risques ?

La gestion du risque Compliance

1) Quelles sont les risques majeurs auquel votre entreprise doit faire face ?
    a. Régulatoire
        i. Dans quelques mois, une nouvelle réglementation verra le jour, le RGDP, pouvez-vous nous expliquer comment avez-vous procéder avec cette nouvelle régulation ?
    b. Corruption (Foreign corrupt pratice act - FCPA)
    c. Éthique
    d. Fiduciaire (distribution) – Conflit d'intérêt bancaire
        i. Ex avec le conflit d'intérêt entre le banquier et le client, banquier par communication et doit prester le meilleur produit pour le client et pas pour lui ni pour son entreprise
    e. Protection de donnée (RGDP – règlement européen de protection de données)
    f. Blanchiment d'argent (BSA – Bank secretary bank)

2) Pour chaque Key risk analyse leur méthode de contrôle
    a. Identification, comment avez-vous identifié ce risk ? a quel endroit ?
    b. Pourquoi est-il un Key risk ?
    c. Quelles sont les procédures de contrôle ?
        i. Y-at'il une concertation sur ces contrôles avec le risk management afin de parfois tacler un même risque ?
            1. Quelles sont-elles ?
    d. Comment ces risques sont-ils communiqués ?
        i. Newsletter ?
        ii. Documentation de processus
        iii. Training
        iv. Est-ce vous avez une communication conjointe de vos risques avec le risk management ?
        v. Est-ce ce Key risk est-il repris dans le reporting du risk management ?
    e. Comment ce risque est-il monitorer/tester ?
        i. Par qui ?
        ii. A quelle fréquence

iii. Est-ce certains indicateurs sont aussi contrôlés par le risk management ?

f. Comment le risk appetite influence ce risque ?

Conclusion

1) A l'avenir, pensez-vous que la fonction de compliance restera indépendante ou qu'un possible rapprochement entre les fonctions de risk management et de compliance soit à nouveau possible afin d'avoir une vision plus globale des risques d'une entreprise ? Quelles seraient les raisons qui pousseraient les deux départements à collaborer de manière plus étroite sur certains risques ?
2) Selon vous, quelles sont les pistes d'évolution pour une meilleure gestion des risques de Compliance ?

*B) **Questionnaire soumis auprès du responsable RSE/Communication***

Introduction

3) Quel est votre parcours ? Pourquoi avoir choisi de travailler dans la RSE ?
4) Dans quelle mesure trouvez-vous que votre entreprise comme socialement responsable ?
5) Quelles sont les actions RSE (sociales/environnementales) entreprises par la compagnie ?
    a. En termes d'initiatives sociales, est-ce que l'entreprise propose à ses employés des formations continues et des opportunités d'améliorer leurs compétences ?
    b. Qu'en est-il de la diversité au sein de l'entreprise ? (Age/Hommes-Femmes/Qualifications/Expériences professionnelles)
    c. Qu'est-ce qui est mis en place pour qu'au moins ⅓ des membres du conseil d'administration soit de sexe opposé au 2/3 restant ?
    d. Est-ce que la banque à comme politique de n'accorder de prêts et de n'investir qu'à des entreprises ayant des activités socialement responsables ?
    e. Est-ce que la banque contribue à la protection de l'environnement en refusant d'investir ou d'accorder des prêts à des industries polluantes ?
    f. Est-ce que la banque sponsorise des associations ? Lesquelles ?
6) Selon-vous, quel est la différence entre RSE et compliance ?

La gestion de risques/opportunités RSE :

1) Êtes-vous en charge de la gestion des risques/opportunités lié à la RSE ?
2) Considérez-vous avoir une gestion des risques RSE centralisée ou décentralisée dans votre société ? (Gérez les risques/opportunités liés aux actions ainsi qu'à la réputation)
3) Selon le modèle des 3 lignes de défenses, ou situeriez-vous votre département ?
4) Comment évaluez-vous les risques/opportunités liées à la RSE/Reputation ?
    a. Matrice de la matérialité ?
5) Quelles sont les contrôles mis en place pour gérer ces risques/opportunités ?
    a. Due dilligence dans la sélection des clients/fournisseurs ?
6) Comment communiquez-vous aux parties prenantes (internes et externes) votre performance de la RSE ainsi que les risques ?
    a. Interne
        i. Training
        ii. Newsletter
        iii. Documentation de processus
    b. Externe
        i. Rapport annuel
        ii. Rapport a part
7) A qui faite vous votre reporting des risques/opportunités lié à la RSE ?

    a. Quelles sont vos KRI (Key risk indicators ?)
8) Comment procédez-vous pour monitorer/tester vos processus de contrôle des risques ?

La relation avec le risk management

1) Est-ce que le risk management incluse des KRI liés à la RSE dans son reporting ?
    a. Jugeriez-vous être une bonne solution et pourquoi ?
2) Au vu des mêmes méthodes d'évaluation des risques (matérialité vs risk impact), estimeriez-vous que cela soit bonne option que le risk management s'occupe de l'évaluation des risk/opportunités dans son risk management ?
3) Collaborer-vous avec le risk management dans l'élaboration de processus de contrôle commun permettant de tacler un même risque ?

L'influence de la RSE sur la stratégie

1) Estimez-vous être écouté/avoir une bonne influence sur la stratégie de l'entreprise ?
2) Pensez-vous que si le risk management intègrent des KRI liés à la RSE dans son reporting, a RSE aurait une plus grande influence sur la stratégie d'entreprise ?
3) Comment la stratégie influence vos actions RSE
    a. Le risk appetite entre-t'il en compte ?

La maîtrise du risque RSE

1) Estimez-vous avoir un bonne maîtrise des risques/ opportunités RSE ?
2) Pensez-vous que si le risk management s'occupe intégralement de la gestion des risques/opportunités liés à la RSE , cela permettrait une meilleure maîtrise des risques ainsi que vous permettre de plus vous concentrez sur vos actions RSE ?

Conclusion

h) Selon vous, quelles sont les pistes d'évolution pour une meilleure gestion des risques/opportunité RSE ?
i) A l'avenir, pensez-vous que le tone at the top influencera cette plus grande intégration des risques RSE à l'ensemble de l'organisation ?

Annexe n°18: Résumé des interviews

1. *Alpha Banque*

a. *Risk officer*

Nous devons donc faire face à une série de risques (point de vue RM) :

1) **Risques opérationnels :** Assurer que l'échange de securities pour du cash se passe bien
2) **Risque crédit & de liquidité** : Exposés à ces risques dû à la casquette de banque
    a. **Risque crédit** : Si l'un des deux acteurs de la transaction tombe à court de cash en plein milieu de la transaction d'où viendrait le cash alors ? nous devons nous assurer d'avoir des garanties (deposit gardés au cas où) au cas où ça arrive.
    b. **Risque de liquidité** : Risque de tomber à court de cash pour payer les factures/fournisseurs quand elles arrivent à échéance.
3) **Risque de marché** : Le risque que les garanties offertes par le client perdent de la valeur dû aux mouvements du marché. Du coup, on s'expose à un risque crédit (tu penses avoir 100€ en garantie et en fait il n'en vaut plus que 80€)

➔Très bon dans la gestion de ces risques.

Là où on était un peu moins bon (parce que ça ne génère pas de revenus) c'est pour les risques suivants (conduct, legal and compliance, culture, etc.) et c'est une des raisons pour lesquelles on a lancé cette transition.

En effet, on est en pleine transformation de la fonction de Risk Management. Nous avons eu un certain cadre pendant des années mais on s'est rendu compte il y a deux ans qu'il n'était probablement pas aussi bon qu'on le pensait. Du coup, on transit d'un focus sur les risques opérationnels et risques bancaires à l'intégrations d'autres risques notamment liés à l'Ethics & Compliance.

- *Utilisez-vous plutôt le COSO I ou COSO II?*

On se concentre sur l'Entreprise Risk Management. On ne l'applique pas à la lettre mais on garde le même esprit.

- *Est-ce que vous travaillez ensemble avec le département compliance sur le Risk cycle des risques liés à la compliance ?*

1st line : s'occupe des affaires opérationnelles (owns the risks)
2nd line : RM + Compliance & Ethics (independent risks oversight)

Techniquement, le RM doit avoir un regard sur TOUS les risques liés à l'entreprise (risques liés à la comliance & Ethics inclus).
Maintenant, comme nous avons un département Compliance, on a tendance à les laisser gérer les risques liés à la compliance et à l'éthique.

Risques Compliance & Ethics :

1) Ethics ➔ Risques de comportement (doing the right thing, not the wrong one) → CoE & CoC
2) Compliance ➔ Risques liés à la non-conformité des lois et régulations en vigueur

Ensuite, nous monitorons les processus et activités de contrôles liées aux risques compliance. Les auditeurs internes vont aussi passer ces processus et contrôles en revue pour s'assurer de leur efficacité.

Pour une question de ressources, nous nous contentons d'analyser si les processus et contrôles des risques compliance sont gérés efficacement. Si c'est le cas, cela nous permet de concentrer nos ressources sur d'autres risques.

Exemple :
Le département identifie des risques liés à l' AML (Anti-Money Laundering) et les communique au management avec les contrôles nécessaires pour mitiger ces risques.

Le département de Risk Management ne va pas aller vérifier que les contrôles des risques AML sont en place. S'ils ont fait leur travail correctement, on ne devrait pas identifier de nouveaux risques. Donc notre implication dans l'identification des risques liés à la compliance est vraiment limitée puisqu'on a une fonction dont c'est la spécialité. (Gardons à l'esprit que c'est à la première ligne d'identifier les risques et à la seconde de fournir un support adéquat + un contrôle à la première pour identifier ces risques)

D'ailleurs le RM et la compliance sont obligés d'être séparés par la loi. La Compliance ne s'occupe pas de tout ce qui est opérationnel. Donc on ne peut pas vraiment parler de collaboration. Si jamais nous devions découvrir un nouveau risque lié à la compliance alors nous leur communiquerions (à la première ligne et à la compliance) mais sinon, nous n'intervenons pas pour les risques de compliance. Mais les chances sont minces que nous découvrions un risque compliance que la compliance n'ait pas déjà découvert.

Pour l'évaluation c'est pareil. C'est la responsabilité de la compliance. Ensuite, ils établissent en collaboration avec la première ligne, des contrôles efficaces pour mitiger ces risques. Puis c'est à eux de monitorer ces contrôles. Nous partons du principe que la compliance fait son travail et donc nous n'intervenons pas plus que ça. Les auditeurs internes (3ème ligne) vérifient et monitorent quand même les activités de contrôles. Tant que nous avons des rapports positifs des auditeurs internes concernant l'efficacité des contrôles de compliance, nous ne gaspillons pas nos ressources à ajouter une vérification.

Dans le cas contraire, si on s'aperçoit que certains risques de compliance ne sont pas bien mitigés ou que certains contrôles ne sont pas efficaces, alors on s'en mêlerait. Parce que techniquement, le département RM est responsable de TOUS les risques.

- *Comment est-ce que vous vous en rendriez compte ?*

Il y a quelques mécanismes formels comme l'audit interne qui tirerait la sonnette d'alarme
Sinon, si nous devions faire une évaluation indépendante quelque part et que nous nous rendions compte de quelque chose d'inquiétant concernant les risques compliance, alors nous poserions des questions pour savoir comment on en est arrivé là.

- *Quand et à quelle fréquence est-ce qu'il y a un dialogue entre Compliance et RM ?*

Pour ce qui est du dialogue entre les deux départements, il y a une réunion formelle entre le Compliance Chief Officer et le Chief Risk Officer tous les mois, tous les mois et demis pour échanger des informations.

Pour les niveaux moins haut dans la hiérarchie, il n'y a pas de réunion formelle organisée d'office tous les X temps.

Nous ne travaillons pas au même étage non plus, donc pas beaucoup de contacts informels non plus.

Mais ce n'est pas pour autant qu'il n'y a pas de communication entre les deux départements. On travaille par exemple avec eux sur le cadre légal. Mais on organise des meetings quand nous le jugeons bon pour s'échanger des informations.

- *Comment se passe le reporting des deux fonctions ?*

Compliance reporte directement au comité de direction et peut aussi reporter directement au comité d'administration si nécessaire.

Pareil pour la fonction de RM. On reporte au CEO mais il y a aussi une ligne directe de reporting jusqu'au comité de risques (non-executive).

Exemple :

Si on avait eu un problème avec l'AML, le CEO ne pourrait pas dire au chef de compliance de ne pas le reporter puisque le chef de compliance peut le reporter directement au comité d'administration. Le management ne peut pas non plus licencier le chef de compliance et est nommé par le comité de risque.

- *Quels pourraient être les améliorations possibles pour une meilleure collaboration entre compliance et RM ?*

On travaille bien ensemble. Cependant, l'entreprise en général est assez organisée en silos donc la collaboration pourrait être meilleure. On devrait avoir des réunions planifiées entre Compliance, Risk et Legal Officers avec une structure, une prise de notes, un follow-up.
Une autre méthode qui devrait être utilisée et qui est moins formelle serait d'engager des conversations dans l'ascenseur, à la machine à café et sonder les rumeurs et les petites histoires à gauche à droite et voir si on ne peut pas en retirer quelque chose d'intéressant sur les risques. C'est pour cela qu'il est important que le CRO ait un réseau de personnes de contact à travers l'organisation de qui il peut avoir un écho de ce qui se dit dans l'entreprise. Il est important par après, s'il y a suite, de sensibiliser les gens et leur faire comprendre que si on fait suite à l'une ou l'autre de leur déclaration c'est pour le bien de la compagnie et donc indirectement pour leur bien car si on arrive à mieux mitiger un risque, on aura de meilleurs résultats et donc potentiellement de plus gros bonus etc.

- *Comment gérez-vous le risque réputationnel ?*

Cela peut paraître un peu étrange mais nous n'avons pas le risque réputationel comme faisant partie de la liste des risques que nous traitons car le risque de réputation est la conséquence d'un risque. Les régulateurs parlent de risques réputationnels. Par exemple, si un risque opérationnel se réalise, il aura

sans nul doute un impact sur la réputation de l'entreprise. Il va de même pour les risques de compliance & ethics. On l'appelle le risque de réputation mais c'est plutôt l'impact sur la réputation.

Il est très difficile d'avoir des contrôles axés sur le risque réputationnel et il est très compliqué de le quantifier par ce que c'est la conséquence d'autres choses. Si jamais on a de bons contrôles en places pour les risques de crédit, liquidité, compliance ou peu importe, nous ne devrions pas avoir de conséquences négatives sur notre réputation.

- *Comment s'assurer que l'entreprise agissent de façon socialement et environnementalement responsable ?*

Le board et le senior management doivent se poser la question : « Quel genre d'entreprise est-ce que nous voulons être ? »

Ca se reflète ensuite dans les actions prises dans l'entreprise. Un exemple parmi tant d'autres, nous n'avons plus de verres en plastiques. On ne veut pas finir par avoir de la mauvaise presse à cause du fait que nous ne fassions pas assez socialement ou environnementalement et que ça se répercute sur notre réputation.

Nous devons aussi faire attention aux sanctions internationales sur certains pays parce que si on contracte avec des entreprises issues de ces pays, on pourrait très vite se retrouver avec des problèmes de compliance. Au final, ce genre de décision dépendent beaucoup de l'aversion au risque, de la risque culture et de l'appétit au risque.

Les régulateurs mettent vraiment l'accent sur la culture risque de l'entreprise. Il faut bien faire la différence entre « Hard controls » et « Soft controls ».

Les Hard controls sont tangibles, empiriques, quantitatifs, standards.
Les Soft controls sont culturels, comportementaux

Les softs controls vont toujours surpasser les hard controls. C'est pour cela qu'envoyer le bon « tone at the top » est crucial (est-ce que le senior management dit et prône les bonnes choses, les bonnes valeurs). Le board doit définir sa culture risque. On veut que les gens se posent la question de savoir si ce qu'ils font ou ce qu'on leur a demandé de faire est correct, éthique et bon ou pas.

Maintenant la question se pose de savoir comment est-ce que le management monitor et reporte le fait que cette risk culture est bien implantée dans l'entreprise. L'une des manières de faire est de réunir un échantillon représentatif de l'organisation (verticalement, au travers les différents départements et horizontalement, les différentes positions des employés au senior management) et d'effectuer une étude sur la culture risque. Et faire cette étude tous les quadrimestres. Les questions doivent être assez ouvertes pour essayer de comprendre les comportements, les opinions. →Top Down picture of risk culture

Sinon, entant que Risk Officer ou Compliance Officer, une autre chose à faire quand on va interviewer les employés pour l'une ou l'autre raison, on conclue par une question sur la culture de risque comme : « Comment se reflète la culture risque de votre domaine/département ? » « Avez-vous été témoin d'un mauvais comportement ou de quelque chose qui vous semble étranger ? » → Bottom Up picture of risk culture

- *Avez-vous des indicateurs pour analyser cela ?*

Oui, le département RH effectue ce que l'on appelle la Climate survey qui une enquête annuelle qui reprend des questions autour de : « Dans quelle mesure êtes-vous content de votre rôle, votre position ? », « Que pensez-vous de la façon dont le management opère et communique ? ». Si les résultats de cette enquête s'avèrent mauvais, il y a de fortes chances que le staff turnover augmente et que ça représente un risque. En effet, ça peut être difficile de recruter des gens qualifiés si certains étaient amenés à partir. Les résultats de cette étude sont ensuite reportés au board.

- *Est-ce que vous effectuez des due diligence ?*

Avant d'accepter un client, on l'analyse sur base de certains critères qu'on ne peut by passer. Pour être sûrs que contracter avec eux n'endommagerait pas notre réputation. Le département de procurement effectue également une due diligence pour nos fournisseurs. Ce contrôle a pour but de déterminer les risques liés à un contrat et l'éthique fait aussi partie de ces risques analysés (en bas de la liste des priorités). Après, la question se pose de savoir jusqu'où est-ce que vous remontez la chaine d'approvisionnement.

Nous, entant que RM, on s'intéresse de savoir si les risques liés au procurement sont bien gérés. Donc on va bien-sûr analyser si on a assez de back-up plans si un fournisseur critique pour une activité critique devait faillir à ses obligations. Puis en fin de liste, on arrive aux questions sur la CSR. Les questions liées à la CSR sont immanquablement moins prioritaires que le reste sauf si bien-sûr on traite avec des pays plus à risque.

Pour que le département de RM alloue du temps et des ressources à l'analyse du procurement, il faut que certaines inquiétudes ou incidents remontent jusqu'à eux via les contrôles mis en place, via la compliance ou l'audit interne. Sinon, ils ne vont pas allouer du temps et des ressources s'ils peuvent les allouer ailleurs où c'est plus pertinent.

A côté de cela, on organise deux fois par an un meeting avec des gens de différents départements et de différentes lignes de défense et on brainstorming pour savoir où est-ce qu'on devrait concentrer nos ressources et savoir quelles sont les tendances qui se dessine dans le secteur.

- *Y-a-t-il une collaboration, un dialogue entre le département de RM et celui de RSE ?*

Je ne pense pas qu'il y ait de dialogue formel entre les deux chefs de département. Et nous ne voyons pas la RSE comme étant un domaine très risqué. Nous ne faisons pas de forages, de destruction de forêt, etc. Mais on fait attention à avoir une bonne diversité dans l'entreprise en termes de sexe, background, origines et compétences.

- *Est-ce que vous vous chargez d'identifier les opportunités en plus des risques ?*

Dans la théorie, le risque management doit identifier les risques et les opportunités qui pourraient avec respectivement des conséquences négatives ET positives sur l'atteinte des objectifs. Maintenant, on appelle cela le RISK management, donc naturellement, on aura tendance à se pencher davantage sur les risques que sur les opportunités. A côté de cela, les régulateurs mettent vraiment l'accent sur la gestion des risques et nous forcent donc à nous focaliser sur les risques. Ils se moquent de savoir si la compagnie saisit des opportunités, ce qu'ils veulent c'est que la compagnie gère ses risques efficacement et délivre un bon service à la société.

- *Est-ce que vous pensez que si le board et le management se fixaient des objectifs RSE, la fonction de RM devrait plus se focaliser sur les risques liés à la RSE ?*

Nous avons pour le moment 4 top objectifs stratégiques du conseil d'administration (board) :

1) Strategic Objective
2) Compliance Strategic Objective
3) Operational Strategic Objective
4) Viability Objective (Etre un business viable et sûr)

Objectif critique secondaire :

1) Financial objective (on fait assez de profit pour maintenir la satisfaction de nos actionnaires)

Mais pour le moment nous n'avons pas d'objectifs RSE. Mais si nous devions en avoir un dans le futur, alors soudainement, le RM devrait faire davantage attention aux risques et opportunités liés à la RSE.

Comment s'assurer que la compagnie s'intéresse davantage à la RSE ? Il faut en faire un objectif stratégique**.**

Pour ce faire, le board doit prendre cette décision. Et pour convaincre le board, il faut premièrement que les membres du management committee soient convaincus que c'est une bonne chose à faire. Puisqu'en effet, c'est le management committee qui propose des objectifs stratégiques au board et le board en discute et donne son aval.

Nous avons déjà essayé de proposer un objectif stratégique lié à la RSE mais cela n'a pas été couronné de succès. Il est en effet relativement difficile de démontrer, de prouver que la RSE ajoute de la valeur à l'entreprise. De plus, la compagnie ne ressent pas autant de pression du public que si nous étions présents en B2C. Nous sommes plutôt axés B2B et le commun des mortels ne comprend même pas les activités de notre entreprise. Par ailleurs, notre compagnie n'est pas présente dans un secteur spécialement non-éthique. On suit les standards européens en terme de pratiques de business et on ne travaille pas avec les pays à risques. Nous travaillons avec des entreprise d'IT en Inde mais on a bien réalisé une due diligence avant de contracter.

Par contre, nous recevons aussi des questions de due diligence de la part de nos clients. Donc on nous demande aussi d'être orientés RSE mais quelle importance est-ce que cela a vraiment sur la décision de contracter avec nous ? Je ne sais pas. Qu'est-ce qui nous fait dire que ce n'est pas simplement cocher la case RSE et on passe à autre chose ? Probablement quand dans le future, les banques B2C auront de plus en plus de pression de leurs clients pour être RSE et ça risquera de créer une réaction en chaine poussant ensuite les banques de banques (B2B) à aussi être plus actifs en termes de RSE dû à la pression de leur propres clients (B2B). Par ailleurs, nos collaborateurs, les employés et le personnel de façon général a aussi tendance à de plus en plus faire attention à la RSE et veulent travailler dans une entreprise responsable. Donc si nous voulons continuer à attirer les jeunes talents et les garder, c'est crucial d'avancer en termes de RSE. D'une certaine manière, c'est un risque lié à la RSE → Workforce retention.

Donc au final, est-ce qu'on peut encore faire du progrès en termes de RSE ? Oui, mais où se trouve valeur ajoutée dans le fait d'aller encore plus loin en termes de RSE et comment prouver que cela augmente la valeur de l'entreprise ? Ca c'est vraiment là où le bât blesse.

b. Chief compliance officier

3 ème ligne : audit interne
2ème ligne : DPO, Compliance (document a part, on est en train de définir doivent être géré, pour chaque grand risque il y a des policy spécifique) on respecte la méthodologie du risque mais de manière différente et risk (responsable de définir le risk framework management avec un Corporate Risk Board Policy qui est approuvé avec le BOD définissant le risk appetit qui est découlé en une entreprise risk management qui sera approuvé par le comité de direction expliquant la méthodologie)
1 er : first ligne control units et Chief technology officer

- *Il existe une assez grande collaboration entre CSR et la compliance au sein de votre entreprise, selon vous, quelle est la différence entre CSR et compliance ?*

CSR c'est comment la société se comporte d'une manière sociétale et nous on va plus s'occuper du comportement par rapport à l'ensemble de nos employés par rapport aux législations existantes. Nous on va avoir plus le hard law et le soft law tombera chez CSR. Et les aspects organisationnel, plus bien être sont géré par HR.
On a beaucoup d'interaction avec HR mais personnellement la partie éthiques n'est pas encore assez développée. La compliance on en est toujours à cet aspect texte de la loi. Mais prendre en considération de manière plus forte pourrait être intéressant. Et là on est pas assez articulé, ni coordonné entre les différentes fonction (ex Starbuck combat contre la pauvreté mais est-ce que c'est en coordination avec nos valeurs ?)

- *Comment est-ce que l'éthique est gérée en interne ?*

On a une équipe qui s'occupe essentiellement de fraude et ethics mais plus focalisé sur la fraude. On a un COC qui définit les valeurs de la société et approuvé par le bod. On a un système de reporting interne (whistleblowing). Et puis on le gère.

- *Quelle est votre relation avec le risk management ?*

Le risk management monitor certains programme que l'on fait, comme nous, nous avons des contrôles qui devront être effectué par le risk management. Nous on va avoir un rôle similaire à l'audit interne, et eux vont plus rester à un niveau directionnelle. Nous on va tester les contrôles. Et eux ne vont jamais tester ce que nous on fait. C'est plus des discussions, ils vont prendre une position quant aux risques que les programmes que l'on gère peuvent faire problème à la société. Alors que nous, nous avons certains contrôles précisément alloué au risk management que l'on va aller tester en prenant des samples.

Si une issue est soulevé quant à savoir comment le risk management gère les contrôles.
Le risk management doit gérer deux grandes types de risques prudentielle (quanti) et non-prudentielle (quali) (organisationnelle et opérationnelle) on doit avoir des risk appetit et des contrôle ça, on prend en place.
notre indépendance est récente, avant on était rattaché au CRO aussi. Donc in fine ça n'a rien changé à la manière dont on a travaillé. Car le but c'est toujours de rapporter le moindre problème, au comité de direction et au comité d'audit. J'ai toujours une place auprès du CEO pour lui rapporter et notre charte

d'audit nous permet de rapporter le moindre problème auprès du BOD. La position n'a pas changer énormément.

- *Par rapport aux entreprises avec une très forte synergies, l'ID se fait de manière indépendante, il y a un énorme dialogue pour éviter les doublons au niveau des processus de contrôles, ainsi qu'au niveau du reporting ?*

On a une répartie des tâches assez claire entre risk management et compliance. On va s'occuper de tout ce qui vient des législations, tout ce qui est prudentielle. Mais les domaines sont assez varier, AML, privacy. Nous on va essayer de répondre à la question du BOD, Are you compliant ? Donc on a cartographier l'ensemble des domaines juridique qui doivent être sous contrôles et on a identifié clairement ce qui tombait dans le scope de la compliance, risk et HR. Mais en matière d'évaluation des risques, on utilise ce que le risk management fait, et on a des dialogues régulier pour être aligner. In fine, tout ça va se retrouver dans le positive assurance report, reprenant la vue des différentes lignes de défense quant à la maitrise de gestion du risque.

Maintenant, on a des discussions très fréquentes avec le risk management. Comme par exemple avec le GDPR, on a travaillé ensemble pour avoir une vue compliant et un des slides a été complété par le risk management pour avoir un aspect risque. Donc eux, vont nous donner des recommandations pour savoir comment mieux gérer le programme pour diminuer les risques qu'ils identifient. Maintenant on est pas au niveau optimal pour tous les types de risques.

Un des commentaires que l'on reçoit du board c'est qu'ils reçoivent des rapports du légal, risk et de la compliance traitant des mêmes problématiques mais qu'ils ne sont pas coordonner. Pour les domaines qui nous sont propres, j'aimerais bien qu'il y a plus de collaboration entre le CSR 3 départements pour qu'il y ait un meilleure alignement et s'assurer qu'il n'y ai pas de doublon, à moins qu'ils soient voulu.

- *Est-ce que le risk appetit influence énormément vos prises de décisions ?*

Non pas vraiment, il n'a pas vraiment été implémenter.

- *Est-ce que vous trouvez que cela a du sens d'avoir une meilleure collaboration avec la RSE ?*

Pour tout ce qui est soft law et ethic cela a du sens, mais pour tout ce qui est hard law et compliance car on a des fonctions plus de contrôle que la RSE n'a pas. Pour moi cela doit faire partie d'un framework commun avec une claire description des attentes de tout à chacun, afin d'éviter que HR, RSE et Compliance disent des choses différentes. Là on y est pas du tout. La vision est là, mais l'implémentation n'y est pas du tout.

C'est de la culture à 100%, maintenant j'aime pas l'aspect du mot soft control, car il faut convaincre les gens que c'est dans leur intérêt et dans l'intérêt de la boite d'agir d'une certaine manière. Le contrôle à une connotation négative. Mais l'idée est bonne.

Mais on parle déjà de ces soft controls, pour le moment les contrôles que l'on met en place, ce sont des contrôles purement juridiques, on avait commencé avec des soft control avec des interviews et on testait le réaction des employés par rapport à des scénarios bien précis pour essayer de se faire une idée au sein de la culture. Mais par priorisation, c'est quelque chose qui n'a pas été mis en place. C'est p-e quelque chose que l'on mettre en place, mais on a beaucoup de changement régulatrice pour le moment qui nous

occupe la grande majorité de notre temps. Mais d'abords il faut faire un travail pour implémenter cette culture forte.

- *Est-ce que le risque réputationnelle a un impact selon vous ?*

Le risque de réputation, il y a pas mal d'étude sur les conséquences d'une sanction financières sur le share price et elles ne sont pas univoques. On parle beaucoup du risque réputationnelle, c'est pas certain que cela a un impact économique. Des clients vont surement vous quitter, mais cela n'aura pas une incidence aussi forte de manière économique que la sanction. Maintenant l'aspect réputationnelle auprès du.

- *Est-ce que la compliance va avoir un regard sur la réputation ?*

Oui nous avons un regard. Maintenant, il ne faut pas le quantifier, cela reste une donnée plus qualitative. Si on devait commencer à le quantifier, cela serait surement le risk management qui serait en lead et nous en tant que contributeur. On aura notre rôle à jouer en matière de gestion du Framework d'éthique.

La méthodologie dans le risk management framework, serait définit par le risque. L'identification, on a leak data base, on va établir une base de données de contrôle que l'on estimera nécessaire pour gérer le risque de réputation de manière correcte. Par exemple :
Future : Comment on se positionne en tant que green company ? on mettra donc la base de donnée qu'il nous faut des procédures de contrôle de notre empreinte écologique, communiquer correctement aux employés et ensuite une communication de notre empreinte écologique pour nos investisseurs.

GRI on a aidé CSR a écrire le rapport. On a aidé à décrire ce que l'on faisait en tant que gestion du risque non financier.

- *Est-ce que vous pensez que le fait que la gestion du risque de réputation est un problème comment elle est gérée actuellement ?*

En soit, le fait qu'elle soit disséminé n'est pas un problème. Le défaut actuel c'est que l'on a pas dessiné un Framework compétent pour le gérer en identifiant bien les rôles de chacun.

- Quelles sont les risques les plus important pour vous ?

1er : sanctions, trump contre la Russie
2ème : Fraude, au vue des montants, on parle de trilliard d'euros qui bouge chaque année.
3ème : AML

- *Comment faites-vous pour lutter contre ce risque de fraude suivant le processus du COSO ?*

On utilise le framework COSO

- Entreprise risk assessment, qui est constitué de dialogue avec le business pour savoir où se trouve les risques de fraudes. (Cash, False supplier, Factures falsifiés, des faux employés créé)
- Detail risk assessment, là on va vraiment tester les contrôle et on regarde là ou on peut passer les contrôles. Et ces contrôles que l'on considère les plus important à pérenniser, on les introduits dans la base de donnée. Et cela fera l'objet d'un contrôle annuelle des équipes de contrôle de 2 ème ligne.

- Exemple de contrôle :
    - Losque l'on reçoit une facture d'un supplier avec un nouveau numéro de compte, on va d'abords téléphoner au supplier pour savoir si c'est bien lui qui l'a envoyé.
    - Pour les employés fictifs, on va voir si il y a une corrélation entre les employés du mois précédent et ceux du mois actuel. Et pour les nouveaux, on va vérifier.
    - En matière de cash, on va avoir le principe de double signature
- Les contrôles sont signé par les risk owners de manière annuel dans la base de donnée. Les risks owners sont responsables de mettre en place les contrôles et nous ont fait que les contrôler.

Je ne pense pas, mais lorsque nous faisons des assessments avec les business owerns, risk assessment est autour de la table aussi. Donc l'identification des risk se fait avec le risk assesment et l'audit. On a un fraude forum qui est un comité que nous présidons qui regroupe le risk et l'audit interne, cyber, les business owners les plus importants où sont discutés les risques les plus importants en terme de fraude.

C'est un core ownership. Lors des investigation c'est moi qui fait les interviews avec quelqu'un de risk management.

Risk de fraude = risque d'erreur humaine.

- *Avec le GDPR, comment avez-vous entreprises de l'identification à la mise en place des procédurs de contrôles ?*

On prend une législation, on l'analyse et on l'interprète, on la mets dans une spreadsheet, et article par article ca en fonction des fonctions et on fait un gap assessment (exigences vs ce que l'on a en place) et on y remédie. Puis on identifie ce qui est le plus important en terme de contrôle, car on ne sait pas avoir un contrôle sur tout. On identifie les Key risk et les Key control, et ces Key controls entrent dans ma data base pour future analyse.
Les contrôles : S'assurer que lorsque qu'on monitor les activités des employés dans l'utilisation des emails, que cela soit fait selon une procédure prédéfinie, et s'assurer que l'IT ne sait pas avoir accès aux emails sans avoir demander l'autorisation de RH ou compliance.

S'assurer que lorsqu'il y a un nouveau produit qui est mis sur le marché, comporte des données à caractère personnel, il faut qu'il y ait eu une revue formalisée par le DPO. On va aller voir dans nos testing des 6 derniers mois par exemple. On va aller voir donner moi les données validées par le DPO.

Mise a part pour la fraude, car il n'y a pas de loi la dessus, il est à chaque fois discuté avec le business avant de le mettre dans notre base de donnée.

On monitor de manière journalière toutes les sanctions. Car nous sommes présents dans le monde entier, on doit se conformer à toutes les législations.

- *Pour les sanctions, avez-vous parfois des méthodes de calcul ?*

Pour la loi, on ne prend aucun risque, on est compliant à 100%. On a trop peur du risque réputationnel.

Pour le cas libien, on savait d'où venait cette argent, mais le jour où il y a eu les allégations, on a directement gelé cet argent.

L'impact des sanctions est tel que c'est du high d'office.

1er sanction et fraude
2 eme blanchiment
3ème cyber et GDPR / competition law
4ème conflits
5ème MIFID
6ème EMIR

- *Pour tout ce qui est blanchiment d'argent ?*

Monitoring de toutes les transactions de manière journalière pour détecter des comportements inhabituel qui pourrait être utilisé à des fins de blanchiment d'argent. Dans mes équipes, on va directement au business pour essayer de comprendre.

- *Selon vous quelles seraient les pistes d'évolution pour une meilleure gestion des risques d'éthiques et de compliance ?*

Mieux articuler et inclure le management dans le risk éthique, plus les conscientiser de manière formelle. On doit s'assurer que le testing de 2ème ligne soit un testing plus intelligent. En matière de testing, ne pas juste penser in the box. Donc si jamais je demande de tester un processus, ne pas juste le tester mais essayer de comprendre ce qui se passe ou pourrait se passer. Pourquoi ce contrôle est mis en place, est-ce que c'est le bon contrôle ?

Documentation. On travaille beaucoup en mode firefigthing depuis des année. De par l'ensemble des nouvelles législations qui arrivent, on a eu très peu de temps pour documenter de manière correcte ce que l'on fait. Surtout en matière de méthodologie, on doit formaliser pourquoi on a pris telle décision sur base de quelle méthodologie et documenter tous les processus. (Utilité : pour si jamais anciens partent, les nouveaux sont au courant, satisfaire les demandes des auditeurs internes et régulateurs qui nous demandent pourquoi on a mis ces contrôles, sur base de quelle méthodologie pour leur donner le confort de la qualité des contrôles) .

c. Responsable RSE

- *Quels sont les domaines d'activité RSE ?*

Market place : La diversité, la sécurité, les droits de l'Homme
Nous sommes particulièrement actifs dans ce domaine.

Envrionment : Management des déchets, l'emprunte carbone, voyages d'affaire, électricité
Nous sommes une des seules compagnies en Belgique à établir des objectifs basés sur des valeurs scientifiques.

Comunity & Workplace: Les impacts sur les communautés locales
Nous sommes un peu moins actifs dans ce domaine parce que, du à notre core business, notre impact sur ce domaine est moindre. Comme nous sommes plus tournés vers les entreprises et moins vers les particuliers, nous avons plus de difficultés à proposer des options de prêt avantageuses pour des gens dans le besoin (ex : les gens qui ont plus de difficultés à acheter une maison).

Ethics & Compliance :
L'éthique et compliance rentre dans le domaine de la RSE. Et tous ces éléments rentrent dans la stratégie d'entreprise. Cependant, il est important de noter que les 4 composantes dans la RSE sont gérées séparément mais avec un dialogue et une collaboration soutenue entre les 4 services.

Moi, je me retrouve au milieu des 4 et j'assure le contact, le partage d'information et la collaboration entre ces 4 composantes. Et je m'occupe d'établir la stratégie RSE en lien avec la stratégie d'entreprise.

- *Est-ce que vous faites du benchmark de vos concurrents pour guider vos actions RSE ?*

Oui, lorsque nous effectuons une enquête sur les besoins et exigences de nos différentes parties prenantes, nous effectuons également un benchmark de nos concurrents.

A côté de cela, je fais partie d'un réseau de RSE pour entreprises, on se réunit 4 fois par an et les gens présents partagent leurs opinions sur quels sont les sujets sensibles, leurs pratiques RSE. C'est très informel mais cela reste confidentiel. A côté de cela, le rapport GRI est également une bonne façon de récolter de l'information sur les pratiques RSE et les performances extra-financières de ses concurrents.

- *Comment procédez-vous pour identifier quelles sont les meilleures opportunités à saisir en termes d'actions RSE ?*

Nous choisissons nos programmes RSE en fonction des besoins et exigences de nos différentes parties prenantes ainsi qu'en rapport avec la stratégie d'entreprise.

Il est donc important de comprendre toute la variété de besoins et exigences de ces parties prenantes. Ces exigences peuvent provenir des régulateurs, des clients, des fournisseurs, du personnel, des seniors managers.

- *Comment est-ce que vous évaluez ces besoins ?*

Nous effectuons une enquête sur les différentes parties prenantes qu'on organise avec la consultance puisqu'ils sont neutres et objectifs. Cette enquête regroupe 17 questions et ils évaluent l'importance de leurs exigences sur une échelle. Et ainsi on peut savoir à quoi est-ce que les parties prenantes accordent le plus d'importance.

Bien sûr, en plus de ces besoins et exigences, nous devons prendre en considération d'autres facteurs : nos ressources, notre budget, les priorités des seniors managers, la prise de conscience des employés etc.

On doit choisir entre des « Quick-wins » faciles à atteindre, n'ayant pas le plus gros impact mais qui, en s'additionnant peuvent construire notre crédibilité. A l'inverse, on peut se pencher sur les actions qui ont de plus gros impacts. Le senior management doit être convaincu par ces dernières et doivent devenir partie intégrante de la stratégie d'entreprise pour avoir le plus gros impact.

- *Comment définiriez-vous la relation entre le département RSE et le conseil d'administration ? Sont-ils réceptifs à ces ambitions RSE ?*

Nous n'avons pas de contact direct avec le conseil d'administration mais bien avec le comité exécutif. Chacune des 4 composantes de la RSE sont contrôlées par le senior management donc évidemment, aux vus des progrès déjà effectués, on peut dire qu'ils croient en l'importance de la RSE. Cependant, que ce soit à nous ou dans les autres compagnies, vous trouverez différentes opinions, différentes priorités au sommet de l'entreprise. Donc si vous vous trouvez dans le cas où le CEO est très engagé, vous allez être relativement bien écoutés. Cependant, dans le cas où cette personne devait quitter la compagnie, vous pourriez être amenés à faire quelques pas en arrière.

- *Est-ce que pour le moment vous estimez que vous êtes écoutés ?*

Cela peut toujours être mieux mais oui, d'une certaine manière certainement mieux qu'il y a 5-6 ans les executifs sont réceptifs. Nous leur présentons nos ambitions et plans 3-4 fois par an, ils nous écoutent, nous donne leurs opinions.

Le rêve serait d'avoir un responsable RSE siégeant au comité d'exécutifs mais c'est assez rare.

Mais nous faisons du progrès. D'ailleurs, nous sommes sur le point de publier notre premier rapport durable reportant nos performances non-financières. Nous suivons les standards GRI donc c'est totalement volontaire (pas légalement obligés puisque nous ne sommes pas inscrits en bourse et pas « public facing »).

- *Comment mesurez-vous les performances des actions RSE entreprises ?*

Comme la RSE est décentralisée, chacune des 4 composantes a ses propres objectifs et ses propres standards. Certaines mesures sont quanti d'autres quali. Dans le domaine de l'environnement, c'est plutôt quanti (% d'émissions). Dans ce qui est community c'est plutôt quali (feedback des communautés locales) et quanti (nombre de fermiers impactés, enfants scholarisés, etc.) . Workplace c'est quanti avec des objectifs axés sur la diversité (femmes ayant des séniors positions, etc.). Puisque nous ne sommes pas une entreprise manufacturière, nous allons moins avoir des objectifs en termes de sécurité sur le lieu de travail mais plutôt faire attention au stress, aux absences (quanti).

- *Retournez-vous voir les parties prenantes pour avoir un feedback sur vos performances ?*

Absolument. Tout ceci fait partie d'un cycle. Le rapport GRI est un très bon moyen de leur communiquer nos performances. Ce rapport publié en ligne permet à tout le monde de comparé les performances annuelles années après années pour analyser la progression.

C'est la première année que nous le faisons. Ils seront publiés fin mai.

- *Est-ce que ces parties prenantes reviennent vers vous pour vous interpeller sur ces performances ?*

Hormis les régulateurs, les parties prenantes externes ne reviennent généralement pas vers nous. Les membres du board non plus pour le moment mais peut-être dans le futur. Pareil pour les investisseurs.

Pour ce qui est des parties prenantes internes par contre, ils reviennent plus facilement vers nous pour avoir des explications s'ils sont mécontents (gender pay gap for exemple).

Donc c'est un peu différent des compagnies très tournées vers le publique qui auront des parties prenantes très impliquées. Hormis les régulateurs, pour nous les parties prenantes sont relativement moins exigeantes.

- *Est-ce que vous faites attention à vos fournisseurs en termes de RSE ?*

Jusqu'à récemment, on ne faisait pas trop attention à cette partie de la chaine de valeur. Aujourd'hui, nous sommes sur le point de publier un supplier code of conduct.
Nos fournisseurs devront se plier aux standards éthiques auxquels nous adhérons. De plus, nous allons ajouter des questions liées à la RSE aux questionnaires que nous donnons aux nouveaux fournisseurs.

Nous nous faisons moins de soucis pour les gros fournisseurs comme les compagnies de softwares mais là où cela a plus de sens c'est pour les plus petits fournisseurs comme le service de nettoyage. Nous déterminons s'ils ne sont pas liés à de mauvaises conditions de travail, de l'esclavage moderne ou ayant un passé frauduleux.
Donc pour conclure, bien que nous ne soyons pas une compagnie de produits tournée vers le publique, si nous ne gérons pas ces risques liés aux fournisseurs, cela pourrait se répercuter sur nous et notre réputation.

- *Est-ce que vous effectuez aussi une due dilligence sur vos clients ?*

Oui, cela a toujours été le cas. Il y a des critères stricts pour devenir client chez nous. Aucun individu ne peut devenir client chez nous (hormis un roi ou un client très riche). Nos clients sont surtout de grosses banques et elles ont des conditions à respecter pour devenir client chez nous.

Nous respectons à la lettre les lois et règles en application. (Ex : sanctions des Etats-Unis sur la Russie, on respecte la blacklist à la lettre).

Nous avons donc une liste de compagnies, de pays avec lesquels nous ne traitons pas. Par contre, comme toute compagnie, on se doit de peser le pour et le contre de traiter ou non avec certains clients. On se rapporte au Risk appetite de l'entreprise et on fait la balance entre risques et opportunités pour prendre notre décision.

- *Comment précédez-vous pour gérer le risque réputationel ?*

C'est principalement la responsabilité du Brand/Communication Manager avec l'aide du chef du département press. Ce n'est pas explicitement lié à la responsabilité du département RSE.
Ils analysent comment notre réputation pourrait être mise à mal.

D'une part, nous nous focalisons principalement sur les market risks, operational risks et liquidity risks et si gérons bien ces derniers, notre réputation ne sera pas endommagée. Mais dans une autre proportion, il s'agit aussi de bien gérer notre image de marque dans la presse, sur les réseaux sociaux.

Je ne suis personnellement pas responsable pour la gestion des risques liés à la réputation ni la personne qui mettra en place des contrôles ou processus pour éviter ces risques.

D'une part, j'irai reporter au département de compliance si j'ai le sentiment que nous sommes exposés dans certains domaines ou s'il me semble qu'il y a un manquement au niveau de notre politique d'entreprise.

D'autre part, si jamais je trouve que nous n'avons pas les bonnes politiques en ce qui concerne l'aspect workplace, j'irai probablement rapporter cela au département de Ressources Humaines. Donc cela dépend vraiment d'où est-ce qu'on pense que le risque se situe.

- *Est-ce que vous avez des rapports/contacts avec le département de de Risk Management ?*

Lorsque nous faisons notre rapport, nous leur demandons leur contribution en termes de risques. Mais ce contact ce fait principalement via la personne en charge de la compliance travaillant dans le département RSE.

- *Lorsque le Brand manager et le Risk manager gèrent le risque réputationel, viennent-ils vous concerter ?*

Pas nécessairement, je ne fais pas nécessairement partie de ce processus, cela dépend vraiment des sujets adressés.

Puisque vous analysez les oppotunités avec la Risk Matrix et le brand manager en collaboration avec le risk manager s'occupe de la gestion des risques réputationels avec une matrice similaire, pensez-vous que ce serait une bonne idée que le Risk Management reprenne aussi la gestion des opportunités pour avoir une vue plus globale ?

Je ne suis pas sûre que ça puisse fonctionne dans l'immédiat. Mais oui, c'est une possibilité pour le futur car cela a du sens d'aligner les pratiques déjà mises en place, éviter les doublons. Cependant, je ne suis pas sûr que le Risk Management regarderait la gestion des opportunités de la même façon que nous le faisons. Ce que je veux dire c'est que pour le moment il y a forcément des doublons au niveau des pratiques mais je pense aussi que nous faisons attention à des choses auxquelles ils ne font pas attention.

L'une des raisons peut être liée à l'engagement RSE du comité exécutif. Car leur focus se porte surtout sur le fait de bien gérer les opérations financières et éviter tout disfonctionnement et éviter d'exposer l'économie à des accidents. Ils sont très avers au risque opérationnel.

- *A votre avis, quelle serait la meilleure manière de gérer opportunités et risques ?*

Est-ce que je verrais cela comme devant la responsabilité du manager RSE ? Pas vraiment, car je ne pense pas avoir le bon profil, les compétences appropriées à la gestion des risques. Mais je vois réellement l'intérêt d'avoir une relation plus rapprochée entre ces deux éléments.

Si vous avez un modèle plus centralisé avec un très gros département RSE ça peut être intéressant d'avoir quelqu'un responsable du risque réputationel qui rapportait cela au comité exécutif.

Si vous avez un modèle plus décentralisé, comme nous, cela a plus de sens d'avoir un alignement entre les deux notions mais pas nécessairement avoir la fonction de risque incorporée au département RSE.

- *Quelles sont les mesures à entreprendre pour améliorer la gestion des opportunités et risques liés à la RSE ?*

Prendre conscience que la gestion des risques réputationels ne doit pas être prise à la légère et avoir une personne qualifiée pour focalisée sur la gestion de ce risque. Ce serait ensuite à cette personne de réfléchir à des contrôles et procédures à mettre en place. Cette personne aurait à la fois un pied dans le département RSE et un pied dans le département de Risk Management.

Par exemple, nous avons 2 personnes liées au département compliance mais ayant un aspect RSE dans leur titre. Ce qu'il veut dire qu'ils sont un pied en compliance et un pied en RSE. Ils ne me font pas leur rapport mais la RSE fait intégralement partie de leur job.

Ainsi, une gestion efficace des risques réputationels passe par le fait d'avoir une personne du Risk Management ayant la RSE comme faisant part de leur fonction/responsabilité.

- *Que reportez-vous et à qui ?*

Je ne fais aucun reporting au département de Risk Management. Je rapporter au Global Head of Communication faisant partie de département de Ressources Humaines. Mon supérieur est le chef des Ressources Humaines.

- *Est-ce que votre supérieur est responsable de l'évaluation des risques réputationels ?*

Je ne pense pas qu'elle soit entièrement responsable de cela. Elle a une certaine responsabilité vis à vis de cela mais pas totalement.

- *Selon vous, vous faite partie de la première ou deuxième ligne de défense ?*

Sans hésiter la deuxième ligne pas la première. Nous avons plus un rôle de conseillés.

- *Est-ce que vous pensez que ce serait une bonne idée que vous fassiez directement votre reporting au Risk Management ?*

Je ne suis pas sûre à 100%. Pas pour le moment parce qu'ils sont surtout axés sur les risques opérationnels et les risques financiers.

d. Responsable communication

- *En quoi la RSE impacte le risque réputationnel ?*

Il faut comprendre que la majorité des compagnies qui prennent l'INITIATIVE de se lancer dans la RSE, le font pour intensifier leurs engagements vis à vis de différentes parties prenantes. Ce qui veut

dire que ces compagnies vont principalement opter pour des initiatives ayant une bonne visibilité à l'égard de ces parties prenantes. Cette visibilité a pour but d'impacter la réputation de la compagnie.

La réputation est vraiment clef pour l'organisation car il y a un lien très fort entre réputation et confiance. Plus une firme agit de façon responsable, plus cela renforce sa réputation et par conséquent renforce la confiance que les différentes parties prenantes ont en la compagnie. (Attention aussi qu'on ne fait pas de la RSE simplement pour avoir une bonne image)

En clair, si jamais on décide de construire une réputation très forte à l'égard d'un groupe de parties prenantes, prenons les clients ; si jamais quelque chose devait mal se passer au cours de nos activités avec ces clients mais qu'on a toujours renforcé notre réputation via certaines pratiques et actions, la probabilité que ces clients nous laissent tomber sera nettement moindre. Donc, bien sûr, c'est un investissement mais au final cela vaut vraiment la peine.

Donc tant les actions RSE que la communication avec les parties prenantes aide à créer cette réputation et cette relation de confiance.

A côté de cela, si nous ne faisons pas attention à ce qu'il se passe dans un plus grand rayon que nos parties prenantes directes ou si nous ne faisons pas attention à ce que la concurrence fait, nous finirions par avoir un sérieux risque réputationnel.

Plus haut est la réputation d'une compagnie, plus haut sera la shareholder value.

- *Comment est géré ce risque réputationnel dans l'entreprise ?*

Nous avons toujours eu 3 parties prenantes clefs à l'entreprise :
<u>En interne :</u>

1) Le board
2) Les clients
3) Les employés

Mais les parties prenantes suivantes n'étaient pas vraiment pris en considération pour l'aspect réputation de l'entreprise. On évoluait dans une optique « vivons heureux, vivons cachés » mais maintenant que le régulateur nous pousse de plus en plus, que les médias s'intéressent de plus en plus à nous, on intègre davantage les autres parties prenantes plus externes à l'entreprise.

<u>En externe :</u>

1) Le régulateur
2) Les médias
3) L'opinion publique
4) Les fournisseurs

On s'est rendu compte que personne, ni de la compliance, ni du département légal, ni du risk management ne savait vraiment comment s'y prendre pour tacler des problèmes réputationnels.

- *A votre avis, est-ce que la gestion du risque réputationnel dépend surtout d'une communication efficace ?*

Non, tout ne dépend pas de la communication.

Avant de communiquer, il faut forcément avoir du contenu à communiquer (exemples, actions, practices, etc.)

Il faut aussi garder à l'esprit qu'on ne détient pas notre réputation. Extérieurement, n'importe qui peut essayer d'attaquer notre réputation ou intérieurement, n'importe qui peut commettre une erreur et endommager notre réputation. C'est la raison pour laquelle il faut mettre en place des mécanismes pour gérer au maximum cette réputation.

- *Qui vous pousse à faire de la RSE ?*

Il faut garder à l'esprit que personne ne nous demande explicitement de lancer des actions RSE. C'est le top management qui prend l'initiative de développer la RSE. Il faut ensuite savoir jusqu'où on veut aller et il faut décider soit de se tourner davantage vers les parties prenantes internes ou externes à l'entreprise.

- *Puisqu'il n'y a pas de centralisation de la gestion du risque réputationnel, comment s'assurer de la bonne gestion de celui-ci ?*

Il y a toujours des parties qu'on peut gérer, d'autres auxquelles on ne peut rien faire.
Nous n'avons pas une véritable gouvernance concernant le risque réputationnel. Donc, c'est certainement quelque chose que nous devons mettre en place. Je pense qu'il faudrait que cela parte de notre équipe de risk management. Pour l'instant, le département de risk management ne s'en inquiète pas plus du risque réputationnel que ça. Il m'est déjà arrivé de leur demander d'organiser une réunion de crise avec des acteurs clefs pour décider de ce que nous devons faire/dire mais ils ne voyaient pas un véritable intérêt. J'ai donc du moi-même mener cette réunion de crise.

Pour le moment, il manque de la coordination et de l'organisation puisque nous sommes à l'initiative de ces réunions de crise à la place du risk management. Cependant, en cas de crise nous savons exactement qui nous devons convoquer à notre réunion de crise : des gens du département légal, des gens du département compliance, des gens du risk management.
Lors de ce meeting, nous décidons de comment nous devons gérer et tacler ce risque réputationnel ainsi de comment communiquer par rapport à un certain incident. Donc d'une certaine manière, ça fonctionne mais ce n'est pas encré dans la fonction de risk management, ce qui n'est pas normal.

- *Qu'est-ce qui est mis en place pour éviter ces incidents réputationnels d'arriver ?*

On doit mettre en place un atelier pour vraiment comprendre quelles sont tous les situations que le risk management connait qui pourraient potentiellement se retourner contre nous.

Parce que pour le moment, c'est les médias qui viennent nous poser des questions, on va ensuite trouver le département légal et compliance qui nous disent qqch comme : « Oui nous sommes au courant, il existe telle ou telle procédure » alors que moi je n'en avais aucune idée.

- *On peut donc dire que vous être occupés à construire également un cadre de risque management pour votre département ?*

Oui, nous avons déjà pu identifier certaines catégories de risques liées au risque réputationnel.

- Les activités qui ont un impact direct sur le business
- Les activités qui ont un impact secondaire sur le business
- Les activités qui ont un impact sur le business mais de nature moins matérielle

Nous nous servons d'un manuel issu du risk management pour les identifier mais nous n'avons pas encore de véritable marche à suivre. Nous avons aussi un manuel de communication de crise qu'on a développé et qui nous donne la possibilité de mandater des gens provenant de différents départements pour une réunion exceptionnelle. En effet, ce manuel (handbook) nous donne des informations du genre : « Contacter Mr X de chez Compliance, Mme Y du legal department, etc. »

- *Est-ce que vous pouvez nous donner des exemples de risques clefs liés à la réputation ?*

Gardons bien à l'esprit que le risque réputationnel à proprement parlé n'existe pas. Il est toujours lié à d'autres risques.

Premièrement, des risques qui sont liés à l'efficacité de nos systèmes. Si nos systèmes plantent, ce sont des centaines de milliers d'euros qui sont bloqués, ce serait un désastre. C'est la raison pour laquelle on a 3 systèmes de secours. Donc un premier risque est lié à la Cyber sécurité.

- *Qu'en est-il des risques liés à la compliance et aux activités de RSE ?*

Dans un sens, la RSE a plus pour rôle de construire une bonne réputation d'entreprise plutôt que de la protéger, la conserver.

Contrairement à la compliance, qui est là pour s'assurer qu'on soit bien conformes avec les lois et les régulations et qui est donc là pour protéger notre réputation. Si nous venions à ne pas être conformes, nous nous exposerions à un sérieux risque réputationnel. On perdrait la confiance des régulateurs, de nos clients, nos fournisseurs seraient eux aussi plus méfiants.

- *Comment est-ce que vous arrivez à capter les opportunités liées à la RSE pour construire cette bonne réputation ?*

Nous avons commencé à reporter nos performances extra-financière via les Global Reporting Initiative standards (GRI). Le but est de vraiment créer la plus grande transparence possible et de démontrer aux parties prenantes que nous prenons des initiatives pour agir de façon responsable. Bien-sûr, nous avons encore du chemin à parcourir, nous ne sommes pas parfaits. Mais au moins, nous montrons de manière transparente où nous en sommes en matière de performances non-financières. (Exemple du système de refroidissement pour les 16 étages avec le glaçon qui consomme moins d'énergie qu'un AC)

- *Pourquoi est-ce que le risk management ne s'occupe pas de ce risque réputationnel ?*

Il est bien présent dans leur manuel de risques. Ils ont identifié le risque réputationnel comme étant un risque. Mais actuellement, il n'y a pas de guidelines, de marche à suivre. Pourquoi ? Parce qu'ils se focalisent tout simplement sur d'autres priorités.

- *Est-ce que vous pensez que c'est dû à la pression des régulateurs sur les risques financiers, de liquidité et de crédit ?*

Clairement. Après la crise de 2008, les régulateurs ont renforcé leurs restrictions. Donc il y a un certain ordre de priorité à respecter. (S'assurer que les banques aient assez d'argent en réserve si les choses devaient tourner au vinaigre une nouvelle fois) Nous devons, au maximum, réduire le risque de marché.

- *La compliance et le risk management travaillent avec la première ligne pour établir des contrôles et des procédures pour contrer les différents risques. Est-ce que vous ajoutez des procédures ou des contrôles additionnels concernant le risque réputationnel ?*

Oui, dans la mesure où je fais partie de activités de contrôles implémentées par la compliance ou le risk management. Il y a probablement des activités de contrôles dont je ne suis même pas au courant qu'elles existent. Bien que nous ayons beaucoup dialogué ces derniers temps, c'est souvent à mon initiative. Bien qu'ils soient conscients qu'il n'y a pas encore une bonne gouvernance du risque réputationnel, je ne suis pas vraiment sollicitée dans le processus d'établissement des activités de contrôles.

Il faut vraiment qu'on arrive à créer une gouvernance (avec des gens issus des département compliance, risk management et légal) pour gérer efficacement ce risque réputationnel. Savoir comment l'identifier, le mesurer, le tacler et le communiquer.

2. ***Beta Assurance***

a. *Chief risk officer*

- *Est-ce que vous travaillez plus avec le COSO I ou le COSO II ?*

Nous travaillons l'Internal Control et l'ERM. Mais la Compliance, le DPO et la fonction actuarielle fait aussi partie du CRO office. De plus on a le DPO (Data Protection Office). On bosse tous au même niveau et on essaye de collaborer et aligner au maximum la méthodologie entre les différents services.

Le ERM s'occupe de tout le Risk Management Cycle ce qui veut dire : identification, assessment, reporting des risques et Internal Control c'est le monitoring et le testing de l'efficacité des contrôles et processus qui existent dans la compagnie. (2ème linge) On analyse les contrôles de manière globale et on aide la 1ère ligne à faire leur self-assessment.

L'audit interne, considéré comme 3ème ligne, analyse les contrôles de manière individuelle.

- *Est-ce que le département de Risk Management s'occupe aussi de capter les opportunités en plus de contrôler le risque ?*

Nous, nous sommes principalement axés sur les risques. Il existe aussi un suivit des opportunités mais c'est plutôt le performance management qui est en charge de cela.

Nous, on s'occupe essentiellement des risques. Nous avons des contacts partout dans l'organisation et au niveau de la première ligne pour identifier tous les risques clefs.

- *Quelles sont les méthodes que vous utilisez pour contrôler les risques ?*

Nous utilisions une matrice probabilités/impacts pour évaluer et hiérarchiser les risques.

- *Est-ce que vous utilisez la même matrice pour évaluer les opportunités ?*

Pour les opportunités c'est une autre forme de mesure qui est utilisée. Il s'agit plutôt de classifier les opportunités qu'on classifie, celles pour lesquelles on fait un monitoring, celles pour lesquelles on prévoit des actions par rapport à leurs probabilités.

Opportunités : nouvelles technologies (appareils de contrôles à placer dans les voiture par exemple)

- *Comment est-ce que vous communiquer les risques dans l'organisation ?*

L**'identification** se passe en discutant avec la première ligne. On **mesure** ces risques avec la matrice. Ensuite, on montre cela au management pour approuver une décision finale et on retranscrit cela dans un rapport trimestriel.

Nous travaillons en collaboration avec des ***Decentralized risk entities*** présentes dans les différentes business lines et support units avec lesquelles on a des réunions toutes les 2 semaines. Où on discute ces rapports, on fait le suivi des actions. On a donc des contacts réguliers avec des gens très proches de la première ligne.

- *Est-ce que vous sentez que vous avez une certaine influence sur la stratégie mise en place ?*

Nous faisons un rapport ORSA annuel qui est un rapport obligatoire qu'on présent au board et on constate qu'il y a beaucoup de questions et de réactions à ce moment-là donc on peut dire qu'on est écoutés.

- *Comment est-ce que le risk appetite influence votre décision ?*

Il est vraiment le cadre permettant au RM de fonctionner. A la fois sur des aspects quantitatifs vis à vis du Profit&Loss. Mais aussi des critères plutôt qualitatifs qu'on appelle la franchise quality qui est toute la valeur de l'entreprise qui n'est pas reprise dans les chiffres de solvabilité et de P&L et c'est notamment sur ces critères qualitatifs qu'on garde un œil sur notre risque de réputation.

Pour ce qui est le suivi de ces critères qualitatifs, on va établir des KRI's.

- *Comment est-ce que le les processus et contrôles sont mis en place ?*

Ils sont mis en place dans la première ligne via notre rapport annuel du internal control assessment. On demande à cette première ligne de démontrer que ces contrôles soient efficaces. Si nous constatons, qu'il y a des contrôles qui ne fonctionnent pas bien, nous mettons en place des plans d'actions.

L'initiative vient d'abord de la première ligne puis nous on vient avec des plans d'actions le cas échéant.

- *Comment qualifiez-vous la relation qui existe entre le RM et la compliance ?*

Transposition de « SOC 2 » (Exception de la FSMA)

La Compliance et le RM sont relativement bien intégrés. Les synergies se trouvent surtout au niveau de la méthodologie. On utilise par exemple le même outil informatique pour faire le suivi des actions. Si par exemple nous mesurons les risques selon (Impacts/Likelihood), on essaye de le faire de manière consistante. Donc c'est surtout au niveau de la méthodologie qu'il y a des discussions. A part cela, la fonction de Compliance fonctionne de manière assre indépendante du RM.

- *Est-ce que dans votre reporting de RM, vous incluez certains KRI issus de la compliance ?*

Non, les KRI de compliance sont dans le reporting de la compliance.
La fonction de compliance a son propre reporting.

Maintenant, si la compliance signale qu'il y a un certain risque par rapport au fait d'être conforme avec une législation, nous le reprendrons dans nos Key risks et nous discuterons avec eux des actions à prendre (Par exemple le GDPR). Nous reprenons les risques qui peuvent avoir un impact sur le P&L ou sur la franchise quality.

- *Est-ce que l'intégration de ces KRI's permettent d'avoir un plus gros impact sur la stratégie d'entreprise ?*

Pour ce qui est de la conscientisation du board par rapport à la compliance, c'est surtout grâce au rapport de compliance qu'il y aura un impact.

- *Est-ce que vous vous concertez avec la compliance pour éviter les doublons sur les activités de contrôles ?*

Pour le risque de fraude par exemple, chez nous on le considère comme un risque opérationnel et donc c'est plutôt dans le scope de RM. Là où les doublons pourraient apparaître c'est lorsque la compliance identifie des contrôles pour être en conformité avec la loi. Donc on gère ces doublons par des discussions pour garder ces risques sous contrôle sans avoir des activités de contrôle trop pesantes sur les employés.

- *Est-ce que vous pensez que le fait que la compliance soit intégrée dans la fonction de RM soit un avantage ou un inconvénient ?*

Difficile à dire … Une des raisons derrière ce système est historique. Je constate que ça fonctionne plutôt bien.

- *Est-ce que vous pensez intéressant d'intégrer la gestion des opportunités liées à la RSE au département RM ?*

Pour le moment nous ne le faisons pas. C'est plutôt le département de performances qui s'en occupe. Bien sûr, il y a beaucoup de similitudes. Notamment dans la phase d'identification, d'assessement des opportunités/risques on passe énormément par les gens de la première ligne pour récolter leurs idées.

On va plus s'axer risques. Donc dans ce registre, on fait de plus en plus attention au risque réputationnel. On est plus présents sur les réseaux sociaux donc on évalue les risques qui y sont liés (est-ce qu'il y a

des choses qu'on doit garder à l'œil ?). On essaye d'identifier les choses auxquelles le public accorde de plus en plus d'importance et qui présente un risque si on ne l'intègre pas. Donc au moment où au niveau des impacts/likelihood ça devient important, on le prend en considération.

Notons toutefois que mitiger un risque peut se traduire par une opportunité in fine. Le fait de maintenir une certaine satisfaction des employés et d'adresser des problèmes éthiques, faire des actions RSE peut permettre d'attirer et garder des talents. Le but est de maintenir notre franchise quality et si jamais on ne fait rien, il y a certains de KRI qui vont arriver dans la zone « rouge ».

- *Est-ce que vous pouvez nous donner un exemple de KRI's liés à la réputation que vous reportez ?*

Les KRI's qu'on utilise pour controler la franchise quality,il y a par exemple : la satisfaction des clients, la satisfaction des intermédiaires, le turnover du personnel, la facilité avec laquelle on engage du personnel. On va aussi regarder le résultat des études de brand awareness. A partir d'un moment où on dépasse certains taux, on doit définir des plans d'actions.

Par ailleurs, nous avons aussi une personne issue du département de RM qui se trouvera dans le comité de sponsoring et avec qui nous discuterons des risques éventuels liés au sponsoring. Attention, c'est plus une personne de contact qu'un risk manager travaillant entant que decentralized risk entity qu'on retrouve au niveau des premières lignes.

Conclusion : Risques réputationnels bien intégrés mais les opportunités pas intégrées au RM.

« On garde notre rôle de pessimistes professionnels »

- *Pensez-vous que l'intégration de KPI's aurait une valeur ajoutée au RM ?*

Je vous ai parlé du département performances qui analyse les opportunités globales de la compagnie. Au moment où le département performance procède à son identification des opportunités et discute de la stratégie avec le management, on essaye de mettre leur analyse d'opportunités à coté de notre analyse de risques pour essayer de déceler si certaines des tendances qu'ils ont identifiées que nous considérons comme importantes également. Donc bien qu'on ait des méthodologies différentes, on a quand même une mise en commun des deux quand on parle stratégie avec le comité de direction. On essaye de présenter les risques et les opportunités dans la même session pour donner au management une vision équilibrée.

Avoir une seule session pour présenter les deux aspects du scope permet de donner une image la plus représentative de la situation au management et donc oui, arriver à prendre de meilleures décisions stratégiques.

- *Pensez-vous que la RSE devrait se centraliser ?*

Je pense que la RSE va suivre le même processus de développement que la compliance et le risk mangement. Avant c'était pas du tout centralisé et géré un peu comme ça, au « gut feeling » de façon intuitive dans l'entreprise et petit à petit on a été amenés à plus centraliser. Suite à « SOLVA 2 » beaucoup a été centralisé/formalisé.

Mais par exemple pour les contrôles internes, quand on a commencé à faire des rapports de contrôle sur la première ligne, on s'est rendu compte qu'il y avait déjà énormément de contrôles qui était en place sans forcément être centralisés. Puis on les a recensés et centralisés pour avoir un assessment plus formel et voir si quelque chose ne manquait pas.

Donc pareil pour la RSE, même s'il n'y a pas grand-chose de formalisé, je pense qu'il y a déjà pas mal de choses mises en place implicitement.

- *Selon vous, qu'est-ce qui pourrait être mis en place pour améliorer la gestion des risques liés à la RSE ?*

Pour les risques, nous avons déjà quelque chose de plus formel. L'intégration de la franchise quality (valeurs : satisfaction des clients, satisfaction des intermédiaires, bien être des employés, etc. toutes des choses qui ne se traduisent pas immédiatement en chiffres mais très importants pour la viabilité de la compagnie sur le long-terme) dans le risk appetite a été un grand pas vers l'avant dans la gestion des risques liés à la RSE. Avant, on était concentrés sur des aspects purement quantitatifs et des répercutions sur le P&L et maintenant on voit une certaine intégration d'aspects qualitatifs. Donc c'est un pas en avant pour le développement de la RSE.

- *Comme ça se passe la gestion du risque réputationnel ?*

Avant, on gérait l'aspect de risque réputationnel exclusivement au niveau de la première ligne. Maintenant, on est aussi très attentifs à la communication externe. On a été discuter (Ex : Quel serait l'impact négatif de communication faite sur les réseaux sociaux, etc.) avec le département de communication pour voir si la façon dont ils mesurent l'impacts de la communication n'est pas plus intéressante que les KRI's qu'on avait jusqu'ici. Et donc on a essayé de trouver une synergie à ce niveau-là.

- *Est-ce que vous pensez intéressant d'intégrer les opportunités à la fonction de RM pour avoir une vue plus globale de la situation de l'entreprise ?*

Très souvent, une même tendance aura un impact négatif ET positif. Donc elle se retrouverait des deux cotés du schéma. Actuellement, le fait que performance s'occupe des opportunités et nous que nous nous focalisions sur les risques fonctionne bien et permet de vraiment avec une vue globale et en profondeur des deux aspects quand on les présente au management.

- *Est-ce que vous effectuez des due-diligence au niveau des clients/fournisseurs ?*

De notre côté (RM), ça ne se fait pas non.

Pour les fournisseurs, il y a une équipe qui s'occupe de cela dans le département de purchase. Et le dialogue se porte plus entre eux et le service de compliance.

Pour les fournisseurs, c'est la première ligne qui effectue la due diligence.

- *Comment se passe l'identification/évaluation/reporting des opportunités pour le département performances ?*

Premièrement, du reporting classique sur les performances financières.

Deuxièmement, du reporting sur les tendances futures. Et c'est à ce niveau-là qu'il y a discussion entre performance derpartment et RM department.

L'identification des tendances se fait selon la matrice PESTL et l'assessment se passe en trois niveaux :
1)**Keep an eye on** (opportunités potentielles à garder à l'œil mais on n'investit pas encore trop de temps dedans)
2) **Analyse** (opportunités intéressantes en termes d'impacts mais pas assez d'infos pour se dire qu'on va agir dessus)
3) **Act** (opportunités à intégrer dans la stratégie)

Remarque : Dans le secteur de l'assurance, les Risk Manager sont souvent issus du business et donc de base sont très risk-driven et c'est pour ça que dans la culture du risk management dans notre secteur on est très axés sur les risques et un peu moins sur les opportunités.

Mais on travaille en grand collaboration avec le département performance et le fait qu'on soit au même étage permet vraiment d'accentuer les échanges et la coopération entre les deux départements.

Pour l'instant, on travaille bien comme ça. Si jamais ne on était amenés à fusionner les deux départements, on risquerait de perdre un peu notre indépendance de reporting et notre objectivité. Si jamais on était amenés à bosser dans des bâtiments et étages différent, là ça changerait peut-être la donne.

b. Chief compliance officer

- *Quelle est le champs d'application de la compliance et les liens avec CSR*

Tout ce qui est trait valeur interne c'est dans le champ d'application de tout ce qui est compliance mais là aussi ça touche aussi CSR parce que là il y a aussi de la discrimination.
tout ce qui est des emplois, et comment on traite les clients, et tout çà et là on est vraiment dans le nerf de compliance. Il y a un gros doublon entre les deux. CSR c'est plus de la première ligne tandis que la compliance c'est de la seconde ligne. La CSR c'est un choix de la société. je veux vraiment que le marché me voit comme étant une société qui respecte les droits de l'employeur qui respecte tout ce qui est la nature, qui respecte tous les champs d'application CSR.

Après il peut y avoir pas mal de doublons et il y a des aspects qui touchent la CSR mais qui sont compliant car ils touchent la loi. Naturellement certaines choses compliantes sont CSR aussi. Si la CSR nous dit on n'accepte pas de discrimination chez nous oui c'est bien vrai mais c'est aussi une obligation légale. Là on touche à la compliance que tout le monde soit respecté ou traité d'une même façon, c'est la compliance de base

En somme la loi c'est la loi, csr on va au-delà. La compliance c'est vraiment le minimum. Prenons le cas de proximus, la loi stipule qu'il faut une proportion 1/3, 2/3 dans le board. Ils ont stipulé que dans le futur ils seront à 50/50, là on dépasse le cadre de la loi et donc on devient CSR.

- *Nous avons vu précédemment que le risk management pense généralement en termes de risque seulement et a du mal a intégré les opportunités ? Est-ce le cas également pour la compliance ?*

Oui c'est un peu le cas ici aussi, on parle tout le temps en risque car c'est plus facilement mesurable. On ne peut pas descendre en dessous de tel indicateur. Pour la compliance ça doit toujours être mesurable mais c'est plus facile car on dit soit on se plie à la loi, soit on ne se plus pas. Tandis que dans le risk management c'est pas noir ou blanc. Il faut dire je veux avoir un taux de satisfaction d'autant, et c'est à partir de là que l'on peut faire de la gestion des risques. Il faut mesurer et comprendre où sont les problèmes. Et effectivement, on ne regarde que le problème plutôt que de regarder quelles sont les opportunités. On traite énormément de risques opérationnels à même titre que le risk management dans les conditions de sécurités dans les bâtiments, nos systèmes informatiques pour les employeurs. Nous notre travail c'est vraiment de mesurer le risque. Mais je vous avoue à l'époque, on a essayé de travailler avec des opportunités. On a commencé à essayer de mesurer les risques et de les quantifier de manière financière mais cela s'est avérer extrêmement difficile. Par exemple la sécurité au travail, avec les suicides parce que les employés sont trop stressés ou ont trop de pression. C'est évidemment quelque chose que l'on veut absolument éviter. Mais à quel moment cela devient vraiment dommageable ? Une personne, deux personnes, un directeur ?? Là on a décidé d'arrêter car on essayait de quantifier quelque chose qui n'étais pas quantifiable. On s'est aussi dit on va essayer de prendre d'autres KPI, comme le taux de satisfaction, mais à nouveau, pour pouvoir quantifier et gérer cela, il faut un minimum à ne pas atteindre, nous on mitige en fonction pour ne pas atteindre cette limite. On a eu de longue discussion avec Erik, la personne responsable du risk management pour établir nos KPI pour les risques opérationnels, cela nous a presque pris 1 an pour les définir. Mais on en est toujours arrivé à définir des seuils à ne pas dépasser pour que cela soit plus facilement quantifiable pour ainsi mesurer l'impact. Donc on en est arrivé à toujours parler de risques

- *Donc si je reprends bien ce que vous venez de dire, vous ne prenez pas en compte ce qui pourrait améliorer vos performances car vous ne savez pas quantifier et pas mettre de seuil ?*

Oui les opportunités c'est au dela d'un seuil. Nous en compliance et risk management, on se dit, on ne doit pas dépasser ce seuil. Après on peut très bien l'augmenter le seuil de tolérance en fonction des demandes du management, mais ça sera toujours un seuil à ne pas atteindre et pas quelque chose à maximiser car c'est difficilement quantifiable. Nous ici à la compliance c'est toujours le respect par rapport à la loi. Mais ces seuils bougent au fils des années, il y a 10 ans, les seuils étaient vraiment plus bas mais maintenant il y a une pression de plus en plus forte de part les régulateurs et les clients sur notamment tout ce qui est CSR. Il y a une pression sur tout ce qui est risk management. Beaucoup de personnes n'acceptent plus ce qu'il se passait il y a 10 ans, donc les seuils doivent être tout le temps réadapter mais cela reste toujours des seuils à ne pas dépasser. Prenons l'exemple des niveaux de rémunération. Il y a 10 ans cela ne posait pas problèmes. Mais maintenant cela n'est plus acceptable et on a dû mettre en place des politiques de rémunération justifiant pourquoi le CEO gagne tel salaire. Pareil pour le risk management, avant l'entreprise ne faisait que du financial risk management, mais maintenant on doit prendre en compte l'aspect opérationnel et on a donc renforcé ce qui et compliance business contiuity a cause de la pression des régulateurs.

- *Donc vous les régulateurs ont mis une pression sur la gestion des risques des entreprises et c'est pour ca que la compliance est devenue une fonction de gestion des risques ?*

Oui on peut dire ça, les régulateurs ont créé cette gestion. Il y a 3-4 ans, personnes ne s'occupaient des risques liés aux cloud, maintenant ce sont des risques opérationnels supplémentaires que nous devons gérer au jour le jour, on est là pour aider la gestion des risques mais au niveau des régulations. Mais c'est aussi une vision d'entreprise qui n'acceptent plus qu'il n'y ait aucun contrôle en place sur certains

domaines. Pour ce qui touche à la sécurité informatique, si on est sujet à une attaque et que l'on ne peut pas démontrer que des moyens de sécurités ont été mis en place, notre réputation sera touchée et comme on est les plus grand, on doit toujours faire plus que la moyenne. De part notre position, on doit toujours pourvoir expliquer au public que l'on a mis des contrôles en place pour éviter que cela se passe. Après le risque 0 n'existe pas sauf évidemment à un prix très élevé et qui n'est pas rentable. Mais on doit être capable d'expliquer que l'on a pris des mesures pour éviter que l'on nous reproche de ne pas avoir fait assez. Mais ca c'est au niveau réputation, au niveau de la conformité c'est plus simple, c'est je respecte la loi ou pas.

- *Dans le cadre de votre identification des risques, êtes-vous amené à réfléchir sur le risque de réputation ?*

Souvent. Comment je viens de dire la compliance c'est noir ou blanc. Mais le problème c'est que la loi c'est pas toujours noir ou blanc car elle n'est parfois pas exécutable telle quel car il y a des inconvénients à prendre en considération. Maintenant moi, je ne décide pas, c'est le CA et le CD qui décide et moi je donne simplement mon avis. Par exemple pour le GDPR on ne peut pas satisfaire à 100% la régulation, car il y a des choses qui sont difficilement intégrable. Donc il y a certains points que je décide de ne pas intégrer et c'est alors que je prends une autre variable comme le montant de l'amende qui peut déjà être dur, mais ça peut aller aussi jusqu'au pénal, et à la perte de notre License d'assureur. Lorsque ces variables ont été prise en compte, ce qui reste c'est le risque sur la réputation. Si un client nous accuse de n'avoir pas respecter ces droits en tant que consommateur, il y aura évidemment la FSMA qui va tout étudier, nous donner des recommandations et peut-être nous donner une sanction. Mais ce client peut mener une enquêter et nous accuser de n'avoir pas respecter ces droits. Et là c'est à nous de pouvoir démontrer que nous avons mis tel ou tel chose en place et que nous avons fait le nécessaire.

- *Dans les processus de contrôle, est-ce que vous vous concerter avec le risk management pour éviter les doublons ?*

Moi je m'occupe d'écrire les politiques à suivre au niveau de l'entreprise, aussi bien au niveau des risques géré par le risk management mais aussi de la compliance. La compliance fait partie du risk management. Tout ce qui est compliance fait partie du risk management. Il y a beaucoup de doublons sur tout ce qui est GDPR et politique de confidentialité. Il y a beaucoup de concertation entre nos deux équipes, d'une part parce que nous sommes physiquement proche l'un de l'autre et parce que nous voulons une politique en commun. De ce fait, nous relisons chacun les politiques de l'autres pour ne pas avoir de conflit entre nos politiques. Nous au niveau de la compliance on a des personnes de contact réparties dans les lignes de business. De manière mensuelles, on se réunit avec le risk management et on discute des choses que l'on a découvert. Si moi par exemple je découvre un problème pour la protection de donné et que le risque opérationnel également, on discute des genres de problèmes et on essaye de trouver une solution ensemble pour contrer ces risques.

- *Le fait que vous soyez ensemble physiquement aide à la collaboration pour les contrôle mais vous garder votre indépendance malgré que vous soyez tous les deux rattaché au chief risk officer ?*

Administrativement je rapporte au CRO, mais fonctionnellement je rapporte au conseil d'administration et au comité d'audit. Mon responsable direct est le CRO mais je garde mon indépendance. Si le risk management dit que c'est un risque à courir, moi je peux toujours dire ok mais je ne te suis pas. Naturellement ça ne doit pas arriver trop souvent car nous sommes tous des

fonctions de deuxièmes lignes et on essaye toujours d'avancer dans la même direction. Mais nous restons tous indépendants.

- Au niveau du reporting, cela signifie donc que vous ne faites pas de rapport au CRO

Non, je ne rapporter pas au CRO, c'est mon patron mais cela s'arrête là. Je dépends du comité d'audit, du conseil d'administration et du comité de direction.

- *Au niveau du reporting, comme la collaboration est grande, est-ce que le risk management intègre certains de vos KPI dans son reporting ?*

On n'est pas encore à ce niveau-là mais dans le futur c'est le but. On travaille de plus en plus en collaboration avec le risk management pour présenter un dashboard commun au CA et CD reprenant l'ensemble des risques des deux fonctions. Car nos policy sont évidemment différents. Nous on va plus s'occuper du blanchiment d'argent, la corruption, discrimination, traiter les clients de manière correcte. Notre vision du business est différente mais la finalité est la même, gérer des risques. Ainsi on essaye de créer un dashboard, où le CA et le CD pourra directement voir sur les processus en place, où se situe les risques de compliance et où se situe les autres risques. Par exemple pour le processus de sales, ils verront quelles sont les risques de compliance et quels sont les risques opérationnels.

- *Est-ce que vous considérez cela comme une bonne solution ?*

Oui, cela donne un confort au CA et CD, car ils ne sont pas là au jour le jour mais c'est eux qui assument. Ils dépendent vraiment de ce que l'on a fait, donc le fait que cela soit intégré leur permette d'avoir une meilleure vision d'ensemble de ce qu'il se passe au jour le jour dans la société. Il faut se dire qu'un rapport au conseil d'administration c'est 500 pages, et ce n'est pas visuel, ici on leur propose une solution visuelle et donc ils n'ont plus besoin de lire ce rapport. Prenons l'exemple d'un risque opérationnel, comme la distribution, ils vont voir dans le rapport que c'est rouge mais sans avoir la raison. Mais la raison est peut-être simple car c'est un changement de régulation. Avoir le dashboard financier, opérationnel et compliance cela rends la chose difficile. Avec une solution visuelle, ils vont directement avoir la réponse.

- *Quelle sont les plus gros risques auxquels vous devez faire face ?*

Le blanchiment d'argent car les régulateurs nous mettent énormément de pression et cela touche l'ensemble de la société. La protection du consommateur car cela devient de plus en plus important. Distribution, comment on s'organise avec les courtiers et la banque, faire attention aux conflits d'intérêt avec les commissions.

Ensuite nous avons les manipulations de marché. C'est très difficile à traiter car ce sont des informations cachées. Nous pouvons simplement aller au CA et CD et stipulez qu'il faut faire attention lorsque vous parler à vos concurrents pour ne pas se mettre d'accords sur certains points. Et c'est un cas très important car les pénalités sont très élevées.

- *Quelles sont les canaux de communication utilisé ?*

Pour la compliance, on communique par les politiques mise en place sur notre site intranet ainsi qu'une brève explication sur ce que cela comporte. Pour les nouveaux entrants, ils doivent suivre une formation

au niveau du risque opérationnel, du business continuity, de la protection des données et il y a également un volet compliance. Je fais aussi personnellement le tour des différents business et j'explique ce que j'attends d'eux. Car nous mettons en place les politiques mais après c'est à eux de faire des contrôles pour que cela soit respecter. Ensuite chaque mois, je me rends au comité de direction et j'explique ce que j'ai constaté et aussi pour donner mon avis. Nous avons accès à chaque étage de la société pour donner notre avis.

De plus, nous avons des personnes de contacts dans les business lines qui vont s'occuper de veiller à la bonne mise en place de nos politiques. Ce qui nous permet d'être présent à chaque échelon de l'entreprise.

- *Qu'en est-il des relations que vous avez avec les parties prenantes externes, par exemple, vos fournisseurs ou vos clients. Est-ce que vous communiqué avec eux ?*

Client facile, on a peu de clients car généralement cela se fait par des courtiers et des banquiers. Nous on donne des instructions à la banque et eux nous donne des échantillons que nous pouvons vérifier si eux ils ont bien respecté les règles que nous avons imposée. La différence entre un agent lié et un courtier, pour tout ce qui est protection du consommateur, un courtier est responsable pour les obligations des protections du consommateur, un agent lié c'est l'assureur qui est responsable pour la mise en place de ça. La banque on doit vraiment vérifier si eux ils ont respecté tout cela. Alors ça c'est facile pour tout ce qui costumer, fournisseur ça c'est un peu plus difficile, on a des contrats en place où on dit normalement ce fournisseur ce qu'il devrait respecter. Mais cela reste difficile il faut essayer de dire : « ok ibm je vais venir faire un audit chez vous pour voir si vous respecté bien gdpr ». Dans la pratique c'est plus compliqué, on passe de plus en plus vers une sorte de certification que nous on dit ok fournisseur pour autant que vous êtes iso certifed et que vous montrez chaque année votre certification c'est bon pour nous. Le rapport d'un big four aussi car nous n'avons ni les moyens financiers ni les compétences de faire un audit complet.

Effectivement, le processus est tel on dit ok, on exige qu'eux soit certifié, s'ils ne le sont pas, ça se peut que le fournisseur soit un bon fournisseur, que c'est un fournisseur avec lequel on veut vraiment travailler, mais le prix pour être compliance certifed est très élevé. Ça se peut que le fournisseur dit ok pour moi c'est trop cher, je ne le fais pas, c'est son choix. A ce moment-là, c'est risque management, sont les gens de YT qui font l'analyse si les contrôles en place sont comparables aux exigences de iso certification

- *Comment qualifiez-vous votre risk appetit concernant l'aspect de la compliance ?*

Il est très bas, un seul avertissement nous suffit à nous conformer car on veut avoir une image irréprochable auprès des clients. Une lettre du président de la nbb ou de fsma c'est bon. Et là tous les clignotant vous s'allumer ici parce que l'on ne veut pas avoir des ennuis et là je suis d'accord, notre niveau risque appetite compliance on ne veut pas avoir des ennuis. Ça ne veut pas dire que de temps en temps on peut avoir des lettres de la nbb qui dit on constate que vous n'êtes pas allez aussi loin qu'on s'attendait, par exemple de temps en temps on voit des bêtises ici que des conditions générales sont pas bien adaptés. Tu peux pas tout vérifier, ça se peut aussi pour un produit qui n'est quasiment pas vendu, mince qu'est ce qui s'est passé ici, ils ont carrément oublié, mais là c'est le risque appétit, les efforts tu les faits sur les plus gros processus et de temps en temps, tu nettoies au fur et à mesure les autres, mais là je sais vivre avec ça. A ce niveau le risque appétit, chez nous au niveau compliance c'est facile. Le

risque appetite je vais utiliser un mot technique « we will not be reliable not compliance with legislation »

- *Donc cela veut dire que vous ne faites aucune analyse de risque pour savoir si vous allez gérer ce risque de cette facon ou pas ?*

Non non pas du tout, Etre à 100% compliant envers une loi est impossible, financièrement c'est juste inconcevable. On analyse la loi est ensuite on décide ce que l'on va faire en fonction de nos capacités et de l'importance que l'on accorde à ce risque. Prenons un exemple comme le blanchiment d'argent, la loi stipule que tu ne peux pas faire accepter un client avant d'avoir faire une analyse sur lui. Il faut vérifier que la personne n'est pas impliquée dans tout ce qui est blanchiment d'argent international financy. Ça veut dire qu'il faut faire l'analyse avant que le client vienne chez toi, ça veut dire qu'auprès d'une agence que lui il souscrit son contrat, le contrat arrive chez nous et nous on dit « tuut » il est à l'agence hein, et la personne encode les données, ça entre chez nous et nous on dit « tuut » vérifions d'abord, ça donne une alerte et là la personne dans l'agence on doit lui dire, monsieur il y a un petit souci, veuillez revenir demain. Pourquoi. Parce qu'il y a petit souci d'un mail, ils sont en train d'étudier cela. Ce n'est pas possible ça, sinon tu perds ton client. Alors ce qu'on fait, la loi dit littéralement il faut avoir fait ton analyse avant. Ok on fera l'analyse dans la semaine, si nous on a toujours unilatéralement on peut mettre fin. Il y a déjà un contrat et nous on peut mettre terme à un contrat dans un délai d'un mois.

il n'est pas possible d'être compliant à 100% mais avec cet exemple-là. Je peux défendre cela auprès des autorités de contrôle, et ça passe.

c. Responsable communication

On vient de se rendre compte en interne de l'importance de la RSE. Donc on est vraiment à un stade embryonnaire du développement de la RSE.

Ce qui nous pousse à développer la RSE c'est assurer une bonne image de l'entreprise à l'extérieur. Il y avait un fossé entre les attentes RSE qui viennent des parties prenantes externes et la communication externe qu'on en fait.

On dépense déjà 500.000€ pour notre campagne de solidarité.

Ca a donc fait l'objet de discussion auprès du comité de direction donc c'est déjà une première victoire d'avoir abordé ce sujet avec eux. Le premier débat était de savoir comment est-ce qu'on définit la RSE. Puis mesurer nos performances dans les différents domaines qui composent la RSE.

Premièrement, on effectue un benchmark de nos concurrents qui est en cours pour le moment.

Deuxièmement, comme il n'y a pas de gestion centralisée, on fait une sorte de synthèse de toutes les actions RSE qui étaient réparties de façon décentralisées dans l'entreprise. Que faisons-nous au niveau RH, au niveau produit, investissement, etc. Donc dans les interviews qu'on a avec les responsables de départements, on se rend compte qu'on ne communique pas assez avec les parties prenantes et plus particulièrement avec les pp externes. Du coup, on est mal cotés dans les rakings RSE du secteur puisqu'on ne communique pas assez. Et comme il y a de plus en plus d'entreprises clientes qui tiennent compte de ces aspects RSE, le board n'est pas insensible.

On se rend compte que le board est convaincu de l'importance de la RSE et qu'on fait quand-même pas mal de choses mais ça va un peu dans tous les sens. Par exemple : On a une bonne diversité dans l'entreprise (genre, nationalité, origines, etc.), une gestion des déchets et de l'énergie, réduction de papier. Pour les voitures de société c'est encore sensible mais ça va dans le bon sens. On a installé des douches pour pousser les gens à venir en vélo au travail. Sinon, on a des salles de fitness ou des mini-shop inter-entreprise pour que les employés puissent faire leurs courses directement.

Par contre, il n'y a pas encore la conviction qu'il faut centraliser tout ça, qu'il faut établir des KPI's et des directives.

Pour le moment, ce sont des initiatives individuelles prises par les entités et acceptées par le comité de direction mais c'est plus dans l'optique. « Ok, c'est vous qui voyez par rapport à votre budget ». Il n'y a pas de budget global pour l'entreprise attribué au développement de la RSE.

- *Pourquoi la RSE ?*

L'entreprise se rend bien compte que l'impact de l'image RSE de l'employer est primordial.
Pour attirer et garder les nouveaux talents, on doit faire des progrès en RSE parce que c'est un sujet de préoccupation pour beaucoup de gens et encore plus pour la nouvelle génération.

Business-driven : A côté de cela, nous avons un partenariat avec BNP Paris-Bas Fortis pour les produits d'investissements qui nous poussent à avoir une approche RSE et à intégrer de plus en plus la RSE dans nos pratiques (diversité, environnement). Autrement, il n'y a plus de partenariat.

- *Est-ce que vous ne pensez pas que ça a plus de sens de faire des progrès sociaux plutôt qu'environnementaux pour une firme de services ?*

Tout à fait. Le défi sera de faire le plus possible le lien avec les activités opérationnelles. On va se focaliser sur la prévention puisque que c'est en lien avec la nature de nos activités qui sont les assurances. Nous avons un comité de sponsoring. On va mettre l'accent sur des thèmes comme la santé, le sport, la prévention, etc. Ce qui est axé sur la culture par exemple, on va directement exclure parce que cela ne correspond pas à nos activités.
Faire des actions environnementales, c'est envisageable mais si ça n'a pas de lien avec les activités de l'entreprise, c'est moins intéressant.

D'ailleurs, dans le passé, nos activités de sponsoring (supporter des clubs de foot par exemple) n'avaient pas des masses de liens avec notre core business. C'est la raison pour laquelle maintenant on se focalise plus sur l'athlétisme parce que c'est un sport que tout le monde peut pratiquer et qui est très accessible. On va s'associer dans le futur dans des activités de promenades.

Là on est vraiment dans la phase d'identifications des opportunités RSE.

- *Quel est le processus derrière l'identification/évaluation de ces opportunités ?*

Nous recevons beaucoup de demande de sponsoring aussi. Il s'agit de sélectionner la bonne.
Dans le comité de sponsoring, il y a des représentants opérationnels.

D'une part, il y a des enquêtes « marché » standardisées du secteur réalisées par les courtiers qui sont disponible donc ce n'est pas seulement notre initiative. Et ça nous permet de voir comment on est positionnés parmi marché.

D'autre part, pour ce qui est satisfaction clients, nous faisons des enquêtes de satisfaction. On travaille avec des entreprises externes spécialisées pour mesurer efficacement cette satisfaction.

- *Comment est-ce que vous évaluer les impacts et les répercussions de ces activités de sponsoring ?*

On va regarder que l'activité de sponsoring match bien avec nos activités de sponsoring. On va aussi regarder si la visibilité de ce sponsoring est intéressante. Et répertorier ces activités de sponsoring selon la matrice probabilités/Impacts sur les parties prenantes.

Le comité de sponsoring va aussi avoir un regard sur les risques liés aux choix de sponsoring. Par exemple, on va éviter de se lancer dans du sponsoring d'équipes de cyclisme pour éviter qu'un éventuel scandale de dopage ait des répercutions sur nous.

- *Dans la mesure où il y avait un département RSE dans l'entreprise, serait-il considéré comme deuxième ligne de défense ?*

Oui je pense bien. Parce que jusqu'ici le comité de direction et le board n'ont pas encore exprimé l'idée d'avoir une centralisation et une politique bien structurée « top-down » pour la RSE. Donc ce serait plus 2ème que première ligne.

- *Est-ce que vous pensez qu'avoir une personne en charge de faire du reporting RSE auprès du board et du comité de direction pourrait être efficace pour conscientiser le board à la RSE ?*

Oui, forcément.

- Q*uelle est la next-step pour une meilleure gestion des opportunités liées à la RSE ?*

L'étape suivante doit être de responsabiliser certaines entités de l'organisation à la RSE et à déterminer où sont les points d'attention et quel est le contenu de cette fonction.

Est-ce que cette fonction doit faire partie de la stratégie ou plutôt avoir un rôle de coordination et de stimulation de réflexion RSE pour les différentes entités ? On doit encore décider. On doit se mettre d'accord de quelle entité sera responsable de la RSE, on doit déterminer quelle forme prendra la RSE. On n'en est pas encore là.

Première chose à faire c'est certainement plus communiquer vers l'extérieur.

- *Est-ce que vous gérez le risque réputationnel ?*

C'est nous qui analysons les impacts potentiels de la communication externe sur le risque réputationnel et on le communique au RM via une personne de contact du RM qui travaille avec nous.

3. ***Delta Assurance***

a. *Chief risk officer*

- *Est-ce que vous vous situez dans le COSO 1 ou 2 ?*

On a un dispositif de gestion des risques propres du domaine enterprise risk management. On a un exercice annuel d'évaluation des risques principaux chez nous. C'est une obligation réglementaire pour les compagnies d'assurance de réaliser une évaluation propre des risques. Dans le cadre de solvabilité 2 ; (explication de solvabilité deux : est une révolution dans le monde de l'assurance en termes de gestion des risques au sens large, cela impose beaucoup de contraintes aux compagnies, à la fois en terme de calcul, calculer qu'une compagnie est solvable ou pas mais aussi en terme d'organisation, en terme de gestion des risques

- *Solva 2 est un peu comparable à Basel pour les banques ?*

Solvabilité est beaucoup plus exigent pour les compagnies d'assurance que ne l'est le régime bal actuel pour les banques, en termes de suivi de l'ensemble des risques. Dans le cadre de solvabilité 2, il est demandé aux compagnies d'assurance de réaliser une évaluation de leurs risques principaux au moins une fois par an et un rapport qui est produit approuvé par le CA et la BNB. Dans le cadre de ce rapport, avant de pouvoir réaliser cette évaluation des risques, l'entreprise doit réfléchir qu'elles sont les systèmes qu'elle met en place pour identifier les risques, les faire remonter, les analyser. On n'a des documents internes qui décrivent de manière très précise pour chacun des types de risque et les responsabilités, qui fait quoi, quel reporting, quelles contraintes on a. Les gens ne peuvent pas faire n'importe quoi, il y a un cadre qui est bien fixé, avec parfois des dérogations, Donc on détermine le cadre, la manière dont les gens doivent travailler, faire du reporting, analyser le risque. Dans ce cadre-là, il leur est demandé sur un canevas qui est bien précis de faire une auto-évaluation de leur risque et nous en tant que deuxième ligne on challenge en fait leur conclusion pour arriver à un consensus d'évaluation des risques par domaine d'activité

- *Le reporting de la première ligne a lieu tous les combien de temps ?*

reporting qui sont chiffrés : sont produits, la rentabilité de l'entreprise, sont niveau de solvabilité, il y a beaucoup d'indicateurs qui sont suivis, aussi le niveau de sinistralité, les fameux ratio s/p

Mais plus sur des aspects qualitatifs c'est a dire où on n'en est par rapport à la réalisation des plans d'action qui sont là pour mitiger les risques ou pour les réduire. Par exemple, on a fait une évaluation des risques il y a un an, on a vu avec certains départements que je vais dire un exemple le risk ciber donc d'avoir des attaques via le net a augmenté périodiquement tous les 3 mois il nous faut un état des lieux de l'avancé des plans d'action. Un an plus tard., est-ce que ciber est un risque toujours aussi important en terme d'impact et de probabilité que l'année passée, on devrait s'attendre à ce que l'impact du risque ou la probabilité de survenance diminue, c'est vraiment il faut se dire on fait un petit tableau impact/probabilité.

L'évaluation des risques en deux temps c'est à dire on fait ce qu'on est occupé de faire pour l'instant c'est un top risk assesment. On analyse des rapports qui sont fait par des experts en risque management

etc. on leur donne des tas d'informations pour se préparer à un workshop, une réunion avec eux où on passe en revue les évaluations de l'année passée et en discute.

- *Avez-vous des correspondants comme la compliance pour faire ce genre de rapport de gestion ?*

Oui on a des correspondants qui sont chargés au sein d'un département d'agréger cette vision au sein du département et d'aider le directeur à faire sa proposition. On a des correspondants risque opérationnel qui font ça et qui participe aussi d'ailleurs aux réunions. On appelle cela top risk On sort du workshop avec notre petit graphique en disant, ben voilà ça c'est les risques pour cette direction là, ce sont les risques qu'on a identifiés. Et bien entendu on va s'intéresser très très fort aux risques si on a une matrice.

- *En tant que risk management, vous vous occupez de tous les risques, hormis ceux de compliance ?*

Pour les risques de compliance on se fait aidé alors par compliance. Nous le risque, on a la mission de dresser la photo globale mais bien entendu que quand on touche au domaine qui sont de nos collègues, fonction de contrôle de deuxième ligne, c'est d'abord eux qui nous fournisse l'input pour qu'on ait la photo totale

- *Comme vous avez en charge d'avoir la vue globale, vous prenez en charge la totalité des risques dans votre reporting ?*

En fait l'exercice dont je vous parle ici, c'est pour arriver à produire ce rapport, qui est un rapport du comité de direction. Parce qu'il faut bien savoir que nous on aide à mettre ce rapport en place, donc c'est un rapport du comité de direction dans lequel nous avons des chapitres, dans lesquelles on libre de s'exprimer et de faire tous les commentaires indépendants qu'on veut et c'est un rapport de l'entreprise, du comité de direction qui est ensuite soumis à la banque nationale et au conseil d'administration. Le but du rapport c'est justement d'avoir une vue globale et exhaustive de tous les risques. Alors bien entendu quand il y a des plans d'actions qui doivent être déployés qui concerne la compliance, c'est bien entendu la compliance qui veille au suivi et à la mise en œuvre des plans d'action de compliance par les départements

- *Si vous pouviez reprendre 3 des risques les plus importants en ce moment ?*

La capacité de l'entreprise à se transformer pour passer à un monde qui est plus digital aujourd'hui et surtout par rapport aux nouveaux clients, les nouvelles générations. Mais c'est un risque un peu global car on retrouve des risques liés à la gestion de projets. On doit être capable de gérer de grands projets. Ce n'est pas donné à tout le monde de gérer des projets d'une telle ampleur. C'est la capacité d'intégrer dans la maison une culture de changement. Ça veut dire qu'un gestionnaire, on va lui demander de ne plus travailler comme il travaillait avant, mais de travailler autrement, avec des nouveaux outils.
Les risques professionnels que cela engendre, le fait de changer d'applicatif, les erreurs humaines et aussi on passe à un monde qui est différent, il faut aussi des personnes, des talents, des gens qui soient capable de maîtriser ses nouvelles compétences.

- *Est-ce que des collaborations existent entre les départements de compliance, est ce que vous avez vraiment un travail de commun accord pour justement identifier ses risques pour pouvoir aller de l'avant ou bien s'est vraiment chacun va s'occuper de ses risques*

On se concerte très régulièrement, on a des réunions de concertation entre l'audit interne, compliance et risque pour justement beaucoup se parler. D'ailleurs on s'échange beaucoup d'information ce qui nous permet d'être meilleur dans notre travail. On fait ses réunions formellement tous les 3 mois, mais nos collaborateurs se voient plus fréquemment, mais une fois qu'on a fait notre évaluation des risques globaux sur lesquelles tout le monde est d'accord après chacun prend sa partie et veille à ce que sa partie soit bien suivi dans le business avec ses propres correspondants, avec ses propres processus, mais on est cohérent avec l'évaluation globale que l'on a faite. Donc dans l'évaluation globale, par exemple la mise en place de la réglementation gdpr, qui est un risque important en termes de règlementation, mais aussi réputation etc. Il va faire partie du rapport final de la totalité des risques important, après bien entendu c'est compliance qui va suivre ce risque là avec ses correspondants et veiller à ce que ce soit bien mis en ordre et soi bien suivi et moi je vais m'occuperais des risques qui sont dans mon domaine et la fonction actuarielle dans son domaine et on continue à se parler en cours de route, chacun on travaille de manière cohérente. Chacun reprend ses risques sur lesquelles.

- *Vous restez plus indépendant sur vos risques, après il a des communications qui existent, mais c'est plus une aide que vous apportez à l'autre, ce n'est pas vraiment une synergie totale qui existe*

Il faut bien se rendre compte qu'il faut une expertise bien précise pour être compliance qui est différente de l'expertise qu'il faut pour être risque manager, etc. chacun à sa force en termes d'expertise, donc moi je ne peux pas demain dire je remplace compliance. Chacun dans son rayon, mais en concertation.

- *Prenons l'exemple de gdpr, est-ce qu'à un certain moment vous vous mettez autour d'une table et vous dites tiens est-ce qu'on ait pas un doublon quelque part, est-ce qu'on peut ensemble penser à une méthode efficace de contrôle pour contrer un risque ?*

Par exemple dans ce cas-là c'est d'abord compliance qui est en lead, c'est d'abord compliance qui sait ce qu'il faut mettre en place. Et puis à un certain moment nous on fera notre propre évaluation de ce point-là comme on fait l'ensemble des évaluations mais voilà on pourra faire éventuellement un commentaire en disant nous on pense que ceci devrait être renforcé ou pas à postiori mais on ne va pas empiéter sur les plates-bandes de compliance qui est d'abord la personne l'experte en termes de ligne 2 à ce qu'il faut mettre en place. On aura plus un rôle d'avis sur ce que fait la compliance.

- *Mais avez-vous des processus en commun ? 2 processus de contrôle qui se rejoindraient un petit peu et qui infine serait un petit lourd sur les collaborateurs*

On ne mettra jamais 2 processus de contrôle différent. Il n'y en aura qu'un et peut-être qui en aura dans lequel on demandera de rajouter tel et tel élément, mais il n'y aura jamais 2 processus de contrôle.

- *Pouvez-vous nous donné un exemple de rajout à un processus de contrôle ?*

Pour l'instant ce qu'on fait c'est que pour gdpr, il y a projet, il est en train d'être déployé et on le laisse se développé. Après ce processus-là rentrera dans l'évaluation comme un autre processus, et on fera l'évaluation dans les évaluations qu'on a avec nos correspondants qui sont d'autres correspondants, on fera le point avec eux sur les risques, on fera notre propre avis indépendant mais plus pour gdpr que sur d'autres éléments sauf si bien entendu nous remonte le fait que il y a des risques important par rapport

à gdpr, alors on le mettra dans nos risques important, dans notre map et on le suivra de plus près, mais toujours en collaboration avec compliance

Depuis longtemps on a mis en place une concertation entre les fonctions de contrôle pour rester cohérent, aussi parce que ce qu'on veut justement éviter c'est que 2 fonctions de contrôle débarquent auprès d'un même département pour regarder les mêmes problématiques, pour ne pas se concerte. Ce ne serait pas très intelligent que cette semaine ci compliance débarque, enfin demande pour poser un certain nombre de question sur le risque et nous la semaine d'après sur la même problématique, soyons plutôt complémentaires, tout en gardant notre indépendance, ça c'est important.

- *Est-ce que l'on pourrait émettre avis justement sur les risques rse et les opportunités ? Par exemple si vous avez une matrice d'identification et d'évaluation de risques, est-ce que vous allez avoir une matrice similaire pour l'identification et l'évaluation de potentiel opportunité ?*

Nous pouvons, je vais prendre un exemple concret, le volet opportunité c'est aussi un volet qui est dans notre radar et comment est-ce que l'on peut le percevoir ? Un exemple très simple, dans les règles qui ont été mises en place en interne, si a un certain moment on considère qu'on a une richesse trop importante par rapport au risque qu'on court, on a identifié cela comme étant quelque chose qui doit nécessiter une réflexion, une décision. Ça veut dire que peut-être que soit on ne prend pas assez de risque par rapport aux activités qu'on a, ou soit que on aurait des opportunités de déployer de nouvelles activités et ça sa fait partie aussi du radar

- *Est-ce que ça voudrait dire, parce que quand vous parlez de prendre plus de risque, du coup on parle aussi de changer le risk appetite de l'entreprise ?*

Dans ce cadre d'appétence au risque on s'est fixé des limites en termes de ration de solvabilité. Par exemple la cible vers laquelle on veut tendre, mais on a une limite inférieure et supérieure càd que si on dépasse un certain niveau ça veut dire qu'on n'utilise pas de manière optimale, donc dans le cadre d'appétence au risque qu'on vient de finaliser maintenant.

- *Quelle est la raison qui ne vous poussent pas à inclure des aspects RSE à votre analyse des risques ?*

Le fait par exemple que les employés se sentent mieux, etc. et que ça va se retrouver dans le compte des résultats, on n'est plus dans un concept de Balanced scorecard, identifiant tous les éléments qui fait qu'on a bon compte de résultat. → ca n'influence pas le bilan.

Je ferais une distinction entre ça et le point que vous soulevez par rapport à la responsabilité sociétale, si j'essaye de trouver le lien avec mon évaluation annuelle des risques. Le risque de réputation est un risque important qui est relevé et qui est très important et qui a fait aussi l'objet de discussion dans le cadre de la révision du cadre d'appétence au risque. C'est quelque chose d'extrêmement sensible pour nous le risque de réputation, parce que comme nous mettons en avant nos principes et nos valeurs de solidarité, sociale, etc. Un exemple concret, ce serait certainement beaucoup plus dommageable par rapport au rôle sociétal que nous mettons en avant que l'on se rende compte que tout d'un coup dans la presse que nous avons des pertes importantes, parce qu'il a investi dans une entreprise d'armement ou que nous avons investi dans des produits dérivés hautement spéculatif, on ne s'attendrait pas à ça de nous et donc cela serait encore plus dommageable.

- *Comme votre entreprise est active de manière sociétale, pourquoi n'incluez-vous pas le management de cette opportunité pour booster votre réputation ?*

Pour répondre de manière terre à terre, aujourd'hui on ne le fait pas de manière direct et consciente par rapport à ça, on le fait de manière indirecte. Par exemple quand on voit qu'on un risque de réputation important, on discute avec les départements des plans d'action qui vous être mis en place pour faire en sorte qu'on limite ce risque de réputation et bien entendu par rapport à l'ensemble des activités qui sont mises en place. Il y a effectivement le fait de veillez à ce que nos investissements financiers soient, répondre à des critères d'économie sociale, de veiller à ce que dans les produits qu'on vend il y a bien ses éléments là. Donc c'est de manière indirecte, ce n'est pas le risque management qui le pousse, le risque management fait en sorte qu'il y ai une évaluation qui soi sur la table dans lequel, risque de réputation soit discuté. Donc ce n'est pas de manière directe, nous qui disons on devrait par ça pour améliorer notre image, etc.

- *En somme vous vous focalisez sur l'impact négatif que peut avoir ces investissements, mais vous ne prenez pas en compte l'impact que cela peut avoir sur les parties prenantes qui sont positif. (explication matrice de la matérialité) Donc vos méthodes sont plus ou moins similaires et on se rend compte que dans très peu d'entreprise voir pour l'instant aucune, on se rend compte que le risque management n'intègre pas cette vision dans son analyse de risque. Et on essaye de comprendre pourquoi est-ce qu'ils ne veulent pas intégrer le fait d'avoir un impact positif au lieu de prendre un impact négatif ?*

En théorie on a aussi cette vision d'impact, mais c'est vrai qu'on se focalise sur éviter des impacts négatifs

- *Est-ce que vous pensez que cette vision pourrait évoluer dans le temps et essayer de prendre en compte tous ses impacts qui soient positifs aussi ? Mettre en place vraiment des processus pour vraiment essayer de capter au maximum ses opportunités et essayer de les maximiser, au même titre que des processus de contrôle pour éviter le risque, les processus de contrôle pour capter les opportunités*

Je pense que c'est plus compliqué d'établir une liste des opportunités que d'établir une liste des choses qui pourraient avoir un impact négatif pour l'entreprise. (déformation professionnelle.

Résumé, tout est tourné en termes de risque, un investissement durable pas une opportunité mais un risque de ne pas le faire car pas en accord avec nos valeurs.

- *Quelle sont les investissements durables que l'entreprise entreprends ?*

Elle fait fort attention à son rôle sociétal, aider les gens qui ont des problèmes, donc par rapport aux produits qu'elle vend, elle décide de rester sur certains produits qui ne sont peut-être pas les plus rentables mais parce qu'elle considère que d'un point de vue social c'est important que nous donnions une aide à un public cible avec un public particulier, ça nous on le fait. Mais c'est une préoccupation de notre rôle sociétal

Ne va pas investir dans des produits dérivés spéculatifs

- *Comment la politique de gestion du risque de réputation a-t'elle été mise en place ?*

On met les parties autour de la table qui sont concernés pour qu'on fixe un cadre cohérent. C'est à travers le fait qu'on met les personnes autour de la table pour fixer ce cadre qu'on réparties bien les responsabilités et que on sait bien qui est responsable de quoi. Je pense que c'est surtout un aspect de gouvernance et de bonne organisation, il faut que qqu'un retrousse ses manches, mettre les parties autour de la table pour définir ce cadre ou produit un document qui est validé par l'ensemble des parties

concernées et une fois que ce cadre existe ça aide. Une fois qu'on a fixé ce cadre, on peut se dire, gestion de la communication de crise. Il faut qu'il y ai une gouvernance, il faut que l'entreprise définisse clairement sa gouvernance et la communique en interne, il faut que tout le monde dans l'entreprise sache quel processus appliqué.

On a analysé tous les risques sous adjacent de réputation avec des discussions avec la compliance qu'on identifie les différents domaines des sous-risques liés au risque de réputation, qu'on les identifie

PS : une difficulté que le risk manager a relevé c'est que le monde est en perpétuelle mouvement à même titre que les exigences et donc la difficulté c'est d'adapter constamment tous les processus, les communiquer à tout le monde de manière efficace, identifier les bonnes personnes qui est un exercice très laborieux et qui change chaque année.

Le gros challenge ici, c'est de bien coordonner tout le monde et que chacun sache ce qu'il doit faire.

- *Pourquoi dans le volet des opportunités, vous n'essayez pas de maximiser le bien être des employés par exemple au lieu d'avoir une limite à ne pas atteindre ?*

Parce que c'est plus simple à gérer, mais de manière implicite nous avons une sorte de maximisation du bien être car les objectifs sont très haut. Maintenant il faut comprendre le scope du risk management qui est d'allouer les ressources de manière efficaces. Si nous n'avons pas de seuil à atteindre, nous ne savons pas quand nous allouons trop de ressources quelque part et il faudrait peut-être les rediriger vers un autre risque qui lui est en manque d'allocation des ressources ?

- *Selon vous, qu'est ce qui bloque cette ouverture d'esprit sur le volet opportunité et pas risque.*

Je pense que ça il faudrait influencer aussi dans le cadre dans lequel les compagnies d'assurance travaillent. Je suis allez à un meeting compliance organisé par une association où il n'y avait pas que des assurés, pas que des banquiers et on parlait de compliance et de risque management. On se rend compte quand on parle avec ces gens-là que la réglementation pour les banques et les assurances, la règlementation en terme de risque management et toutes les contraintes, c'est quand même à des années lumières de ce qui se trouve sur la table des compagnies industrielles normales et donc il y a un poids de contrainte qui nous est imposé par la règlementation et qui peut expliquer aussi qu'on est plus dans regarder le côté éviter les impacts négatifs, il faut savoir que si nous on a des impacts négatifs, moi j'ai des réunions avec la banque national tous les 3 mois, et on a des inspections aussi de la banque national, vous n'imaginez pas le nombre d'inspection. Il faut savoir que le poids de la règlementation nous pousse fortement à regarder d'abord en priorité les impacts négatifs

Il y a aussi une contrainte qui empêche les compagnies de faire ce qu'elles veulent à cause des régulateurs : EX avec les politiques d'investissement en actions qui est fortement contrôlé par SOLVA II (si je veux investir 100,00eur en action, je dois avoir 45-50,00eur de capital à côté de mon investissement de 100,00eur)

il y a un rôle bien défini qui est alloué aux risques et à la compliance mais la règlementation n'impose pas d'avoir un responsable rse et peut-être qu'il y a d'autres règlementation dans d'autres domaines, dans d'autres secteurs qui donnent un rôle à ce rse ?. Mais c'est bien la preuve que même au niveau des autorités de contrôles, ce rôle n'est pas n'est pas prioritaire pour la bonne gouvernance d'une entreprise financière

Maintenant, je dis que nous sommes très régulées mais il ne faut pas voir que le côté négatif, La mise en place de la réglementation solva 2 a fait faire un bond en avant énorme a beaucoup de compagnie en gestion des risques. Moi je peux vous le dire car j'ai coordonnée la mise en place de solva 2 ici en

interne, ça nous a fait faire des bonds en avant en gestion des risques assez important qu'on aura peut-être pas faits s'il n'y avait pas eu la réglementation. Ca fait pas mal d'années que sous l'impulsion de ces règlementations, etc. toutes les compagnies ont vu leur gestion des risques s'améliorer, c'est indéniable

b. Chief compliance officer

- *Quelle est la différence entre la Compliance et la RSE?*

La RSE est très récente. Dans les domaines de la compliance, il faut vérifier que la compagnie exécute sa mission de façon intègre. C'est de cette façon que notre mission rejoint un peu celle de la RSE. Dans notre département, nous vérifions que notre compagnie applique les règles et les lois pour éviter des risques de réputations et risques financier. Notre intégration se fait donc dans la partie intégrité/éthique. Nous sommes d'une certaine façon les gardiens de la politique d'éthique qui a été validé par le comité de direction, ainsi que de la faire vivre. Par exemple les nouveaux collaborateurs ont des séances d'information et une fois tous les 2/3, nous transmettons des slideshow aux team leader pour qu'ils puissent remettre à jour les questions d'éthiques auprès des employés.

- *Existe-t'il une relation entre vous et la personne en charge de la RSE ?*

Non, il n'y a pas de relation entre moi et la personne en charge de la RSE car il n'y a pas de personne réellement en charge de tous ce qui est RSE. Selon moi la RSE, c'est plutôt des missions dans plusieurs département, et surtout en HR, et encore plus un état d'esprit qui doit être dans la culture. On peut comparer ca à la compliance. Mon rôle est fait pour que l'entreprise soit respectueuse des lois mais il est aussi d'inculquer cette culture à tous les collaborateurs pour qu'il y ait une conscientisation car la compliance comme la RSE est dans le rôle de chacun.

- *Quelle est votre part de travail entre le fait d'instaurer une éthique de la compliance et de faire attention à ce que l'entreprise soit respectueuse des lois ?*

Les deux vont de paires. Il est évident que l'entreprise doit être respectueuse des lois mais aussi faire vivre l'intégrité au sein de l'entreprise. Pour moi la culture de la compliance, c'est faire vivre le respect des règles et des lois mais il faut que cela soit naturel pour nos collaborateurs.

- *Comment faites-vous pour implémenter cette éthique ?*

Nous avons au sein du groupe une forme décentralisée de la compliance. Nous sommes 3 compliance officer, et nous avons dans chaque direction des correspondants compliance qui sont vraiment nos relais. (Vie, non-vie, claims, finance, …) Nous les réunissons 2-3 fois par an, parfois plus en fonction des dossiers comme le GDPR, et nous avons bon soutient également de la direction. Pour implémenter cette éthique, je considère qu'il faut prendre la loi assez tôt, et directement appliqué des processus en fonction en expliquant bien pourquoi le processus n'est pas bon.
Prenons l'exemple des ventes téléphonique, si j'arrive à la fin du processus et que je me rends compte qu'il y a telle ou telle chose à changer en fonction de la loi cela coûte du temps et de l'argent. Par contre si on s'y était pris dès le début et parfois même de manière proactive en sensibilisant les personnes de contacts a ces risques, cela permet de réduire les coûts en temps et en argent. Évidemment cette vision des choses ne peut fonctionner qu'avec un soutient du comité de directions ainsi qu'avec les personnes de contacts et les managers.

- *Quelles sont vos contacts avec les personnes du risk management malgré le fait que la FSMA a stipulé que la Compliance doit demeurer indépendante ?*

Nous dépendons du CRO et cela est admis par la BNB. Notre CRO est membre du comité de direction et il est le responsable de toutes les fonctions de la seconde ligne de défense avec le risk management ainsi que la fonction actuarielle et nous sommes totalement indépendant du business.

- *A qui s'adresse donc votre reporting ?*

Nous sommes invité permanant auprès du comité d'audit et des risques. Les 3 composantes de la seconde ligne de défense sont invités permanant. Nous assistons à tous les comité des risques car ils se font en même temps que celui du risk management et de l'actuariel. Nous avons cette réunion 1 fois par an et aussi de façon semestrielle auprès du comité de direction qui est validé par le comité des risques. Nous avons bien des rapports différents mais qui nous présentons notre rapport au même moment que les autres fonctions de la seconde ligne.

Nous reportons aussi auprès de l'ICC (internal control committee) au minimum 3 fois par an permettant de discuter de manière conjointe avec le risk management sur des sujets que nous allons/avons aborder.

- *Existe-t'il une certaine collaboration dans le contrôle des risques avec le risque management ou travaillez-vous totalement de manière indépendante.*

Nous travaillons de manière indépendante mais nous nous concertons. Nous devons restons indépendant selon Solva 2 car nos domaines sont différents. Moi je vais plus m'occuper de ce qui est gouvernance in sulato (Fit & proper, sous-traitance, fraude, blanchissement), mais nous travaillons de concert. On se voit et on se concerte à l'ICC et au réunion et comme nous travaillons au même étage cela permet une meilleur concertation.

- *Donc il existe une concertation formelle entre vos 2 fonction ?*

Non pas vraiment, mise à part en ICC bis où cela est vraiment formelle.

On se rend compte qu'il existe beaucoup de similitude dans la gestion des risques de compliance et du risque opérationnel qui est géré par le risque management. Pouvez-vous nous expliquer s'il existe un travail/ collaboration plus conjointe et à quel moment ?

On a pas mal d'interaction avec le risque management lors de leur rapport ORSA qui est un rapport reprenant des données quantitatives et qualitatives non-financières. Dans le cadre de ce rapport, nous travaillons avec eux pour analyser tout ce qui est risque juridique des risques opérationnels.

- *Existe-t'il un monitoring commun entre le risque management et la compliance ?*

Non, ce sont biens 2 monitoring distincts, je vais être en charge d'établir un plan d'action annuel que je remettrais au comité d'audit qui sera en charge de monitorer les risques liées à la compliance.

- *Selon-vous, quelles sont les Top risques dans votre organisation ?*

Selon moi, le risque qui pourrait avoir un gros impact sur l'entreprise ce sont les nouvelles régulations. Il y a tellement de nouvelles régulations qui arrivent très régulièrement et l'ampleur de ces lois comme le GDPR, AML, l'IDD. Ce sont des lois avec beaucoup d'ampleur demandant beaucoup de travail et de mise en œuvre.

Je mettrais la fraude en seconde lieu. Car malgré le fait que nous avons un système bien en place, les fraudeurs sont très créatifs et arrivent toujours à trouver une nouvelle faille.

Et je mettrais en 3 ème position, mais plus pour le futur c'est ce qui toucherait à la cybercriminalité qui pourrait vraiment être un danger. Nous mettons en place un programme un forum IT ou nous les teams de compliance et de l'IT se rencontrent. On met en place des mesures mais quand on voit que des sites ultra sécurisé arrivent à se faire hacker.

- *Pourriez-vous retracer un schémas type par lequel vous passer pour gérer le risque régulatoire par exemple ?*

En premier on est alerté des nouvelles lois et on regarde les impacts que cela put avoir dans les services, dans les documents par l'intermédiaire d'une vieille juridique, ensuite on parle avec nos correspondants sur le terrain qui sont mieux placer pour identifier les risques dans leur processus.

Une fois par an, on fiat une analyse des risques où chaque année ils doivent répondre aux questions par rapport à la corruption, la concurrence, AML, les codes assuralia, la protection du consommateur. Et on challenge pour voir si tout fonctionne et si il y a des manquements
Un point important que l'on doit surligner c'est que l'on doit comprendre le but de la loi pour pouvoir l'expliquer aux collaborateurs et les sensibiliser, ex mifid c'est la transparence). Donc par rapport à ça, on doit prendre en considération l'impact sur le client. Et on va surtout aller dans l'accompagnement.

En fonction de l'ampleur de la loi, on peut faire un projet complet, qui implique une vue horizontale, donc aide d'un Project manager.

Au niveau de l'évaluation, on discute avec les gens. Impact financier = risque réputationnel. Mais le risque réputationnel est plus important car le risque financier au pire c'est l'autorité de contrôle qui nous met des sanctions. Car l'image que l'on donne au client est très importante, on doit les protéger et être transparent, toutes les lois vont dans cette direction.

Utilisation de la matrice à impact avec le risk inhérent et résiduel pour l'évaluation des risques.

- *Quelles sont les contrôles et processus que vous avez mis en place pour le GDPR ?*

Point important droit des personnes concerné et nouvelle politique :

Publication sur le site de formulaire pour que les gens puissent exercer leur droit
Processus avec les correspondant pour quand les gens veulent avoir des données
→ processus IT avec les formulaires, processus politique avec procédure

Data Bridge, sensibiliser toutes les personnes concernées, et communiquez si jamais cela arrive.
Création d'une cellule.

On fait un DPA qui est une analyse d'impact d'un projet pour savoir si on gère bien les données sensibles d'un projet et si oui ou non on doit prévenir , puis on fait un PIA qui permet de savoir qui donnée est utilisée et par qui et à partir de là, on sait si on fait un DPA.

MIFIID : Stream information contractuel de nos collaborateurs, rémunération des intermédiaires.

- *Quelles sont les contrôles pour MIFID ?*

On vérifie chaque année les règlements commerciaux, tout ce qui est marketing, on fait du monitoring sur les voies de dilligence, sur le conflit d'intérêt. Mais on fait beaucoup de sensibilisation.

Êtes-vous amené à faire de la Due diligence sur les clients mais sur les fournisseurs aussi ?

Ca nous est arrivé mais c'est plus l'audit. Mais sinon c'est global vendor, on a établi des politiques mais c'est lui qui s'en charge au jour le jour. On va juste avoirun regard pour monitorer. Maintenant pour un sous-traitant, oui on fait un screeaning avec le risk management pour savoir s'il n'y a pas de problèmes d'éthiques.

- *Dans votre reporting, quelles sont vos KPI ?*

On a pas de KPI pour l'instant mais on aimerait bien. C'est juste une discussion, je donne mon assurance au board que nous sommes conformes par rapport au dossier que j'ai vu. On a des aspect qualitatif sur dans reporting en jugeant de l'efficacité d'un contrôle mais pour tous ce qui est KRI et l'aspect plus quantitatif, c'est le risk qui s'en occupe.

- *Comment faites-vous contrer les risques de fraude ?*

Pour fraude nous avons une politique et une commission fraude. Nos correspondants fraude présente ce qu'est la commission fraude et lorsqu'il y a un cas de fraude, il reporte ça chez moi et puis on prend des dispositions.

On a donc des correspondants, fraude, blanchiment (contrôle des opérations atypiques, GDPR et vie) parfois ils prennent plusieurs fonction.

Exemple de contrôle : les quittances sont faites sur des papiers spéciaux, avec du sulfite que l'on ne peut pas photocopier. Le principe des 4 yeux. On vérifie si le numéro bancaire est le même, copie de carte identité/carte d'identité, double check.

- *Comment faites-vous pour évaluer l'impact d'une fraude ?*

La fraude interne et externe c'est pour nous. On a pris ce rôle car cela touche aussi la réputation, plus que le financier. Pour eviter un doublon, on a mis ca ensemble. Et évidemment on analyse l'impact

- *Au niveau du risque fiducier, quelles sont les contrôles ?*

On a que des agents liés ca permet plus de contrôles mais on a plus de responsabilité. Pour savoir si l'agent est conforme, il doit remplir une analyse des besoins pour correspondre au profil du client par une série de question et en fonction du profil. On a mis des contrôle en place pour vérifier si cela correspond au profil des clients.

- *Comment faites-vous pour établir le plan annuel d'action ?*

Nous sommes invités au comité des risques et au comités d'audit. Pour le risk committee, il faut faire valider toutes les politiques (rémunération, intégrité, rémunération, fit and proper) ainsi que la partie chiffre. Rapport RSE. Au comité d'audit, c'est la validation des processus de contrôle, des comptes annuel.

- *Quelle est votre contact avec assuralia ?*

Il y a un groupe de travail compliance, il y a des groupes de discussions légal, ils sont là pour nous aider interpréter des lois, c'est une aide extérieure

- *Quelles seraient les pistes d'évolution pour une meilleure gestion des risques ?*

Avoir une culture de la compliance pour que cela soit une mission à tout un chacun. Cela doit surtout passer par de la sensibilisation et que l'on soit là pour accompagner les business. On doit plus avoir une vision de prévention et d'aide pour les business que de contrôle. Mais garder un contrôle avec un accompagnement ce qui nous donnera plus de crédibilité pour les gens.

c. Responsable RSE

- *Comment la fondation fonctionne-t'elle?*

Fondation : Depuis 2000 la fondation travaille sur la RSE, donc le groupe donne une partie de ses bénéfices à la fondation et nous on gère assez indépendamment des actions sur ses terrains là et on travaille surtout par des grands projets. Tous les 3, 4 ans on change de thématique, toujours sur l'exclusion des jeunes et la sécurité active ??? et on part aussi de la recherche scientifique

- *Quelles sont les liens avec le core business de l'entreprise ?*

Fondation : Cela n'a pas vraiment de rapport avec le business de l'entreprise. c'est vraiment sur l'exclusion des jeunes. Il y a 4 an on a travaillé sur le décrochage scolaire des jeunes et le chômage des jeunes. Maintenant on est plus l'action collective des jeunes, les jeunes qui ensemble veulent traiter un problème qu'ils ont, de trouver une solution collective. Mais les actions dépendent vraiment des valeurs de notre entreprise qui sont la solidarité et l'émancipation.

- *Vous travaillez donc de manière indépendante mais avez-vous des consignes de la direction ?*

Fondation :Oui il y a des membres qui comité de directions qui sont présents aux réunions mais également des partis externes comme des scientifiques et des journaliste. Mais oui on a des comptes à rendre au comité de direction. La direction nous donne les lignes conductrices, ce sur quoi ils aimeraient que l'on travaille et ensuite on organise des réunions avec des journalistes et des scientifiques ainsi que des jeunes pour savoir ce qu'ils aimeraient que l'on fasse exactement. Nous ne recevons pas vraiment d'ordre.

- *A quelle fréquence est-ce que vous reportez à ce comité ?*

Fondation :De manière formelle, on report une fois par an au CA. Maintenant de manière informelle, ils sont invités aux conférences ainsi que par mail, ils savent sur quoi on travaille. Tous les ans ont fait un prix de la citoyenneté, là aussi les membres du comités sont présents, on a des contacts avec des médias et on essaye de communiquer nos actions et le nom de notre entreprise aussi évidemment mentionné.

- *Comment la RSE est gérée en interne ?*

Il y a un groupe de travail qui se réuni 4 fois an et là-dedans tu vas trouver des gens qui s'occupent des bâtiments par exemple. De la mobilité, je parle de la mobilité des employés, tout ce qui est déchets, c'est vraiment des gens qui travaillent au quotidien sur des aspects qui sont important pour le côté écologique qui a été créé autour d'un label, qui est le label éco dynamique qui vaut pour les entreprises de Bruxelles et qui donne des 1, 2 ou trois étoiles en fonction des performances, on va dire au niveau écologique et là nous depuis 2010 on participe à ça et 3 fois on a eu des étoiles, donc on fait pas mal de chose. Je pense par exemple au niveau mobilité on n'est assez fort, on est bien situé aussi, on est pas loin des gars et donc il y a presque 80% du personnel qui vient train, en transport en commun, à pied ou à vélo

- *Vous êtes donc plus axé sur le côté environnemental ?*

Avec ce groupe de travail oui, si on regarde l'ensemble de l'entreprise, les autres aspects rse sont également très présent, comme la fondation, on peut dire que c'est un côté social

- *Avez-vous un aspect social également en interne ?*

C'est très large finalement la rse et tu peux parler de formation, de bien être en effet. Au personnel, là il y a une personne qui s'occupe de ça aussi. Nous travaillons aussi sur tout ce qui est prévention avec Pink ruban qui lutte contre le cancer du sein. On fait beaucoup de projets comme ça, avec la fondation il des projets avec le personnel interne pour aider des associations, donc il y a l'expertise de certaines personnes chez nous sur base volontaire est utilisée pour aider des asbl. Et comme ça il y a 5 projets qu'on aide et une vingtaine de personnes de notre entreprise qui vont voir les organisations pour leur stratégie de communication. C'est chouette car ils aident des asbl mais eux aussi se forment dans une autre discipline, pas dans les assurances mais dans autre chose. Ils reçoivent aussi une formation

- *Avez-vous une méthode de gestion des risques et des opportunités, similaire au risk management ?*

On commence à en faire, mais on ne tient pas compte des risques et opportunités, on n'arrive pas à les contrôler en fait, c'est plus qque chose qu'on fait sans les contrôler. Dans ma fonction relation publique, je suis en contact avec des gens qui s'occupent de tout ce qui est risk mangement, notamment pour tout ce qui est risque de réputation, c'est un risque important. On ne peut pas dire qu'on le gère, mais on fait partie de ceux qui ont une influence là-dessus, par exemple quand on n'est contact avec des journalistes, etc. *Mais ce n'est pas spécifiquement lié à la rse*

- *Comment identifiez-cous les opportunités qui sont les plus intéressante en termes d'action sociale ou environnementale ? est-ce que vous allez identifier les besoins, les exigences des différentes parties prenantes, via un questionnaire, comment est-ce que vous arrivez à évaluer ces actions ?*

Fondations : appel à projet, d'abord on se dit à partir de la recherche qu'est-ce qu'on va faire ? Qu'est-ce qui est important ? avec notre comité consultatif des experts on va définir des critères. Après on s'sélectionne les dossiers, on n'a beaucoup de dossiers, entre 150 et 250 et sachant que souvent on peut financer que 8 projets parce qu'on préfère donner des grandes bourses, d'avoir de grand projet que plusieurs petits. Pour sélectionner les bons dossiers, on travaille avec un jury externe qui est spécialisé sur les thématiques. On prend des personnes externes car nous ne sommes pas capables de voir toutes les opportunités. Ensuite les candidats exposent leurs projets et nous décidons avec les experts, quel projet nous allons choisir. Ce n'est pas une externalisation du processus mais c'est plutôt une co-creation. Nous utilisons les personnes externes car nous ne sommes qu'une personne et demie qui travaillons à la fondation. De cette façon-là on a aussi, on peut travailler, on peut dire que on est vraiment indépendant, ce n'est pas que la fondation ou l'entreprise qui choisit, mais c'est vraiment une décision commune, entre notre fondations et les personnes externes.

- *Utilisez-vous une matrice de la matérialité pour juger de l'importance des actions RSE sur vos parties prenantes*.

Fondation : Jusqu'à présent c'est assez informel. On va plutôt regarder l'impact après avoir effectué l'action. . Dans notre projet précèdent, on a fait un document avec un journaliste, on est allé visiter tous les projets. Après j'ai essayé d'évaluer un peu avec les chiffres qu'eux nous donne, mais c'est assez informel. Depuis cette année on travaille avec organisation flamande qui justement cherche avoir comment des fondations et des philanthropes peuvent évaluer leur impact. On est en train de réfléchir comment on pourrait dans nos prochaines actions mieux intégrer cet aspect, mais c'est difficilement mesurable.

- *Quelle a été la motivation pour entreprendre cette démarche ?*

Fondation : Essayer savoir si on a un impact et aussi si on a fait les choses bien. Aussi au niveau de l'entreprise, ça serait aussi intéressant que le CA soit au courant de l'impact qu'a nos actions. Si notre action à un grand impact, ça le sera également pour l'entreprise. On ne nous a pas demandé d'entreprendre cette démarche, c'est plutôt une envie personnelle.

- *Comme vous travaillez de manière indépendante, allez-vous priorisés l'impact sur les parties prenantes ou l'impact sur l'entreprise ?*

Fondation En premier lieu l'impact sur les parties prenantes, mais indirectement cela va également avoir un impact positif pour l'entreprise.

- *Y a-t-il un travail conjoint entre la fondation et vous, qui est contact presse pour essayer de capter les opportunités liées aux actions de la fondation et donc les communiquez ?*

Oui il y a un travail commun entre nous deux, on fait les communiqués de presse ensemble. Mais nous avons tout le temps choisi de ne pas utiliser la communication de la fondation dans la communication de notre entreprise. On a toujours essayé de séparer les deux pour séparer le business de la fondation. Quand l'entreprise communique c'est sur ces produits et ses résultats mais nous ne communiquons pas sur les actions de la fondation. On indique que nous possédons une fondation mais cela ne va pas plus loin que ça.

- *Avez-vous un rapport extra financier ? et stipulez-vous les actions RSE dans ce rapport ou est-ce un rapport distinct ?*

Dans le rapport on a des données chiffrées et ensuite il y a une brochure commerciale et la on stipule les actions de la RSE. On utilise pas les GRI standards . On a pas un reporting spécifique a la RSE. On suit quelques guidelines de la nouvelle législation de 2017 pour le rapport non financier mais pas de GRI .On suit les guidelines la directive européenne sur le non financial reporting l'an dernier. C'est la première fois que l'on communique vraiment en suivant un canevas, on le faisait avant mais pas de cette manière.

- *Il y a une certaine identification, évaluation des potentiels d'opportunités par rapport aux parties prenantes. Maintenant vous allez commencer à entreprendre plus une démarche qu'on appelle risque management avec des contrôles* ?

Fondation : On n'a pas vraiment des make process, c'est plus informel , on va demander à mi-chemin est-ce que vous pouvez nous donner un petit rapport, qu'est-ce que vous avez fait et puis on va les voir tous les projets à mi-chemin, ce sera près des grandes vacances. A la fin on a une conférence finale, tous les projets viennent dire ce qu'ils ont réalisés, les difficultés

- *Utilisez-vous des KPI pour reporting au CA ?*

Fondation On travaille de manière plus informelle, de temps en temps on peut avoir des KPI, mais on ne cherche pas non plus a créer des KPI. Comme par exemple avec les décrochages scolaires, il fallait voir si c'était des sortes de workshops pour garder les élèves à l'école à la fin de l'année. Oui combien d'élèves 80%. Mais ce n'est pas toujours facile . Par exemple il y avait un projet qui travaillait avec de jeunes Roms. Donc là c'est plus dur les chiffres. On essaye de trouver des chiffres comme ça mais ce n'est pas qu'après on va dire il n'y avait que 40% de Roms qui sont restés, alors on va plus vous financer. On sait qu'avec ce public c'est plus difficile On demande des chiffres oui mais on n'a pas une base comme ça. Mais quantifier c'est délicat car je sais aussi que c'est plus facile de faire un projet avec des jeunes dont les parents sont tous hautement éduqué que là le succès sera garanti et qu'avec des jeunes Roms, quand ils ont 15 ans ils doivent se marier, ben oui ils ne vont plus à l'école après. Mais on va essayer de formaliser ca mais en garder des critères réalistes.

- *Comment communiquez- vous en interne les actions entreprises par la fondation ?*

Intranet généralement. On communique sur les projet et on invites les membres du personnels à participer aux actions liés aux ASBL

- *Quel serai le top 3 des action RSE pour la fondation ?*

C'est difficile a dire car on fait des appel a projets, on n'a pas de classement vraiment pré etabli car c'est en fonction des parties prenantes et de ce qu'elle veulent.

- *Quelle a été la raison pour créer une fondation au lieu d'un département ?*

Avant la société faisait déjà beaucoup de social, mais cela était assez disséminé dans l'entreprise. Jusqu'au début des années 90 c'était complètement différent parce que ça faisait partie du groupe.

Depuis environ les années 1930, il y avait tout un réseau d'œuvre social avec des bâtiments où les gens étaient traités contre la tuberculose, il y avait des spas, des thermes pour la peau. Je ne sais pas combien de membres du personnel qui était sur le payrol qui travaillaient dans les œuvres sociales et donc c'était un truc énorme, très original, personne ne faisait ça et à cause du changement du marché d'assurance début les années 90. On a du complètement abandonné ça, sous cette forme-là, pour rester concurrentiel et pour ne pas être complètement abattu ont va dire et là il y a eu des initiatives pour quand même, parce que ce côté social on l'avait et on voulait le garder. Il voulait aussi un peu plus regrouper, que ce soit plus clair. Effectivement i y avait partout un spa, partout il y avait des actions sociales. Maintenant en interne c'est plus sous forme de soutient, avec par exemple la fcd, où on soutient des asbl en Amérique du sud par l'intermédiaire d'organisation coupoles mais aucun membre de l'entreprise ne travaille là-bas.

- *Maintenant pour les parties prenantes internes, pour les employés par exemple, comme est-ce que vous diriez que l'entreprise met en place des mécanismes pour améliorer le bien-être des employés., comment ça se passe ? L'évaluation ou l'identification d'opportunité pour améliorer le bien-être des employés ? Est-ce qu'il y a des surveys ?*

Oui il y a mais c'est plus des questions pour les ressources humaines. Tous les 3 ans il y a un sondage auprès des employés sur le stress, sur la qualité de la nourriture dans le restaurant, comment arriver ici la mobilité, plein de chose comme ça et les résultats de ses sondages sont utilisés pour améliorer des choses

- *Y a-ti une personne en charge de centralisé toute la RSe ?*

Non, ce n'est pas centralisé. Vu qu'on a un groupe de travail, mais comme je disais c'est surtout écologique. Ce que l'on a fait l'an dernier c'est, parce qu'évidemment on peut faire des choses isolés dans notre bâtiment et faire en sorte les gens viennent plus en train qu'en voiture, c'est des choses faciles. On a reformulé notre vision et nos missions et c'était l'occasion d'un peu plus voir comment on peut vraiment intégrer des aspects rse dans notre fonctionnement. J'ai travaillé avec 2 membres du comité de direction et l'idée c'était de faire une note de cadrage et de présenter ça au directeur qui va faire son plan annuel. Ces notes de cadrages du comité de direction qui vont dire, ça c'est la stratégie globale et pour vous ce qui est important c'est de regarder tel et tel point et la RSE fait partie de ses points. Cela étant, je ne connais pas à ce jour l'impact qu'a eu cette note, car il y a beaucoup de note de cadrage, il n'y a pas uniquement rse et les directeurs ont beaucoup de chose à penser, la rentabilité, le personnel, etc. C'est un truc en plus, c'est toujours compliqué, donc il faut répéter. A ce jour je ne connais pas l'impact de ce rapport car cette note de cadrage date de 2017 et il n'aura un effet sur la stratégie globale qu'apres le cycle de 3 ans donc en 2010

- *Donc vous diriez que le comité de direction a établi des objectifs rse ?*

Ouais, enfin des objectifs, je dirais qu'il y a des éléments rse qui vont paraître dans les plans mais il y a une hiérarchisation, si tu n'es pas rentable, tu n'existes plus à un moment donné et donc tu peux avoir des objectifs rse qui sont bien remplis, mais si t'es pas rentable, ben voilà. L'un vient après l'autre.

- *Y a-t-il des objectifs à atteindre ? des quotas plus quantitatifs ?*

Non c'est plus qualitatif c'était plus de pouvoir agir sur des projets ; par exemple des départements qui s'occupent des offres d'assurances, et bien ce serait bien que cette année vous y intégré, que vous développiez 3 projets qui sont liés à la rse. C'est plus dans ce sens là

- *ces initiatives qui ont été établies par le comité de direction, est-ce qu' il y a une sorte de risque management qui est intégré pour pouvoir contrôler tout çà, contrôler la mise en application ?*

Il y a des filtres risque management qui vont regarder les plans, et s'il y a des aspects rse ça va en faire partie mais je ne pense pas qu'il y a un regard risque management spécifique sur les aspects rse

- *C'est plus intégré dans les plans, si jamais ça touche les opérations, là ils vont un peu regarder, mais ils ne vont pas tellement mesurer l'impact que ça pourrait avoir, essayer de maximiser ?*

Je ne pense pas non

- *Qu'est-ce cela veut dire pour vous le risque réputationel, êtes-vous en charges de le contrôler ?*

C'est très flou, très large parce que, qui a la réputation d'une entreprise, ce n'est pas un département qui détient cela ou qui est responsable. N'importe quel collaborateur qui est en contact avec un client, va contribuer à l'image de l'entreprise à l'extérieur

On ne peut pas le contrôler, on peut à la limite mitiger des choses, par la prévention.

- *C'est vous qui mettez plus ou moins des procédures pour essayer de le mitiger et vous collaborer avec le risque management pour améliorer ces procédures ?*

On a eu des contacts, mais déjà depuis quelques années avec le risque mangement pour justement pour définir quelles sont les risques et sur quoi on peut mitiger. Par exemple, on ne peut pas contrôler la presse, mais s'il y a des journalistes qui nous posent des questions, à la limite ça peut arriver chez n'importe qui, On a fait des communications pour que les gens viennent chez nous, pour n'importe quelle question qui vient de la presse, que ce soit centralisé chez nous, qu'il n'y a pas quelqu'un dans un département qui va répondre à des questions à des journalistes. Si jamais il y a quelque chose qui se passe, qui pourrait amener à des journalistes à être intéressés, aussi de nous le dire. Par exemple, on peut avoir un client qui va dire je ne suis vraiment pas content, je ne suis pas d'accord avec le règlement de ce sinistre, je vais à la presse.

- *Et comment vous testé l'efficacité les procédures qui ont été mise en place pour mitiger ce risque opérationnel. Vous avez des procédures de testing qui ont été mises en place ?*

Non mais on voit bien que depuis qu'on a communiquer ca il y a quelques années, il y a beaucoup plus qui remonte. Avant, c'était notre faute aussi, les gens ne savaient même pas qu'il fallait qu'ils arrivent chez nous et donc il y a de plus en plus en plus des choses négatives, mais aussi positives où des gens vont venir nous dire ça c'est intéressant d'en parler à la presse.

Concernant le groupe de travail, vous nous avez stipulé que vous vous réunissez 3-4 fois par an pour discuter des possibles actions RSE en interne, pouvez-vous nous dire quelles sont les personnes présentes ?

1 RH responsable de tout ce qui est mobilité, bien être.
1 facility management qui est responsable pour le bâtiment et les déchets ainsi que les achats

1 personne qui vient de partir mais qui était du risk management, il est venu à ma demande car il avait une fibre RSE aussi. Il était bon avec les chiffres et avait une expérience du risk management
1 personne du comité de direction

Résumé de la situation :, il y avait une sorte de part de risque management dans la gestion de la rse interne à l'entreprise. De là on se rend compte qu'en fait vous avez plus un département qui est informel, vous travailler ensemble sur les actions rse de manière informelle. Est-ce que vous pensez mettre un département formel au lieu d'avoir un groupe de travail, faire un département justement qui ne s'occupe que de ça avec des gens de différents horizons, de différentes expertises seraient peut-être une meilleure idée pour favoriser et améliorer tout ce qui est processus, mise en application, réflexion sur les actions, vraiment faire un département avec plusieurs profils comme il y a pour l'instant en risque management.

- *Est-ce que vous pensez que ce serait une bonne piste d'évolution pour pouvoir avoir un département plus formel ?*

Oui c'est une question que l'on se pose de temps en temps mais dans les autres entreprises, le département RSE est fort axé sur le reporting et la sensibilisation interne, ce qui est très important. Chez nous ce qui serait intéressant c'est d'avoir un lien très fort avec le business, car c'est vers ça qu'on veut aller. C'est que la rse ce n'est pas quelque chose d'à côté mais quelque chose d'intégré. Comprendre le métier d'assurance et où est-ce qu'on peut avoir un maximum d'impact, mais qui doit aussi avoir ce lien avec l'expertise rse en soi, et sensibiliser le reporting. Oui un jour ça peut arriver qu'on crée une fonction à part, on est justement en train de réfléchir et le bord est ouvert à ces idées.

- *Existe-t'il une forme de reporting auprès du comité de direction pour ce groupe de travail avec des KPI ?*

La personne qui préside ce groupe de travail fait partie du comité de direction et moi je m'occupe d'établir un rapport. Cette personne est très sensibilisée à la question.

- *Pensez-vous que si cette personne quitte le groupe de travail, l'implication de l'entreprise pour tout ce qui concerne la RSE sera identique ?*

Je suis convaincu que tu peux avoir quelqu'un de super enthousiaste qui travaille dans un département qui est très enthousiaste pour la rse, mais si tu n'as pas l'aval du plus haut niveau, il n'y a rien qui va avancer, c'est très important

- *Selon vous qu'elle serait les pistes d'évolution dans le futur pour pouvoir implémenter une meilleure maîtrise des opportunités et des risques, une meilleure gestion ?*

Il y a beaucoup à structurer, c'est assez informel, il n'y a rien de structuré, il n'y a pas de KPI, Je pense surtout que les 2 points où une compagnie d'assurance peut avoir un impact c'est via les investissements et c'est via les produits d'assurances. Et la personne qui est responsable pour les investissements est sensible à ça aussi. Ce qui bloque pour le moment, je sais qu'au niveau européen ils sont en train de travailler là-dessus, c'est que, ce qui n'est pas très claire, c'est qu'est ce qui est un investissement durable responsable parce que c'est jamais noir ou blanc. On a besoin d'un cadre qui va définir qu'est ce qui a un investissement durable. Il y a des labélisations qui ne sont pas claire, qui sont pas tout à fait crédible, … Là il y a encore du travail Mais en tant qu'assureur c'est là qu'on peut avoir un vrai impact, si on a 18 milliards d'investissement là on peut faire quelque chose. Si tous les secteurs financier ou assureur belge dit on investit plus dans les entreprises qui sont rémunérés à 80% sur tout ce qui est revenu first fuel. Si on investit plus ce secteur est fini, on peut

avoir un énorme impact, des investisseurs institutionnels, donc on pourrait avoir de grand impact et c'est là que j'aimerais qu'on avance.

- Vous pensez que l'initiative doit plus venir des régulateurs, un cadre qu'est ce qui est durable et ne les pas et ceci influencera justement et aidera les entreprises à être plus durable ?

Tout à fait

4. ***Charlie banque***

a. Chief compliance officer

Chez nous la fonction de compliance rapporte au CRO. C'est autorisé à conditions qu'il l'instant sacrifie autant de temps à la fonction de compliance et aux fonctions de risques. Chez nous on voit que ce n'est pas réparti de façon égale. Le risque management prend 2x et demi plus que. Même chose au niveau de ligne de reporting, il y a 3 slots pour le comité de direction qui sont prévus pour les équipes cro et donc il y en a une qui est systématiquement pris par tout ce qui est retail risque, un autre qui est pris par le non retail risque et un troisième qui est partagé par des risques opérationnels et compliance. Si vous cherchez un souci peut exister dans cette constellation c'est bien celle-là quand les 2 rapporte à la même personne, il y a une inégalité en termes de temps qui est consacré au 2. Le problème c'est qu'on n'a pas suffisamment de temps ou d'occasion d'aller rapporter des risques en haut. Il en résulte une moins grande écoute des problèmes liés à la compliance.

- *Par contre, elle est mieux d'être indépendante mais avec une certaine corrélation entre les deux fonctions ?*

On voit systématiquement qu'on travaille plus souvent avec les gens des risques opérationnels qu'avec les autres types de risques. Il y a aussi la philosophie du groupe où le risque compliance est calculé par les modèles des risques opérationnels. Donc si nous ont fait un risque assesment les résultats sont quantifiés par le risque opérationnel. Il faut aussi spécifier que nous sommes un groupe d'assureur principalement et qu'on est presque la seule banque dans ce groupe et qu'on a dur à expliquer que pour la banque ce serait mieux de tout à fait séparer les cycles d'indentification des risques. D'avoir le cycle compliance et le risque opérationnel et ne pas mélanger les 2. Mais bon on n'a pas encore réussi à obtenir cela.

- *Donc si j'ai bien compris, la compliance est un risque opérationnel et rien de plus ?*

Oui effectivement, ça peut comporter certains avantages pour implanter une entreprise risk management puisque vous avez une vision globale en termes de risque et en termes de mise en place de processus de contrôle, pour avoir des contrôles qui sont globaux, mais justement, ça c'est un avantage. Mais vous pouvez dire comme inconvénient que vous avez moins d'écoute et que vous avez moins de temps pour pouvoir vraiment implémenter des contrôles qui permettent d'avoir une conformité réglementaire meilleure que dans l'autre cas. Alors les échanges avec le retail risques, le retail risque chez nous couvre principalement tout ce qui est les risques sur le portefeuille de crédit, donc le crédit client, crédit à la consommation et donc là de temps en temps, mais pas très souvent, on se touche quand on parle sur un assesment d'un nouveau produit.

- *Donc vous travaillez sur des processus avec eux et là-dedans entre la conformité, enfin la compliance est intégrée avec le risque*

On a chacun notre rôle mais tout est intégré dans ce processus de product aprouval. Dans ce cadre-là qu'on travaille ensemble et puis et pour le non retail risque c'est à peu près la même chose et là il s'agit principalement des assesment sur les produits d'investissement

- *Quel est le scope de la compliance selon vous ?*

Déjà pour vous dire les fraudes ne se trouvent pas chez moi. Les fraudes sont intégrées dans la cellule audit fransique qui est ici dans le département audit interne. Règle de conduite, éthique, anti blanchiment, les mécanismes particuliers, abus de marché, les crédits, hypothécaires, professionnels, corruption

- *Selon vous c'est quoi alors le rôle de la compliance chez axa banque ?*

On est maintenant une fonction de 2ième ligne de contrôle, mais on reste toujours encore conseillé. C'est un peu ambiguë c'est deux rôles là car on peut tomber dans des scénario Enron. Donc qu'est-ce qu'on essaye de faire avec les conseils, on demande toujours au business de préparer le travail et puis on contrôle et on donne des recommandations sur leur travail

- *Quelle a été l'évolution de la compliance au fil des années ?*

Quand on a commencé en 2001, on était plus conseillé, on écrivait des procédures. Le ciseau est encore à ce stade là et petit à petit il va aussi évoluer vers la fonction de contrôle mais n'est pas encore là. Ce ciseau c'est l'abréviation de chief information security officer, il se trouve entre les 2 lignes, il est aussi avec le business. C'est un rôle qui vas encore évoluer celui-là au moins (Ciseaux = personne de contact compliance)

- *Avez-vous les mêmes méthodes d'identification des risques que la fonction de risk management ?*

Non on n'a notre propre méthodologie, parce qu'on a découvert qu'en fait axa groupe a créé cette méthodologie de risque d'identification de risque évaluation de risque qui prenait comme point de départ un inventaire d'événement de risques. Ce n'est pas une bonne méthode car on a raté la moitié du travail. Il faut commencer avec le cadre, regarder si oui ou non il a des événements qui peuvent toucher à ce cadre on prend ce cadre réglementaire et puis on va le mettre sur notre pratique, on va le scooper et puis on va faire l'analyse du risque inhérent bien évidemment et puis on va regarder toutes les mesures qu'on pris d'un point de vue procédurale, d'un point de vue de contrôle première et deuxième ligne et on va juger la qualité de nos mesures de mitigation ??? pour tomber sur le risque résiduel

- *Quels ont vos critères de sélection pour pouvoir évaluer un risque ?*

On utilise quand même le cadre référentiel au niveau fréquence, sinon ça devient impossible pour eux de calculer.

- *En terme de contrôle, établissez-vous des contrôles commun ?*

Non, du tout, on n'essaye de ne pas avoir des overlaps pour ne pas pousser les gens vers une situation de over contrôle et on essaye de se complémenter. Mais on va se concerter et ça va être le cas en mettant les contrôles compliance en place, de toute façon on va diminuer les risques compliance et les risques opérationnels.

- *Et c'est à quel moment qu'il y a cette concertation entre le risque management et la compliance pour justement identifier ok ici on a un contrôle, ça ne sert à rien d'en avoir deux ?*

Il y quand même des réunions assez fréquentes et au moins une fois par semaine notre groupe, on est tous sur le même plateau. Il y a une grande collaboration entre le risk opérationnel et la compliance. On a le même rôle à des stades différents avec des zones différentes et maintenant bon pour assurer que nous on n'est pas dans une situation d'autocontrôle on a aussi des contrôles sur la fonction et la gouvernance de la fonction. On ne fait pas la deuxième ligne nous-même. On opère de façon de première ligne et c'est le risque opérationnel qui prend le rôle de deuxième ligne, pour toujours bien garder le cadre

- *Au niveau du reporting, vous avez un rapport commun avec le risque management ou bien vous reportez chacun avec le board ?*

Non en direct avec bon le bord avec le cro qui est membre du comité de direction c'est elle qui est notre membre du comité de direction et puis vers le comité d'audit, vers le conseil d'administration Nous avons chacun notre rapport mais lors des rapports au niveau

- Est-ce que le risk management utilise certain de vos KRI ?

Oui, parce qu'il faut aussi des qualitatives donc la compliance fait des indicateurs qualitatifs.
Dashboard commun global pour la banque qui reprend à la fois tout ce qui est indicateur de risque financier, crédit mais aussi les risques plus qualitatifs comme dans la compliance. Ensuite on a un rapport dans le Icap, on est aussi tous ensemble. Dans le rapport sur l'efficacité contrôle, on est là aussi tous ensemble et dans le globaly risk reporting où tout est ensemble mais à côté de cela chacun a ses rapports

→ ce sont des rapports indépendants qui sont quand même repris dans les rapports du risque management mais vous avez votre rapport que vous reportez directement à votre cro.

- *Combien de fois reportez-vous au board* ?

Le rapport annuel sur le fonctionnement et le rapport sur tout ce qui est les activités anti-blanchiment, ceux-là passent d'office
Il y a tout ce qui est questionnaire pour la banque national, à nouveau sur l'anti-blanchiment
Puis passe pour le compliance risk assesment et donc ça c'est des situations intermédiaires et puis la fréquence fixe est deux fois par an au comité de direction et deux fois par an pour le comité d'audit. Le premier trimestre c'est le comité de direction, le deuxième c'est le comité d'audit et puis le troisième le comité de direction, quatrième comité d'audit

- *Monitoring testing, est-ce que c'est vous qui élaborez votre plan d'action annuel ?*

  Présentation au board de manière annuelle d'un plan annuel d'action. Mais de manière individuelle, pas de lien avec les autres risques pour garder l'indépendance.

→ Problème de communication entre la compliance et le risk de temps en temps. Il faut essayer de parler en termes de risque. Mais ça prend du temps avant de comprendre comment on peut communiquer de façon efficace car prends du temps de parler en termes de risque.

- *Risque fiducier : surtout en banque un conflit d'intérêt qui est très fréquent le risque fiducier. Ce sont tous les conflits d'intérêts qui peuvent exister par exemple entre le banquier ou le client, entre les banquiers et les actionnaires, tous des conflits d'intérêts. Par exemple dans votre cas comment est-ce que les banquiers sont rémunérés, sous base de commission, salaire fixe ?*

Donc les agents ont un système de commissionnement qu'on appelle le barème. Ils ont des commissions qui sont à la fois quantitatif et qualitatif et il y a aussi un système de sanctions qui est intégré là-dedans, c.à.d. qu'ils risquent de perdre leur commission si on mesure ou on constate des manquements de comportements. Ils ont reçu des instructions sur l'extranet. Ils ont des objectifs jamais sur un produit spécifique mais toujours sur des familles, une gamme de produit, bien diversifiée pour ne pas les pousser vers un seul produit. Ils ont des objectifs sur le crédit professionnel et le crédit hypothécaire, et le crédit à la consommation, ils ont des targets sur tout ce qui est épargne et les produits normaux de banque, donc les comptes à vue et à terme et sur l'invest. Donc c'est bien diversifié dans tout ce qui est quantitatif et puis il y a les éléments qualitatifs derrière, leur score d'inspection va être nickel, ils ne peuvent pas avoir des plaintes de leurs clients par rapport à l 'invest et à la suite de la règle de la fsma sur l'expertise et le professionnalisme, celui qui n'a pas fait ses trainings ou n'a pas réussi les tests pour le training, il perd aussi de sa commission et en plus on va lui couper l'accès aux outils banquiers. Il **n'est pas contrôlé à 100%,** il ne doit pas suivre une procédure à 100% mais il est quand même aiguillé dans sa manière d'agir

Petit à petit on a mis en place aussi un équilibre entre le qualitatif et le quantitatif. En fait les agents respectaient bien les limites, mais derrière il y avait les business manager qui poussaient à vendre donc ce qui les mettaient en conflit avec leur business manager, donc on a pour commencer par adapter le système du business manager au système d'agent et puis on a parlé des étapes et on a pris des mesures plus loin voilà petit à petit on va essayer de trouver pour la partie variable des business manager, une compensation qui sera purement quantitatif pour travailler sur le professionnalisme, l'expertise, etc. tous ce que le client veut de son agent, de mettre le focus là-dessus et pas sur les produits, plus sur la personne,

sur la relation client. Chaque année on prend des étapes pour bouger vers le qualitatif et moins le quantitatif

- *Qu'est-ce qui différencie être compliant et être RSe ?*

On a un point commun avec le blanchiment d'argent. Le reste à voir avec le cadre éthique axe a décidé de ne plus investir dans le tabac, mais ça n'a rien avoir avec moi on avait l'idée de lancer un produit sur les métaux précieux, là on a dit écouté quand même si on regarde les sous-jacent on a quand des doutes, donc quand ils ont lancé le product approuval on l'a mis dedans mais c'est du CSR. On fait pour la société : d'activités pour les moins valides, maman pour maman. On a maintenant commencé à discuter qu'il ne peut pas y avoir des fournisseurs qui se gare sur le trottoir, parce que ça dérange les piétons et surtout les cyclistes, donc si on veut vraiment être une société… ça fait beaucoup de responsabilité. Axa était le premier groupe d'assurance mondial qui a mis charter data privacy. Tout ce qui est corporate responsability notre compagnie sœur axa belgium l'avait mis très vite sur le site web, la banque était quand même un peu plus prudente. C'est quand même une grande responsabilité qu'on prend en mettant ce message mais avec le gdpr ça devient plus réaliste, de donner plus ownership au client sur ses données et être transparent sur tout ce que l'on fait avec les données

- *Comment faites-vous pour vérifier que les contrôles mis en place sont efficaces ?*

On peut le constater aussi dans les résultats des contrôles de première ligne, où on se dit ce n'est pas possible d'avoir ce résultat. Exemple très banal, on n'avait un contrôle sur les profils de risque pour les investissements qui allaient voir s'il n'y avait pas des agents qui allaient changer très vite le profil juste avant de proposer un investissement, et ce contrôle donnait toujours un résultat nihil. Connaissant les agents, ce n'était pas réaliste qu'il n'y a aucun agent qui va changer le profil juste avant de faire l'investissement, parce qu'ils veulent toujours vendre plus et donc ils vont pousser leurs clients à prendre plus de risque pour créer plus de possibilités dans le portefeuille, donc d'avoir plusieurs mois d'affilés un résultat nihil, il faut se poser des questions, ne faut-il pas regarder ce problème d'une autre façon et voir s'il n'y a vraiment pas de cas. On avait ça comme indicateur mais aussi un whistleblowing case, nous disant qu'on le poussait à faire prendre plus de risque au client.

Donc il y a aussi la possibilité de voir des choses dans les plaintes par exemple. Donc il faut bien prendre en compte tout le scope possible pour voir si le contrôles fonctionnent de façon efficace, donc ça c'est un problème qu'on peut rencontrer qu'il y ait un contrôle qui soit n'est pas là, soit n'est pas fait, soit ne fonctionne pas très bien, donc ça c'est un problème et puis l'autre effectivement qui peut exister c'est qu'on a pas d'écoute

- *Donc vous avez des lignes de reporting pour ce genre de cas ?*

Oui il y a un canal anonyme mais qui est auprès de l'auditeur interne.

- *Est-ce que vous sentez que vous avez un pouvoir pour influencer les comportements déviants ?*

Quand nous on fait une recommandation au business et le business décide de ne pas l'implémenter, moi j'ai l'obligation de porter cela au comité de direction pour qu'eux sache que le business ne veut pas le faire et pour qu'eux prennent la responsabilité finale de ne pas le faire ou de le faire. On a un format

risk acceptance form et ils doivent signer en stipulant qu'il accepte de porter la responsabilité. Maintenant c'est rarement le cas, car lorsque l'information remonte au board, celui-ci ne tolère pas que l'on ne soit pas compliant.

b. Risk officer

- *Que pensez-vous de la relation entre Compliance et Risk Management ?*

Je ne vois pas de problème à combiner les deux. C'est une bonne façon de faire (travailler en collaboration avec la compliance). L'indépendance entre le Risk Management et la Compliance n'est pas aussi cruciale que l'indépendance entre la fonction de Risk Management, la fonction de Compliance et le reste des activités de l'entreprise.

Pour moi, cela n'a pas beaucoup de sens que la fonction de compliance reporte séparément à un autre membre de l'executive board.

Dans le monde financier, il n'est pas anormal de combiner la fonction de Risk management et de compliance. Nous essayons aussi de nous calquer sur la structure, la façon dont c'est géré au niveau de nos activités d'assurance.

- *Est-ce que dans votre rapport que vous faites au conseil d'administration, vous incluez également les KRI's de la compliance ?*

Je ne pense pas que vous les incluions systématiquement.

Par exemple, pour le reporting au commité d'audit, nous faisons une distinction entre le reporting de la fonction de compliance et de la fonction de RM.

Dans le reporting du RM, il n'y a pas de KRI's issus du département Compliance.

Cependant, en termes d'éthique, il n'y a pas que le département qui travaille dessus. Par exemple, je suis en charge des Retail Risks et je vais avoir un regard sur le risque de fraude. Mais le département de Compliance s'intéressera aux risques de fraude. Bien que c'est le même sujet, nous l'analysons de manière différente.

Par exemple, Anti-Money Laundering, c'est n'est pas mon domaine d'expertise. Ce sera à la Compliance de diriger la gestion de ces risques. Dans ce cas-ci, la compliance ne peut pas nous communiquer certaines informations liées à l' AML.

- *Est-ce que, dans le cadre de la collaboration entre vos deux fonctions, vous travaillez ensemble pour implémenter des contrôles et procédures ?*

Si nous pouvons collaborer pour mitiger un risque, nous le faisons. Mais on n'essaye pas non plus de combiner un maximum nos contrôles et processus. Le monde de la compliance et du RM sont différents et nous essayons de travailler ensemble et c'est d'ailleurs la raison pour laquelle on a une même personne à la tête des deux services, qui est le CRO.

Dans le cadre de cette collaboration, il se peut par exemple que nous envoyions une data query au département de compliance si nous voulons investiguer certaines questions et vice versa. Ce n'est pas à

nous de dire au département Compliance ce qu'ils doivent investiguer ni à eux à de faire pareil mais on s'échange certaines informations quand on en a besoin.

- *Est-ce que la RSE est incluse dans la stratégie d'entreprise ?*

Bien-sûr. Mais nous ne l'appelons pas forcément « RSE ». Nous ne voyons pas cela forcément comme étant explicite.

Par exemple, quand je fais mon rapport au board sur le retail loan portfolio, je parle de responsible lending (prêt responsables). On fait en sorte que nous n'endettions pas plus que ce qu'il ne faut les citoyens belges.

Un autre exemple, nous n'investissons plus dans l'industrie du tabac. Nous ne supportons pas les organisations criminelles ou terroristes.

(On a vu qu'ils sont présents aussi au niveau de l'aide apportée à des patients atteints de trisomie 21)

Nous avons uniformisé le nombre de jours de congés accordés aux jeunes parents après qu'ils aient eu un enfant (20 jours) pour tous les pays dans lesquels ils sont présents. Cela veut dire que même si la loi prévoit 10 jours de congés, AXA bank ira plus loin en leur offrant 20 jours.

Pour le bien-être des employés, nous avons un des douches pour pouvoir faciliter la venue en vélo des employés par exemple.

- *Est-ce que vous intégrez des KRI's liés à la RSE dans vos rapports ?*

Non pas nécessairement.

- *Au final, en quoi est-ce que la RSE intervient dans le travail de Risk Managers ?*

Quelqu'un responsable pour la RSE vient m'interviewer chaque année et les seniors managers en me demandant : « Voyez-vous des initiatives que nous devrions prendre pour votre département ? » ou encore : « Est-ce que nous atteignons nos ambitions RSE ? »

Mais il est important de comprendre que la RSE et le rapport de Risk Management ne sont pas liés.

En revanche, entant que Risk Managers, il nous arrive de nous prononcer en disant : « Désolé, nous trouvons qu'offrir ce genre d'investissement n'est pas une bonne idée car pas très éthique ». En effet, même si l'investissement semble intéressant aujourd'hui, dans quelques années cela pourrait se retourner contre nous en termes de réputation. Il y a 10 ans on ne faisait pas forcément aussi attention à cela mais aujourd'hui le risque réputationel est réel.

- *Est-ce que votre département est en charge de la gestion du risque réputationel ?*

Oui, on s'intéresse également aux risques de réputation, pas seulement aux risques financiers. Par exemple, un sujet clef concerne tout ce qui à avoir avec l'optimisation fiscale.

- *Est-ce que vous vous chargez d'évaluer les risques réputationels ?*

C'est le communication/brand officer qui est réellement responsable de la gestion, de l'évaluation du risque réputationnel.

- *Est-ce que vous pensez qu'une communication officer a les compétences pour évaluer les risques ?*

Bien-sûr. N'oublions pas qu'il travaille de façon complémentaire au département de Risk Management aussi. Il est mieux placé pour savoir ce qui est sensible ou pas pour l'entreprise.

- *Etes-vous en charge d'évaluer les risques liés aux actions RSE entreprises par la compagnie ?*

C'est plus le travail du brand manager puisque c'est lié à la réputation de la compagnie. Il y a toujours des risques.

Concernant les risques liés aux actions RSE entreprises par la compagnie, il n'y a pas fort à s'inquiéter puisque ce sont des actions réfléchies et en accord avec les valeurs de l'entreprise.

En revanche, un risque réputationel peut provenir d'un manque de positionnement CSR.

- *Est-ce que vous pensez que si c'était le département de Risk Management qui était en charge de la gestion du risque réputationnel, ces risques seraient encore mieux gérés ?*

Non cela fonctionne très bien comme cela.

- *Est-ce que vous utilisez une matrice pour évaluer les risques ?*

Ma responsabilité principale est la gestion des risques financiers. On utilise énormément la matrice de matérialité (quantitatif) pour classifier les risques (Probabilités vs. Impacts). Mais on fonctionne aussi à l'instinct (qualitatif).

- *Est-ce que vous avez des processus et contrôles liés spécifiquement à la RSE ?*

Non. Nous avons une manière globale pour identifier, évaluer et gérer les risques. Pas une spécifique pour la RSE.

- *Comment évaluez-vous les risques réputationels liés aux fournisseurs ?*

Le département procurement est en charge d'effectuer une due diligence pour évaluer les fournisseurs de l'entreprise (software company par exemple). Et par moment, entant que Risk Management department, nous faisons un double check en vérifiant également.

- *Est-ce que le département procurement travaille ensuite en collaboration avec le brand manager pour évaluer les risques réputationels liés aux fournisseurs ?*

Non. Mais c'est une bonne question. A l'heure d'aujourd'hui, il n'y a pas de dialogue entre Brand manager et Risk Manager à ce niveau-là mais il n'y a pas eu de problème lié au fait que le brand manager

ne se charge pas de la due diligence des fournisseurs. Mais il peut, en effet, être intéressant que le fait que le brand manager reprenne le rôle de due diligence pour les fournisseurs ou en tout cas ait un regard sur le procurement.

Au final, le Brand manager fait son rapport au Risk Management mais pas pour la due diligence des fournisseurs.

- *Considérez-vous la RSE comme étant du 1st ou 2nd line of defense ?*

Pour moi, la RSE et le brand management sont du 1st line.

- *Quels éléments reportez-vous en termes de reporting RSE ?*

Nous reportons en termes d'incidents, de plaintes provenant des tiers, des manquements aux règles et aux politiques d'entreprise.

- *Quelles sont les améliorations qui pourraient être apportées au RM en termes de gestion de risques liés à la compliance et à la RSE ?*

La gestion des risques non-financiers doit s'améliorer pour l'ensemble du secteur.

Nous devrions trouver une personne hautement qualifiée pour gérer ces risques. L'idée serait que cette personne ait un bon flair, un bon instinct pour tout ce qui est des risques non-financiers auxquels s'expose l'entreprise.

Un énorme challenge se pose également dans la gestion des données. Comprendre les risques qui y sont liés et éviter la mauvaise utilisation de ces données.