



HAL
open science

L'approche par les risques en audit interne: des normes aux pratiques décrites par les directeurs d'audit

Coskun Cakar

► To cite this version:

Coskun Cakar. L'approche par les risques en audit interne: des normes aux pratiques décrites par les directeurs d'audit. Gestion et management. IAE de Paris - Université Paris 1 Panthéon Sorbonne, 2016. Français. NNT: . tel-01433592

HAL Id: tel-01433592

<https://ens.hal.science/tel-01433592>

Submitted on 12 Jan 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

UNIVERSITE PARIS I - PANTHEON SORBONNE
Institut d'Administration des Entreprises de Paris

École doctorale de Management Panthéon-Sorbonne - ED 559
Equipe de Recherche GREGOR - EA 2474

L'approche par les risques en audit interne
Des normes aux pratiques décrites par les directeurs d'audit

THESE
présentée et soutenue publiquement le **9 décembre 2016**
en vue de l'obtention du
DOCTORAT EN SCIENCES DE GESTION
par

Coskun ÇAKAR

Directeur de recherche : **Monsieur Frédéric Gautier**
Professeur des Universités, IAE de Paris

Rapporteurs : **Monsieur François Aubert**
Professeur des Universités, IAE d'Orléans

Madame Anne Pezet
Professeure titulaire, HEC Montréal

Suffragants : **Monsieur Olivier Danière**
Head of Internal Audit, Groupe CHOPARD

Madame Catherine Kuszla
Professeure des Universités, Université Paris Ouest
Nanterre la Défense

Monsieur Marc Lassagne
Maître de conférences, ENSAM-Paris Tech

Monsieur Eric Séverin
Professeur des Universités, IAE de Lille

L'université de PARIS I – Panthéon Sorbonne n'entend donner aucune approbation ni improbation aux opinions émises dans les thèses ; ces opinions doivent être considérées comme propres à leurs auteurs.

À mes parents, ma sœur, mon épouse et mes filles

Remerciements

Je remercie chaleureusement mon directeur de thèse, le professeur Frédéric Gautier, pour m'avoir donné l'opportunité de réaliser ce projet qui me tenait tant à cœur et pour tout le soutien qu'il m'a apporté pour réussir à le réaliser. Sa grande disponibilité et toute l'attention qu'il y a portée resteront pour moi l'exemple à suivre. Il m'a transmis un grand nombre de principes fondamentaux en recherche, plus particulièrement la rigueur méthodologique et la persévérance qui me seront fort utiles tout au long de ma carrière. Merci du fond du cœur pour tout.

J'aimerais aussi remercier les deux autres membres de mon jury qui m'ont fait l'honneur de rapporter sur ma thèse, le Professeur François Aubert de l'IAE d'Orléans et la Professeure Anne Pezet de HEC Montréal. Ils ont tous deux grandement contribué à la qualité de cette thèse grâce à leurs lectures critiques et constructives. Je remercie la Professeure Catherine Kuszla de l'Université Paris Ouest - Nanterre la Défense, le Professeur Eric Séverin à l'IAE de Lille, Marc Lassagne, Maître de Conférences à l'école ENSAM Paris-Tech et Monsieur Olivier Danière, Responsable de l'audit interne du groupe Chopard d'avoir accepté de participer au jury de thèse.

Il me faut aussi remercier les directeurs d'audit interne qui ont agi en tant que répondants au cours de la collecte de données. Sans leur précieuse collaboration et leur considérable ouverture à l'égard de ce projet de recherche, cette thèse n'existerait pas.

Je remercie Stéphanie Serve pour ses précieux conseils. Je remercie Gilbert Frade et Olivier Pélissier pour leur amitié sincère. Je remercie Pierre Falkenheim, sans qui beaucoup de choses auraient été différentes dans mon parcours et dans ma vie. Je remercie mon ami Erkin Diyarbakirlioglu pour toute l'aide qu'il a pu m'apporter pour réussir à surmonter certaines périodes difficiles que tous les thésards connaissent au cours de leur recherche. Je remercie Gérard Melyon pour son soutien et son amitié infaillible depuis que j'ai eu la chance de croiser son chemin sur les bancs de l'université et pour m'avoir fait découvrir une vocation en me confiant mon premier cours à l'université. Ce fut le déclic. Je remercie Francis Deblaine et Izet Caltir mes deux amis d'enfance ainsi que Pascal Jeanne pour leur fidèle amitié depuis toutes ces années.

Je remercie mes parents Fevzi et Melek pour tout leur amour et tout ce qu'ils ont fait pour moi au cours de leur vie. Les mots ne suffiront jamais pour exprimer toute la gratitude et l'amour

que j'ai pour eux. Je remercie ma sœur Reyhan pour son amour et toute l'aide fraternelle qu'elle m'a apportée. Enfin, je tiens à remercier tout particulièrement mon épouse sans qui ce projet n'aurait peut-être jamais abouti, pour son soutien sans faille durant ces quatre années de thèse. Merci à toi Mehtap pour ta patience et ce grand amour qui nous unit. Enfin, je remercie mes deux filles Ela et Eda, qui m'ont donné l'énergie et l'amour dont a besoin un père pour avancer dans la vie. Je peux souffler à présent.

SOMMAIRE

INTRODUCTION.....	1
1^{ER} CHAPITRE : REVUE DE LA LITTERATURE	21
1 - 1 L'AUDIT INTERNE : UNE ACTIVITE NORMEE.....	21
1 - 1 1 <i>L'historique institutionnel de l'audit interne.....</i>	22
1 - 1 2 <i>L'audit interne : l'émergence d'une profession ?</i>	26
1 - 1 3 <i>Les normes pour la pratique professionnelle de l'audit interne.....</i>	30
1 - 2 L'AUDIT INTERNE DANS LE DISPOSITIF DE GOUVERNANCE.....	37
1 - 2 1 <i>La théorie de l'agence et l'audit interne</i>	37
1 - 2 2 <i>L'audit interne comme troisième ligne de défense dans le dispositif de gouvernance</i>	38
1 - 2 3 <i>L'audit interne et le comité d'audit</i>	41
1 - 3 L'AUDIT INTERNE ET LES RISQUES	45
1 - 3 1 <i>L'audit interne et les processus de gestion des risques</i>	45
1 - 3 2 <i>Le modèle du « business risk audit » (BRA)</i>	55
1 - 3 3 <i>L'audit interne et l'approche par les risques</i>	58
1 - 4 LA QUALITE DE L'AUDIT INTERNE : QUELS CRITERES POUR L'EVALUER ?.....	61
1 - 4 1 <i>Les critères traditionnels.....</i>	61
1 - 4 2 <i>L'appréciation de la qualité par les auditeurs externes</i>	63
1 - 4 3 <i>L'appréciation de la qualité par une approche plus globale</i>	67
2^{EME} CHAPITRE : CADRE THEORIQUE	73
2 - 1 LE RISQUE COMME CONSTRUIT SOCIAL	74
2 - 1 1 <i>L'approche culturelle de Mary Douglas et Aaron Wildavsky</i>	74
2 - 1 2 <i>Les conséquences de la modernité pour Anthony Giddens.....</i>	82
2 - 1 3 <i>La théorie des systèmes sociaux et la sociologie des risques de Niklas Luhmann</i>	90
2 - 1 4 <i>La société du risque d'Ulrich Beck</i>	99

2 - 2	LE CHOIX DU CADRE D'ANALYSE ET LES QUESTIONS DE RECHERCHE	106
2 - 2 1	<i>La problématique</i>	106
2 - 2 2	<i>Le choix du cadre d'analyse.....</i>	107
2 - 2 3	<i>Les attributs pour étudier le phénomène du risque ?</i>	109
2 - 2 4	<i>La formulation des questions de recherche</i>	110
3	^{EME} CHAPITRE : METHODOLOGIE	112
3 - 1	LA STRATEGIE DE RECHERCHE APPLIQUEE.....	112
3 - 2	L'APPROCHE METHODOLOGIQUE.....	113
3 - 2 1	<i>L'unité d'analyse.....</i>	114
3 - 2 2	<i>Le processus de sélection des entreprises et des répondants</i>	115
3 - 2 3	<i>Les répondants</i>	121
3 - 2 4	<i>Les sources des données et les procédures de collecte.....</i>	126
3 - 2 5	<i>La procédure de traitement et d'analyse des données.....</i>	132
3 - 3	LES CONSIDERATIONS ETHIQUES.....	142
4	^{EME} CHAPITRE : PRESENTATION DES DONNEES	145
4 - 1	LE PROCESSUS DE CARTOGRAPHIE DES RISQUES	145
4 - 1 1	<i>Le portage du processus de cartographie des risques.....</i>	146
4 - 1 2	<i>L'identification des risques</i>	149
4 - 1 3	<i>L'évaluation des risques.....</i>	170
4 - 1 4	<i>Le classement par catégorie et la synthèse des risques</i>	176
4 - 1 5	<i>La validation de la cartographie des risques</i>	184
4 - 1 6	<i>La mise à jour de la cartographie des risques.....</i>	185
4 - 2	L'ELABORATION DU PLAN D'AUDIT	187
4 - 2 1	<i>La construction de l'univers d'audit</i>	187
4 - 2 2	<i>L'identification des sujets (potentiels) d'audit en lien avec les risques</i>	190
4 - 2 3	<i>L'identification des sujets (potentiels) en fonction de critères spécifiques.....</i>	195
4 - 2 4	<i>La sélection des missions d'audit et l'élaboration du plan d'audit.....</i>	208
4 - 2 5	<i>La validation du plan d'audit</i>	220
4 - 2 6	<i>La flexibilité du plan d'audit</i>	226

4 - 3	L'ELABORATION DU PLAN DE MISSION.....	229
4 - 3 1	<i>La préparation de la mission et l'analyse préliminaire des risques.....</i>	229
4 - 3 2	<i>Le choix des axes d'intervention (périmètre de revue).....</i>	238
4 - 3 3	<i>L'allocation des ressources et la durée de la mission.....</i>	243
4 - 3 4	<i>L'élaboration du programme de travail.....</i>	245
5	^{EME} CHAPITRE : CONTRIBUTIONS.....	253
5 - 1	L'ECART ENTRE UNIVERS DES RISQUES ET UNIVERS D'AUDIT	253
5 - 1 1	<i>Les différentes dimensions de l'écart entre univers des risques et univers d'audit.....</i>	255
5 - 1 2	<i>Les causes potentielles de l'écart entre l'univers des risques et l'univers d'audit ?.....</i>	270
5 - 2	LE PROCESSUS D'AUDITABILITE : LA TRANSFORMATION DES RISQUES EN RISQUES AUDITABLES	284
5 - 2 1	<i>La distinction entre risque auditable et non auditable.....</i>	284
5 - 2 2	<i>Le processus de transformation du risque en risque auditable</i>	287
5 - 3	LES CONSEQUENCES SUR LA QUALITE DE L'AUDIT ET LE LIEN ENTRE AUDIT INTERNE ET GOUVERNANCE.....	300
5 - 3 1	<i>Le lien entre audit interne et gouvernance.....</i>	300
5 - 3 2	<i>La qualité de l'audit.....</i>	303
	CONCLUSION.....	309
	BIBLIOGRAPHIE.....	313

LISTE DES TABLEAUX

Tableau 1. Extrait des normes d'audit interne – Normes 2000, 2100 et 2200 (IIA, 2014)	34
Tableau 2. Extrait des normes d'audit interne – MPA 2010.1 et MPA.2010.2 (IIA, 2014)	35
Tableau 3. Processus de gestion des risques – Modèle du COSO 2 – ERM	47
Tableau 4. Comparaison des cadres normatifs de gestion des risques	52
Tableau 5. Dimension de la « Confiance » (Giddens, 1991)	85
Tableau 6. Stratégie et méthodologie de recherche	114
Tableau 7. Entreprises du secteur industriel	122
Tableau 8. Liste des sociétés qui ont participé à l'étude	123
Tableau 9. Liste des entretiens	125
Tableau 10. Typologie d'organisation des directions de l'audit	126
Tableau 11. Guide d'entretien	128
Tableau 12. Grille de codage – approche globale	133
Tableau 13. Processus d'élaboration du plan d'audit et du plan de mission	134
Tableau 14. Processus d'élaboration de la cartographie des risques	134
Tableau 15. Grille codage – méthode d'élaboration	135
Tableau 16. Grille de codage : codes relatifs aux acteurs impliqués	136
Tableau 17. Grille de codage : codes relatifs au processus de cartographie	137
Tableau 18. Grille de codage : codes relatifs à l'élaboration du plan d'audit	138
Tableau 19. Grille de codage : codes relatifs à l'élaboration du plan de mission	139
Tableau 20. Portage du processus de cartographie des risques	148
Tableau 21. Cartographie des risques – les approches de type « top down »	151
Tableau 22. Cartographie des risques – les approches de type « bottom up »	154
Tableau 23. Cartographie des risques – les approches de type « mixte »	156
Tableau 24. Cartographie des risques – origine des événements « risqués »	158
Tableau 25. Cartographie des risques – dimension temporelle	161
Tableau 26. Cartographie des risques – synthèse des modes d'observation par type d'approche	162
Tableau 27. Modalités de recensement mis en œuvre lors du processus de cartographie des risques	169
Tableau 28. Cartographie des risques – modes d'évaluation du risque	175
Tableau 29. Cartographie des risques - processus de hiérarchisation des risques	178
Tableau 30. Cartographie des risques – consolidation des risques	180
Tableau 31. Synthèse sur la nature des risques recensés lors du processus de cartographie	183
Tableau 32. Cartographie des risques – instances de validation	184
Tableau 33. Cartographie des risques – modalités de mise à jour	186
Tableau 34. Plan d'audit – construction de l'univers d'audit	189
Tableau 35. Plan d'audit – modes d'observation pour l'identification des missions	192
Tableau 36. Plan d'audit – Choix des missions en fonction du niveau de risque de la cartographie	194

<i>Tableau 37. Plan d'audit – typologie des objectifs de rotation retenue pour le choix des missions</i>	198
<i>Tableau 38. Plan d'audit – typologie des objectifs de couverture retenue pour le choix des missions</i>	201
<i>Tableau 39. Plan d'audit – principaux critères de choix des missions d'audit</i>	207
<i>Tableau 40. Plan d'audit – critères de hiérarchisation des sujets</i>	212
<i>Tableau 41. Plan d'audit – critères d'exclusion des missions</i>	219
<i>Tableau 42. Plan d'audit – intensité du lien entre les risques de la cartographie et le plan</i>	225
<i>Tableau 43. Plan d'audit – nature des informations communiquées lors de la validation du plan</i>	225
<i>Tableau 44. Plan d'audit – nature de la flexibilité du plan d'audit</i>	227
<i>Tableau 45. Plan de mission – mode d'observation des risques</i>	237
<i>Tableau 46. Plan de mission – critères de choix des axes d'intervention</i>	242
<i>Tableau 47. Plan de mission – types de programme de travail</i>	251
<i>Tableau 48. Illustration de l'approche d'audit sur un risque de fraude</i>	289
<i>Tableau 49. Illustration de l'approche d'audit sur un risque de fraude sur les paiements</i>	290
<i>Tableau 50. Exemple de déclinaison du risque de la cartographie en risque spécifique</i>	292
<i>Tableau 51. Exemple de déclinaison du risque spécifique en événements risqués</i>	293

LISTE DES FIGURES

<i>Figure 1. Le plan général de la thèse</i>	20
<i>Figure 2. Société de l'audit – représentation de l'audit en tant que pratique obscure</i>	27
<i>Figure 3. Structure générale des normes professionnelles de l'audit interne</i>	30
<i>Figure 4. Structure détaillée des normes professionnelles de l'audit interne</i>	32
<i>Figure 5. Le modèle des trois lignes de maîtrise (Amrae et Ifaci, 2014)</i>	39
<i>Figure 6. Modèle du COSO 2 – Enterprise Risk Management (COSO, 2004)</i>	47
<i>Figure 7. Exemple de cartographie des risques</i>	48
<i>Figure 8. Gestion des risques, dispositifs de contrôle et risque acceptable</i>	49
<i>Figure 9. Référentiel ISO 31000</i>	50
<i>Figure 10. Facteurs explicatifs de la qualité de l'audit</i>	68
<i>Figure 11. Collecte des données - profil du chercheur sur le réseau « LinkedIn »</i>	119
<i>Figure 12. Collecte des données – exemple de prise de contact – utilisation des réseaux sociaux</i>	120
<i>Figure 13. Collecte de données – exemple de prise de contact direct</i>	121
<i>Figure 14. Grille d'analyse des données codées – une approche matricielle</i>	141
<i>Figure 15. Normes d'audit : exigences en matière de planification</i>	254
<i>Figure 16. Ecart entre univers d'audit et univers des risques</i>	255
<i>Figure 17. Dimensions de l'écart entre univers des risques et d'audit</i>	256
<i>Figure 18. Cartographie et univers des risques</i>	257
<i>Figure 19. Univers des risques en fonction des personnes interrogés</i>	258
<i>Figure 20. Univers des risques en fonction de l'horizon de temps</i>	259
<i>Figure 21. Univers des risques en fonction du moment d'observation</i>	260
<i>Figure 22. Outils de collecte et d'évaluation des risques de la cartographie</i>	261
<i>Figure 23. Origine des missions inscrites au plan d'audit</i>	263
<i>Figure 24. Heuristiques organisationnelles pour transformer les risques en risques auditables</i>	296
<i>Figure 25. Représentation du processus d'auditabilité</i>	298

INTRODUCTION

Le choix du thème de recherche

Le début des années deux mille a été marqué par deux crises majeures. Il s'agit des attentats du 11 septembre 2001 perpétrés aux États-Unis et le scandale financier du groupe Enron à la fin de l'année 2001 qui a ébranlé le monde des affaires et celui de l'audit avec la chute du cabinet d'audit Arthur Andersen. Les années qui ont suivi n'ont pas été épargnées avec de grandes catastrophes comme celles de l'accident nucléaire de Fukushima au Japon et la crise financière de 2008 qui a ébranlé le monde économique et dont les effets se font encore ressentir. Les crises successives ont amorcé le début d'une longue crise de confiance non seulement dans le monde des affaires mais également dans la société dans son ensemble.

Face à la crise de confiance grandissante des marchés financiers, les législateurs ont essayé d'apporter des réponses avec le vote des différentes lois. Suite à la crise d'Enron, des lois de sécurité financière tout d'abord aux États-Unis avec le vote de la loi « *Sarbanes-Oxley Act* » en 2002 suivis de diverses législations dans de nombreux pays. C'est en 2003 que la « *Loi de Sécurité Financière* » a été votée en France. Ces lois exigent notamment que les dirigeants des sociétés cotées identifient, évaluent et communiquent sur leurs risques et leurs procédures de contrôle interne à leurs actionnaires ainsi qu'aux différentes parties prenantes. Suite à la crise financière des sub-primes de 2008, la « *Dodd-Frank Act* » a été votée aux États-Unis en juillet 2010. Elle est présentée comme la plus vaste réforme financière depuis le Glass Steagall Act, établi en 1933 et aboli en 1999.

C'est dans ce contexte de crise de confiance et de nouvelles exigences réglementaires que l'audit interne a pris tout son essor en se positionnant comme une « fonction experte » au service des directions générales et des instances de gouvernance pour les aider à mieux apprécier, prévenir et maîtriser les risques au sein de leurs organisations.

Contrairement aux auditeurs financiers, les auditeurs internes ne sont pas soumis à un cadre réglementaire spécifique. La fonction d'audit interne est régie par les normes professionnelles édictées par l'*Institute of Internal Auditors (IIA)*, association professionnelle constituée aux États-Unis en 1941 pour promouvoir la profession. L'audit interne autrefois cantonné au périmètre de l'audit financier s'est ainsi repositionné sur le thème du risque. La nouvelle définition de l'audit interne qui fait partie intégrante des normes est relativement récente

puisqu'elle a été établie en juin 1999. Les normes définissent l'audit interne comme une activité indépendante et objective en charge d'évaluer la robustesse des processus de gestion des risques, de gouvernance et de contrôle au sein des organisations. La notion de risque est au cœur de son activité puisqu'elle constitue non seulement l'objet même de l'audit mais également le fondement de sa méthodologie.

Il y a donc un besoin d'étudier les pratiques des auditeurs internes pour mieux comprendre comment ils prennent en charge leur nouveau rôle dans le dispositif de gouvernance des organisations et savoir si les normes permettent d'améliorer la qualité de l'audit. Ce sujet a un intérêt du point de vue scientifique dans la mesure où ce thème reste relativement peu abordé dans la littérature existante et qu'il y a un véritable besoin d'être en mesure de mieux apprécier ce que l'audit produit. Il a un intérêt du point de vue sociétal dès lors que l'audit déclare pouvoir contribuer à améliorer la gestion des risques qui sont à l'origine de la crise de confiance actuelle et des attentes qui en découlent. Enfin, il y a un intérêt pratique pour répondre aux difficultés que peut poser potentiellement la mise en œuvre des normes d'audit.

La littérature existante sur le thème de l'audit interne

- *Les normes d'audit interne*

La revue détaillée des normes professionnelles de l'audit interne fait apparaître un paradoxe surprenant. La notion de risque sur laquelle est principalement fondée dans ces normes la pratique de l'audit reste relativement « ambiguë ». Elle n'est pas définie de façon précise et présente par ailleurs une faiblesse majeure : elle ne permet pas de traiter du risque au niveau organisationnel qui constitue pourtant le véritable enjeu dans le cadre des dispositifs de gestion du risque.

La définition qui est donnée du risque est qu'il s'agit de « *tout événement qui, s'il se produit, peut remettre en cause l'atteinte des objectifs d'une organisation* ». Le risque tel que défini dans les normes ne distingue pas la notion de risque réputée calculable et celle d'incertitude qui se caractérise selon Knight (1921) par l'impossibilité de les mesurer dès lors que les événements ne sont pas connus.

Une autre difficulté que pose la définition du risque est qu'elle fait référence dans les normes à la notion d'appétence au risque qui détermine le type de réponse à apporter face à un risque, à savoir l'accepter ou bien chercher à le réduire. C'est d'ailleurs une des critiques apportées dans la littérature sur les cadres de références qui existent en matière de gestion des risques. Power

(2009) précise que la notion d'appétence au risque du modèle de l'ERM (*Entreprise Risk Management*) auquel se réfèrent les normes d'audit pose problème. Ce modèle considère l'appétence au risque comme étant une notion unique et homogène pour l'ensemble de l'organisation et qu'il est possible de le déterminer sans ambiguïté. Cette conception du risque « acceptable » exclut l'existence de conflits entre différents types et niveaux d'appétence au sein d'une même organisation.

L'absence de définition précise amène dès lors à s'interroger sur l'intérêt d'avoir fondé une pratique comme l'audit interne sur le risque. La théorie de la société de l'audit (Power, 1999) apporte un début de réponse à cette interrogation. Son auteur, M. Power, décrit le nombre croissant d'activités qui sont réalisés en se référant au « savoir abstrait » de l'audit. M. Power distingue d'une part le savoir abstrait et d'autre part la pratique concrète de l'audit. L'audit est présenté comme une pratique objective pour répondre aux attentes sociétales. Or, selon Power, la pratique de l'audit reste « obscure » et n'exclut pas une dimension subjective. Lorsque de nouvelles demandes sont adressées à l'audit pour fournir de nouveaux types d'informations objectives, l'audit accepte d'y répondre en intégrant ces nouvelles demandes dans son savoir abstrait. Power précise qu'un écart apparaît dès lors entre le savoir abstrait réputé être reproductible et objectif et sa pratique qui reste fondamentalement inchangée avec la mise en œuvre d'une succession d'étapes.

- *Les principaux travaux sur l'audit interne en lien avec le thème du risque*

Les travaux de recherche menés jusqu'ici sur le thème de la pratique de l'audit interne au regard de son nouveau rôle dans l'évaluation des dispositifs de gestion des risques et de son approche fondée sur les risques restent relativement limités (Coetze et Lubbe, 2014).

Les principaux axes développés dans la littérature se sont intéressés tout d'abord au lien entre l'audit interne et la gouvernance qui ne traite pas de l'impact de l'audit sur l'amélioration des dispositifs de gouvernance. Les travaux qui ont porté sur l'approche par les risques en audit interne ne décrivent pas suffisamment les pratiques de l'audit interne. En ce sens, ils demeurent insuffisants. Enfin, la qualité de l'audit a fait l'objet de nombreux travaux mais en s'attachant à l'apprécier en fonction des attributs individuels des auditeurs et en interrogeant principalement les auditeurs externes pour traiter de cette question (Roussy et Brivot, 2016). La littérature ne traite pas de l'évaluation par l'audit du risque au niveau organisationnel alors qu'il constitue un enjeu sociétal majeur.

Le cadre théorique et les questions de recherche

▪ *Le choix du cadre théorique*

Notre recherche vise à traiter du risque non pas au niveau individuel mais organisationnel. La définition actuelle qui est retenue par l'audit en référence à l'approche traditionnelle est qu'il s'agit d'une mesure résultant du produit de la probabilité par l'impact et dont la gravité est à apprécier en fonction de l'appétence au risque. Cette conception du risque présente des limites pour traiter du risque en audit interne au sein des organisations. La première résulte du fait que cette approche semble inopérante en l'absence de données abondantes puisqu'à l'audit ne dispose pas de données historiques pour tous les événements possibles mais redoutés. La seconde porte sur la difficulté que pose la détermination de l'appétence au risque au niveau organisationnel.

La sociologie du risque qui est retenue dans ce travail de recherche comme cadre théorique nous permet de dépasser ces deux limites et d'avoir un éclairage particulier sur le concept de risque. Elle nous apporte aussi des concepts intéressants pour questionner l'audit interne et ses normes professionnelles qui fondent sa méthodologie sur l'identification et l'évaluation des risques au sein des organisations. L'analyse renouvelée de la conception du risque proposée par la sociologie du risque permet d'étudier les processus mis en œuvre par l'audit interne tout en considérant les contraintes et les intérêts institutionnels ou organisationnels.

Le risque y est défini non pas comme un objet accessible et mesurable de façon objective mais comme un construit social. Cette construction résulterait alors des modes d'interaction entre les acteurs dans un contexte social et organisationnel particulier et des facteurs sociaux, culturels et politiques. Vu sous cet angle, il apparaît essentiel de mieux comprendre le rôle que joue la fonction d'audit interne dans le processus d'identification et d'évaluation des risques au sein de son organisation et quelle est la nature de ses interactions avec les autres acteurs.

Notre objectif est d'étudier le processus de construction sociale des analyses de risque formelles réalisées au sein des organisations en mettant en relation les procédures mises en œuvre par les acteurs avec les résultats produits. À ce titre, il est nécessaire d'analyser les heuristiques mises en œuvre au sein des organisations ainsi que les modes d'interaction des acteurs pour construire les objets de risque.

De nombreuses approches ont été développées au sein de la sociologie du risque. L'ensemble de ces approches théoriques (la théorie culturelle de Douglas, la théorie des systèmes sociaux

de Luhmann, la société du risque de Beck et Giddens) contribue à mieux comprendre dans quelle mesure et de quelle manière le risque est un objet socialement construit. Leur étude permet de mettre en évidence à la fois des similitudes et des différences significatives.

▪ *Le cadre d'analyse retenu*

La théorie des systèmes sociaux (1986) et la sociologie des risques (1993) de Niklas Luhmann apportent un cadre particulièrement riche pour étudier le phénomène de construction sociale du risque. Luhmann fournit dans le cadre de sa théorie une définition du concept de risque qui n'est pas explicité aussi précisément chez Giddens, Beck ou Douglas. C'est la raison qui justifie son choix comme cadre d'analyse.

Selon Luhmann (1993), les risques n'existent pas indépendamment de notre mode d'observation. Pour être capable d'observer, il faut procéder à une distinction. Si nous voulons désigner quelque chose comme étant un risque, nous devons le distinguer de ce qu'il n'est pas. Il introduit quatre concepts fondamentaux qui sont mobilisés dans cette thèse : la distinction risque/danger, les codes de communication, l'observation de premier ordre et de second ordre et le futur comme risque.

Un apport fondamental des travaux de Luhmann (1993) est d'avoir apporté une définition du concept de risque en introduisant la distinction risque/danger. La distinction risque/danger ne fait pas référence à une question de probabilité ou d'improbabilité. Le problème est de savoir si la possibilité d'une déception dépend de notre conduite préalable ou non. L'accroissement de notre sensibilité aux risques peut être expliqué par la manière dont les événements sont observés dans notre société moderne et aussi attribués à nos décisions (plus qu'à des causes externes). Selon Luhmann (p3, 1993), l'évaluation des risques et la volonté à les accepter sont des problèmes avant tout d'ordre social. La prise de risque n'implique pas de communication entre ceux qui décident et ceux qui sont indirectement impactés par la décision prise. Il n'est pas possible d'avoir une évaluation objective du risque en l'absence de critères universellement acceptés par tous : ceux qui sont indirectement impactés auront une évaluation différente de ceux qui décident de prendre le risque.

Pour Luhmann (1986), la société est fonctionnellement différenciée est composée de sous-systèmes sociaux afin de réduire la complexité. Les sous-systèmes sociaux sont opérationnellement clos et ne communiquent pas entre eux.

Chaque sous-système social observe son environnement et communique à son sujet avec ses propres codes. Le risque résulte des conséquences des décisions prises au sein d'un sous-système donné sans pouvoir envisager leurs conséquences sur les autres sous-systèmes.

Rien ne peut être observé sans établir de distinction, ce qui signifie que toute observation comporte des points aveugles. Un point aveugle ne peut devenir visible que pour une autre observation qui observe elle-même la première observation. C'est l'observation de second ordre.

Luhmann (1993) définit le futur comme risque, notamment du fait que celui dépend de nos décisions. Les risques ne sont pas les mêmes selon l'horizon temporel qui est considéré lorsque nous établissons des distinctions pour observer. Par ailleurs, les risques et leurs évaluations varient dans le temps.

▪ *Questions de recherche*

La question de recherche principale de cette recherche est la suivante : « *Comment les organisations construisent-elles leurs objets de risques et par quelles heuristiques ?* » en lien avec les activités de l'audit interne.

Il faudra dès lors répondre à plusieurs questions qui en découlent pour comprendre *comment les directions d'audit construisent leurs objets de risque ... pour les rendre auditables* :

- Comment les risques identifiés dans l'organisation (cartographie des risques) orientent-ils les travaux des auditeurs internes ?
- Comment sont évalués les risques de l'organisation lors de la construction du plan d'audit ?
- Comment sont définies les missions sur la base de l'évaluation préliminaire des risques ?
- Dans quelle mesure l'auditeur interne peut être un observateur pertinent des risques de l'organisation ?

La méthodologie de recherche

▪ *Le chercheur*

Il est important de préciser en préambule le statut du chercheur qui est un professionnel de l'audit interne au sein d'un grand groupe industriel français. Il y a occupé successivement le poste d'auditeur, de chef de mission, de superviseur avant de devenir le directeur adjoint du

département d'audit. Cette expérience est importante dans le cadre de cette recherche puisqu'elle a permis au chercheur d'acquérir une bonne connaissance de la dynamique du milieu et de ses codes spécifiques de communication. Enseignant l'audit interne et la gestion des risques depuis plusieurs années à l'université, Il a pu prendre un certain recul sur la pratique de l'audit et sur la sienne également. Il a mené cette recherche en dehors de son entreprise pour lui permettre d'avoir la distance suffisante et nécessaire.

- *La stratégie de recherche*

La méthodologie utilisée dans le cadre de cette recherche est qualitative et se fonde principalement sur des entretiens réalisés auprès des directeurs d'audit de grands groupes français du secteur industriel, commercial et des services.

- *L'unité d'analyse*

L'unité d'analyse retenue pour cette recherche est la direction de l'audit interne qui permet de répondre à l'ensemble des questions de recherches établies. La direction de l'audit interne n'agit pas indépendamment du contexte organisationnel dans lequel elle réalise ses activités. Il est dès lors essentiel de mieux comprendre la nature de ces interactions.

- *Le choix des répondants*

Cette recherche a été conduite auprès de plusieurs directions de l'audit interne de grands groupes du secteur industriel, du secteur commercial et celui des services. Les entreprises de ce secteur ne disposent pas, contrairement à celui des assurances, de données suffisantes pour appréhender le risque par une approche fréquentiste et probabiliste. Cette difficulté pratique soulève dès lors la question de savoir comment ces sociétés procèdent pour identifier et désigner les risques au sein de leur organisation. Ont été exclus de cette étude le secteur financier (banques et assurances) qui est soumis à des obligations réglementaires particulièrement contraignantes et les petites et moyennes entreprises puisqu'elles ne disposent souvent pas d'une direction de l'audit à part entière.

Afin de réaliser le choix des directions de l'audit, le chiffre d'affaires et les effectifs de la société ont été retenus comme principaux critères. La sélection comporte des groupes issus principalement du CAC 40 et du SBF 120 puisqu'il s'agit de groupes qui sont soumis à des obligations de communication en matière de risques et de dispositif de contrôle interne dans le cadre des exigences réglementaires (lois de sécurité financière, huitième directive Européenne).

- *Procédé empirique pour la constitution du groupe de répondants*

L'accès aux données est particulièrement difficile dans le domaine de l'audit interne. Il s'agit de traiter, lorsqu'il est question d'audit interne, d'informations jugées confidentielles et potentiellement préjudiciables pour les organisations puisqu'il s'agit de leurs risques. Malgré le fait que les grandes entreprises communiquent sur ce thème dans le cadre des rapports annuels, les informations restent le plus souvent très descriptives. Il n'est pas possible sur cette base de connaître les processus d'identification et d'évaluation qui sont mis en œuvre en amont.

Pour réussir à constituer la liste des répondants, différentes ressources ont dû être mobilisées. La première ressource a été le réseau professionnel du chercheur. Le chercheur a ainsi pu obtenir l'accord de quatorze directeurs d'audit pour participer à ce travail de recherche.

La deuxième ressource mobilisée a été la prise de contact via les réseaux sociaux (principalement le réseau « *Linkedin* »). Le chercheur a obtenu l'accord de onze directeurs d'audit pour participer à ce travail de recherche.

Enfin, la dernière ressource mobilisée a été la prise de contact direct lors de séminaires professionnels animés par le chercheur lui-même sur le thème de l'audit interne. Il a pu obtenir l'accord de sept autres directeurs d'audit pour participer à son étude.

- *Les répondants*

Le chercheur a pu réaliser des entretiens avec trente-deux directeurs d'audit interne au sein de grands groupes du secteur Industriel, Commercial et des Services. Il s'agit de groupes pour la plupart cotés (26 sur 32) assujettis à des obligations de communication sur leurs dispositifs de contrôle interne et processus de gestion des risques. Parmi les répondants, quinze directeurs exercent leurs activités dans le secteur industriel, huit dans le secteur commercial et sept dans celui des services.

- *Les modalités de collecte des données*

L'entretien est le principal outil de collecte mobilisé pour cette recherche. L'originalité des modalités de collecte repose sur la combinaison d'entretiens individuels et collectifs. Le chercheur a rencontré individuellement chaque répondant puis organisé deux « focus group » avec une dizaine de répondants.

- *Les données collectées*

Au total, trente-deux entretiens ont été réalisés avec une durée moyenne d'une heure et quarante-cinq minutes, soit au total quarante-sept heures qui ont une fois retranscrit de façon intégrale représentent près de mille cent pages d'entretien. Les données collectées sont

extrêmement riches et particulièrement difficiles à obtenir compte tenu de leurs natures hautement confidentielles. Le chercheur a pu avoir accès à des cartographies des risques, des plans d'audit et des rapports d'audit.

- *Modalités de traitement et d'analyse des données*

Le chercheur a établi une grille de codage qui a permis de croiser les principaux concepts du cadre d'analyse et les normes d'audit interne. L'ensemble des entretiens a été codé à l'aide de l'outil NVivo 10 et fait l'objet d'un double codage pour ajuster et valider la grille de codage initiale. Ce travail a permis de faire le lien entre les concepts théoriques et les données pratiques à un niveau méso pour identifier des catégories et sous-catégories. Ces catégories ont fait l'objet d'une seconde analyse qui a consisté à identifier pour chacune des catégories les ressemblances et dissemblances entre les répondants et qui témoigne de la grande diversité des pratiques.

Les principales contributions

Cette thèse apporte trois contributions principales. La première est de démontrer les différentes dimensions de l'écart décrit par Power (1999) entre le système abstrait de l'audit et sa pratique et d'explorer les causes potentielles qui permettent de l'expliquer. La seconde est de mieux comprendre le processus d'auditabilité, c'est-à-dire le processus mis en œuvre par l'audit interne pour transformer les risques en risques auditables. Enfin, ces travaux permettent de porter un regard renouvelé par rapport à la littérature existante sur le lien entre audit interne et gouvernance, ainsi que sur l'appréciation de la qualité de l'audit pour améliorer les pratiques managériales.

- *Les différentes dimensions de l'écart entre univers des risques et univers d'audit*

La norme d'audit interne relative à la planification annuelle des travaux de l'audit précise que « le responsable de l'audit interne doit établir un plan d'audit fondé sur les risques afin de définir les priorités cohérentes avec les objectifs de l'organisation ».

Les résultats issus de l'analyse de nos données mettent en évidence que le taux de couverture des risques de la cartographie par les missions d'audit peut être plus ou moins important selon les organisations. Le plan d'audit contient des missions qui ne sont pas en lien direct avec la cartographie des risques et qui reposent sur des critères spécifiques à l'audit interne. La décision de réaliser ces missions permet à l'audit interne d'appréhender d'autres sources de risques qui n'apparaissent pas dans la cartographie. Ce constat se traduit dès lors par un écart entre l'univers d'audit et l'univers des risques.

Selon Power (1999), il existe un écart entre le système abstrait de l'audit représenté par les normes et la pratique effective des auditeurs. Ce travail de recherche confirme l'existence de cet écart mais va au-delà en spécifiant les différentes dimensions qu'il revêt et en explorant les causes potentielles qui permettent de l'expliquer.

L'univers des risques peut être plus ou moins accessible en fonction des choix méthodologiques et donc des distinctions qui sont retenues par les acteurs pour identifier les risques au sein de leur organisation. Les acteurs seront soumis à des points aveugles lorsqu'ils chercheront à observer et à reconstituer leur univers des risques.

Tout d'abord, l'univers des risques est constitué de l'ensemble des risques potentiels mais le résultat du processus de recensement est conditionné par le niveau organisationnel interrogé.

Une seconde dimension clé qui peut conditionner le résultat de la cartographie est l'horizon de temps retenu pour identifier les risques. Selon l'horizon de temps retenu, la nature des risques sera sensiblement différente avec d'une part des risques « opérationnels » qui portent sur le court terme et d'autre part des risques « stratégiques » qui portent sur le moyen et long terme.

Une troisième dimension porte sur les outils de collecte utilisés pour recenser les risques ainsi que différentes modalités d'évaluation. Le fait de soumettre par exemple un questionnaire aux managers pour recenser les risques donnera certainement des résultats sensiblement différents suivant qu'il s'agit d'un questionnaire ouvert ou bien fermé.

Une quatrième dimension concerne les modalités d'évaluation des risques qui peuvent aussi amener à exclure certains risques lors du recensement des risques du fait de règles ou de critères restrictifs. Pour certains, seuls les risques pouvant être traduits en impact financier sont retenus alors que pour d'autres, le risque revêt d'autres dimensions mais qui sont eux-mêmes restreints par souci de simplification. Les modalités d'évaluation appliquées par les organisations sont multiples et amènent dès lors à retenir certains risques plutôt que d'autres en fonction des règles qui sont définies.

Enfin, les organisations se distinguent dans leur approche par la nature des événements qu'elles prennent en compte lors de l'élaboration de la cartographie. Pour certaines d'entre elles, les risques ont pour origine les facteurs internes à l'organisation alors que pour d'autres il s'agit principalement de facteurs externes. La nature des risques sera de surcroît sensiblement différente selon les approches retenues.

Le résultat de la cartographie des risques est conditionné par les modes d'observation qui sont

mis en œuvre et des variables associées (niveau organisationnel interrogé, horizon de temps considéré, outils de collecte, modalité d'évaluation, origine des événements). De surcroît, l'accès à l'univers des risques ne peut être que partiel et dépend des approches méthodologiques retenues. La question qui se pose dès lors est de savoir dans quelle mesure l'approche retenue par l'audit permet de compléter cette vision partielle des risques.

Le processus d'élaboration du plan d'audit tel que décrit par les directeurs de l'audit met en évidence qu'il est bâti à partir de la prise en compte de certains risques de la cartographie mais également à partir d'autres sources de risque.

Les risques considérés par les auditeurs se rapportent à des processus d'entreprise et se distinguent des risques de la cartographie qui peuvent pour certains avoir comme origine des facteurs externes à l'organisation. Les risques ne sont donc pas appréhendés de la même manière par les opérationnels et les auditeurs internes.

Les auditeurs se basent pour le plan d'audit sur les risques qui sont en lien avec les processus internes à l'organisation qui sont considérés comme étant tous porteurs de risques. Les risques appréhendés par l'audit sont les risques inhérents aux activités réalisées, c'est-à-dire qui sont indissociables des activités. Le risque d'avoir des produits périmés est inhérent à l'activité de la grande distribution tout comme le risque d'avoir des pannes de machine est inhérent à l'activité de production pour une usine.

Puisque les risques inhérents découlent directement des activités, l'audit recense les entités, les métiers, les activités, les processus et sous-processus qui existent au sein de son organisation. Une fois ce travail réalisé, il peut rattacher aux différentes entités de son organisation des risques inhérents en lien avec leurs activités et donc leurs processus. Ce travail d'inventaire constitue l'univers d'audit.

Le risque inhérent est considéré comme un événement pouvant avoir des conséquences négatives sur les processus et donc sur l'atteinte des objectifs de l'organisation. Dès lors qu'il est inhérent à une activité, il devient possible. Il n'est pas appréhendé comme dans la cartographie des risques de façon quantitative en termes d'impact ou de probabilité mais comme une source de dysfonctionnement potentielle.

En complément de cette approche processuelle mis en œuvre par l'audit pour déterminer les risques inhérents, le plan d'audit se fonde aussi sur les risques de la cartographie. De nouveaux,

l'audit s'attache à établir un lien entre les risques de la cartographie et des processus de l'organisation qui constitueront les objets d'audit.

L'audit utilise des critères spécifiques qui nous informent sur la manière dont l'audit appréhende le risque. Dans le cas par exemple des changements organisationnels qui interviennent, l'audit considère qu'ils sont de nature à pouvoir générer des dysfonctionnements faute de réviser et d'adapter les dispositifs de contrôle existants. Un processus qui évolue sans adapter les dispositifs de contrôle interne est source de nouveaux risques inhérents.

Enfin, l'audit est amené à exclure de son plan d'audit certains risques de la cartographie. Parmi les différents critères d'exclusion, le critère d'auditabilité peut être retenu. L'audit considère en effet que certains risques ne sont pas auditables, Il est ainsi possible d'avoir un risque évalué comme important au niveau de la cartographie et qui est exclu du plan d'audit s'il est considéré comme non auditable.

- *Les causes potentielles de l'écart entre univers des risques et univers d'audit*

Notre cadre d'analyse et les principaux concepts mobilisés par Luhmann (1993, 1995) apportent un éclairage particulièrement riche pour étudier les pratiques d'audit interne. Il permet notamment de mieux comprendre l'écart entre l'univers des risques et l'univers d'audit.

La première explication de cet écart est l'absence de distinction entre les risques et les dangers. Les entretiens réalisés avec les directeurs d'audit montrent que la distinction risque/danger est absente des approches mises en œuvre dans le cadre des processus de cartographie des risques. Pour certains les risques sont liés principalement aux dysfonctionnements internes alors que pour d'autres, ce sont les éléments externes à l'organisation qui constituent des risques. Dès lors, les organisations concernées sont amenées à établir des cartographies des risques qui peuvent inclure aussi bien des risques que des dangers sans opérer de distinction entre ces deux notions. Or, certains dangers qui sont qualifiés de risque dans les cartographies des risques sont exclus du plan d'audit par les auditeurs internes qui les considèrent comme des objets non auditables. Les facteurs externes sont aux dires des directeurs de l'audit plus difficiles à auditer dès lors qu'ils ne sont pas couverts par des processus, d'où la décision de les exclure du plan d'audit.

La seconde explication est que l'audit interne représente un sous-système social au sens de Luhmann qui dispose de sa propre sémantique et de ses modes opératoires. L'audit interne en tant que sous-système social couvre partiellement les risques de la cartographie qu'il perçoit comme des « bruits » externes et qu'il observe avec ses propres codes afin de pouvoir les

traduire en mission d'audit. Cette difficulté résulte en partie du fait que l'audit ne dispose pas des codes de communication des autres sous-systèmes au sein de l'organisation. L'absence de code de communication commun explique en partie l'écart entre l'univers d'audit et l'univers des risques. Les objets de risque considérés par l'audit portent non pas sur tous les risques mais uniquement sur ceux qui correspondent à ses codes de communication. C'est d'ailleurs pour cette raison que les risques de la cartographie sont rattachés à des processus et des risques inhérents que l'audit connaît et que d'autres sont exclus en étant considérés comme non auditables.

La troisième explication est que l'audit est un observateur de second ordre au sens de Luhmann. La méthodologie d'audit repose sur plusieurs actions qui confèrent à l'audit interne une position d'observateur de second ordre. Les auditeurs n'observent pas directement les risques mais demandent à ceux qui sont en charge de les gérer aux différents niveaux organisationnels. Puisque les risques ne sont pas les mêmes en fonction du point d'observation, les auditeurs interrogent à la fois le management et les différents membres de l'organisation. En procédant ainsi, l'audit est en mesure d'identifier les risques retenus au sein de chacun des sous-systèmes sociaux de l'organisation et les points aveugles qui en découlent. Les points aveugles portent notamment sur les conséquences des décisions prises au sein d'un sous-système sur les autres sous-systèmes. Ces conséquences ne sont pas appréhendées dès lors que chaque sous-système observe avec ses propres codes. L'audit procède en pratique par recoupement lorsqu'il interroge les différents niveaux de l'organisation.

L'explication de l'écart entre univers des risques et univers d'audit est liée à la dimension temporelle. L'existence de temporalités multiples au sein de l'organisation en fonction du niveau organisationnel interrogé et donc les sous-systèmes sociaux.

- *Le processus d'auditabilité*

Selon Power (1999), contrairement à l'image officielle de l'audit souvent présenté comme une activité neutre, l'audit met en œuvre un processus actif qui vise à « rendre les choses auditables ». La négociation d'une base de connaissance légitimé et institutionnalisé ainsi que la création d'un environnement qui est réceptif à cette base de connaissance sont nécessaires. Toutefois, Power ne décrit pas comment l'audit procède pour rendre les objets de risque auditables. La description du processus d'auditabilité, c'est-à-dire de transformation des risques en risques auditables, constitue la deuxième principale contribution de cette thèse.

Les auditeurs considèrent que tous les risques ne sont pas auditables ou bien qu'ils le sont mais

partiellement. Le critère d'auditabilité se traduit de différentes façons avec néanmoins un certain nombre de points communs.

Tout d'abord, les directeurs de l'audit illustrent leurs difficultés pour passer des risques de la cartographie aux missions du plan d'audit tout d'abord par le faible niveau de description des risques dans la cartographie. De surcroît, les risques de la cartographie ne font pas toujours référence à des processus. Or, l'audit appréhende les risques par une approche processuelle.

La deuxième caractéristique associée à un risque qualifié de non auditable concerne l'origine des événements qui sont qualifiés comme étant des risques. Lors de l'élaboration des cartographies des risques, certains éléments sont qualifiés comme étant des risques alors qu'il s'agit de danger au sens de Luhmann (1993). De surcroît, il s'agit de facteurs externes pour lesquels il n'existe pas toujours de processus identifiables. Lorsque des processus existent pour minimiser les impacts liés à la survenance d'un danger, la couverture ne peut être que partielle. Tout comme les dangers, les risques identifiés dans la cartographie qui ne sont pas couverts par des dispositifs de maîtrise destinés à en minimiser les effets sont jugés comme étant difficiles à auditer.

Enfin, certains risques de la cartographie sont considérés comme difficiles à auditer du fait de l'absence de compétence au sein de l'équipe d'audit. Au sens de Luhmann (1993), les auditeurs jugent que certains risques ne sont pas auditables dès lors qu'ils ne rentrent pas dans leurs codes de communication.

Malgré ces difficultés, l'audit parvient à traiter des risques de la cartographie en mettant en œuvre un processus spécifique de transformation des risques pour les rendre auditables.

Power (1999) décrit dans sa théorie sur la société de l'audit comment l'audit contribue pour donner à une organisation l'illusion de la transparence de ses activités. Le paradoxe décrit par l'auteur est que ce qui est considéré comme pouvant être le défaut de l'audit, à savoir le fait qu'il ne détecte pas un dysfonctionnement ou une faiblesse renforce sa position et sa prise sur le fonctionnement même de l'organisation. Selon l'auteur, en tant que telle, une entreprise ne peut être soumise à un audit : seuls les systèmes laissant une trace publique de ses activités le peuvent. Dès lors, pour que l'audit soit en mesure d'évaluer et de vérifier, il faut rendre les choses auditables. L'audit, qui déclare réaliser une observation neutre et objective des activités influe en réalité sur celle-ci. Ce qui devient officiellement visible aux yeux du public est alors considéré et reconnu comme étant important. À l'inverse, les activités et les pratiques privées

de cette visibilité ont un problème de légitimité, ce qui occasionne un transfert des ressources et des énergies vers les activités "auditables".

L'auditabilité n'est pas une propriété naturelle des opérations ni fonction non plus de la qualité des preuves qui existent dans l'environnement dans lequel l'audit opère. Au contraire, l'audit construit activement la légitimité de sa propre base de connaissances et cherche à créer un environnement favorable pour rendre celle-ci efficace. Les techniques de l'audit font partie de cette base de connaissance qui doit répondre à un impératif : rendre les objets auditables. Toutefois, l'auteur ne décrit pas comment l'audit procède pour y parvenir. Cette recherche permet d'améliorer les connaissances sur cette question (tel que décrit dans le cinquième chapitre).

Le risque une fois identifié dans le cadre du processus de gestion des risques est en principe adressé par le management qui peut décider soit de l'accepter en l'état ou bien de le réduire par la mise en place de dispositif de contrôle interne. L'audit considère qu'il doit pouvoir s'appuyer sur des éléments vérifiables pour établir son opinion d'audit. C'est la raison pour laquelle il considère qu'un risque identifié en tant que tel mais qui ne fait pas l'objet d'un plan d'actions ou d'un dispositif de contrôle interne est difficile à auditer. L'auditabilité est ainsi liée à la notion de vérifiabilité. Un risque qui est considéré comme non auditable le devient dès lors que l'audit dispose pour ce même risque d'un plan d'actions formel établi par le management pour le traiter. Dans une telle situation, l'audit n'évalue pas le risque en soi mais le plan d'actions destiné à le traiter. Le processus de transformation mis en œuvre par l'audit consiste à considérer qu'auditer le plan d'actions permet indirectement d'auditer le risque auquel il est associé. Le plan d'actions constitue dès lors l'objet auditable auquel se raccroche l'audit.

Parmi les options de traitement possibles face à un risque, le management peut décider de le partager (assurance, partenariat, ...) ou bien de le réduire en mettant de place des dispositifs de contrôle interne. Les dispositifs de contrôle interne représentent l'ensemble des dispositifs de maîtrise d'un risque qui sont déployés au sein d'une organisation. Le plan d'actions est l'étape préalable à la mise en place de ces dispositifs de maîtrise.

Une fois ces dispositifs définis, l'audit peut aller au-delà de la simple évaluation du plan d'actions qui avait été initialement établi et s'appuyer sur de nouveaux objets auditables. Dans ce cas, les objets auditables ne sont plus les plans d'actions mais les dispositifs de contrôle interne qui ont été déployés à l'issue du plan d'actions. Le processus de transformation mis en œuvre par l'audit consiste à considérer qu'auditer les dispositifs de contrôle interne liés à des

processus sous-jacents à un risque permettent indirectement d'auditer le risque auquel ils sont associés implicitement par l'audit. L'audit parvient ainsi à établir un lien entre les conséquences d'un risque et des décisions prises pour les maîtriser.

L'audit peut être confronté à des difficultés pour apprécier la qualité de certains dispositifs de contrôle interne et réussir à émettre une opinion sur leurs robustesses. Pour pallier ces difficultés, les auditeurs internes peuvent alors recourir à une procédure spécifique qui vise à construire ce qu'ils nomment un référentiel de contrôle interne. Afin d'établir ce référentiel, l'auditeur se fait décrire les processus dont les managers sont en charge, les risques associés aux processus et les contrôles nécessaires pour y faire face. Une fois le référentiel de contrôle interne établi, l'audit est en mesure d'apprécier l'écart entre les pratiques effectives constatées dans le cadre de ses missions et les principes de bonne gestion du risque issus du référentiel.

Un moyen pour l'audit de les faire appliquer par le plus grand nombre au sein de l'organisation est de s'appuyer sur la mise en place d'un système d'auto-évaluation du contrôle interne. Dès lors que l'audit interne construit le processus d'auto-évaluation du contrôle interne en lien avec son référentiel de contrôle interne, il lui donne un caractère prescriptif qui oblige les entités de son organisation à s'y conformer. Le système d'auto-évaluation permet à l'audit de transformer les risques de son organisation en traitant des risques de contrôle interne au travers des questionnaires d'auto-évaluation du contrôle interne.

Les résultats de cette recherche décrivent les différentes dimensions techniques que peut revêtir le processus d'auditabilité. Néanmoins, il est essentiel de comprendre qu'il présente des enjeux qui vont au-delà d'un simple problème technique et qui sont d'ordre sociétal. L'activité d'audit n'est pas neutre sur la construction des objets de risque au sein des organisations. L'audit façonne au sein de son organisation la manière de voir les risques des autres membres et va au-delà en désignant les risques qui sont importants et cela peut-être même au détriment d'autres risques ou menaces qui pourraient être plus graves.

- *Le lien entre audit interne et gouvernance*

L'écart constaté entre l'univers d'audit et l'univers des risques ainsi que le processus d'auditabilité ont des conséquences sur le rôle et l'efficacité de l'audit interne dans le dispositif de gouvernance ainsi que sur les critères pour apprécier la qualité de l'audit.

La littérature sur l'audit interne s'est particulièrement développée ces dernières années et les travaux montrent que l'audit interne représente une des composantes clés du dispositif de

gouvernance. Un courant relativement récent s'intéresse au positionnement et au rôle de l'audit interne dans le dispositif de gouvernance.

Selon les normes d'audit interne, l'indépendance de l'audit est une condition nécessaire pour assurer son efficacité. Elle préconise à ce titre un double rattachement de l'audit interne dans lequel l'audit reporte fonctionnellement au comité d'audit et hiérarchiquement au management de l'organisation. Cette règle est considérée comme une pratique qui permet d'assurer le niveau d'indépendance nécessaire afin que l'audit puisse remplir son rôle de façon efficace. L'indépendance est, selon les directeurs de l'audit, permise par le fait de ne pas être impliqué dans les opérations et d'être rattaché au plus haut niveau de l'organisation.

Lenz et Sarens (2012) avancent l'idée que le positionnement de l'audit tel que préconisé dans les normes pose problème. Le double rattachement de l'audit préconisé par les normes d'audit ainsi que leur volonté de prendre en charge à la fois des services d'assurance et de conseil pour évaluer les processus de gestion des risques, de gouvernance et de contrôle présente des difficultés. Le fait que l'audit cherche à remplir plusieurs rôles à la fois et ce pour beaucoup de personnes en même temps génère un certain flou sur le niveau auquel il s'adresse et sur ce qu'il doit fournir comme service. Les auditeurs proposent d'un côté un service d'assurance au comité d'audit et de l'autre ils se positionnent comme étant un « *business partner* » en offrant au management un service de conseil. Les auteurs suggèrent que pour améliorer le positionnement de l'audit interne dans le dispositif de gouvernance, il est nécessaire de clarifier envers qui l'audit doit véritablement rendre compte et se concentrer en priorité sur les services d'assurance.

La distinction risque/danger établie par Luhmann (1993) a une implication forte sur les pratiques d'audit interne dès lors que nous cherchons à répondre à la question suivante : « *l'audit interne évalue les risques pour qui ?* ». Or, pour Luhmann les risques des uns ne sont pas les risques des autres. Dans cette perspective, les risques des actionnaires ne sont pas les mêmes que ceux de la direction générale et du management.

Ce problème est aussi soulevé par Power (2009) qui juge que le concept d'appétence au risque tel que développé dans le modèle de l'*Entreprise Risk Management* est contestable. L'appétence au risque y est décrite comme une notion unique et homogène pour l'ensemble de l'organisation et qu'il est possible de la déterminer sans ambiguïté. Cette conception de l'appétence au risque exclut l'existence de conflits d'intérêts entre les différents types et niveaux d'appétence. Les travaux de Lenz et Sarrens (2012) confirment la nécessité de clarifier le rôle et le positionnement de l'audit interne et combien il est nécessaire de préciser envers qui

l'audit doit véritablement rendre compte.

Nos données permettent de soulever une autre question sur le rôle que devrait jouer le comité d'audit en matière de supervision des activités d'audit et les moyens dont il devrait disposer pour pouvoir le faire de façon efficace. Les directeurs de l'audit déclarent que les membres des comités d'audit expriment rarement des demandes auprès de l'audit et certains vont au-delà en s'interrogeant sur la capacité de ces membres à poser les « bonnes » questions.

L'indépendance de l'audit qui repose selon les normes d'audit sur le double rattachement de l'audit au management puis au comité d'audit apparaît comme une condition nécessaire mais non suffisante. Notre recherche confirme la nécessité de clarifier le positionnement et le rôle de l'audit comme le préconise Lenz et Sarrens (2012) mais d'aller au-delà en précisant aussi le rôle et les moyens dont doivent disposer les comités d'audit et les instances de gouvernance.

- *La qualité de l'audit*

Il n'existe pas aujourd'hui de consensus selon DeFond et Zhang (2014) sur ce qui pourrait constituer le bon critère de mesure de la qualité de l'audit. Pour Peecher et al. (2013) la perception de la qualité de l'audit varie en fonction des parties prenantes. Lenz et Sarens (2012) considèrent que l'audit interne dans sa configuration actuelle peut difficilement satisfaire tout le monde et qu'il est nécessaire de clarifier son rôle et son positionnement. Selon Roussy et Brivot (2016), la revue de la littérature montre que la qualité de l'audit interne a été essentiellement traitée sous l'angle des auditeurs externes et de leurs appréciations fondées principalement sur les attributs des auditeurs (indépendance et compétence). Les travaux existants abordent la qualité de l'audit principalement du point de vue des attributs de l'audit, à savoir son indépendance et sa compétence. Ils ne traitent pas de la pratique de l'audit interne au regard de la question du risque au niveau des organisations qui en constitue pourtant le fondement.

Le processus d'auditabilité montre que le processus mis en œuvre par les auditeurs pour rendre les risques auditables pose une question fondamentale quant à ses conséquences sur la qualité des observations réalisées par l'audit. Pour que leurs observations soient de qualité, elles doivent être objectives selon les normes d'audit qui rappelle qu'il s'agit d'un des principaux critères d'efficacité de l'audit.

La distinction introduite par Luhmann (1993) entre observation de premier ordre et observation de second ordre nous amène à nous interroger sur la pratique de l'audit du point de vue notamment de la méthodologie qu'il met en œuvre pour lui assurer cette objectivité nécessaire.

Dès lors la question qui se pose est de savoir dans quelle mesure la méthodologie d'audit permet à l'auditeur interne d'être un observateur de second ordre pertinent dont le jugement n'est pas altéré par celui d'un observateur de premier ordre.

L'auditeur interne peut être un observateur de second ordre pertinent au sens de Luhmann (1993) grâce à la méthodologie qu'il met en œuvre sous certaines conditions. L'une des principales conditions est que les auditeurs n'observent pas directement les risques mais évaluent comment les managers identifient eux-mêmes les risques. Pour cela il doit les interroger pour être en mesure d'apprécier comment ces derniers observent les risques et ceux qu'ils ne voient pas.

Toutefois, le processus d'auditabilité décrit précédemment est de nature à altérer cette position d'observation de second ordre. Dès lors que l'audit fonde ses contrôles sur des risques et des dispositifs décrits par les managers sans les remettre en cause, l'auditeur perd le bénéfice de sa position d'observateur de second ordre. Pour faire le lien avec les normes, l'audit subalterne son jugement professionnel à celui des managers en procédant ainsi.

Le fait d'établir des référentiels de contrôle interne sur la base des risques tels qu'ils sont appréhendés par les managers sans chercher à avoir un regard critique maintient aussi l'audit dans un simple position d'observation de premier ordre. L'audit n'observe pas la manière dont les managers observent et ce qu'ils ne voient pas. Par ce procédé, l'audit duplique le mode d'observation des managers et est soumis aux mêmes points aveugles. La standardisation des programmes de travail de l'audit est de nature à altérer la position d'observation de second ordre des auditeurs.

Enfin, l'écart constaté entre l'univers d'audit et l'univers des risques a aussi des implications fortes sur l'appréciation de la qualité de l'audit. Les processus de cartographie des risques ainsi que d'élaboration du plan d'audit peuvent être menés selon différentes approches et suivant l'approche qui sera retenue, les personnes interrogées ne sont pas les mêmes. La distinction risque/danger introduite par Luhmann (1993) pour définir le concept de risque est éclairante pour comprendre qu'il n'est pas possible d'évaluer le risque sans préciser au préalable en fonction de qui et ce malgré que les conditions d'indépendance soient remplies. La littérature la perception de la qualité de l'audit varie en fonction des parties prenantes. Cette question a été abordée dans la partie gouvernance et montre que l'audit souffre d'un manque de clarté sur son rôle ainsi que sur son positionnement.

Ce travail de recherche est structuré en cinq chapitres qui sont présentés à la page suivante.

Figure 1. Le plan général de la thèse

INTRODUCTION

CHAPITRE 1 : REVUE DE LA LITTERATURE

- L’audit comme activité normée
- L’audit dans le dispositif de gouvernance
- L’audit interne et les risques
- La qualité de l’audit interne

CHAPITRE 2 : CADRE THEORIQUE

- Le risque comme construit social
- Le cadre d’analyse retenu et les questions de recherche

CHAPITRE 3 : METHODOLOGIE

- Stratégie de recherche appliquée
- Approche méthodologique
- Considérations éthiques

CHAPITRE 4 : PRESENTATION DES DONNEES

- Le processus de cartographie des risques
- L’élaboration du plan d’audit
- L’élaboration du plan de mission

CHAPITRE 5 : CONTRIBUTIONS

- L’écart entre univers des risques et univers d’audit
- Le processus d’auditabilité
- Les conséquences sur la qualité de l’audit et le lien entre audit interne et gouvernance

CONCLUSION

1^{er} CHAPITRE : REVUE DE LA LITTÉRATURE

Ce premier chapitre propose une revue de la littérature sur le thème de l'audit interne au regard de son nouveau rôle en matière d'évaluation et d'appréciation des processus de gestion des risques.

L'objet de ce chapitre vise à établir une revue des principaux travaux qui portent sur le thème de l'audit interne et à voir dans quelle mesure ils traitent de l'audit interne sous le prisme du risque. L'objectif est d'apprécier de quelle manière les travaux existants abordent le thème de l'audit interne sous le prisme de son nouveau rôle relatif à l'évaluation des dispositifs de gestion des risques.

Nous tenterons d'établir dans ce chapitre une synthèse des principaux écrits relatifs à l'audit interne au travers des quatre parties suivantes :

- l'audit interne et les normes professionnelles ;
- l'audit interne dans le dispositif de gouvernance ;
- l'audit interne et l'approche par les risques ;
- la qualité de l'audit interne et les critères pour son évaluation.

1 - 1 L'AUDIT INTERNE : UNE ACTIVITE NORMEE

Un auditeur est avant tout un individu à l'écoute d'informations (le mot « audit » a d'ailleurs pour racine le verbe latin « *audire* » : écouter). Mais il ne suffit pas de collecter des informations pour faire un audit. Il faut aussi les traiter, les analyser et en faire la synthèse pour en définitive prendre la mesure d'une situation. Effectuer un audit consiste à rendre intelligible une information qui a priori ne l'est pas.

Un audit peut être « interne » ou « externe ». Il peut être « de certification », « de performance », « opérationnel » ou « de stratégie ». Il peut porter sur des questions environnementales, sociales, industrielles, économiques, comptables ou financières. Il peut être réalisé dans un laps de temps très court ou mobiliser des équipes nombreuses pendant plusieurs semaines. Il n'existe pas qu'une seule façon de faire de l'audit et les sujets susceptibles d'être audités sont variés. Mais tout rapport écrit n'est pas pour autant un rapport d'audit.

Avant de définir de façon plus précise ce qu'est l'audit interne en particulier, il est important de rappeler au préalable que cette activité a évolué au regard des missions et responsabilités qui lui ont été assignées au fil des années.

Nous traiterons dans un premier temps de l'histoire de l'audit interne et de son évolution jusqu'à l'émergence d'une profession. Nous approfondirons ensuite les normes professionnelles qui ont été établies pour encadrer la pratique de cette activité dite « professionnelle » pour réaliser une revue approfondie de son contenu.

1 - 1 1 L'HISTORIQUE INSTITUTIONNEL DE L'AUDIT INTERNE

L'évolution de l'audit interne est étroitement liée à plusieurs facteurs dont notamment l'influence de l'*Institute of Internal Auditors* (IIA) ainsi que la réglementation en matière de gouvernance et de sécurité financière des entreprises cotées.

1 - 1 1 1 L'INSTITUT DES AUDITEURS INTERNES

L'histoire communément admise quant à l'origine de cette fonction est qu'elle découle de l'audit financier et de conformité. Son champ d'intervention aurait été élargi à des domaines beaucoup plus large que l'audit financier afin de répondre à une difficulté nouvelle des managers pour mieux appréhender leur environnement devenu beaucoup plus complexe (Ramamoorti, 2003).

Toutefois, avant de retracer cette évolution de la fonction d'audit interne, il est important de présenter l'*Institute of Internal Auditors* (IIA) ou Institut des Auditeurs et d'expliquer le rôle qu'il a pu jouer dans le développement de l'activité d'audit interne.

Cet institut a été créé au début de la seconde guerre mondiale, en 1941, par trois membres fondateurs qui sont Victor Brink, John Thurston et Robert Milne. Ils se sont tous les trois réunis autour d'un projet commun : promouvoir et de développer l'activité d'audit interne pour en faire une profession reconnue.

C'est tout d'abord en 1947 que l'IIA a établi le premier document officiel intitulé « Déclaration des responsabilités de l'audit interne » afin de préciser les rôles et responsabilités de l'audit interne et son champ d'action. Cette déclaration, votée au conseil d'administration de l'IIA le 15 juillet 1947, a ainsi été publiée dans le numéro du mois de septembre de la revue trimestrielle « *Internal Auditor* ».

Puis, progressivement, l’IIA a continué à œuvrer pour la promotion de l’activité d’audit interne tant par ses actions destinées à sa professionnalisation (élaboration de normes internationales pour la pratique professionnelle de l’audit interne, d’un code éthique et même d’un certificat diplômant d’auditeur Interne) que par des liens qu’il a pu établir avec d’autres organismes et professions pour mieux légitimer sa position.

L’*Institute of Internal Auditors* (IIA) ou Institut des Auditeurs Internes est aujourd’hui devenue une association professionnelle qui regroupe plus de 170.000 membres à travers le monde. Des organismes affiliés à l’IIA ont aussi été créés au niveau des pays tel l’« *Institut Français de l’Audit et du Contrôle Interne* » (l’IFACI) en France pour être le porte-parole de l’IIA. Certains de ces organismes se sont regroupés au niveau régional avec notamment la « *European Confederation of Institutes of Internal Auditors* » (l’ECIIA).

Ainsi, l’IIA entretient des liens étroits avec d’autres organismes normalisateurs tels que l’« *International Federation of Accountants* » (l’IFAC) qui est en charge d’établir les standards en matière d’audit légal. Ces liens ont notamment permis de clarifier les rôles respectifs entre les auditeurs internes et les auditeurs légaux, tout en mettant en relief leur complémentarité. Les standards d’audit légal précisent à cet effet que les auditeurs externes peuvent utiliser les travaux des auditeurs internes après avoir évalué la qualité de l’audit interne.

L’IIA est par ailleurs membre du COSO (« *COmmittee of Sponsoring and Organization* »), comité spécialisé en charge de définir les référentiels en matière de contrôle interne et de gestion des risques, plus connus sous le nom des modèles du « COSO I » et « COSO II ». Il est important de rappeler que ces référentiels constituent des éléments essentiels auxquels se réfèrent de nombreuses réglementations financières, votées depuis le début des années deux mille, destinées à restaurer la crise de confiance des investisseurs suite aux scandales financiers ainsi qu’à la crise financière de 2008.

La présence de l’IIA au sein d’un des principaux organismes en matière de normalisation du contrôle interne et du processus de gestion des risques comme le COSO n’est pas neutre dès lors que les normes d’audit interne s’y réfèrent pour définir l’objet même de l’audit. Nous y reviendrons de façon plus détaillée dans la dernière partie de ce sous-chapitre.

Ces éléments nous permettent de comprendre comment cette fonction s’est progressivement institutionnalisée au fil des dernières décennies grâce à la fois aux actions menées depuis plusieurs années par l’IIA et aux facteurs externes telles que la réglementation (Carcello, 2005).

Au-delà du rôle qu'a pu jouer l'IIA, il est important de comprendre dans quelle mesure les éléments liés au contexte institutionnel et/ou réglementaire peuvent expliquer l'existence et/ou la nature des travaux d'audit interne. Nous pouvons identifier plusieurs changements institutionnels ou réglementaires qui ont pu avoir une influence sur l'activité des auditeurs internes. Parmi ces changements, nous pouvons notamment souligner quelques-unes de ces initiatives.

Le « *Foreign Corrupt Practices Act* » (1977).

A l'issue de l'enquête sur l'affaire du Watergate ainsi que plusieurs affaires de corruption mises en évidence durant les années 70, une loi fédérale anti-corruption a été votée : le « *Foreign Corrupt Practices Act* » (FCPA, 1977). Chaque société doit maintenir un système de contrôle interne comptable et financier ainsi qu'une méthode pour l'évaluer et le piloter. L'audit interne s'est ainsi positionné pour endosser une nouvelle responsabilité afin de répondre aux exigences du FCPA au sein de son organisation : évaluer les systèmes de contrôle interne en vue d'avoir l'assurance de bien respecter les exigences de la loi anti-corruption. Les auditeurs internes ont ainsi vu leur rôle s'accroître pour répondre au besoin du management de se conformer à la loi. Le nombre d'auditeurs internes a ainsi augmenté à la suite du vote de cette loi (Flesher, 1991).

La loi « *Sarbanes-Oxley Act* » (2002).

Suite aux scandales financiers, cette loi exige que les sociétés cotées établissent un rapport sur leur système de contrôle interne et que les dirigeants des sociétés concernées dévoilent les éventuelles faiblesses en matière de contrôle interne. Ainsi, cette loi exige des dirigeants qu'ils évaluent leur contrôle interne et communiquent sur son niveau d'efficacité. Cette même loi prévoit de lourdes sanctions pénales en cas d'omission des dirigeants de sociétés dans le rapport qu'ils établissent. Même si la loi ne fait pas référence directement au rôle de l'audit interne, celle-ci a eu des conséquences sur le développement de l'audit interne qui a joué un rôle significatif pour permettre au management des organisations de se conformer aux exigences de la loi en évaluant l'efficacité de leurs systèmes de contrôle interne comptables et financiers (Rittenberg et al., 2005).

Les exigences du NYSE (2004).

Suite aux scandales financiers (Enron, Worldcom, ...), le New York Stock Exchange (NYSE) a fait évoluer son code de gouvernance et ses règlements. Ainsi, selon les nouvelles exigences,

toute société cotée sur le marché du NYSE doit disposer d'un service d'audit interne qui doit notamment rapporter au Comité d'Audit pour remplir pleinement sa mission.

Le « Dodd-Frank Act » (2010)

Cette loi votée à la suite de crise des sub-primés de 2008 est présentée comme la plus vaste réforme financière depuis le *Glass Steagall Act*, établi en 1933 et aboli en 1999. Elle a vocation à promouvoir la stabilité financière aux Etats-Unis, à limiter l'aléa moral inhérent au caractère « *too big to fail* » de certaines institutions financières et à protéger les contribuables et les consommateurs de produits financiers. Elle a également pour ambition d'améliorer la transparence et le contrôle des institutions financières concernées.

La réforme de Bale 3 (2010)

Cette réforme (*Basel III, A global regulatory framework for more resilient banks and banking systems, 2010*) constitue la réponse du Comité de Bâle à la crise financière et vise notamment à renforcer le niveau et la qualité des fonds propres, mettre en place un ratio de levier, améliorer la gestion du risque de liquidité, etc. Elle vient compléter une première série d'amendements à l'accord de Bâle II intervenus en juillet 2009.

L'ensemble de ces évolutions conduisent à s'interroger sur la définition de l'audit interne.

1 - 1 1 3 NOUVELLE DEFINITION DE L'AUDIT INTERNE

Selon Ramamoorti (2003), La première définition officielle de l'audit interne a été établie par l'Institut des Auditeurs Internes en 1947 dans un document intitulé « Déclaration des responsabilités de l'audit interne ». Ce document qui précisait les objectifs et le champ d'action de l'audit interne a été publié au mois de septembre dans la revue trimestrielle *Internal Auditor* de l'Institut des Auditeurs Internes.

L'activité autrefois cantonnée essentiellement aux opérations comptables et financières a fortement évolué depuis les années cinquante. La définition de l'audit interne a ainsi été révisée à plusieurs reprises (1957, 1971, 1981, 1990) par l'IIA afin de traduire l'évolution des rôles et responsabilités assignées à l'activité d'audit interne au fil du temps.

A la lecture des différentes versions qui ont été publiées, nous pouvons identifier trois périodes distinctes pour ce qui concerne les missions et responsabilités des auditeurs internes telles que définies par l'Institut des Auditeurs Internes. En 1947, l'accent était mis sur le fait que la priorité de l'audit interne était de traiter des sujets comptables et financiers. Ceci va dans la continuité

des pratiques jusqu'alors. En 1957, il était précisé que l'audit interne pouvait traiter tant des sujets comptables et financiers que des autres opérations (notion d'audit opérationnel mis en valeur par Victor Brink notamment). Il ne se limite ainsi plus aux activités comptables et financières et assure même un certain équilibre dans le traitement de ces deux domaines distincts. C'est finalement en 1971 que son champ d'intervention prend la forme actuelle, c'est-à-dire une fonction qui traite de l'ensemble des opérations au sein de l'organisation, réduisant ainsi le domaine financier à un type d'opération comme tous les autres.

La dernière définition de l'audit interne établie par l'Institut des Auditeurs Internes date du 29 juin 1999 et indique que « *L'Audit Interne est une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée. Il aide cette organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle, et de gouvernement d'entreprise, et en faisant des propositions pour renforcer leur efficacité* ».

Cette définition permet de clarifier les rôles et responsabilités de l'audit interne en matière d'évaluation des processus de gestion des risques et de contrôle interne. Il est important de souligner le fait que cette définition est avant tout un projet normatif, c'est-à-dire qu'il correspond à ce que l'audit interne « devrait être ». Cette définition traduit l'évolution du positionnement de l'audit interne souhaité par l'institut.

1 - 1 2 L'AUDIT INTERNE : L'EMERGENCE D'UNE PROFESSION ?

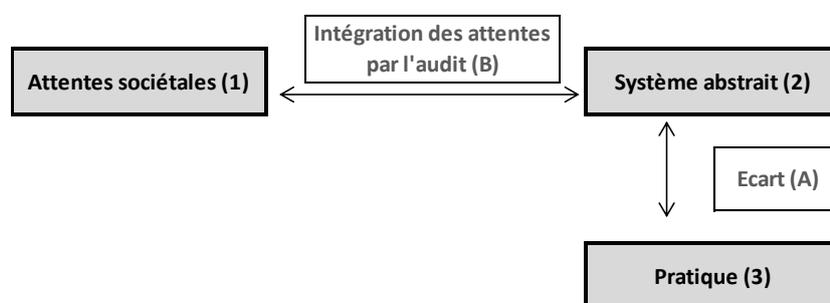
La théorie de la société de l'Audit de Michael Power (1999) complétée par la théorie du système des professions d'Andrew Abbott (1988) nous permet de mieux comprendre le développement et le nouveau positionnement de l'audit interne sur le thème de la gestion des risques.

1 - 1 2 1 LA SOCIÉTÉ DE L'AUDIT

La société de l'audit (Power, 1999) désigne le nombre croissant d'activités qui sont réalisés en se référant au « savoir abstrait » de l'audit. Power distingue ainsi d'une part le savoir abstrait (2) de la pratique concrète (3) de l'audit. L'audit est présenté comme une pratique objective pour répondre aux attentes sociétales (1). Or, selon Power, la pratique de l'audit reste « obscure » et n'exclut pas une dimension subjective : deux auditeurs peuvent aboutir à des

conclusions différentes sur un même objet audité. Ainsi, il existe un écart (A) entre le système abstrait de l'audit et sa pratique « obscure », tel que représenté dans le schéma ci-dessous.

Figure 2. Société de l'audit – représentation de l'audit en tant que pratique obscure



Lorsque de nouvelles demandes sont adressées à l'audit pour fournir de nouveaux types d'informations objectives, l'audit accepte d'y répondre en intégrant (B) ces nouvelles demandes dans son savoir abstrait. Power précise qu'un écart apparaît dès lors entre le savoir abstrait (réputé être reproductible et objectif) et sa pratique (idiosyncrasique et subjective) qui reste fondamentalement inchangée avec la mise en œuvre d'une succession d'étapes. Ainsi, un écart (A) se creuse entre le système abstrait de l'audit et sa pratique.

Comme le caractère « obscur » de l'audit est caché derrière son savoir abstrait, Power (1999) affirme qu'aucun non-auditeur n'est en mesure de vérifier l'étendue de cet écart. La profession d'audit peut dès lors poursuivre l'intégration de nouvelles demandes sociétales dans son savoir abstrait qui s'applique dès lors à un nombre sans cesse croissant de nouvelles activités qui mènent finalement à une société de l'audit.

Power souhaite attirer l'attention sur le décalage qui existe entre le système abstrait de l'audit et sa pratique réelle. Cet objectif a pour but d'aider la société à mieux décider de confier ou non de nouvelles missions à l'audit sur la base du potentiel réel limité et non pas de celui proclamé.

1 - 1 2 2 LE SYSTEME DES PROFESSIONS

Andrew Abbott (1998) considère qu'il n'existe pas un, mais plusieurs groupes professionnels susceptibles de recourir au mécanisme mis en lumière par Power pour s'approprier des activités. Cette appropriation, une fois réalisée, est appelée juridiction. Reformulée dans le langage d'Abbott, la société de l'audit signifie que le groupe professionnel des auditeurs possède un

nombre sans cesse croissant de juridictions dont l'audit interne fait partie. Abbott (1998) définit les groupes professionnels comme des groupes appliquant un savoir abstrait à des cas concrets : l'écart entre le caractère « fondamentalement obscur » des pratiques et leur représentation abstraite est, pour Abbott, précisément ce qui distingue les professions des autres groupes occupationnels.

Cet écart permet aux professions d'intégrer dans leur savoir abstrait différents problèmes humains (Abbott, 1998) et de revendiquer le droit exclusif de s'en charger. Pour y parvenir, les professions recourent à différents mécanismes rhétoriques tels que la réduction (reformulation d'un problème comme étant soluble par un savoir abstrait particulier), la métaphore (diffusion d'une façon de penser un problème selon le vocabulaire d'un savoir abstrait), le traitement (revendication de la capacité d'un savoir abstrait de résoudre des problèmes identifiés par d'autres). Le cadre normatif établi pour encadrer la pratique de l'audit interne correspond à ce savoir abstrait. La théorie des systèmes de professions nous apporte ainsi un éclairage différent sur l'intérêt des normes d'audit interne.

Les groupes professionnels déposent leurs différentes revendications devant trois auditoires : l'opinion publique, l'État et le lieu de travail. Abbott (1998) insiste sur le décalage entre les règlements juridictionnels sur ces différents auditoires. Ces auditoires apprécient les revendications selon leurs propres critères : alors que l'objectif du groupe professionnel est d'obtenir la responsabilité du problème à régler et les ressources matérielles et symboliques qui s'y rattachent, l'auditoire est censé vouloir voir le problème en question résolu.

Dès lors qu'une revendication répond aux intérêts d'un auditoire, une juridiction naît : une juridiction est la ratification par un auditoire de la compétence exclusive d'un savoir abstrait et de son dépositaire institutionnel à prendre soin du problème en question. Abbott distingue les situations pour lesquelles la juridiction est vacante, c'est-à-dire celles où aucun autre groupe ne se charge déjà d'aborder le problème dont il est question, de celles où la juridiction est occupée par un autre groupe concurrent. Dans le premier cas, les mécanismes mis en lumière par Power peuvent opérer. Dans l'autre cas, nous explique-t-il, des conditions supplémentaires doivent être remplies afin que s'opère un transfert juridictionnel. D'une part, le groupe revendicateur doit être enclin à déloger son concurrent (Abbott, 1998). C'est le cas lorsqu'un nouveau groupe est créé, lorsqu'un groupe existant perd des juridictions ou lorsqu'il a construit son savoir abstrait de façon à entrevoir de nouvelles applications possibles. D'autre part, le groupe

occupant doit détenir sa juridiction faiblement (Abbott, 1998), c'est-à-dire qu'il doit être perçu comme ayant échoué à résoudre le problème dont il avait la charge (Champy, 2009).

Enfin, à l'inverse de Power qui considère potentiellement comme infini l'écart entre le savoir abstrait et les pratiques concrètes, Abbott (1998) y pose une limite. Dès lors qu'un savoir trop abstrait (risque de déconnexion du travail réel) ou qu'un savoir trop concret (risque de marchandisation du savoir – (Abbott, 1998) est susceptible de permettre à un concurrent d'établir l'échec de l'occupant et de le déloger, il soutient que les groupes professionnels cherchent à se neutraliser à long terme, pour tendre vers une situation d'équilibre dans laquelle chaque groupe professionnel détient une seule juridiction qu'il est en mesure d'effectuer convenablement. Cette théorie peut expliquer le nouveau positionnement des auditeurs internes qui sont ainsi parvenus à prétendre pouvoir mieux remplir que leurs concurrents une attente sociétale particulière : maîtriser les risques au sein de notre société devenu trop complexe et incertaine.

Le cadre normatif de l'audit interne (code de déontologie, normes pour la pratique professionnelle, ...) que nous allons voir plus en détail dans cette partie représente ainsi le savoir abstrait sur lequel s'appuient les auditeurs internes pour s'appropriier et conserver leur « juridiction » au sens de Abbott (1998).

Ce cadre a notamment évolué depuis sa constitution par l'IIA en 1947 en réponse à la forte concurrence exercée par les cabinets d'audit qui ont cherché à se positionner sur les missions d'audit interne pour compléter leurs revenus liés aux missions légales (Covaleski et al., 2003).

1 - 1 3 LES NORMES POUR LA PRATIQUE PROFESSIONNELLE DE L'AUDIT INTERNE

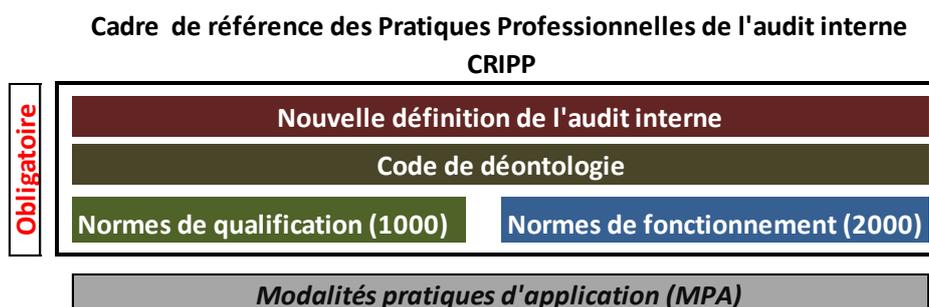
Les normes constituent un des éléments du savoir abstrait (Power, 1999) des auditeurs internes. Il est dès lors essentiel de voir plus en détail leur contenu.

1 - 1 3 1 INTRODUCTION AUX NORMES PROFESSIONNELLES DE L'AUDIT INTERNE

Le 1er janvier 2009, l'*International Professional Practices Framework* (IPPF) de l'*Institute of Internal Auditors* (IIA, 2014) est entré en vigueur. L'IPPF constitue la base fondamentale de la profession de l'audit interne et constitue une amélioration sensible du Professional Practice Framework (PPF). Il est le résultat d'études approfondies, de consultations et de délibérations concernant les principes de base de l'audit interne. L'IPPF qui a été traduit par l'IFACI (l'Institut Français de l'Audit et du Contrôle Interne, qui représente localement l'IIA en France), porte l'appellation de **Cadre de Référence International des Pratiques Professionnelles de l'Audit interne** (CRIPP).

Il comprend tout d'abord la nouvelle définition de l'audit interne, le code de déontologie qui décrit les règles minimales de conduite des auditeurs internes, des normes dites de qualification et enfin des normes dites de fonctionnement. Tous ces éléments sont des dispositions obligatoires pour les membres de l'IIA. Elles sont complétées par des Modalités Pratiques d'Application (MPA) et des guides pratiques.

Figure 3. Structure générale des normes professionnelles de l'audit interne



Le respect de la définition de l'audit interne, du code de déontologie et des normes IIA est obligatoire pour tous les membres de l'IIA. La prochaine section fournit une revue détaillée sur le contenu des normes d'audit interne.

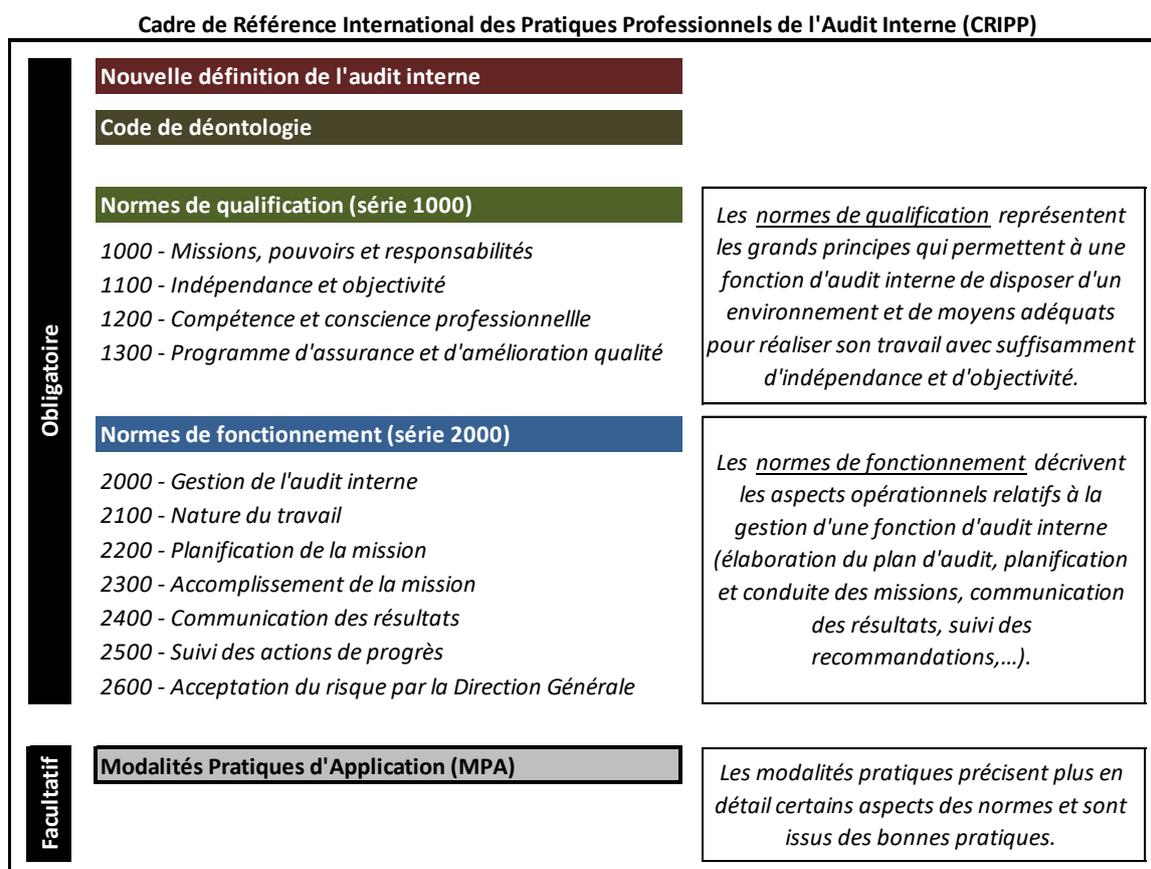
Il est dès le début de cette section de préciser que la revue détaillée de ces normes d'audit interne met en évidence un concept clé autour duquel s'articulent et se structurent les normes. Il s'agit du concept de « risque ». C'est élément qui apparaît tout d'abord dans la définition de l'audit interne qu'il est utile de rappeler : « *L'audit interne est une activité indépendante et objective qui aide l'organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de gouvernement d'entreprise, de management des risques et de contrôle, en faisant des propositions pour renforcer leur efficacité* » (IIA, 2014).

Cette définition souligne que l'objet même de l'audit interne est d'évaluer au sein des organisations les processus de gestion des risques et de contrôle. Nous allons voir dans cette section comment les normes sont structurées autour de ce concept de risque.

Comme nous l'avons introduit dans la section précédente, les normes sont constituées par la définition de l'audit interne, un code de déontologie et des normes dites de qualifications (série 1000) et des normes dites de fonctionnement (série 2000). Les normes de qualification (série 1000) précisent quels sont les grands principes à respecter pour que la fonction d'audit puisse disposer d'un environnement et de moyens adéquats pour réaliser son travail avec suffisamment d'indépendance et d'objectivité. Les normes de fonctionnement (série 2000) décrivent quant à elles tous les aspects opérationnels liés à la gestion d'un service d'audit interne et la réalisation de ses missions.

Le tableau de la page suivante récapitule l'ensemble des thématiques couvertes par les normes d'audit interne qui font partie du cadre de référence des pratiques professionnelles.

Figure 4. Structure détaillée des normes professionnelles de l'audit interne



Nous allons toutefois développer dans cette section les normes de fonctionnement qui traite du processus d'audit en tant que tel. Les normes sont établies dans un ordre qui est assez didactique puisqu'elles décrivent toutes les étapes d'un processus d'audit.

La norme 2000 précise que le « *le responsable de l'audit interne doit établir un plan d'audit fondé sur les risques afin de définir les priorités cohérentes avec les objectifs de l'organisation* » (IIA, 2014).

La norme 2100 décrit l'objet de l'audit interne et son champ d'intervention en précisant qu'il porte sur les processus de gestion des risques, de gouvernance et de contrôle interne : « *l'auditeur doit évaluer l'efficacité des processus de management des risques et contribuer à leur amélioration* » (IIA, 2014). Les missions d'audit du plan doivent donc contribuer à évaluer la robustesse des dispositifs de gestion des risques au sein de l'organisation. Une fois les missions d'audit planifiées et donc inscrites au plan d'audit, intervient la phase de réalisation.

La norme 2200 précise comment les auditeurs doivent préparer chacune des missions inscrites au plan d'audit. Cette norme exige notamment que : « *l'audit interne doit procéder à une évaluation préliminaire des risques liés à l'activité soumise à l'audit. Les objectifs de la mission doivent être déterminés en fonction des résultats de cette évaluation* » (IIA, 2014). Il s'agit dans les faits de déterminer sur un thème d'audit le périmètre et les thèmes qui devront être couverts par l'équipe d'audit au cours de la mission. Le choix du périmètre et des axes d'intervention devra découler encore une fois d'une analyse des risques qui vise à prioriser les choix. Le tableau ci-dessous reprend de façon plus synthétique les normes relatives à la planification des activités d'audit et à la nature de leur travail qui montre que le concept de risque est repris au sein de chacune des normes et qu'il constitue le cœur d'activité de l'audit interne.

La norme 2300 correspond à la phase de réalisation de la mission. Cette phase va consister à couvrir le périmètre qui aura été défini en amont durant la phase de préparation et à émettre une opinion à l'issue des travaux. Cette opinion d'audit devra être justifiée par un certain nombre de travaux en suivant un programme de travail qu'ils auront dû définir.

La norme 2400 concerne la communication des résultats à la fin de la mission. Cette communication prend la forme d'un rapport d'audit qui comprend à la fois des conclusions d'audit et des recommandations. Les recommandations visent à améliorer l'efficacité des processus de gestion des risques et des contrôles existants.

La norme 2500 « Suivi des actions de progrès » porte sur le suivi des plans d'actions établis par les unités auditées en réponses aux recommandations émises par l'audit à l'issue de leur mission.

Le tableau qui figure à la page suivante récapitule les normes relatives aux activités de planification des travaux de l'audit ainsi que la nature de son travail. La notion de risque est au cœur des normes d'audit interne comme l'illustre le contenu de ce tableau.

Tableau 1. Extrait des normes d’audit interne – Normes 2000, 2100 et 2200 (IIA, 2014)

Cadre de Référence International des Pratiques Professionnels de l’Audit Interne (CRIPP)			
Extrait des normes de fonctionnement (série 2000)			
	2000 – Gestion de la Direction de l’Audit	2100 – Nature du travail	2200 – Planification de la mission
NORMES OBLIGATOIRES	2010 – Le responsable de l’audit interne doit établir un plan d’audit fondé sur les risques afin de définir les priorités cohérentes avec les objectifs de l’organisation.	2120 – L’audit interne doit évaluer l’efficacité des processus de management des risques et contribuer à leur amélioration.	2210 – Les objectifs doivent être précisés pour chaque mission.
	2010.A1 – Le plan d’audit interne doit s’appuyer sur une évaluation des risques documentés et réalisés au moins une fois par an. Les points de vue de la direction générale et du Conseil doivent être pris en compte dans ce processus.	2120.A1 – L’audit interne doit évaluer les risques afférents au gouvernement d’entreprise, aux opérations et au système d’information de l’organisation. 2120.A2 – L’audit interne doit évaluer la possibilité de fraude et la manière dont ce risque est géré par l’organisation. (Commentaire IFACI : afin d’évaluer l’efficacité des processus de management des risques de son organisation, l’audit interne s’appuie utilement sur des référentiels reconnus comme le COSO 2 – Enterprise Risk Management Framework)	2210.A1 – L’auditeur interne doit procéder à une évaluation préliminaire des risques liés à l’activité soumise à l’audit. Les objectifs de la mission doivent être déterminés en fonction des résultats de cette évaluation. 2210.A2 – En détaillant les objectifs, les auditeurs internes doivent tenir compte de la probabilité qu’il existe des erreurs significatives, des cas de fraude ou de non-conformité et d’autres risques importants.

La revue détaillée de ces normes soulève néanmoins un certain nombre de questions. Alors que l’objet même de l’audit interne est d’évaluer les processus de gestion des risques et que les normes sont elles-mêmes centrées sur le concept de risque, ce dernier n’est pas précisément défini et reste relativement ambigu. Pour pallier cette lacune, les normes précisent que « *l’audit interne s’appuie utilement sur des référentiels reconnus comme le COSO 2 – Enterprise Risk Management* ». Il est donc important de compléter l’analyse des normes avec celles des

référentiels auxquels renvoient les normes d’audit pour préciser la notion de risque. Cette revue est présentée en détail dans le troisième chapitre (relatif à l’audit interne et les risques).

Une revue complémentaire des modalités pratiques ainsi que des guides pratiques associés aux normes obligatoires ont confirmé l’absence d’une définition précise de la notion de risque qui est pourtant central dans les normes et la nécessité de compléter cette revue sur la base des référentiels de gestion des risques auxquels renvoient les normes d’audit.

Tableau 2. Extrait des normes d’audit interne – MPA 2010.1 et MPA.2010.2 (IIA, 2014)

Recommandations non obligatoires	MPA.2010.1	Prise en compte des risques et des menaces pour l’élaboration du plan d’audit	MPA.2010.2	Utilisation du processus de gestion des risques dans la planification
	L’actualisation de l’univers d’audit : étape de l’élaboration du plan d’audit		Définition du processus de gestion des risques (définition de l’ERM-COS02)	
	Univers d’audit : l’ensemble de tous les audits pouvant être réalisés		Le plan d’audit interne doit refléter les résultats du processus de gestion des risques	
	Hierarchisation des audits : matérialité du risque et probabilité d’occurrence		Quelle que soit la source de l’évaluation des risques, l’auditeur interne doit considérer les facteurs suivants dans l’élaboration du plan d’audit : le risque inhérent, le risque résiduel, l’étendue des contrôles et du suivi	

Conclusion :

Nous avons vu dans ce chapitre que l'audit interne est une activité normée et que les normes ont certainement contribué à renforcer l'idée que l'audit n'est pas une activité ou une fonction au même titre que les autres. L'audit interne se positionne aujourd'hui comme une profession dont les activités sont régies par des normes. Ces mêmes normes précisent que la mission des auditeurs internes est d'évaluer les processus de management des risques, de gouvernance et de contrôle au sein des organisations.

La revue critique des normes d'audit interne nous a permis de mettre en évidence que la notion de « risque » qui constitue le cœur des activités de l'audit interne n'est pas précisément définie dans les normes d'audit.

Ce constat nous amène à nous interroger sur la manière dont les auditeurs procèdent en pratique pour pallier cette difficulté. Nous pouvons nous interroger sur l'intérêt d'avoir fondé sur normes d'audit sur les risques. La théorie de la société de l'audit de Power (1999) nous apporte un début de réponse qui mérite d'être approfondie.

Nous allons aborder dans le chapitre suivant la place qu'occupe l'audit interne dans le dispositif de gouvernance.

1 - 2 L'AUDIT INTERNE DANS LE DISPOSITIF DE GOUVERNANCE

Depuis ces quinze dernières années, en réponse à la crise de confiance des marchés financiers, de nombreux programmes politiques et réglementaires se sont multipliés afin de restaurer celle-ci. Nous pouvons notamment faire référence au vote de lois telles que la *Sarbanes Oxley Act* (2002) aux Etats-Unis destinées à améliorer la transparence et la gouvernance des entreprises qui doivent à présent communiquer sur leurs risques et leurs procédures de contrôle interne.

Ces exigences en matière de communication ont été complétées, avec le vote de la huitième directive européenne (2006), par le renforcement du rôle des comités d'audit au sein des organisations. Les comités d'audit sont chargés d'évaluer l'efficacité des systèmes de contrôle interne et des processus de gestion des risques.

L'audit interne joue un rôle particulier dans le dispositif de gouvernance car il est justement en charge d'évaluer pour le compte du management et des instances de gouvernance la robustesse des dispositifs de gestion des risques.

Il est dès lors important de comprendre comment l'audit interne contribue à améliorer les processus de gestion des risques au sein des organisations et à en rendre compte aux instances de gouvernance. Ce chapitre vise à recenser les principaux travaux qui traitent de ce thème.

Nous verrons dans un premier temps comment la théorie de l'agence peut nous aider à mieux comprendre l'évolution de l'audit interne et la place qu'il occupe aujourd'hui dans le dispositif de gouvernance. Nous présenterons ensuite le modèle de l'audit interne en tant que troisième ligne de défense dans le dispositif de gouvernance. Puis nous terminerons par la nature des relations entre le comité d'audit et l'audit interne.

1 - 2 1 LA THEORIE DE L'AGENCE ET L'AUDIT INTERNE

W. Jensen et W. Meckling (1976) introduisent la théorie de l'agence dans laquelle ils considèrent l'entreprise comme un marché régulé par de nombreux contrats. La relation naissant entre les parties, que ces auteurs nomment « relation d'agence », apparaît comme un contrat reliant un ou plusieurs agents : le « principal », dépositaire d'une autorité à un autre tiers, l'« agent », à qui est déléguée la réalisation d'une tâche. Cette relation d'agence est problématique puisque les intérêts personnels du principal et de l'agent sont le plus souvent divergents. Il existe alors une asymétrie informationnelle, un risque d'opportunisme du dirigeant et des coûts d'agence liés à ce type de relation. La mise en place du commissaire aux

comptes comme gardien de la confiance permet, notamment, de réduire ces caractéristiques propres à la relation d'agence et d'assurer la fiabilité de l'information financière.

Or, cette fiabilité de l'information financière dépend de la qualité de l'audit réalisé. Pour garantir cette qualité, l'auditeur doit être compétent et indépendant, (De Angelo, 1981). Toutefois, selon De Angelo la qualité de l'audit ne peut être garantie que si l'auditeur est compétent et indépendant : en d'autres termes, elle dépend de « la probabilité conditionnelle selon laquelle, étant donné une infraction découverte, l'auditeur rendra compte de cette infraction », (De Angelo, 1981).

Chacune de ces deux dimensions de la qualité de l'audit est influencée par un ensemble de facteurs analysés par de nombreux auteurs. Nous verrons (dans le chapitre 4 de cette première partie) qu'ils ne s'appliquent pas entièrement pour le cas de l'audit interne.

Certains travaux ont cherché à comprendre dans quelle mesure l'audit interne contribuait à créer un sentiment de confort chez les membres du comité d'audit (Sarens et al., 2009). Pour ce faire, une étude de cas multiples a été effectuée au sein de quatre organisations belges de grande envergure. La collecte de données a été réalisée au moyen d'une entrevue semi-dirigée avec des directeurs de fonction d'audit interne et le président du comité d'audit correspondant.

Les résultats ont révélé que l'audit interne apporte effectivement un sentiment de confort aux membres de comités d'audit au regard des contrôles internes et de l'environnement de contrôle en général, contribuant ainsi à l'efficacité du comité d'audit (Sarens et al., 2009). Un ensemble de facteurs semble influencer la création d'un sentiment de confort chez les membres de comités d'audit. Les connaissances particulières des auditeurs internes en matière de contrôle interne et en ce qui concerne les activités de l'organisation. L'ensemble des relations formelles et informelles entre les membres des comités d'audit et les auditeurs internes, de même que les aptitudes personnelles et relationnelles de ces auditeurs ont aussi un effet sur le sentiment de confort que ressentent les membres de comités d'audit (Sarens et al., 2009).

1 - 2 2 L'AUDIT INTERNE COMME TROISIEME LIGNE DE DEFENSE DANS LE DISPOSITIF DE GOUVERNANCE

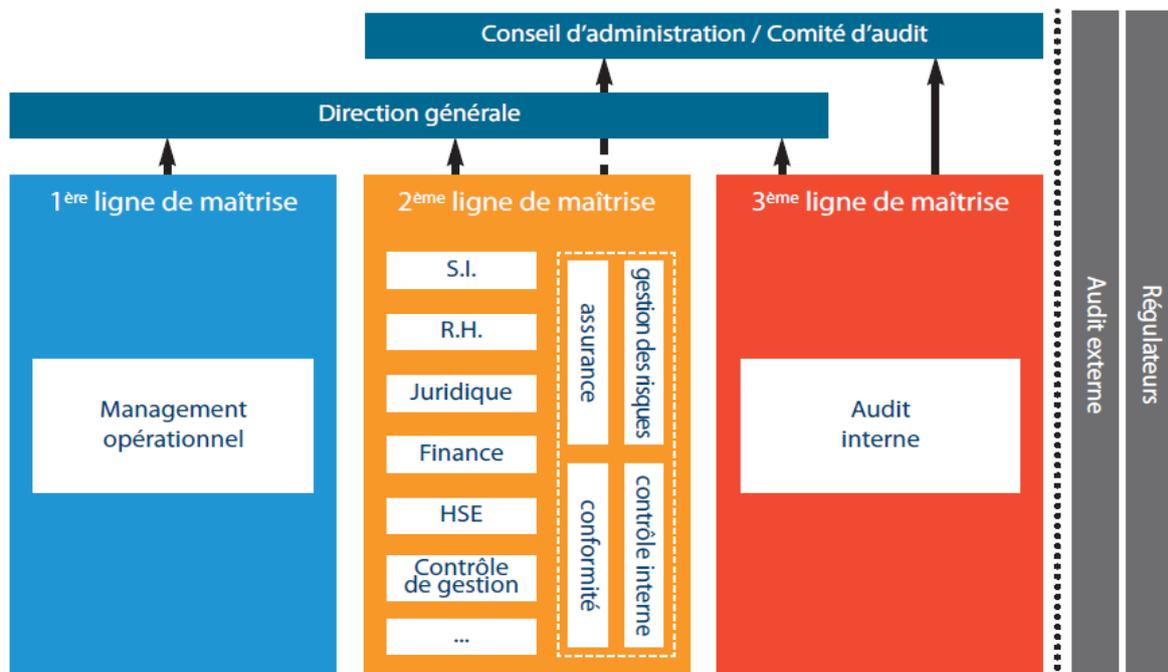
La littérature sur l'audit interne s'est particulièrement développée ces dernières années, notamment à la suite des évolutions réglementaires en matière de sécurité financières comme avec la loi Sarbannes Oxley aux Etats-Unis et d'autres lois au niveau international (Sarens,

2014). Les travaux qui ont été réalisés mettent notamment en évidence que l’audit interne représente une des composantes clés du dispositif de gouvernance (Archambeault *et al.*, 2008 ; Bédard et Gendron, 2010 ; Gramling *et al.*, 2004 ; Holt et DeZoort, 2009 ; Mat Zain et Subramaniam, 2007 ; Prawitt *et al.*, 2009 ; Rezaee, 2005 ; Stewart et Subramaniam, 2010). Cette idée étant mise en perspective des aspects réglementaires qui sont venus renforcer les exigences en matière de gestion des risques au sein des organisations. Les normes d’audit internes traduisent bien cette idée au travers de leur contenu puisqu’elles précisent que l’audit est en charge d’évaluer les dispositifs de gestion des risques, de gouvernance et de contrôle.

L’audit interne représente ainsi un élément dont le but est de contribuer à assurer une plus grande efficacité du dispositif de gouvernance.

L’*Institute of Internal Auditors* (IIA, 2014) a récemment établi un cadre conceptuel de gouvernance. Il s’agit du modèle des trois lignes de maîtrise (ou encore de défense dans l’appellation anglo-saxonne). Ce cadre décrit un dispositif destiné à mieux gérer et maîtriser les risques au sein d’une organisation. L’audit interne est une composante clé de ce dispositif et représente une des trois lignes de défense à part entière.

Figure 5. Le modèle des trois lignes de maîtrise (Amrae et Ifaci, 2014)



Ce modèle présente un intérêt particulier car il précise la place et le rôle spécifique que joue aujourd'hui l'audit interne dans le dispositif de gouvernance en lien avec les processus de gestion des risques. Le modèle des trois lignes de défense traduit l'idée que la gestion des risques et des activités de contrôle est prise en charge par trois groupes au sein de l'organisation. Chacun de ces groupes joue un rôle spécifique et bénéficie d'un degré d'indépendance qui n'est pas le même en fonction des lignes hiérarchiques et fonctionnelles auxquelles ils rapportent.

Ainsi, la première ligne de défense est représentée par les « managers » en charge de gérer les risques dans le cadre de leurs activités. Ils sont en charge de mettre en place des dispositifs de contrôle interne pour maîtriser leurs activités et de définir des actions correctives complémentaires en cas de dysfonctionnement. Ils ne sont pas indépendants de l'organisation puisqu'ils sont directement impliqués dans les opérations et qu'ils rapportent à la direction.

Les fonctions supports (systèmes d'information, finance, ressources humaines, contrôle de gestion, ...) et les fonctions expertes (gestion des risques, conformité, contrôle interne, ...) représentent la seconde ligne de défense. Cette seconde ligne de défense est en charge de s'assurer que les mécanismes de contrôle établis au niveau de la première ligne de défense sont bien définis et qu'ils fonctionnent correctement. Les membres de ce niveau organisationnel peuvent être dans une certaine mesure considérés comme étant indépendant puisqu'ils ne sont pas eux-mêmes « propriétaires » des risques gérés au niveau opérationnel par les « managers ». Cette indépendance est malgré tout limitée par leur statut même de manager ainsi que par le fait qu'ils rapportent aussi à la direction.

L'audit interne représente la troisième et la dernière ligne de défense. Contrairement aux deux premières lignes de défense qui sont représentées par des fonctions managériales de l'organisation, la troisième ligne de défense représente quant à elle une fonction de gouvernance. En tant que troisième ligne de défense du dispositif de maîtrise des risques, l'audit interne doit être indépendant afin d'évaluer la robustesse des deux premières lignes de défense au bénéfice des instances de gouvernance. Son indépendance est un critère essentiel pour assurer l'efficacité du dispositif de gouvernance au travers de son évaluation des dispositifs de gestion des risques et de contrôle.

Un courant de recherche s'est particulièrement développé afin d'évaluer l'efficacité de l'audit interne en tant que composante et mécanisme du dispositif de gouvernance (Norman et al., 2010 ; Lenz et Sarens, 2012 ; Everett et Tremblay, 2014 ; Roussy, 2013 ; Sarens, 2014). Ainsi, Roussy (2013) affirme que les auditeurs internes peuvent s'avérer être les gardiens des secrets

de l'organisation et du management, au détriment des intérêts du comité d'audit et des autres parties prenantes. De même, Norman *et al.* (2010) affirment que les auditeurs internes peuvent avoir tendance à minimiser les risques qu'ils ont en charge d'évaluer lorsqu'ils doivent les rapporter au comité d'audit.

Lenz et Sarens (2012) reconnaissent que l'audit interne est confronté à une certaine marginalisation de son rôle depuis la crise financière de 2008, notamment dans les débats sur la gouvernance. Les auteurs avancent l'idée que le double rattachement de l'audit tel que préconisé par les normes d'audit ainsi que le fait de vouloir assurer à la fois des services d'assurance et de conseil sont à l'origine des difficultés rencontrées par l'audit. Le fait que l'audit cherche à remplir plusieurs rôles à la fois et ce pour beaucoup de personnes en même temps, génère un certain flou sur le niveau auquel il s'adresse et sur ce qu'il doit fournir comme service. Les auditeurs proposent d'un côté un service d'assurance au comité d'audit et de l'autre ils se positionnent comme étant un « *business partner* » en offrant au management un service de conseil. Les auteurs suggèrent que pour améliorer le positionnement de l'audit interne dans le dispositif de gouvernance, il est nécessaire de clarifier envers qui l'audit doit véritablement rendre compte et se concentrer en priorité sur les services d'assurance.

Enfin, nous savons peu de chose sur le travail effectivement réalisé par les auditeurs internes (Norman *et al.*, 2010 ; Lenz et Sarens, 2012 ; Roussy, 2013 ; Everett et Tremblay, 2014 ; Sarens, 2014) ainsi que sur le contenu de leurs échanges avec les comités d'audit du fait d'un accès difficile à ce type d'information. Il s'avère dès lors particulièrement difficile à ce stade d'apprécier l'efficacité de la fonction d'audit au regard de son rôle pour améliorer les mécanismes de gouvernance.

1 - 2 3 L'AUDIT INTERNE ET LE COMITE D'AUDIT

Malgré le manque d'information sur la nature et le contenu des échanges entre l'audit interne et le comité d'audit, il est important de recenser les travaux existants qui traitent de l'audit interne en lien avec le comité d'audit.

Les travaux existants ont notamment porté sur le lien entre la taille d'une fonction d'audit interne et les caractéristiques du comité d'audit, à savoir sa composition et le type de supervision qu'il exerce sur la fonction d'audit.

Ainsi, Barua *et al.* (2010) ont examiné la relation entre les caractéristiques du comité d'audit et l'investissement en ressources (le budget) dans la fonction audit interne. Leur étude quantitative

indique que le budget de la fonction audit interne diminue si au moins un des membres du comité d'audit est un expert-comptable. Aussi, plus les membres du comité d'audit sont expérimentés, moins le budget de la fonction d'audit interne est élevé. Selon les auteurs, cela signifie qu'il y aurait un effet de substitution entre l'expertise des membres du comité d'audit et celle des auditeurs internes.

Sarens et Abdolmohammadi (2011) ont interrogé des directeurs de fonction d'audit interne d'organisations belges afin de déterminer dans quelle mesure la fonction d'audit interne et les membres indépendants du conseil d'administration jouent un rôle complémentaire en matière de gouvernance corporative. Les résultats de Sarens et Abdolmohammadi (2011) indiquent que plus il y a de membres indépendants dans le conseil d'administration, plus la taille de la fonction audit interne diminue. Les auteurs concluent que la fonction audit interne et les membres indépendants du conseil d'administration jouent un rôle similaire en matière de gouvernance de l'organisation.

Leurs résultats indiquent aussi que plus le pourcentage de gestionnaires détenant des actions de l'organisation est élevé, plus la taille de la fonction d'audit interne est grande. Les auteurs présumant que ces observations s'expliquent par le fait que les gestionnaires détenant des actions de l'organisation veulent montrer aux autres actionnaires qu'ils gèrent l'organisation en toute honnêteté. Dans l'ensemble, ces écrits indiquent que le fonctionnement de l'audit interne est influencé par la composition du comité d'audit.

Par ailleurs, les résultats de deux autres études révèlent que le comité d'audit influence la fonction audit interne. Par contre, la relation étudiée provient des activités de supervision du comité au lieu de sa composition. En fait, Carcello et al. (2005) étudient en effet les déterminants de l'investissement financier en audit interne en guise d'indicateur de l'importance accordée à la fonction au sein des organisations. La question de recherche est la suivante : « *quels sont les déterminants de l'investissement budgétaire en audit interne ?* ». Les chercheurs ont questionné 901 présidents-directeurs généraux d'entreprises de taille moyenne et cotées à la bourse américaine. Avec un taux de réponse de 25 %, les résultats tendent à démontrer que le budget total d'audit interne est déterminé par le fait que le comité d'audit le révise. Les autres facteurs qui déterminent le budget accordé à l'audit interne sont : la taille de l'organisation, les flux monétaires d'opération, le taux d'endettement, la valeur des inventaires disponibles et le secteur industriel (en particulier le secteur bancaire, les entreprises de services et les entreprises manufacturières) (Carcello et al., 2005).

Également, Abbott et al. (2010) ont questionné des directeurs de fonction audit interne dans le but de déterminer dans quelle mesure la supervision exercée par le comité d'audit influence le type de mandats réalisés par la fonction d'audit interne. Leurs résultats indiquent que plus la supervision exercée par le comité d'audit est étroite, plus le budget de la fonction audit interne alloué aux mandats d'audit est élevé. Selon les auteurs, la supervision du comité d'audit influence les activités de la fonction audit interne.

À la lumière des écrits recensés, il semble que la présence, la composition et les activités de supervision du comité d'audit influencent de manière positive l'existence et le fonctionnement de la fonction d'audit interne de même que son importance au sein des organisations (sur le plan du budget).

Conclusion :

Nous avons vu dans ce chapitre que l'audit interne occupe une place privilégiée dans le dispositif de gouvernance des organisations. Les travaux réalisés montrent que l'audit interne contribue à fournir un certain niveau de confort aux membres des comités d'audit, et donc aux instances de gouvernance de façon plus large.

Le modèle des trois lignes de défense qui a été développé souligne l'importance d'avoir une fonction d'audit interne qui puisse jouir d'un bon degré d'indépendance qui seul peut lui permettre de correctement apprécier les dispositifs de gestion des risques au sein des organisations.

Les travaux existants traitent des conditions nécessaires pour assurer l'efficacité de l'audit interne au sein des organisations. Ils sont insuffisants pour apprécier la nature de l'impact effectif que peut avoir l'audit interne sur les dispositifs de gouvernance.

Nous allons aborder dans la partie suivante l'activité d'audit interne en lien avec leur approche par les risques.

1 - 3 L'AUDIT INTERNE ET LES RISQUES

Lorsqu'il est fait mention d'audit par les risques (« Risk Based Auditing ») dans la littérature, il est question à la fois du rôle de l'audit interne dans le processus de gestion des risques ainsi que de la planification de ses activités.

La revue détaillée des normes a mis en évidence que le concept de risque sur lequel est fondée la pratique de l'audit interne n'est pas défini de façon précise.

L'objectif de ce chapitre est de recenser les principaux travaux qui ont été menés ces dernières années sur les pratiques de l'audit interne en lien avec leur approche par les risques (« Risk Based Auditing ») pour mieux comprendre comment les auditeurs internes procèdent en pratique pour pallier cette difficulté.

Nous verrons donc dans une première partie les travaux qui ont porté sur l'audit interne en lien avec les processus de gestion des risques puis dans une seconde partie la planification des travaux de l'audit interne en lien avec les risques.

1 - 3 1 L'AUDIT INTERNE ET LES PROCESSUS DE GESTION DES RISQUES

Cette partie présente dans un premier temps les principaux cadres de référence établis dans le domaine de la gestion des risques puis fait un état de la littérature scientifique sur ce thème en lien avec l'audit interne.

1 - 3 1 1 PRINCIPAUX CADRES DE REFERENCE EN MATIERE DE GESTION DES RISQUES

L'IFACI fait référence dans les normes d'audit à trois référentiels qui sont : le « *COSO 2 – Entreprise Risk Management* » (COSO, 2004), l'« *ISO 31000 - Management du risque, principes et lignes directrices* » (ISO, 2009) et enfin le cadre de l'AMF « *Les dispositifs de gestion des risques et de contrôle interne : Cadre de Référence* » (AMF, 2010). Ces référentiels décrivent en quoi consiste le processus de gestion des risques ainsi que les principales étapes qui le composent.

Le modèle du COSO 2 correspond à l'un des référentiels les plus connus en matière de gestion des risques et les autres référentiels s'en sont fortement inspirés même s'ils présentent des spécificités.

Le modèle de l'Entreprise Risk Management a été établi par le COSO - « *COmmittee of Sponsoring Organizations of the Tradeway commission* » (COSO, 2004). La « *Treadway*

Commission », dont le vrai nom est « *National Commission on Fraudulent Financial Reporting* », a été créée aux Etats-Unis dans les années 1980 pour réfléchir aux facteurs à l'origine de la présentation de mauvaises informations financières. Il en a d'abord découlé des recommandations puis, en 1992, un cadre de référence du contrôle interne (*COSO – Internal Control Integrated framework*). Le cadre du contrôle interne du COSO (dans sa première version) distingue cinq composantes : environnement de contrôle, évaluation des risques, activités de contrôle, information et communication et finalement pilotage.

Fin 2004, le COSO a étendu ce cadre à la notion plus générale de gestion des risques en ajoutant une composante « fixation des objectifs » et en précisant la notion d'« évaluation des risques » par l'ajout de deux nouvelles composantes : identification des événements et définition des options de traitement. Le référentiel du COSO devient l'*Entreprise Risk Management – Integrated Framework* qui est aussi connu sous le nom de COSO 2.

Le COSO 2 définit le management des risques comme étant : « *un processus mis en œuvre par le conseil d'administration, la direction générale, le management et l'ensemble des collaborateurs de l'organisation. Il est pris en compte dans l'élaboration de la stratégie ainsi que dans toutes les activités de l'organisation. Il est conçu pour identifier les événements potentiels susceptibles d'affecter l'organisation et pour gérer les risques dans les limites de son appétence pour le risque. Il vise à fournir une assurance raisonnable quant à l'atteinte des objectifs de l'organisation* ». Ce référentiel est représenté par un cube à trois dimensions : organisationnel (entité, activité...), objectifs poursuivis (stratégiques, opérationnels, ...) et le processus de gestion des risques qui comporte huit étapes principales résumées dans le tableau de la page suivante.

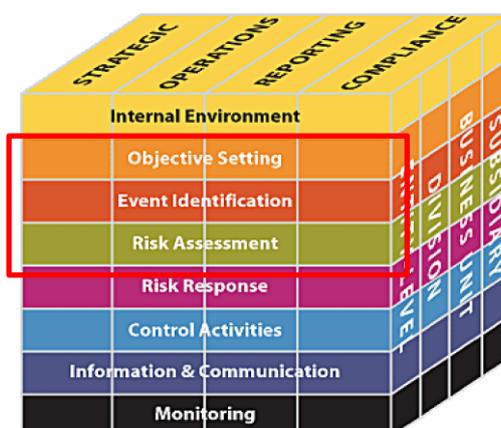
Tableau 3. Processus de gestion des risques – Modèle du COSO 2 – ERM

Principales étapes du processus de gestion des risques		Description
1	Environnement de contrôle	Culture, Valeurs
2	Définition des objectifs	Processus de fixation des objectifs
3	Identification des événements	Événements négatifs (risques) ou positifs (opportunités)
4	Evaluation des risques	Risque = Probabilité × Impact
5	Réponse aux risques	4 options : Evitement, Acceptation, Réduction, Partage
6	Activités de contrôle	Réduction des risques avec la mise en place d'activités de contrôle interne
7	Information et Communication	Informations utiles pour exercer ses responsabilités
8	Pilotage	Le processus de management des risques est piloté et adapté en fonction des besoins

La définition qui est donnée du risque dans le modèle du COSO 2 est qu'il s'agit de « *tout événement qui, s'il se produit, peut remettre en cause l'atteinte des objectifs d'une organisation* ».

Le risque tel que défini ne distingue pas la notion de risque réputée calculable et celle d'incertitude qui se caractérise selon Knight (1921) par l'impossibilité de les mesurer pour les événements qui ne sont pas connus.

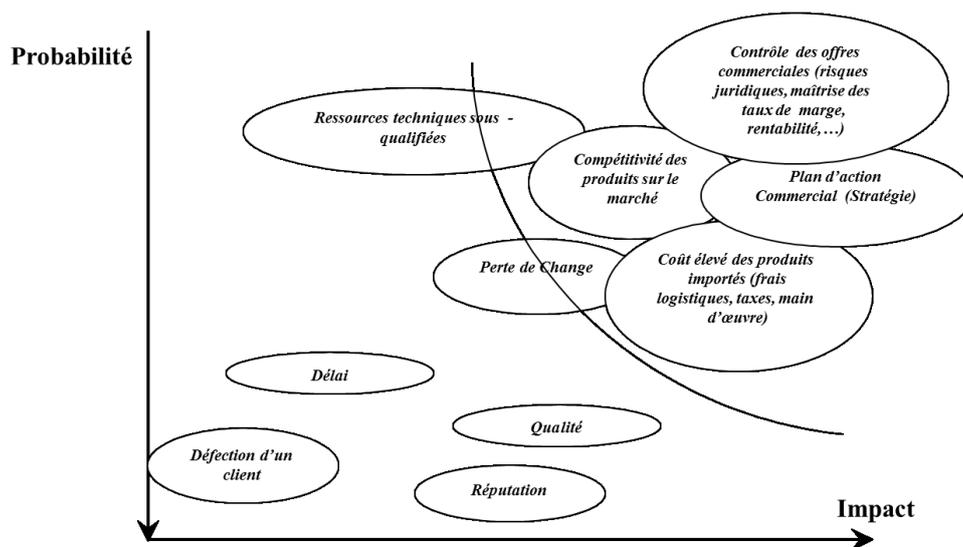
Figure 6. Modèle du COSO 2 – Enterprise Risk Management (COSO, 2004)



Ainsi, afin de gérer efficacement les risques, le modèle préconise de définir en amont des objectifs clairs et cohérents (stratégiques, opérationnels, qualité de l'information et conformité aux lois et règlements) puis d'identifier (au sens anticiper et envisager) les événements qui pourraient, s'ils surviennent, remettre en cause l'atteinte des objectifs ainsi fixés. Les risques (ou événements) une fois identifiés doivent être évalués en fonction de leur probabilité et de leur impact afin de pouvoir les hiérarchiser pour décider de la manière dont ils seront traités.

Une pratique de place s'est répandue ces dernières années. Elle consiste à établir un document intitulé cartographie des risques pour représenter ces risques dits majeurs sous une forme synthétique. Elle consiste en une représentation des risques de l'entreprise classés en fonction de leur probabilité d'occurrence et de leur impact.

Figure 7. Exemple de cartographie des risques

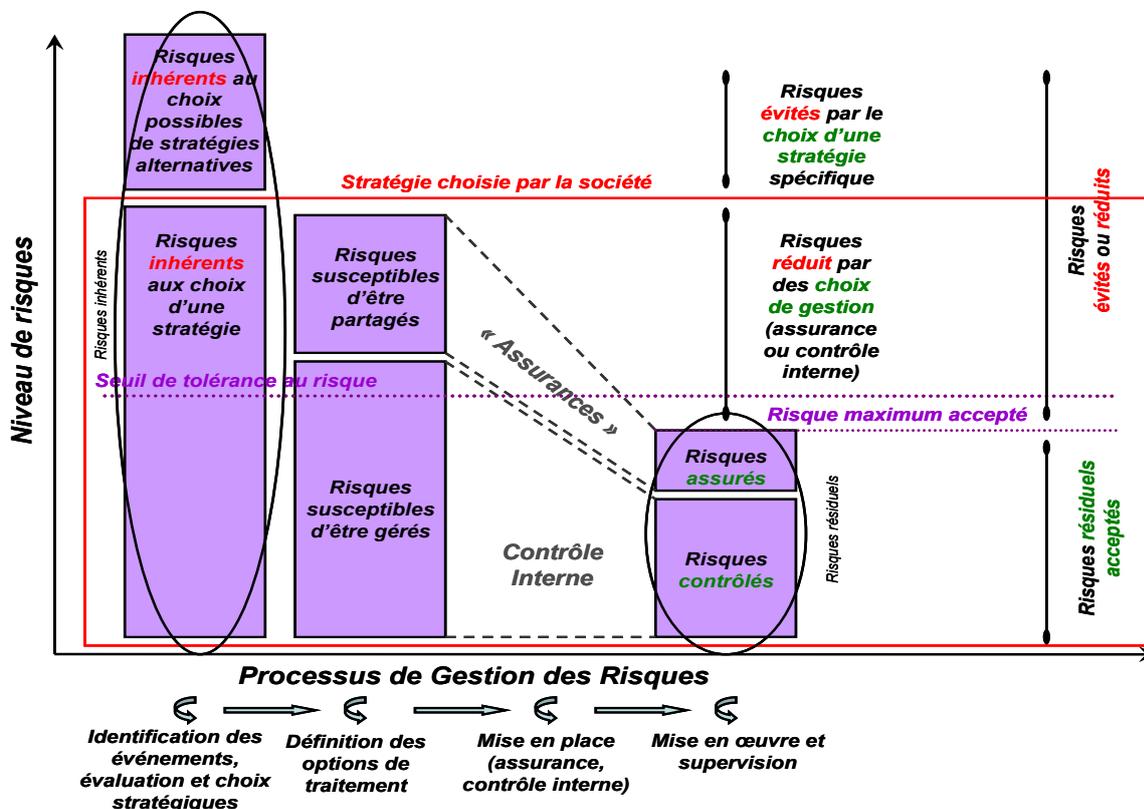


L'évaluation qui est faite distingue les risques inhérents (c'est-à-dire le risque « brut » avant action corrective) des risques dits résiduels (après mise en œuvre des actions correctives). Face à un risque inhérent, plusieurs options s'offrent en matière de traitement du risque (au regard de son niveau d'appétence au risque).

Il est possible d'accepter le risque sans action spécifique, de l'éviter, de le partager (partenariat, assurance, ...) ou de le réduire par la mise en place d'activité de contrôle (interne). Le contrôle interne apparaît comme l'ensemble des actions entreprises pour réduire le risque à un niveau acceptable.

Le schéma ci-dessous décrit les principales étapes de ce processus de gestion des risques :

Figure 8. Gestion des risques, dispositifs de contrôle et risque acceptable



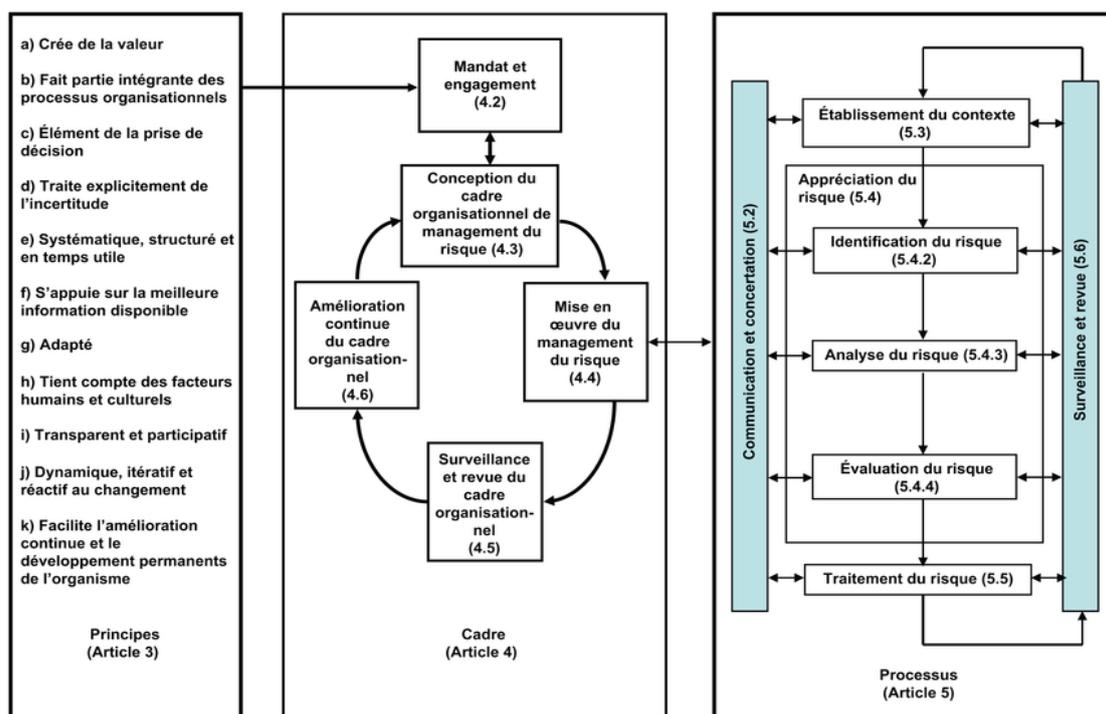
Dans cette logique, le COSO définit le contrôle interne comme le « processus mis en place par les dirigeants et mis en œuvre par le personnel d'une entité (entreprise, filiale ou fonction), lequel processus comprend l'ensemble des dispositifs et des sécurités contribuant à accroître et à maîtriser les opérations ».

Par opposition aux risques que l'on évite (par des choix stratégiques alternatifs) ou que l'on partage (en prenant des assurances, ...), les risques du contrôle interne sont les risques auxquels une organisation s'expose par choix (on parle de « risque inhérents »). Le contrôle interne permet de les identifier et de les réduire jusqu'à un niveau « acceptable » (on parle alors de « risque résiduel »).

Le processus de gestion des risques nécessite pour les organisations qui mettent en œuvre ce processus à hiérarchiser les risques et identifier ceux qu'elles considèrent comme majeurs dans le but d'allouer les moyens nécessaires à leur gestion.

Le référentiel ISO 31000 - *Management du risque, principes et lignes directrices* (version 2009) s'inspire fortement du référentiel COSO 2, même s'il présente des spécificités. L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. L'ISO 31000 a été élaborée par le groupe de travail du Bureau de gestion technique ISO sur le Management du risque. L'ISO 31000 est structurée en 4 grandes sections : la première définit le vocabulaire employé dans la norme, la seconde établit les principes, la troisième décrit le cadre organisationnel et la quatrième expose le processus de Management des risques (représenté à droite dans le schéma ci-dessous).

Figure 9. Référentiel ISO 31000



Le terme de risque y est défini comme étant l'effet de l'incertitude sur les objectifs. Cette définition est complétée par un certain nombre de notes plus spécifiques.

- *Note 1 à l'article : un effet est un écart, positif et/ou négatif, par rapport à une attente.*
- *Note 2 : les objectifs peuvent avoir différents aspects (par exemple buts financiers, de santé et de sécurité, ou environnementaux) et peuvent concerner différents niveaux*

(niveau stratégique, niveau d'un projet, d'un produit, d'un processus ou d'un organisme tout entier).

- *Note 3 : un risque est souvent caractérisé en référence à des événements et des conséquences potentiels ou à une combinaison des deux.*
- *Note 4 : un risque est souvent exprimé en termes de combinaison des conséquences d'un événement (incluant des changements de circonstances) et de sa vraisemblance.*
- *Note 5 : l'incertitude est l'état, même partiel, de défaut d'information concernant la compréhension ou la connaissance d'un événement, de ses conséquences ou de sa vraisemblance.*

Le cadre de l'AMF « dispositifs de gestion des risques et de contrôle interne » (2010) s'inspire très fortement des deux référentiels précédents qui sont le COSO 2 et l'ISO 31000 : « *La gestion des risques est l'affaire de tous les acteurs de la société. Elle vise à être globale et doit couvrir l'ensemble des activités, processus et actifs de la société. La gestion des risques est un dispositif dynamique de la société, défini et mis en œuvre sous sa responsabilité. Elle comprend un ensemble de moyens, de comportements, de procédures et d'actions adaptés aux caractéristiques de chaque société qui permet aux dirigeants de maintenir les risques à un niveau acceptable pour la société. Le risque représente la possibilité qu'un événement survienne et dont les conséquences seraient susceptibles d'affecter les personnes, les actifs, l'environnement, les objectifs de la société ou sa réputation* ».

En l'absence de définition précise de la notion de risque dans le corps de texte des normes d'audit interne, notre revue des référentiels de gestion des risques (auxquels il est fait référence dans les normes) nous a permis d'établir une synthèse des principales définitions du concept de « risque ».

Tableau 4. Comparaison des cadres normatifs de gestion des risques

COSO 2 – ERM (2004)	ISO 31000 (2009)	AMF (2010)
Un risque est un événement qui s'il se produit peut affecter l'atteinte des objectifs.	Un risque est l'effet de l'incertitude sur les objectifs.	Un risque est la possibilité qu'un événement survienne et dont les conséquences seraient susceptibles d'affecter les personnes, les actifs, l'environnement, les objectifs de la société ou sa réputation.

Le risque tel que défini dans ces cadres normatifs efface implicitement le concept d'incertitude et induit l'idée que tous les événements susceptibles d'impacter de façon négative les organisations peuvent être identifiés et gérés. Cette hypothèse est raisonnablement contestable et soulève différentes questions, notamment :

- les principales menaces ne correspondent-elles pas justement à ce qui ne peut pas être prévu et mesuré ?
- ne relèvent-elles pas plus du concept d'incertitude au sens de Knight (1921) qui se distingue précisément de la notion de risque par son caractère non probabilisable ?
- dans cette même perspective, le processus de gestion des risques ne fournit-il pas un sentiment de sécurité illusoire en réponse aux anxiétés sociétales ?

Nous pouvons dans cette perspective nous interroger sur la manière dont les auditeurs peuvent véritablement être en mesure d'identifier et évaluer les risques dans un univers des possibles qui paraît « illimité » et soumis à de l'incertitude qui ne peut pas être mesurée.

I - 3 1 2 PRINCIPAUX TRAVAUX DE RECHERCHE SUR LE MODELE DE L'« ENTREPRISE RISK MANAGEMENT »

En matière de gestion des risques, il existe une conception largement partagée dans notre société moderne selon laquelle une bonne organisation dispose nécessairement d'un dispositif de management des risques structuré et formalisé (Power, 2004).

Certains auteurs s'interrogent avec un certain scepticisme sur ce postulat et l'impact réel des systèmes de management intégrés des risques. Ils considèrent qu'il s'agit de dispositifs qui sont principalement mis en œuvre pour des raisons de conformité (Arena et al, 2011).

Power (2009) critique ce phénomène d'institutionnalisation tout en se plaçant dans une posture normative pour chercher à définir les bases d'un management des risques qui dépasse ces limites. Il considère que la conception comptable et la logique d'auditabilité qui dominent l'*ERM (Entreprise Risk Management)* ont limité le développement des dispositifs de management des risques. Selon Power, ces dispositifs auraient pu produire de meilleurs résultats. Il explique que les méthodes et les concepts de l'*ERM (Entreprise Risk Management)* traduisent une conception cybernétique du management des risques. Cela se traduit clairement à travers la notion d'appétence au risque que l'*ERM (Entreprise Risk Management)* considère comme étant une notion unique et homogène pour l'ensemble de l'entreprise qu'il est possible de déterminer sans ambiguïté.

Cette conception de l'appétence au risque qui constitue un élément fondamental du modèle exclut l'existence de conflits entre différents types et niveaux d'appétence au sein d'une même organisation, ce que qui selon l'auteur est contestable. L'orientation comptable des dispositifs d'*ERM (Entreprise Risk Management)* basés sur le COSO a pour effet de conduire à la conception et à la mise en œuvre d'activités de contrôle formalisées et à la piste d'audit. Bertin (2007) s'interroge sur l'impact que peut avoir ce besoin de rendre les objets auditables décrit par Power sur les pratiques d'audit interne et réciproquement de l'audit sur les pratiques de gestion.

Enfin, Mikes (2009, 2011) étudie de façon plus spécifique le développement des systèmes de management des risques dans le secteur bancaire. Ses travaux mettent en évidence l'existence de deux styles de management des risques. Le premier caractérisé par un "enthousiasme quantitatif" orienté vers la mesure des risques, le second par un "scepticisme quantitatif" basé sur des méthodologies peu quantitatives, non formelles, et orientées vers les incertitudes stratégiques par nature non mesurables.

Mikes décrit, les différences de ces deux modes de gestion des risques et distingue une gestion de type holistique, orientée vers la stratégie, qu'elle oppose à un mode quantitatif, orienté vers des risques plus techniques. Selon elle, le management holistique des risques repose moins sur des modèles formels que sur les structures cognitives des dirigeants pour les aider à construire des futurs alternatifs. Ces dispositifs encouragent la discussion, le débat, plutôt qu'ils ne

fournissent des indications strictes. Mikes (2011) distingue finalement les systèmes orientés vers la mesure des risques et ceux qui sont orientés vers l'*environnement* des risques majeurs pour la réflexion et la prise de décision stratégique.

Le modèle de l'ERM nous amène à nous interroger sur son impact réel et sur son fondement. Le fait de vouloir « normer les risques » ne constitue-t-il pas en soi une source de risque ?

1 - 3 1 3 L'AUDIT INTERNE EN CHARGE D'EVALUER LES PROCESSUS DE GESTION DE RISQUES

Le rôle de l'audit interne et sa contribution au processus de management des risques tel que précisé dans la définition même de l'audit interne a été repris sans être contesté dans plusieurs travaux (Gramling et al., 2004 ; Sarens et Beelde, 2006 ; Spira et Page, 2003). Il est par ailleurs mis en évidence que les budgets alloués à la fonction d'audit interne sont positivement corrélés au niveau de risque de l'organisation (Carcello et al., 2005).

Les travaux de Spira et Page (2003) ont porté sur la réinvention des contrôles internes et sur les changements dans le rôle de la fonction d'audit interne pour donner suite à la publication du Turnbull Guidance au Royaume-Uni (1999). Ces auteurs s'intéressent particulièrement au cas des entreprises britanniques qui ont été assujetties au Turnbull Guidance à la suite de la vague de privatisation des sociétés gouvernementales survenues dans ce pays lors de la période où Madame Margaret Thatcher était première ministre.

Le risque est présenté dans le Turnbull Guidance comme un objet qui peut être identifié, évalué de façon objective et donc géré. L'expertise du risque et des systèmes de contrôle interne constitue dès lors une source de pouvoir pour les auditeurs internes pour jouer un rôle clé dans le domaine de la gestion des risques. Les auteurs soutiennent que le rôle premier de la fonction d'audit interne est en fait de surveiller et de contrôler les risques organisationnels (financiers et autres) au bénéfice de la société britannique dans son ensemble. À ce titre, la fonction est un système social important dans la gestion des risques. Ces auteurs mentionnent aussi que des études empiriques sont manquantes et nécessaires pour mieux comprendre les répercussions du Turnbull Guidance sur tous les aspects de la gestion, de la fonction d'audit interne à celle de l'audit externe, en passant par la gestion des enjeux environnementaux et sociaux qui touchent les organisations.

Dans la continuité de ces travaux, certaines études ont étudié le degré d'implication des auditeurs internes au sein de leurs organisations (Allegrini et D'Onza, 2003 ; Paape et al., 2003 ; Sarens et De Beelde, 2006 ; Sarens et al., 2009).

Allegrini et D'Onza (2003) ont montré le rôle de conseil que pouvaient jouer les auditeurs internes dans le déploiement de dispositif de gestion des risques au sein de leur organisation et ont souligné la forte implication des auditeurs au sein des grandes entreprises italiennes.

D'autres travaux ont mis en évidence que le degré d'implication des auditeurs interne en matière de gestion des risques était lié au degré d'exigence institutionnelle et réglementaire. Plusieurs analyses comparatives des firmes de différents pays et différents codes de gouvernance confirment ce point (Sarens et De Beelde, 2006 ; Sarens et al., 2009).

1 - 3 2 LE MODELE DU « BUSINESS RISK AUDIT » (BRA)

Cette section présente l'approche par les risques mise en œuvre par les auditeurs internes dans le cadre de leur mission. La revue de la littérature montre que cette approche s'est développée dans le domaine de l'audit externe avant d'être reprise par l'audit interne. Nous pouvons néanmoins nous interroger dans quelle mesure cette méthode peut être transposée dans le domaine de l'audit interne.

1 - 3 2 1 DE LA VERIFICATION ARITHMETIQUE A UNE APPROCHE PAR LES RISQUES

Casta et Mikol (1999) ont décrit l'évolution et les enjeux méthodologiques de l'audit. La technologie utilisée par l'auditeur financier afin d'émettre une opinion, qui a fortement inspiré celle de l'audit interne, a considérablement évolué.

Jusqu'aux années 1930, l'activité des auditeurs financiers consistait en une vérification, le plus souvent exhaustive, des enregistrements comptables. Les praticiens ont ensuite développé, durant la période 1940-1960, une approche structurée de l'audit. Cette approche moderne a intégré, dès les années 1950, une perception du risque issue de la théorie statistique de la décision.

Dans les années 1950-1960, la perception de l'entreprise comme un système conduit l'auditeur à privilégier les études de fonctionnement, c'est-à-dire à analyser davantage les flux d'informations et le système de contrôle interne que les enregistrements comptables.

Parallèlement, la méthodologie est profondément marquée par la décomposition du risque d'audit (risque qu'il subsiste une erreur significative dans les comptes annuels) en aléas élémentaires : risque qu'il existe une erreur significative dans les opérations, risque de non-détection par le système de contrôle interne, risque de non-détection par l'auditeur.

Dans la perspective d'une analyse du risque par exception, des instruments spécifiques d'appréciation apparaissent :

- le seuil de signification, montant en dessous duquel une erreur, commise de bonne foi, est réputée sans incidence ;
- et le concept de niveau de confiance dans un système, qui permet l'identification de zones critiques.

Différents outils voient le jour dans les années 1950-1960 en particulier chez les « Big Eight »: diagramme de circulation de l'information, questionnaires d'appréciation du contrôle interne, examen analytique, techniques de sondages statistiques, outils spécifiques d'audit informatique...

En France, c'est dans les années 1970 que ce type d'approche commence à se diffuser, de façon très inégale : tout d'abord, par l'intermédiaire d'accords techniques, en ce qui concerne les cabinets représentant en France les réseaux anglo-saxons, puis par une vingtaine de cabinets français. Ensuite, la nouvelle démarche méthodologique est portée à la connaissance du plus grand nombre par les recommandations des instances professionnelles.

Plus récemment, l'accroissement de la concurrence sur un marché de l'audit parvenu à maturité et la pression s'exerçant sur le montant des honoraires ont favorisé la recherche d'outils de productivité (progiciel d'aide à l'audit, intégration bureautique des papiers de travail, systèmes experts...).

Aujourd'hui, l'accent est aussi mis sur la recherche de méthodes permettant la localisation des zones de risque de façon plus globale. C'est l'objet du « Business Risk Audit ».

1 - 3 2 2 LE BUSINESS RISK AUDIT : INNOVATION OU EVOLUTION ?

C'est dans un contexte de dérégulation du marché de l'audit externe et une concurrence accrue entre les cabinets d'audit externes qu'a été redéfinie l'approche par les risques de l'audit, plus communément appelé « **Business Risk Audit** ». Les cabinets d'audit devant faire face à une demande de plus en plus forte de réduction de leurs honoraires de la part de leurs clients ont dû repenser leur modèle pour gagner en efficacité (Knechel, 2007). Une pression accrue par le développement de l'audit interne au sein des firmes pour prendre en charge une partie des activités d'assurance. Au même moment, était publié en 1992 le référentiel du COSO – Internal Control – Integrated Framework suivi du COSO 2 – Entreprise Risk Management (2004). Le

Business Risk Audit est alors né avec l'idée que l'audit pouvait tout en se focalisant sur les risques majeurs de ses clients réduire ses coûts, avec l'idée que les risques du client pouvaient accroître le risque d'audit (Knechel, 2002).

C'est au même moment que la vague de scandales financiers (Enron, Parmalat, Worldcom...) jetait le discrédit sur le métier de l'audit. Comme le souligne Michael Power (1999), l'audit n'a pas empêché les fraudes et les faillites depuis les années 1980 ; cet écart observé entre les attentes et les réalisations ne semble pourtant pas remettre en cause la foi dans son utilité. Ainsi, les scandales qui ont éclaboussé la profession de l'audit, se sont soldés par un renforcement des normes, élaborées et appliquées par les professionnels eux-mêmes, plutôt que par une réflexion plus profonde sur le processus d'audit et sur le rôle de ces spécialistes.

Knechel (2007) s'est alors intéressé au fait de savoir dans quelle mesure le « Business Risk Audit » avait pu contribuer aux échecs de l'audit. Le BRA consistait pour les auditeurs à aller au-delà de la sphère comptable et mieux comprendre les activités et les risques de leurs clients. La méthodologie implique tout d'abord de comprendre les activités et la stratégie du client ainsi que les risques stratégiques et opérationnels pour ensuite traiter des processus de gestion associés qui permettaient de les gérer et des risques opérationnels. C'est à l'issue de ces analyses que les auditeurs pouvaient identifier les risques résiduels et leurs impacts sur les états financiers.

Selon Knechel (2007), le nouveau processus a souffert d'un nombre important d'obstacles qui n'avait pas été anticipé ni suffisamment géré (formation pour traiter de nouveaux sujets tels que l'analyse stratégique ou bien les activités opérationnelles et non financières, répartition des rôles et allocation des travaux, communication avec les clients, ...). Par ailleurs, les activités d'audit ont été perturbées par l'esprit commercial issu de leurs activités de conseil en développement pour répondre aux nouvelles exigences en matière de gouvernance et de gestion des risques.

Les travaux de Curtis et Turley (2007) ont confirmé les difficultés décrites par Knechel (2007) pour mettre en œuvre le BRA avec une étude longitudinale sur cinq années d'audit. Une des difficultés pour les auditeurs externes était notamment d'établir le lien entre leurs travaux d'audit et les états financiers. Les auteurs ont montré que les auditeurs ont en pratique continué à appliquer leurs procédures et méthodes « traditionnelles ».

Les travaux de Robson et al. (2007) ont mis en évidence comme Knechel (2007) l'intérêt et l'opportunité que pouvait représenter le BRA pour les cabinets d'audit. Le BRA constituait un

moyen de revendiquer une nouvelle expertise à forte valeur ajoutée dans le domaine du contrôle interne et des risques afin d'accroître leurs activités en réponse à une demande accrue du marché. Les travaux de Flint et al. (2008) vont dans le même sens pour conclure que le BRA n'est pas révolutionnaire mais qu'il contribue avant tout au processus de légitimation de l'audit. Il est difficile de ne pas se demander dans quelle mesure le « Risk Based Internal Auditing » (RBIA) ne partage pas les mêmes caractéristiques que le « Business Risk Audit » (BRA).

1 - 3 3 L'AUDIT INTERNE ET L'APPROCHE PAR LES RISQUES

Reding et Sobel (2013) reviennent sur la définition de l'audit interne en rappelant que son activité vise à créer de la valeur en aidant une organisation à atteindre ses objectifs. Il souligne le fait que le meilleur moyen pour l'audit interne d'y parvenir est de fournir un service fondé sur les risques dans le cadre de la planification des travaux de l'audit. L'objectif est d'évaluer les processus de gestion des risques majeurs de l'organisation et d'apporter ses conseils pour les améliorer. Il est nécessaire dès lors que les auditeurs internes possèdent une bonne compréhension et une bonne maîtrise de ce que représente un risque. Redding précise que la définition du risque tels que défini dans le modèle du « *COSO 2 – Enterprise Risk Management* » nous fournit les trois composantes clés du risque : les objectifs, les événements susceptibles de remettre en cause leur atteinte et enfin les conséquences de ces mêmes événements. Ainsi, seuls les risques qui peuvent affecter les objectifs de l'organisation doivent être considérés dans cette approche. Par ailleurs, les événements susceptibles d'impacter l'atteinte des objectifs peuvent avoir soit des effets négatifs, soit des effets positifs. L'audit interne doit donc fonder ses travaux en établissant une planification en lien avec les risques de l'organisation.

Les normes internationales pour la pratique professionnelle de l'audit interne requièrent deux éléments essentiels : un plan d'audit fondé sur les risques et une revue préliminaires des risques de l'entité ou activité auditée. Même s'il existe des travaux de recherches qui ont cherché à étudier ces aspects relatifs à la planification des missions d'audit, ces derniers restent limités. Plusieurs travaux traitent de l'application des normes d'audit interne dans le domaine de la planification des travaux qui doivent être fondés sur une identification et une évaluation préliminaire des risques (Pelletier, 2008 ; Koutoupis et Tsamis, 2009 ; Castanheira et al., 2010). Ces travaux indiquent que malgré le fait que certaines fonctions d'audit utilisent le terme de « Risk Based Auditing » (audit fondé sur une approche par les risques) pour décrire leur

méthodologie, leurs pratiques traduisent une application partielle. L'approche par les risques est essentiellement appliquée lors de l'élaboration du plan d'audit, et pas toujours ou peu durant les phases de planification et de réalisation des missions alors que les normes d'audit requièrent une analyse préliminaire des risques en lien avec l'activité auditée (Castanheira et al., 2010). De surcroît, même si certaines organisations déclarent appliquer une méthodologie d'audit fondée sur les risques, leurs pratiques ne reposent pas sur une documentation suffisante pour le démontrer (Koutoupis et Tsamis, 2009).

Certaines études soulignent combien il était difficile de développer et de mettre en œuvre une méthodologie d'audit fondée sur les risques (Knechel, 2007).

La revue de la littérature nous a montré que les travaux sont limités dans ce domaine. Ce point a été relevé encore récemment (Coetzee et Lubbe, 2014). Nous savons que les auditeurs doivent avoir une approche fondée sur les risques mais il est difficile de savoir comment ils procèdent en pratique.

Conclusion :

Les principaux travaux qui traitent de l'approche par les risques portent sur l'audit externe avec le développement du modèle « Business Risk Audit » (audit sur les risques) en réponse à des contraintes de baisse des honoraires. Plusieurs travaux indiquent que la mise en œuvre du modèle « Business Risk Audit » a constitué un moyen de revendiquer une nouvelle expertise à forte valeur ajoutée dans le domaine du contrôle interne et des risques pour accroître leurs activités.

Les recherches menées sur l'approche en audit interne traitent plus particulièrement du rôle de conseil de l'audit interne auprès du management et des instances de gouvernance lors de la mise en place des dispositifs de gestion des risques. Les travaux traitent également de l'effet du contexte institutionnel et réglementaire sur la pratique des auditeurs internes en matière de gestion des risques.

La revue de la littérature montre que les travaux réalisés sur l'approche par les risques de l'audit interne est un thème peu exploré. Ce point a été relevé récemment par Coetzee et Lubbe (2014). Nous savons que les auditeurs doivent évaluer les risques mais nous ne savons pas comment ils procèdent en pratique.

Nous allons aborder dans la partie suivante la qualité de l'audit interne.

1 - 4 LA QUALITE DE L'AUDIT INTERNE : QUELS CRITERES POUR L'EVALUER ?

L'évaluation de la qualité de l'audit interne est cruciale pour bien des organisations, tant les directions générales que la fonction doit servir que toutes les autres parties prenantes (actionnaires, auditeurs externes, ...).

Selon Gramling et al. (2004), la revue de la littérature nous montre que le thème de la qualité de l'audit interne a été essentiellement vu sous l'angle des auditeurs externes et de leur appréciation. Cette tendance est confirmée dans les travaux beaucoup plus récents qui appréhendent la qualité de l'audit interne sous le prisme de l'appréciation faite par les auditeurs externes. Ce constat s'explique notamment par le fait que les normes d'audit externes recommandent notamment aux auditeurs financiers d'utiliser les travaux des auditeurs internes dans le cadre de leurs diligences s'ils sont jugés de qualité (PCAOB, Auditing standards No. 5).

Cependant, de nombreux travaux mettent aussi en évidence l'évolution du rôle de l'audit interne, notamment en matière de gestion des risques, de gouvernance et de contrôle (Burton et al., 2012 ; Carcello et al., 2005 ; Cohen et al., 2010, Spira et Page, 2003). L'audit interne entretient dans ce cadre-là des relations avec toutes les autres parties prenantes du dispositif de gouvernance qu'elle sert telles que le comité d'audit, la direction générale et non pas uniquement les auditeurs externes (Cohen et al., 2004, 2010). Il est dès lors essentiel de comprendre comment et sur quelles bases ces dernières apprécient la qualité de l'audit interne.

Nous allons voir dans cette section les principaux travaux réalisés sur ce thème afin de recenser les principaux critères d'appréciation qui sont utilisés pour évaluer la qualité de l'audit interne.

1 - 4 1 LES CRITERES TRADITIONNELS

De Angelo (1981a) a défini la qualité de l'audit comme la probabilité jointe que l'auditeur va découvrir les fraudes ou irrégularités dans les états financiers du client et révéler au marché les fraudes ou irrégularités qu'il aura découvertes.

Si la première probabilité dépend de la compétence globale de l'auditeur (de ses capacités technologiques, de son niveau d'expertise, des procédures utilisées...), du niveau d'effort engagé dans la mission, la seconde probabilité dépend du niveau d'éthique professionnelle et d'indépendance du commissaire aux comptes vis-à-vis de son client.

Le modèle présenté par De Angelo indique que l'évaluation de la compétence et de l'indépendance de l'auditeur repose sur la perception du marché. En mettant l'accent sur l'indépendance et la compétence perçues, le modèle de De Angelo a contribué à de nombreuses recherches sur le lien entre la taille du cabinet et son appartenance aux grands réseaux et les résultats comptables et financiers des entreprises.

Ces éléments sont bien entendu transposables à l'audit interne mais seulement en partie. En effet, alors qu'en audit légal, l'indépendance se définit comme étant la capacité de l'auditeur externe à divulguer des fraudes ou des malversations financières (De Angelo 1981a ; 1981b), en audit interne, elle se définit selon la norme 1200 comme étant la « *capacité de l'audit interne à assumer, de manière impartiale, ses responsabilités. Afin d'atteindre un degré d'indépendance nécessaire et suffisant à l'exercice de ses responsabilités, le responsable de l'audit interne doit avoir un accès direct et non restreint à la direction générale et au Conseil. Cet objectif peut être atteint grâce à un double rattachement* ». (IIA, 2014). Également, en audit externe, la compétence de l'auditeur externe est définie comme étant sa capacité à détecter les fraudes et les inexactitudes (De Angelo 1981a ; 1981b) alors qu'en matière d'audit interne, la compétence de l'auditeur interne est associée aux « connaissances, savoir-faire et autres compétences nécessaires à l'exercice de ses responsabilités » (IIA, 2014).

L'indépendance pour les auditeurs internes est assimilée par les praticiens aux « aptitudes comportementales » des auditeurs internes telles que la capacité de respecter le caractère confidentiel des dossiers ou la capacité de travailler en équipe ainsi qu'au niveau hiérarchique de la fonction d'audit interne. La compétence est, quant à elle, une question « d'aptitudes techniques », telles que la compréhension des processus opérationnels et de gestion de l'organisation, incluant notamment le processus de gestion des risques (Burnaby et Hass, 2009). À ces deux critères de qualité s'ajoute le respect du code d'éthique de l'IIA qui reprend notamment les éléments de compétence, de confidentialité, d'intégrité et d'objectivité. L'objectivité étant un élément lié à l'approche méthodique et systématique telle que décrite par les normes professionnelles. Quant à la compétence, les normes d'audit sont peu précises sur la notion de compétence des auditeurs internes afin de permettre une appréciation de celle-ci. Elles précisent juste qu'au-delà des connaissances générales, l'auditeur doit avoir des aptitudes spécifiques en matière de détection de la fraude ainsi que des nouvelles technologies de l'information (IIA, 2014). Les auditeurs internes doivent selon les normes d'audit interne améliorer leurs connaissances, savoir-faire et autres compétences par une formation professionnelle continue.

Les critères d'indépendance et de compétence sont certes importants mais pas suffisants pour réellement pouvoir apprécier la qualité d'un audit. Les récents scandales financiers confirment la relativité de certains indicateurs indirects de la qualité d'audit. Pour l'audit externe, le principe d'uniformité de la qualité des prestations à l'échelle du cabinet ou du réseau a été mis en question. C'est le cas d'Andersen Houston, impliqué dans l'affaire Enron, dont le comportement a été mesuré plus « laxiste » que d'autres bureaux du réseau Andersen (Krishnan, 2005). Les investigations, menées par la SEC en octobre 2001, ont montré que l'audit interne est aussi inefficace dans cette affaire. La fonction, composée en partie d'anciens salariés du cabinet Andersen, a été orientée vers d'autres zones de risque et mise hors état de nuire. Le contexte Européen offre aussi plusieurs exemples d'inefficacité (Vivendi, Parmalat...). L'ensemble de ces constats conforte le besoin, aussi bien chez les praticiens que chez les chercheurs, de redéfinir les règles d'évaluation de l'audit (Chemangui, 2009).

Nous allons à présent voir comment les auditeurs externes apprécient et jugent de la qualité des travaux des auditeurs internes dans le cadre de leurs missions légales, tels que préconisés par leurs standards d'audit.

1 - 4 2 L'APPRECIATION DE LA QUALITE PAR LES AUDITEURS EXTERNES

Plusieurs travaux traitent de la question de la qualité de l'audit interne à travers l'évaluation qui en est faite par les auditeurs financiers. La revue de la littérature montre que le thème de la qualité de l'audit interne a été essentiellement vu sous l'angle des auditeurs externes et de leur appréciation (Gramling et al., 2004 ; Roussy et Brivot, 2016).

Les normes d'audit externes recommandent notamment aux auditeurs financiers d'utiliser les travaux des auditeurs internes dans le cadre de leurs diligences s'ils sont jugés de qualité (PCAOB, Auditing standards No. 5). Pour cette raison, ces études ont cherché à savoir quels étaient les critères d'appréciation de la qualité de l'audit interne retenus par les auditeurs financiers et comment ces critères pouvaient impacter leur décision d'utiliser ou non les travaux des auditeurs internes.

1 - 4 2 1 LES FACTEURS ORGANISATIONNELS (GOUVERNANCE ET MANAGEMENT)

Parmi les critères d'appréciation utilisés par les auditeurs financiers, certains auteurs se sont intéressés aux facteurs organisationnels qui pouvaient impacter la qualité de l'audit, tels que la qualité du comité d'audit et les signaux positifs envoyés par le management.

La qualité du comité d'audit est dès lors un des facteurs d'appréciation de la qualité de la fonction d'audit interne. Desai et al. (2010) ont modélisé l'évaluation de l'audit interne par les auditeurs externes et identifié que les facteurs associés avec le comité d'audit pouvaient impacter la qualité de l'audit interne. Ainsi, leurs résultats montrent que même si les auditeurs externes évaluent positivement la compétence, l'indépendance et la qualité des travaux des auditeurs internes, il leur sera difficile de considérer la fonction d'audit interne comme robuste en l'absence d'appréciation positive du comité d'audit. Ces résultats sont cohérents avec les études de Krishnamoorthy et Maletta (2012) qui confirment que les facteurs associés à la qualité du comité d'audit sont positivement corrélés avec l'appréciation de la fonction d'audit interne ainsi que le degré de coordination entre audit externe et audit interne. Selon Bertin et Godowski (2012), cette coordination est décrite comme étant non systématique dans le contexte français.

Le rattachement de la fonction d'audit interne constitue élément qui impacte l'appréciation de la qualité de l'audit interne. Gray et Hunton (2011) ont ainsi montré que l'appréciation positive des auditeurs externes de la qualité de la fonction d'audit interne pouvait augmenter lorsque celle-ci était rattachée au directeur financier plutôt qu'au comité d'audit. L'explication réside dans le fait que les critères d'appréciation de l'objectivité et de l'indépendance ne sont pas les mêmes en fonction du type de rattachement de la fonction d'audit interne.

La pression exercée par le client sur les auditeurs externes peut dans certains cas avoir des conséquences sur le degré d'utilisation des travaux de l'audit interne. Felix et al. (2005) ont cherché à étudier si la pression exercée par le client pour que les auditeurs externes utilisent les travaux des auditeurs internes avait des effets sur les auditeurs externes. L'étude montre globalement que non sauf dans le cas où l'auditeur externe fournit par ailleurs des prestations de conseil au client, indépendamment du niveau de qualité de l'audit interne.

1 - 4 2 2 LES FACTEURS LIÉS À LA FONCTION D'AUDIT INTERNE

La littérature traite des trois principaux facteurs identifiés dans les standards d'audit externes (SAS No. 65) pour évaluer la qualité de la fonction d'audit interne : l'objectivité, la qualité du travail et la compétence.

Les travaux de Gramling et al. (2004) ont montré que l'appréciation de ces facteurs était particulièrement complexe et qu'il dépendait du type de preuve et la nature des tests (objectif ou subjectif) et du type d'utilisation (travail déjà réalisé ou bien assistance des auditeurs internes durant leur mission).

L'étude de Messier et Schneider (1988) a par ailleurs montré que les critères fournis par les standards d'audit externes (SAS N° 9) sont peu précis en la matière et que la majorité des cabinets d'audit n'ont pas de politique spécifique pour y remédier. Les critères fournis par les standards sont la compétence, l'objectivité et le travail réalisé. Ainsi, l'étude montre que :

- la compétence (un des trois critères fournis par les standards) ressort comme étant le critère le plus significatif avant l'objectivité et enfin la nature du travail réalisé ;
- la pondération des sous-attributs associés (au total 26) à ces trois critères met toutefois en évidence une forte disparité entre les différentes évaluations faites par les auditeurs financiers interrogés.

Plusieurs études ont par ailleurs cherché à identifier le poids relatif de chacun des facteurs dans l'évaluation faite par les auditeurs externes (Schneider, 1984, 1985 ; Margheim 1986 ; Messier et Schneider 1988). Desai et al. (2010) ont mis en évidence au moyen d'un modèle d'évaluation de la fonction d'audit interne la forte interaction qui existait entre les trois facteurs que sont l'objectivité, la qualité du travail et la compétence. Ainsi, même dans le cas d'une évaluation négative d'un des trois facteurs, l'opinion globale reste positive si les deux autres facteurs sont bien évalués.

Enfin, les travaux ont mis en évidence que les auditeurs externes ont tendance à juger les fonctions d'audit interne externalisées comme étant plus objective (Desai et al., 2011 ; Glover et al., 2008 ; Arel, 2010). Ce constat n'est toutefois pas vrai lorsque l'activité d'audit interne externalisée est réalisée conjointement avec d'autres prestations de conseil au bénéfice de l'entité auditée (Brandon, 2010 ; Desai et al., 2011).

L'ensemble de ces travaux ne décrivent pas comment en pratique les auditeurs externes procèdent pour évaluer chacun des facteurs associés à la qualité de l'audit interne.

Enfin, selon DeZoort et al. (2001), le type de rémunération (en fonction des résultats de l'organisation ou un salaire fixe) influence la mesure selon laquelle la fonction d'audit interne est perçue comme étant indépendante. Ainsi, l'auditeur interne sera considéré comme plus indépendant si son salaire est fixe. Les résultats de l'expérience menée par Schneider (2009)

auprès de 157 auditeurs internes expérimentés indiquent que ni la rémunération basée sur les bénéfices, ni la détention d'actions de l'organisation ne semble influencer la planification des travaux de la fonction d'audit interne. En effet, lors de cette expérience, les participants devaient procéder à la planification préliminaire des travaux d'une fonction d'audit interne. Or, le fait que les auditeurs internes soient rémunérés en fonction des résultats de l'organisation ou le fait de détenir des actions de l'organisation n'a pas fait varier le nombre d'heures prévues par mandat, ni les tâches à effectuer.

L'indépendance, prérequis de l'objectivité, est associée à la position de l'audit interne dans l'organisation et à ses liens avec la direction et le comité d'audit (Stewart et Subramaniam, 2010). Ainsi, une fonction d'audit interne sera perçue comme étant indépendante si elle relève du comité d'audit (Archambeault et al., 2008 ; Gramling et al., 2004 ; Holt et DeZoort, 2009 ; Prawitt et al., 2009).

Les menaces à l'indépendance de l'audit interne ont été examinées par Christopher et al. (2009). Ces derniers en ont défini six grâce à un questionnaire d'enquête électronique expédié à quelque 206 directeurs de fonction d'audit interne australiens (taux de réponse de 17 % soit 34 réponses). Les résultats ont été comparés avec les « meilleures pratiques » reconnues en matière d'audit interne afin de faire ressortir les menaces à l'indépendance.

Trois des menaces qui ont été cernées sont liées aux relations entre l'audit interne et la direction des organisations. Les trois autres menaces se rapportent aux relations entre l'audit interne et le comité d'audit.

La première menace liée aux relations avec la direction est le fait que les individus se servent de leur fonction d'auditeur interne pour gravir les échelons plus rapidement dans l'organisation.

La seconde menace porte sur l'approbation du budget de la fonction d'audit interne par la direction de l'organisation, alors que les meilleures pratiques recommandent plutôt que ce soit le comité d'audit qui assume cette responsabilité, constitue la deuxième menace de ce groupe.

La troisième menace est le degré d'influence de la direction de l'organisation sur la planification annuelle des travaux de la fonction d'audit interne. Ainsi, plus la direction influence la planification, plus la menace à l'indépendance est forte.

1 - 4 2 3 NATURE DES TRAVAUX UTILISES PAR LES AUDITEURS EXTERNES

Les études ont porté sur la relation entre la décision d'utiliser le travail des auditeurs internes et plusieurs variables qui sont :

- les comptes et les risques inhérents associés à ces comptes ;
- les types de tâche (tâches subjectives qui requièrent plus de jugement ou bien objectives qui requièrent peu de jugement de la part de l'auditeur) ;
- la nature du travail réalisé (tests substantifs ou tests de contrôle).

Glover et al. (2008) ont montré que les auditeurs externes avaient tendance à moins utiliser les travaux des auditeurs internes pour les comptes associés à des risques inhérents jugés élevés et plus particulièrement pour les tâches subjectives, que la fonction d'audit interne soit sous-traitée ou non.

D'autres études se sont intéressées à cette même question en distinguant la possibilité pour les auditeurs externes de soit se limiter à la revue des travaux déjà réalisés par l'audit interne ou bien de les solliciter pour réaliser leurs missions. Munro et Stewart (2011) ont montré que la nature du rattachement de la fonction d'audit interne ainsi que les risques liés à l'activité influençaient la décision d'utiliser ou non les travaux des auditeurs internes, aussi bien pour utiliser les travaux déjà réalisés par ces derniers que pour leurs propres travaux.

1 - 4 3 L'APPRECIATION DE LA QUALITE PAR UNE APPROCHE PLUS GLOBALE

Même s'il est vrai que l'audit externe et l'audit interne présentent un certain nombre de similitudes comme les techniques d'audit (Abdolmohammadi, 2012), leurs différences limitent la possibilité d'utiliser les mêmes critères pour apprécier la qualité de l'audit interne. Ces différences portent notamment sur les exigences des normes d'audit auxquelles chacun doit se conformer, la nature des informations dont ils traitent et le degré d'homogénéité des rapports qu'ils produisent (Abdolmohammadi, 2012 ; Sarrens et al., 2009 ; Stefaniak et al., 2012). Nous allons voir dans cette section quels sont les apports des autres disciplines pour essayer de mieux appréhender le concept de qualité. Cette démarche vise à compléter les critères existants et à ne pas se limiter aux critères qui sont relatifs aux attributs de l'auditeur (indépendance et compétence). L'indépendance et la compétence constituent les principaux critères utilisés par les auditeurs externes.

1 - 4 3 1 AU-DELA DES CRITERES TRADITIONNELS : UNE APPROCHE « MULTIDIMENSIONNELLE »

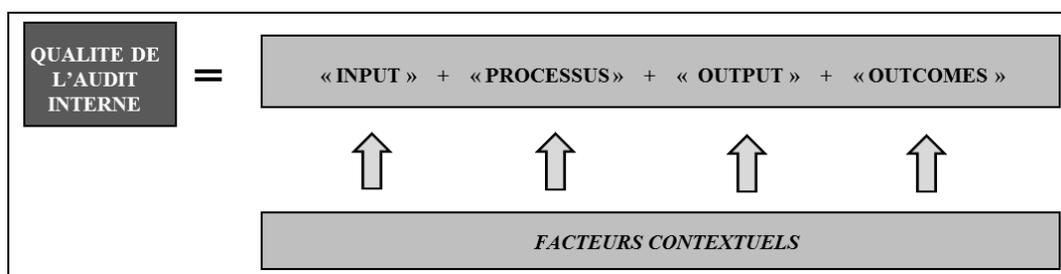
Le fait d'apprécier uniquement les attributs (« inputs ») de l'auditeur au travers de critères tels que leur compétence ou leur indépendance ne permet pas d'appréhender toutes les dimensions qui peuvent être associées à la qualité de l'audit interne.

Il est dès lors utile de s'intéresser aux autres facteurs qui pourraient nous permettre de mieux apprécier la qualité de l'audit interne. Pour ce faire, nous avons mobilisé d'autres disciplines de gestion afin de voir comment elles ont conceptualisé et cherché à mesurer la qualité. L'objectif recherché consiste à établir ou enrichir les critères d'appréciation traditionnels de la qualité de l'audit qui sont issus du modèle de De Angelo (1981a, 1981b).

La revue de la littérature sur le thème de la qualité abordée dans d'autres disciplines (systèmes d'information, marketing, psychologie) nous montre que la qualité est un élément contextuel qui peut varier en fonction des individus qui évaluent la qualité au regard de leurs besoins (Stvilia et al., 2007 ; Neely et Cook, 2011). Par ailleurs, ils montrent que la qualité est un construit multidimensionnel qui fait référence à plusieurs éléments : les données d'entrées, les processus mis en œuvre, les résultats et les facteurs contextuels (De Dreu et Weingart, 2003 ; Dirks, 1999 ; Hackman, 1987 ; Ilgen et al., 2005 ; Taggar, 2002).

Nous pouvons dès lors supposer que même si les attributs des auditeurs sont les mêmes, des différences au regard des informations dont ils disposent et du processus qu'ils mettent en œuvre peuvent donner lieu à des écarts sur les conclusions d'une mission d'audit. Vient s'ajouter à ces facteurs l'influence d'éléments externes (facteurs contextuels) qui peuvent échapper aux auditeurs tels que représentés dans le schéma ci-dessous.

Figure 10. Facteurs explicatifs de la qualité de l'audit



Francis (2011) a récemment apporté un cadre d'évaluation de la qualité de l'audit externe enrichi par rapport au modèle de De Angelo qui intègre ces différentes dimensions. Néanmoins, selon DeFond et Zhang (2014), il n'existe pas aujourd'hui de consensus sur ce qui pourrait constituer le bon critère de mesure de la qualité de l'audit. Certains travaux soulignent le fait que la perception de la qualité de l'audit varie en fonction des parties prenantes (Peecher et al., 2013).

I - 4 3 2 LE RESPECT DES NORMES D'AUDIT INTERNE : UN GAGE DE QUALITE

Un des critères de qualité de l'audit interne est le bon respect des normes professionnelles. En 2010, l'*Institute of Internal Auditors Research Foundation* (IIARF) a réalisé une étude auprès des membres de l'IIA au niveau international (une centaine de pays et plus de 13.500 répondants). Une base de données dénommée *Common Body of Knowledge in Internal Auditing* ou CBOK (2010) a été constituée pour réaliser des analyses et des rapports spécifiques.

À ce titre, l'étude du CBOK (« *Common Body of Knowledge* ») réalisée en 2010 par l'IIARF a permis de mettre en évidence une réduction du taux de conformité avec les normes d'audit internes par rapport à l'étude de 2006. Les répondants qui déclarent en 2010 ne pas totalement respecter les normes d'audit internes représentent 54% (sur un total de 13.500 répondants) contre 40% en 2006. Les principaux écarts avec les normes portent les mêmes éléments qu'en 2006 mais dans une plus grande proportion. Il s'agit notamment du bon dimensionnement des fonctions d'audit interne, des coûts jugés trop importants par les directions pour se conformer aux normes et du manque de soutien du management.

De façon plus spécifique, un des principaux écarts concerne le non-respect de deux normes qui sont les normes 1300 - *Programme d'assurance et d'amélioration de la qualité* et 2600 - *Acception du risque par la Direction Générale*. La norme 1300 requiert que les fonctions d'audit interne fassent l'objet d'une évaluation externe périodique et qu'elles établissent un plan d'amélioration continue de la qualité. La norme 2600 précise que les praticiens doivent informer le conseil en cas de prise de risques « inacceptable » pour l'organisation par le management en place.

Ces résultats ont été complétés par d'autres analyses plus spécifiques avec la dimension géographique (Burnaby et al. 2009 ; Leung et Cooper 2009 ; Marais et al. 2009 ; Abdolmohammadi, 2009).

En l'absence d'évaluation externe de la fonction d'audit interne, les auditeurs financiers doivent dès lors faire plus d'efforts pour apprécier la qualité de la fonction d'audit interne pour décider dans quelle mesure ils pourront utiliser leurs travaux.

1 - 4 3 3 LA COOPERATION ENTRE AUDIT INTERNE ET EXTERNE COMME AUTRE CRITERE

Un des éléments qui contribue à l'amélioration de la qualité d'audit est vraisemblablement la rigueur procurée par l'utilisation de méthodologies plus adéquates aux zones de risque de la firme. Cet élément contribue en lui-même à faire en sorte que le travail accompli apparaisse mieux construit, ne serait-ce que pour respecter les principes de formalisation.

Dans cette perspective, Chemangui (2009) propose une approche d'évaluation permettant de mesurer le niveau d'adaptation des travaux d'audit aux zones de risque de l'entreprise. La mise en œuvre d'un protocole expérimental selon le « paradigme de Churchill » permet la conception et la validation des échelles de mesure nécessaires à l'opérationnalisation de cette nouvelle approche.

La revue des résultats dégagés, quant à la fiabilité des échelles, permet de visualiser au moins deux divergences entre les travaux d'audit interne et ceux d'audit externe dans le contrôle des relations d'agence internes.

En effet, si l'auditeur interne est plutôt intéressé par le contrôle de la performance économique des salariés, l'auditeur externe exerce sa mission dans un souci de respect des obligations légales. La responsabilité légale de l'auditeur externe envers des parties externes à l'entreprise, notamment les institutions dotées d'un pouvoir de réglementation et de contrôle, l'oblige à exercer des contrôles de conformité réglementaire. Il constate par ailleurs que le contrôle du système de communication à l'échelle opérationnelle est une priorité pour l'audit interne, ce qui n'est pas le cas de l'audit externe qui cible les zones de risque à incidence financière significative. Ces deux niveaux de divergence entre les travaux d'audit interne et externe constituent la démonstration empirique d'une différenciation de plus en plus prononcée entre les deux mécanismes. Cette divergence sera vraisemblablement bénéfique pour la qualité globale des contrôles si elle est exploitée via une coopération effective entre les auditeurs internes et externes. Elle permettra un partage des résultats de contrôle et une meilleure appréciation des risques de la firme.

Conclusion :

Un des premiers modèles développés en matière d'appréciation de la qualité est celui de De Angelo (1981a). Ce dernier a défini la qualité de l'audit comme la probabilité jointe que l'auditeur découvre des anomalies ou des fraudes dans les états financiers du client et que l'auditeur les révèle au marché.

Le modèle de De Angelo souligne l'importance de recourir à des auditeurs suffisamment :

- compétents pour détecter les anomalies ;
- et indépendants pour pouvoir les dénoncer.

La revue de la littérature montre que le thème de la qualité de l'audit interne a été essentiellement vu sous l'angle des auditeurs externes (Roussy et Brivot, 2016) dont l'évaluation repose principalement sur les attributs des auditeurs décrits par De Angelo.

D'autres approches se sont développées au cours des dernières années tout en gardant comme fondement ce premier modèle. L'élément mis en avant dans les travaux plus récents souligne l'idée que la qualité de l'audit dépend du point de vue de ceux qui l'évaluent et de leurs attentes spécifiques.

Les recherches qui ont été menées n'adressent que partiellement la question de la qualité de l'audit interne pour être en mesure de l'apprécier au regard de son nouveau rôle en matière d'évaluation des risques organisationnels.

Conclusion générale :

Ce premier chapitre avait pour objectif de faire l'état de l'art sur le thème de l'audit interne au regard de son nouveau rôle en matière d'évaluation des processus de gestion des risques.

Un premier constat est qu'il y a un accord pour dire que l'audit interne :

- doit évaluer les processus de gestion des risques et de contrôle en vue de les améliorer au sein des organisations ;
- doit fonder son propre travail et sa méthodologie sur les risques.

Ce rôle n'est pas remis en cause dans les travaux existants.

Un deuxième constat découle de l'analyse détaillée des normes que nous avons réalisée. Cette revue a mis en évidence un paradoxe : la notion de risque n'est pas définie de façon précise et reste relativement ambiguë alors qu'elle représente le cœur d'activité de l'audit interne. Les normes ne définissent pas directement la notion de risque mais se réfèrent à d'autres cadres normatifs qui concernent les processus de gestion des risques tels que le modèle de l'ERM (Entreprise Risk Management). La revue complémentaire de ces référentiels ne permet pas de combler la lacune qui apparaît au niveau de la définition du risque dans les normes d'audit interne.

Un troisième constat est que le thème de l'approche par les risques en audit interne est relativement peu exploré. Les principaux axes développés dans la littérature se sont intéressés tout d'abord au lien entre l'audit interne et la gouvernance. Les travaux réalisés ne traitent pas de l'impact de l'audit sur l'amélioration des dispositifs de gouvernance. Sur le thème de la qualité, de nombreux travaux ont été réalisés et mettent en évidence le manque de consensus sur les critères d'évaluation de la qualité de l'audit. Toutefois, ils ne permettent pas d'apprécier comment l'audit interne fait en pratique pour évaluer les risques au sein de son organisation et pallier l'absence de définition soulevée précédemment.

Ces résultats confirment l'intérêt de notre recherche qui vise à mieux comprendre comment les auditeurs internes procèdent en pratique pour être en mesure d'évaluer les risques au niveau des organisations.

Nous allons aborder dans le chapitre suivant le cadre théorique.

2 ^{EME} CHAPITRE : CADRE THEORIQUE

La revue de la littérature que nous avons réalisée a permis de mettre en évidence que le risque tel que défini dans les normes d'audit reste une notion relativement « ambiguë » et qu'elle nous amène à nous interroger sur la manière dont les auditeurs internes procèdent pour passer des normes à la pratique lorsqu'il s'agit d'identifier et d'évaluer des risques au sein des organisations.

Les travaux de recherche menés jusqu'ici sur le thème de l'audit interne ne traitent pas véritablement de cette question.

La conception traditionnelle du risque en tant que mesure qui repose sur une approche probabiliste ou fréquentiste présente certaines limites pour étudier la pratique de l'audit interne. La première limite est que cette approche semble inopérante pour les auditeurs en l'absence de données historiques suffisantes. Une seconde limite est qu'elle ne permet pas de traiter du risque au niveau organisationnel. Or, notre objectif est d'étudier non pas le risque au niveau individuel mais collectif puisque l'audit est en charge d'évaluer le risque au niveau des organisations.

La sociologie du risque nous apporte des concepts intéressants pour questionner l'audit interne et ses normes professionnelles qui fondent sa méthodologie sur l'identification et l'évaluation des risques au sein des organisations. L'analyse renouvelée proposée par la sociologie du risque permet d'étudier les processus mis en œuvre par l'audit interne tout en considérant les contraintes et les intérêts institutionnels ou organisationnels.

Elle adresse notamment un certain nombre de questions :

- pourquoi un problème est-il reconnu comme un risque alors qu'un autre ne l'est pas ?
- pourquoi parmi les problèmes reconnus comme un risque, seuls certains sont pris en considération ?
- comment s'effectue la hiérarchisation des risques ?

Plusieurs auteurs (Douglas, Giddens, Beck et Luhmann) ont fortement contribué au développement de ce courant. Ils se distinguent par leurs analyses et leurs contributions respectives. La sociologie du risque cherche à expliquer dans quelle mesure et de quelle manière le risque est un objet socialement construit par les acteurs en interaction, sous l'influence du contexte social, culturel et politique.

C'est la raison pour laquelle nous avons privilégié pour notre recherche ce cadre théorique qui permet de traiter de la question du risque au niveau organisationnel.

Nous verrons dans un premier temps les principales grandes approches issues de la sociologie des risques tout en soulignant leurs spécificités. Nous développerons ensuite plus en détail l'approche que nous avons décidé de mobiliser en particulier dans le cadre de cette recherche. Enfin, nous concluons ce chapitre par une synthèse des principaux concepts mobilisés et des questions de recherche qui résultent de notre cadre théorique ainsi constitué.

2 - 1 LE RISQUE COMME CONSTRUIT SOCIAL

Nous tenterons dans la première partie d'explicitier les principales grandes approches qui se distinguent au sein de la sociologie du risque afin de déterminer. Nous traiterons notamment de l'approche ethnologique et culturelle de Mary Douglas et Aaron Wildavsky, des risques vus sous l'angle de la modernité réflexive avec Anthony Giddens, de la théorie des systèmes sociaux de Niklas Luhmann et nous terminerons par la société du risque décrite par Ulrich Beck.

2 - 1 1 L'APPROCHE CULTURELLE DE MARY DOUGLAS ET AARON WILDAVSKY

Le courant psychométrique qui s'est intéressé aux biais cognitifs des individus pour expliquer les écarts de perception des risques présente une limite majeure. Il n'explique pas pourquoi certains risques apparaissent comme étant plus « effrayants » dans certaines sociétés et moins dans d'autres. La théorie culturelle de Douglas nous apporte un autre éclairage en partant de l'idée que les différences de perception et de sélection des risques ne se jouent pas au niveau des individus mais à un niveau supérieur, celui des groupes et des institutions. C'est donc au début des années 1980 que l'anthropologue Mary Douglas va être amenée à s'intéresser aux risques, et plus particulièrement aux risques technologiques et environnementaux, sur l'invitation du politologue Aaron Wildavsky. Ils ont écrit *Risk and Culture* (1982) qui pose les premiers jalons de leur théorie culturelle des risques et adresse la question de l'impact des valeurs et de la culture sur notre perception du risque. Nous verrons dans cette partie le concept de « biais culturel » développé par Douglas pour expliquer les écarts de perception du risque et ensuite la typologie des groupes culturels qu'elle a appliquée au concept de risque pour approfondir son analyse.

2 - 1 1 1 LES « BIAIS CULTURELS »

En cherchant à la question de savoir pourquoi les individus n'appréhendent pas tous les risques de la même manière, Douglas a pu établir une distinction nouvelle entre les termes « risque » et « danger ». Le terme « Danger » renvoie selon Douglas aux dangers du monde extérieur qui sont bien réels mais pas nécessairement perçus par les individus. Le terme « Risque » désigne quant à lui les dangers socialement sélectionnés sur la base de nos valeurs. Le risque correspondrait ainsi selon Douglas à une représentation contrairement au danger qui conserve un statut ontologique réel. La sélection de certains dangers parmi l'ensemble des possibles est une nécessité car il n'est pas possible de tout appréhender de façon simultanée. Il faut fixer des priorités et hiérarchiser les menaces. Cette hiérarchisation se fait sur la base de nos valeurs.

En effet, ce sont nos valeurs qui nous permettent de définir la valeur positive ou négative que nous accordons à chaque chose. Ainsi, des individus qui partagent des valeurs liées à l'environnement évalueront par exemple des informations relatives à la probabilité d'accident d'une centrale nucléaire de façon totalement différente qu'un autre groupe qui soutient les activités nucléaires. Selon la théorie culturelle, les individus choisissent les risques qu'ils redoutent en lien avec les valeurs et la culture du groupe auquel ils appartiennent. Il existe en effet une certaine cohérence entre un groupe social et son système de valeurs. Afin d'identifier ces différents groupes sociaux, Douglas et Wildavsky ont développé la typologie du « Grid-Group » sur laquelle nous reviendrons plus en détail.

Douglas et Wildavsky soutiennent l'idée que les différences de perception et de sélection des risques ne se jouent pas au niveau des individus mais à un niveau supérieur, celui des groupes et des institutions. Il s'agit d'une démarche « structuro-fonctionnaliste » qui met l'accent sur la pression que les groupes et les institutions exercent sur les individus, plutôt que sur les tactiques éventuellement mises en œuvre par les individus pour y échapper.

La culture nous fournit alors un cadre de perception spécifique, qui détermine la façon dont nous appréhendons le monde et donc les risques avec des biais « culturels ». Dans la culture, M. Douglas et Wildavsky considèrent les principes, les jugements et les représentations qui guident et qui nourrissent les actions des individus. Ils définissent la culture comme « la collection publiquement partagée de principes et de valeurs utilisés à chaque moment pour justifier les conduites ».

Les travaux de Douglas et Wildasky ont contribué à l'évolution du concept de risque en favorisant la reconnaissance d'une conception constructiviste du risque. Leur analyse culturelle du risque a le mérite de montrer qu'il serait réducteur d'attribuer les raisons des « peurs » à un défaut de connaissance des individus et des phénomènes psychologiques. Leur approche permet ainsi de sortir de l'opposition entre « rationalité » et « irrationalité » et de mettre en valeur le fait que les jugements des individus ne se forment pas indépendamment du contexte social et des valeurs.

Selon Douglas, notre rapport au temps est un facteur essentiel dans notre manière d'appréhender les risques.

Notre capacité à nous projeter dans l'avenir est socialement différenciée : la précarité nous amène à nous focaliser sur le présent et à l'inverse la sécurité matérielle à nous préoccuper d'un horizon plus lointain. Le rapport au temps constitue un premier effet de biais culturel.

L'attitude d'un individu à l'égard d'un danger dépend aussi des sources d'information qu'il privilégie. Nous n'accordons pas la même légitimité et le même degré de confiance à toutes les sources d'information en fonction de nos « croyances » et de nos valeurs. Les informations sont filtrées en fonction de leurs origines.

Sur un plan fonctionnel, les risques fournissent des arguments qui permettent d'organiser les relations au sein d'un groupe social et d'assurer sa cohésion. Pour y parvenir, il est nécessaire de définir les responsabilités individuelles ainsi que les solidarités collectives nécessaires pour contrôler les menaces qui pèsent sur le groupe. Dans le dialogue social, les individus utilisent les risques comme argument pour se convaincre ou s'obliger les uns les autres à se comporter d'une certaine façon et pour justifier leurs conduites et leurs actions. Le partage de mêmes craintes et de mêmes attitudes à l'égard des risques participe à la constitution et à l'affirmation de groupes sociaux légitimes aux yeux de leurs membres. Les idées et les attitudes à l'égard des risques ne peuvent pas être expliquées de façon satisfaisante par l'existence d'incertitudes et de dangers, mais qu'elles doivent prendre en compte les biais que procurent les institutions sociales et qu'elles peuvent s'analyser comme des ressources qui participent à la construction d'un ordre social.

Douglas illustre cette idée en décrivant le cas des Himas, une tribu qui vit presque exclusivement de l'élevage. Le risque majeur pour cette tribu est la contamination de leurs troupeaux par le simple contact avec les femmes. Les femmes sont tenues à l'écart des

troupeaux et il est interdit de travailler. Par conséquent, afin de faire face au manque de main-d'œuvre, les hommes mariés partagent leur épouse avec leurs frères, leurs pères et d'autres hommes afin qu'ils travaillent pour eux. Cette situation contribue à maintenir un certain équilibre entre le nombre des membres de la tribu et les troupeaux, le risque étant de ne pas avoir suffisamment de bêtes pour nourrir l'ensemble de la tribu. La peur de voir les troupeaux contaminés par les femmes permet de réguler et de maintenir l'ordre social établi au sein de la tribu. Les risques occupent, dans des sociétés industrielles marquées par une homogénéisation culturelle, une place comparable aux notions de péché et de tabou dans les sociétés à dominante religieuse.

La théorie culturelle de Douglas nous permet de dépasser le simple constat de l'irrationalité des individus face aux risques. Avant d'analyser la manière dont la théorie culturelle de Douglas a été appliquée au concept de risque, il est important de revenir à son modèle du « Grid / Group ».

2 - 1 1 2 LE MODELE DU « GRID / GROUP » ET LA THEORIE CULTURELLE DE DOUGLAS

La théorie culturaliste de Douglas se donne pour objectif de fournir une théorie qui permet d'établir une relation entre « cultures » et « formes sociales ». Il faut comprendre la « culture » comme étant l'ensemble des croyances et valeurs partagées par un groupe et l'expression « forme sociale » comme la manière dont sont structurées les relations interpersonnelles. L'hypothèse de Douglas, dans la théorie culturaliste, est que « formes sociales » et « cultures » contribuent à se stabiliser mutuellement, c'est-à-dire que chaque forme sociale est maintenue par un type de culture et réciproquement. Douglas conçoit la culture comme un cadre de référence que les individus intériorisent et transforment au cours de leurs interactions. Les individus construisent ainsi le sens de leurs actions selon les exigences de la forme sociale dans laquelle ils évoluent.

Mary Douglas cherche à déterminer un moyen qui lui permettrait d'établir une classification des relations sociales applicables aux groupes d'individus. Elle établit deux critères qui sont la « différenciation des rôles » et « l'incorporation sociale » pour analyser et expliquer la manière dont se structurent les relations sociales au sein des groupes.

L'incorporation sociale correspond à l'intensité du lien qui existe entre l'individu et le groupe, c'est-à-dire son degré d'intégration sociale dans une unité sociale. A titre d'illustration, un individu peut faire partie d'un groupe en assistant simplement à une réunion annuelle ou bien en intégrant pour la vie les ordres religieux.

La différenciation des rôles correspond au degré d'organisation interne du groupe et à la nature des interrelations entre les individus qui le composent. Plus la différenciation des rôles est forte, plus les rôles sociaux sont bien déterminés et les relations entre les individus régulés par un ensemble de hiérarchisation institutionnalisées.

La première dimension (Group) renvoie à la façon dont un groupe se définit par rapport aux autres afin d'affirmer son identité propre et représente la « frontière que les gens ont érigée entre eux et le monde extérieur. Cette dimension traduit aussi un degré de contrôle qu'exerce le groupe sur la vie des individus qui le composent. Ses membres doivent, pour pouvoir en faire partie, accepter un certain nombre de contraintes lié au groupe qu'il faudra respecter. Ces contraintes collectives qui doivent être respectées seront plus ou moins exigeantes d'un groupe à l'autre. À titre d'illustration, il sera possible d'appartenir à un groupe religieux en allant une fois par semaine à l'église mais il ne s'agira pas du même que celui des moines qui devront s'investir totalement dans leur vie au monastère.

La seconde dimension (Grid) renvoie à la structure interne du groupe, à la façon dont sont les relations régulées entre ses membres (hiérarchisé, égalitaire, ...). Il s'agit de toutes les autres distinctions et délégations d'autorités qu'ils utilisent pour limiter le pouvoir des gens les uns par rapport aux autres. Cette dimension traduit le niveau de contrôle que les membres sont prêts à accepter.

Ces deux dimensions permettent de définir ce qui constitue la limite externe à un groupement ainsi que les règles de son fonctionnement interne.

Chaque communauté est composée de plusieurs cultures à la fois est chacune de ces cultures s'auto-définit par opposition aux autres. Appliqué à son modèle du « Grid / Group », celui-ci devient une théorie culturelle selon laquelle quatre types de biais culturels sont normalement présents dans chaque communauté. Le modèle initial du « Grid / Group », qui était un modèle statique et descriptif des différents types de culture au sein des organisations, devient un modèle dynamique du fait de la compétition qui naît entre les différentes cultures.

Son approche a pour cadre de référence un individu qui a une conscience plus ou moins grande de son intégration à une totalité sociale et qui choisit entre différents modèles possibles de conduites et de relations. Les quatre types d'institutions constituent des options exclusives les unes des autres pour orienter l'action sociale des individus. En optant pour un modèle de relations, un individu est également contraint d'adopter un style de pensée compatible avec ce

modèle ou, inversement, il doit développer des relations et des actions cohérentes avec les principes auxquels il marque son adhésion.

Selon les quatre combinaisons « Grid / Group » qui sont possibles, Douglas établit quatre types de culture qu'elle a appliqués de façon plus spécifique au concept de risque.

2 - 1 1 3 APPLICATION DU MODELE « GRID / GROUP » AU CONCEPT DE RISQUE

Au cours des années 1970 et 1980, Douglas explore le rapport des sociétés modernes industrialisées au risque tant économique que technologique, soit près de dix ans avant que la question n'émerge en Europe suite à l'accident de Tchernobyl. Ces travaux répondent au débat civil apparu aux Etats-Unis au début des années 1970 sur la question des risques environnementaux. C'est à cette même période que des groupes comme Greenpeace (1971) naissent. Ainsi, la notion de risque, autrefois appréhendée de façon essentiellement calculatoire, s'élargit pour devenir plus flou et diffus sous la pression du mouvement social.

Douglas estime qu'il est difficile de traiter de la question de risque en se fondant sur une échelle de mesure unique. Lorsqu'il s'agit de traiter de la question de l'acceptabilité du risque et de son imputabilité, le calcul probabiliste ne suffit pas et il est alors nécessaire d'envisager d'autres critères pour appréhender et traiter de ces questions. En effet, lorsqu'il s'agit de savoir quels risques valent la peine d'être pris, l'approche probabiliste reste limitée puisqu'elle ne peut intégrer ni les dimensions morales, ni les dimensions politiques.

Parmi les autres critères et dimensions, Douglas (1982) rappelle un certain nombre de travaux dont elle montre l'intérêt mais aussi les limites pour traiter de la question de l'acceptabilité. Parmi les principaux travaux auxquels elle se réfère, aucun n'apporte une réponse satisfaisante. Ni la théorie de Maslow sur la hiérarchie des besoins (la sécurité étant classée comme fondamentale), ni les propositions de C. Starr (opposition entre les risques volontaires pris en connaissance de cause et les risques qui sont imposés par les autres), de J. Ester (distinction entre les risques réversibles et irréversibles), de L. Lave (plus les gens sont en sécurité, et plus ils sont réfractaires aux risques avec l'idée de dire que le « plus vous possédez de choses, plus vous avez à perdre ») ne l'ont convaincue.

À l'issue de cette revue, Douglas considère que ces caractéristiques du risque ne suffisent pas à expliquer les différences socioculturelles dans la perception des risques par de simples oppositions binaires. Selon Douglas, la façon dont nous appréhendons les risques dépend de deux éléments indissociables : notre position sociale et notre système de valeurs.

Elle propose d'enrichir l'approche avec l'utilisation d'une matrice d'attitudes situées en vis-à-vis les unes des autres qu'elle nomme le modèle « Grid / Group ». Ce modèle résulte de l'idée que notre perception des risques est fonction de notre position sociale et de notre système de valeurs. Notre représentation et nos attitudes vis-à-vis du risque dépendront de la catégorie à laquelle nous appartenons.

Douglas identifie alors quatre types de culture pour montrer que la mise en cause d'acteurs ou de comportements au nom des risques qu'ils font subir à la collectivité peut varier selon les principes culturels qui caractérisent chaque institution.

Les fatalistes (ou exclus) représentent les exécutants, caractérisés par une situation de subordination, dans un groupe fermé à forte hiérarchie. Ils sont caractérisés par leur incapacité à se mobiliser et à agir. Ils ne constituent pas un groupe solidaire. C'est ce qui traduit leur attitude fataliste. Pour eux, la nature est capricieuse : sur une surface plane, la bille peut rouler dans n'importe quelle direction. Ils sont preneurs de risque mais de façon passive pensant qu'ils n'y échapperont pas de toute façon. La culture fataliste pratique le déni du risque : « C'est comme ça, on ne peut rien y faire ».

Les individualistes (ou entrepreneur) ne craignent ni le changement, ni l'incertitude. Ils sont caractérisés par l'absence de lien de subordination et de sentiment de groupe entre leurs membres. Pour eux, le risque est une opportunité plus qu'une menace. Ils sont caractérisés par la recherche du risque et l'acceptation de la perte associée. Ils font confiance à leurs capacités pour maîtriser le destin. Ils ne se préoccupent pas du long terme faisant confiance aux mécanismes du marché. Pour eux, la nature est robuste : la bille est en équilibre stable au fond d'un creux. Même si elle est déplacée, elle retrouvera son équilibre. La culture individualiste encourage au contraire les individus à prendre des risques, à investir, à se dépasser : « Qui ne tente rien n'a rien ».

Les bureaucrates ou hiérarchiques sont caractérisés par une frontière fortement marquée et une structure fortement hiérarchisée. Leurs membres vivent dans des mondes compartimentés, où il y a peu de mobilité et où les marges de libertés sont limitées. La structure fournit une liste des problèmes que ses membres sont susceptibles de rencontrer, en décrivant des réponses standardisées à leur apporter. Elle est par essence routinière et rigide pour faire face aux transformations de son environnement. Elle détecte mal les nouveaux problèmes et ne sait y répondre qu'en instituant de nouvelles réglementations. Ses membres sont averses donc aux risques en général et peu réactifs pour réagir à des situations nouvelles de risques. Ils font

confiance au savoir scientifique institutionnel détenu et produit par les savants légitimés par les autorités. La nature est robuste jusqu'à un certain point (la bille ne doit pas dépasser les limites de la butte pour retomber dans son creux). Si les déchets organiques sont assimilés par la nature, il n'en est pas de même pour les déchets chimiques !

Les égalitaires (frontière marquée et structure non hiérarchisée) sont fortement averses aux risques catastrophiques qui mettent en danger la survie de l'espèce humaine et la planète. Cette focalisation sur les risques globaux amène à une dénonciation du système extérieur à l'enclave. Il permet ainsi d'entretenir la cohésion de ses membres. Ils se méfient du savoir validé par la structure hiérarchique et ont tendance à mobiliser leurs propres sources de savoir et contre expertises. Pour eux, la nature est fragile : la bille est posée au sommet d'une butte. Le moindre écart risque de détruire son équilibre.

Toutefois, l'application pratique de ce cadre n'est pas aisée lorsqu'il s'agit de déterminer à quel groupe appartient un individu en particulier. Certains peuvent en effet se reconnaître dans plusieurs groupes (haut fonctionnaire recruté dans une grande multinationale, militant associatif retraité de l'industrie dont il est riverain et ancien élu, ...) de culture et d'autres dans aucun de ces groupes de culture. Il est aussi important de se rappeler le contexte dans lequel cette typologie. La théorie culturelle de Douglas a été adaptée pour étudier les mouvements écologistes aux États-Unis. Le cadre conceptuel présenté peut nécessiter d'être adapté.

Conclusion :

Douglas soutient l'idée que les différences de perception et de sélection des risques ne se jouent pas au niveau des individus mais à un niveau supérieur, celui des groupes et des institutions. Il s'agit d'une démarche « structuro-fonctionnaliste » qui met l'accent sur la pression que les groupes et les institutions exercent sur les individus, plutôt que sur les tactiques éventuellement mis en œuvre par les individus pour y échapper. Le modèle « Grid / Group » qu'elle propose résulte de l'idée que notre perception des risques est fonction de notre position sociale et de notre système de valeurs. Notre représentation et nos attitudes vis-à-vis du risque dépendront de la catégorie à laquelle nous appartenons.

2 - 1 2 LES CONSEQUENCES DE LA MODERNITE POUR ANTHONY GIDDENS

Après avoir proposé la théorie de la structuration, Anthony Giddens aborde la question des conséquences de la modernité. Dans son ouvrage intitulé « les conséquences de la modernité », il traite de la question du risque qui est, comme pour Beck (1986), le résultat de la modernité réflexive et du lien entre le risque et la confiance.

2 - 1 2 1 LA DYNAMIQUE DE LA MODERNITE

Selon Giddens (1991), la dynamique de notre société moderne repose sur trois mécanismes : la séparation du temps et de l'espace, la délocalisation des relations sociales et l'appropriation réflexive des connaissances.

La séparation du temps et de l'espace permet de développer des échanges et des relations entre des personnes qui ne sont pas face à face. La coprésence dans un même lieu n'est plus nécessaire pour établir des relations avec autrui. La dématérialisation des échanges, l'assouplissement des frontières entre marchés et territoires, et la déconnexion des activités humaines ont engendré des processus tels que les risques peuvent apparaître en dehors des zones d'où proviennent leurs causes (faits générateurs). Ces conséquences ne sont plus aisément perceptibles ni dans le temps ni dans l'espace.

La délocalisation des systèmes sociaux (détachement d'une activité de son contexte local) représente l'idée que les relations sociales ne sont plus liées à un lieu grâce à deux mécanismes : les gages symboliques et les systèmes experts. Ces systèmes ont besoin de la confiance pour exister et fonctionner. La confiance en des entités abstraites, des institutions lointaines est à la fois une condition et une conséquence de la modernité.

- Les gages symboliques constituent des éléments d'échange qui peuvent circuler à tout moment quelques soient les caractéristiques des individus qui l'utilisent. L'argent en est un exemple. Il permet des échanges entre des individus éloignés dans le temps et l'espace. C'est un moyen de délocalisation. C'est à l'institution monétaire que l'on fait confiance et non à la personne avec laquelle la transaction a lieu.
- Les systèmes experts sont des systèmes techniques utilisés par des personnes qui n'ont pas besoin de connaître leurs principes et fondements. Se confier à l'hôpital implique une foi dans le savoir expert, plus que dans la personne du chirurgien, sans être pour

autant capable de vérifier la réalité de ce savoir. Son bon fonctionnement repose sur une confiance pratique dans un système abstrait.

La confiance est devenue cruciale car la plupart des opérations se font à distance, sans avoir la possibilité d'avoir des repères visibles dans l'espace et le temps. Il est a priori inutile de faire confiance à quelqu'un ou quelque chose tant qu'on peut le surveiller en permanence mais avec la modernité, la confiance devient une condition nécessaire. La confiance n'est plus attribuée à une personne mais à un système abstrait. Cette confiance prend alors la forme d'un engagement anonyme et impersonnel qui traduit la foi dans un système dont le profane ignore le contenu et le fonctionnement.

Cette confiance envers des systèmes abstraits peut s'établir grâce notamment au respect qui existe chez les individus pour les spécialités techniques issues des sciences. Giddens explique que ce respect résulte de l'influence de l'enseignement des sciences durant notre scolarité puisque nous considérons par la suite ce savoir comme un savoir fiable. La confiance est nécessaire en cas d'incertitude et d'ignorance. Or, l'ignorance nous dit Giddens est de nature à créer du scepticisme et du doute. Cette confiance envers les systèmes abstraits est ainsi décrite non pas comme un engagement sans arrière-pensée mais un engagement pour lequel nous n'avons pas vraiment d'autres choix. Avec le développement des systèmes abstraits, la confiance envers des principes et des inconnus est devenu indispensable à l'existence sociale.

La confiance établie envers les systèmes abstraits doit être entretenue dans le temps et l'espace par ce que Giddens nomme le mécanisme de relocalisation. Celui-ci consiste à créer des points de contact physique de face-à-face entre profanes et représentants des systèmes abstraits qui se donne du mal pour montrer qu'ils sont dignes de confiance. Ce sont pour les systèmes abstraits des lieux de vulnérabilité, mais aussi des points de jonction où peut s'entretenir la confiance.

Giddens précise qu'aucune spécialité, aucun système abstrait, aussi parfaits soient-ils, n'excluent totalement le hasard ou le risque. Les spécialistes estiment selon Giddens que les profanes sont en général plus rassurés lorsqu'on leur dissimule la fréquence de ces aléas. Il insiste notamment sur la différence entre spécialité et spécialiste. Un spécialiste peut se tromper, en interprétant ou en connaissant mal la spécialité qu'il est censé maîtriser.

L'appropriation réflexive des connaissances est le dernier mécanisme décrit par Giddens. Nul n'est sûr que chaque élément du savoir ne sera pas remis en cause. Nous souhaitons augmenter la connaissance du risque et réduire l'incertitude dans une optique de maîtrise. L'être humain contrôle en permanence son action. Il reste en contact avec ses intentions par le contrôle réflexif

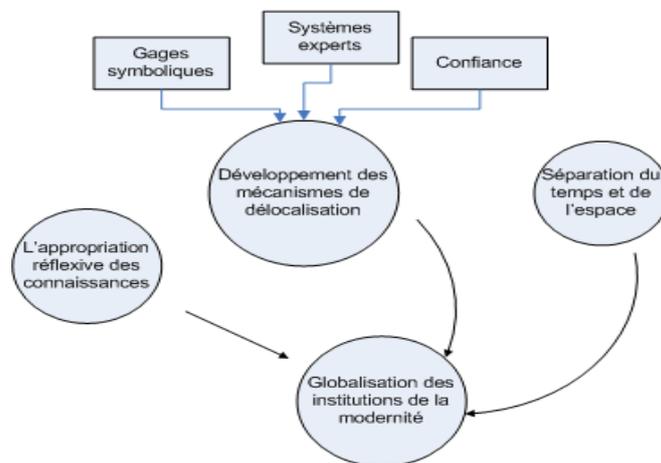
de l'action. L'action et la réflexion se renvoient, l'action est jugée à l'aune du savoir nouveau produit par la connaissance qu'ont les acteurs de leur action. Ainsi, les décisions du profane peuvent ainsi être guidées, par exemple, par sa connaissance des statistiques du mariage, des divorces.

Cependant, cette connaissance ne permet pas un contrôle de notre destinée. Pour cela, il faudrait que la vie sociale soit bien distincte du savoir la concernant et que la savoir cumulé permette d'accroître la rationalité des décisions des acteurs.

Notons que l'attitude des profanes envers le savoir technique comporte une part d'ambiguïté. Beaucoup font un "pacte" avec la modernité en faisant confiance aux gages symboliques et aux systèmes experts, sorte d'attitude pragmatique en somme.

Les attitudes de confiance ou de défiance envers certains systèmes abstraits peuvent en effet être fortement influencées par des expériences vécues aux points d'accès ou par des réactualisations de connaissances qui, via les médias et d'autres sources, sont offertes aux profanes comme aux spécialistes.

Figure 12. Mécanismes de délocalisation (Giddens, 1991)



2 - 1 2 2 LA CONFIANCE ET LE SENTIMENT DE SECURITE

Pour Giddens (1991), la notion de confiance est, comme chez Luhmann, relative au risque. « Risque » et « Confiance » sont indissociables puisque la confiance présuppose une conscience du risque encouru. L'individu est conscient des choix possibles. Selon Giddens, les

travaux de Luhmann sont importants car ils nous orientent vers un certain nombre de distinctions conceptuelles utiles pour appréhender la notion de confiance. Etant en désaccord sur certaines de ses idées, il propose une conceptualisation différente de la confiance et des notions qui lui sont liées qu'il résume en une dizaine de points repris dans le tableau suivant.

Tableau 5. Dimension de la « Confiance » (Giddens, 1991)

1	La confiance est liée à l'absence dans le temps et l'espace. Nous n'avons pas besoin de faire confiance à quelqu'un dont les activités sont visibles en permanence et dont les modes de raisonnement sont transparents, ni de faire confiance à un système dont nous connaissons et comprenons parfaitement les rouages.
2	La confiance est liée à la contingence et non pas au risque. Nous pouvons compter sur quelqu'un ou quelque chose face à certaines contingences liées aux actions humaines ou au fonctionnement des systèmes.
3	La fonction est d'une certaine manière une confiance aveugle.
4	La confiance envers des gages symboliques et des systèmes experts repose sur la foi en la validité de principes que nous ignorons.
5	La confiance peut être définie comme « un sentiment de sécurité justifié par la fiabilité d'une personne ou d'un système, dans un cadre circonstanciel donné ».
6	Le concept de risque remplace celui de fortuna et l'idée de hasard apparaît en même temps que l'idée de risque.
7	Le risque et le danger sont deux éléments liés mais distincts. Toute personne qui prend un risque s'expose à un danger, le danger étant défini comme la menace qui peut affecter un résultat attendu. Toutefois, il est possible que des individus agissent sans avoir conscience du danger qu'ils courent.
8	Le risque et la confiance sont indissociables. Le risque acceptable dépend du savoir induit et il y a équilibre entre confiance et calcul de risque.
9	Le risque n'est pas uniquement un problème lié à l'action individuelle. Il existe des environnements à risque qui peuvent affecter un grand nombre d'individus comme dans le cas d'une guerre nucléaire.
10	Le contraire de la confiance ne se limite pas à la méfiance ou la défiance. Il peut être désigné par les expressions telles que l'« angoisse » ou la « terreur existentielle ».

Après avoir développé le concept de confiance, Giddens développe le concept de sécurité. Il parle plus particulièrement de la sécurité ontologique qui constitue une forme de sentiment de sécurité (phénomène émotionnel enraciné dans l'inconscient). Il nous donne l'exemple d'un individu qui vit dans l'inquiétude permanente d'une guerre nucléaire, incapable d'écarter cette idée de son esprit. Alors que la majorité des individus considèrent ce type d'angoisse comme

irrationnelle, ce comportement est selon lui plus le résultat d'une hypersensibilité que d'une irrationalité. Il cherche alors à répondre à la question de savoir pourquoi la majorité des gens ne sont pas dans un sentiment d'insécurité face à ce type d'interrogations potentielles, étant donné que le risque nucléaire et d'autres sont pourtant bien réels.

Selon lui, le sentiment de sécurité éprouvé par rapport à ces risques remonte en partie à une part d'expériences vécues durant notre enfance. La majorité des individus reçoit une dose de confiance de base au début de leur vie. Une sorte de vaccin émotionnel qui leur est apportée par la personne qui prend soin d'eux, généralement leur mère. Un aspect fondamental dans la confiance qui s'établit dans cette période de l'enfance est la certitude pour le nourrisson, du retour de l'adulte qui s'en occupe. L'absence de la mère ne signifie pas la privation de l'amour. La confiance permet ainsi de mettre entre parenthèses la distance dans le temps et l'espace. La confiance devient un besoin psychologique d'une nature persistante qui se retrouve tout au long de notre vie.

Confiance, sécurité ontologique, continuité des choses et des personnes, routines, sont intimement ainsi liées dans la personnalité adulte. Ainsi la confiance dans la fiabilité des systèmes abstraits est fondée sur une foi dans la fiabilité des êtres humains et la routine nourricière. La confiance dans la fiabilité de l'autre est un besoin psychologique, elle repose sur des routines qui demandent une attention continue de la conscience pratique. Les routines intégrées aux systèmes abstraits sont essentielles pour maintenir la sécurité ontologique. Lorsque de telles routines sont bouleversées, nous pouvons voir apparaître l'anxiété. Ainsi, la sécurité ontologique et la routine sont fortement liées.

La sécurité ontologique qui nous est décrite par Giddens repose sur des éléments de contexte social fondamentalement différents dans les cultures prémodernes et modernes.

Dans les cultures prémodernes, la sécurité ontologique est liée au contexte local. Le premier contexte de confiance est lié à la parenté. La communauté, en tant que lieu des relations sociales, y contribue aussi. Le second contexte de confiance est lié à la religion, la croyance en la divinité. Le dernier est la tradition qui assure la continuité entre le passé-présent-futur par le rituel. La logique de la répétition permet d'organiser le futur. L'environnement à risque des cultures prémodernes était dominé par les dangers du monde physique, les violences humaines et les peurs liés à la religion.

Dans les cultures modernes, la confiance s'établit autour des relations personnelles, des systèmes abstraits et de la prise en compte du futur dans nos décisions. Nous pouvons y observer

le déclin de la religion et de la tradition impactée par la réflexivité. Le risque provient à présent de l'activité humaine et non plus directement de l'extérieur même si les catastrophes naturelles existent toujours. Il en est ainsi des menaces écologiques qui peuvent être la conséquence de l'industrialisation mais aussi des violences militaires dont la puissance destructrice est sans commune mesure avec l'apparition de l'arme nucléaire.

L'opposition entre l'intime et les systèmes abstraits n'a pas de sens puisqu'ils sont fortement imbriqués. Selon Beck (1986), l'évènement intime d'une mère qui allaite est l'évènement lointain comme l'incident nucléaire en Ukraine est en relation directe.

2 - 1 2 3 LES RISQUES ET LES DANGERS

L'idée d'une société du risque pourrait nous faire penser que le monde est devenu plus dangereux que dans le passé. Selon Giddens, ce n'est pas forcément le cas. Il s'agit surtout d'une société qui, selon lui, est de plus en plus préoccupée par le futur (mais aussi la sécurité) et donc les risques. La société est une société qui résulte de la fin de la nature (altérée par les technologies et l'action de l'homme) et la fin de la tradition qui permettait de réduire l'incertitude des trajectoires individuelles. La société du risque vu de façon plus positive est une société avec une expansion des choix possibles.

Giddens, tout en précisant qu'il n'est pas d'accord avec les idées développées par Luhmann, tient à souligner l'importance de ses travaux sur les concepts clés (tels que la confiance, le risque et le danger). Alors que pour Luhmann, « lorsqu'on s'abstient d'agir, on ne court aucun risque », pour Giddens, l'inaction est « souvent risquée et l'on est obligée d'affronter certains risques qu'on le veuille ou non. Il se distingue de Luhmann lorsqu'il précise que le danger est présent dans toutes les situations à risques et qu'il peut être défini comme étant le degré de risque. A titre d'illustration, il nous précise qu'il est certainement plus risqué de traverser l'atlantique dans un petit bateau qu'en paquebot, puisque le danger associé est plus important.

Giddens établit une seconde distinction entre le « risque externe » et le « risque fabriqué ». Les risques externes représentent des événements externes préjudiciables mais suffisamment réguliers pour pouvoir être prédictibles et donc assurés (soit par les assureurs privés ou bien les Etats). Toutefois, la société moderne telle que nous la décrit Giddens est faite d'un autre type de risque. Il s'agit des « risques fabriqués » par l'homme et la technologie pour lesquelles l'histoire nous fournit peu d'éléments d'expérience pour pouvoir les appréhender.

Les risques de la modernité sont d'une tout autre nature du fait de leur nature intensive et extensive. L'intensité des risques liés à la modernité (risque nucléaire, crise financière) est d'une intensité telle qu'ils peuvent affecter l'humanité tout entière. Malgré les hauts niveaux de sécurité des systèmes, en cas de contingences imprévues, il existe un risque de défaillance dans son ensemble qui affecte tous ceux qui l'utilisent. Les systèmes délocalisés abstraits étendent géographiquement le risque. À cette idée d'extension du champ des environnements à risques s'ajoute celle du changement de type d'environnement à risque. Il s'agit essentiellement de ce que Giddens nomme l'environnement créé et transformé par les systèmes de connaissances humains. Il s'agit des risques écologiques. Ces risques finissent par faire partie de notre quotidien et deviennent familiers. Ils font par ailleurs l'objet de controverses lorsqu'il s'agit d'en estimer les probabilités.

Si nous considérons l'exemple de la guerre nucléaire, nous pouvons dire qu'aussi longtemps que durera la dissuasion, la guerre restera une possibilité. La force de dissuasion ne peut fonctionner que si les protagonistes concernés sont effectivement prêts à utiliser les armes nucléaires dont ils disposent. Compte tenu de cette possibilité, personne ne peut garantir aujourd'hui que la dissuasion fonctionnera avec certitude et toujours. La seule chose dont nous pouvons être sûres, c'est que la guerre nucléaire a pu être évitée depuis Hiroshima mais que nous ne pouvons pas présager du futur.

Comment pouvons-nous garder à l'esprit des dangers terrifiants sur lesquelles nous n'avons aucun contrôle en tant qu'individu ? Nous faisons le choix psychologique de ne pas garder ces menaces à l'esprit car elles paralyseraient toute vie quotidienne. Nous pouvons refouler notre anxiété grâce à la réapparition de la croyance au destin, comme aux temps prémodernes. Par ailleurs, tant que ces risques n'auront pas été transformés en situation d'expérience vécue, ils pourront garder un aspect « irréel ».

Telle que décrite par Giddens, la modernité comporte des points faibles. Il est urgent de s'interroger sur la valeur de l'expertise, l'importance du danger et la possibilité du contrôle. La perception des dangers pourrait faire douter de l'expertise. L'humanité peut-elle maîtriser l'emballement du camion de la modernité ? Pourquoi la raison ne peut le contrôler ?

Giddens cite quatre facteurs principaux qui rendent la maîtrise des conséquences de la modernité difficile :

- les défauts de conception des systèmes abstraits, sociaux ou naturels. En principe, les systèmes dépendants de la nature socialisée pourraient être corrigés ;
- les erreurs humaines. Même si elles peuvent être réduites, elles sont inévitables quelle que soit la conception des systèmes sociaux ou naturels ;
- les conséquences imprévues. Les systèmes complexes interagissent entre eux et avec un environnement qui n'est pas un système unique, toutes les conséquences ne peuvent être envisagées ;
- la circularité du savoir social. Il est impossible d'envisager les conséquences d'un système qui modifie lui-même l'environnement du savoir.

Conclusion :

Les risques sont selon Giddens indissociables de la notion de confiance. La société moderne qu'il nous décrit est une société où nous devons faire confiance à des systèmes abstraits (aviation, énergie, médecine, ...) dont nous ne connaissons pas le contenu ni les règles précises de fonctionnement. Le risque dépend du degré de confiance que nous avons dans ces systèmes abstraits. Par ailleurs, ces systèmes sont des systèmes complexes dont les interactions peuvent donner lieu à des conséquences non prévues tout comme les systèmes sociaux chez Luhmann. C'est ce que nous allons développer dans la prochaine section.

2 - 1 3 LA THEORIE DES SYSTEMES SOCIAUX ET LA SOCIOLOGIE DES RISQUES DE NIKLAS LUHMANN

C'est à la suite de la catastrophe de Tchernobyl, tout comme le sociologue Ulrich Beck avec son ouvrage « la société du risque », que le sociologue allemand Niklas Luhmann (1927-1998) a établi sa théorie du risque. Selon Luhmann, notre société est perçue comme étant plus risquée pour trois raisons. Tout d'abord une grande complexité de la société moderne fonctionnellement différenciée, ensuite une plus grande dépendance de notre société par rapport aux prises de décision et le contraste qui existe entre les décideurs et ceux qui sont indirectement impactés par leurs décisions.

Nous allons donc voir dans un premier temps la théorie des systèmes sociaux sur laquelle Luhmann s'appuiera pour traiter de la question du risque puis de la distinction entre risque et danger. Enfin, nous développerons le concept d'observation de second ordre qui seul permet selon Luhmann d'être conscient du risque.

2 - 1 3 1 LES SYSTEMES SOCIAUX AUTOPOÏETIQUES

La théorie des systèmes sociaux autopoïétiques développée par Luhmann (1986) a été établie selon l'auteur à partir des fondements de la théorie de Ludwig von Bertalanffi (1968) et de Talcott Parsons, dont il a suivi les cours à Harvard durant l'année 1961. Afin de comprendre le concept des systèmes sociaux autopoïétiques décrites par Luhmann, il nous faut préciser ce qu'est un système, puis le compléter avec la notion d'autopoïèse.

Le système peut être défini selon trois critères :

- il est toujours quelque chose de composé ;
- il y a entre les éléments qui le composent des actions réciproques ;
- là où s'arrêtent ses relations réciproques s'arrête le système et commence le milieu (l'extérieur du système).

Comme conséquence de cette vision, le monde se décompose toujours en deux parties : le système et le monde qui se trouve en dehors. La frontière d'un système est ce qui le sépare de son milieu (le monde qui lui est extérieur). C'est-à-dire que le système est défini par la différence entre le tout et la partie. Ceci pose une certaine contradiction. Le système est un tout constitué de l'ensemble de ses éléments plus l'ensemble des relations qui relient ces éléments entre eux.

Luhman nous dit que le système social est autopoïétique. L'autopoïèse signifie « se faire soi-même ». Ainsi, un système autopoïétique est un système qui gère lui-même sa reproduction. Selon Luhmann, il existe trois types de systèmes autopoïétiques : les systèmes vivants (cellules, organismes, ...), les systèmes psychiques (conscience, ...) et les systèmes sociaux (interaction, organisation, société). Les systèmes biologiques constituent ainsi un environnement indispensable pour les opérations des systèmes psychiques conscients et les systèmes psychiques constituent un environnement indispensable aux opérations de communication des systèmes sociaux. S'il n'y a pas d'êtres humains vivants, il n'y aura ni systèmes psychiques conscients ni systèmes sociaux offerts à l'observation humaine.

Il précise par ailleurs qu'il n'est pas de système autopoïétique qui n'ait pas son opération spécifique. Par exemple, pour le système psychique, les opérations sont les pensées et pour les systèmes sociaux, ce sont les communications. Ils sont séparés mais coopèrent ensemble. La grande nouveauté de la théorie des systèmes de Luhmann se situe avant tout dans le fait qu'elle trace une stricte différence entre système social et système psychique.

L'opération de communication, pour ne pas échouer, suppose que l'information émise par Alter atteigne Ego, que cette information soit attribuée par Ego comme venant d'Alter et qu'elle soit comprise. Face à ces difficultés, Luhmann nous décrit trois types de solutions (ou médias) qui sont :

- le langage (pour rendre probable la compréhension) ;
- les moyens de diffusion ;
- les moyens de communication généralisée symboliquement (« medium »).

Les éléments du système social ne sont que des communications (et non pas des actions). Le système social est différent de son milieu et opérationnellement clos (opérations de communication). Il est autopoïétique, c'est-à-dire capable de produire ses propres éléments et ses propres structures.

Les systèmes sociaux surgissent à partir des problèmes de double contingence qu'ils permettent d'affronter avec leurs opérations. C'est ce qui permet aux systèmes psychiques de rentrer en contact entre eux.

Luhmann distingue le système de son environnement et précise que la société est fonctionnellement différenciée, c'est-à-dire composée de sous-systèmes sociaux (économique, légal, scientifique, artistique, politique...). Chaque sous-système remplit des fonctions

spécifiques avec ses propres modes opératoires et ses propres codes de communication. La fonction principale du sous-système économique par exemple est de favoriser et permettre les communications d'un certain type pour réguler les échanges de bien. Le médium sens est l'argent et le code qui permet de communiquer est « payer / ne pas payer ». Enfin, le programme qui permet de choisir parmi les deux codes est le prix. Le système renvoie à une offre de communications qu'on peut refuser ou accepter et à laquelle on peut enchaîner d'autres communications.

La complexité du système dépend du nombre de relations possibles qui peuvent exister entre ces éléments. La complexité du système est donc toujours inférieure à celle du milieu. En effet, comme beaucoup de relations du milieu sont inutiles pour la survie du système, celui-ci réduit la complexité au sens réduction de l'image qu'il se fait du milieu. Par la réduction, le système fixe ce qu'il pourra percevoir (le reste deviendra invisible) et une stimulation externe n'a de sens pour le système que si elle est traduite dans son propre langage.

Chaque individu passe d'un système à un autre (par exemple de l'économie à la science) selon le type de communication qu'il met en place (par exemple économique ou scientifique).

Le système s'observe avec ses codes et observe lui-même les opérations de ses codes, uniquement par ses codes. Le code du système scientifique sera vrai/faux, celui du politique pouvoir/opposition. Dès lors, les sous-systèmes sont opérationnellement clos, c'est-à-dire qu'ils ne peuvent pas communiquer entre eux mais juste traiter et interpréter les signaux extérieurs. Les sous-systèmes ne peuvent pas communiquer avec leur environnement mais juste communiquer à son sujet en utilisant leurs propres codes. Il y a dès lors un filtre appliqué par chaque sous-système à la résonance extérieure au moyen du son propre mode opératoire.

Si l'on considère par exemple la catastrophe nucléaire de Fukushima au Japon (2011), cet événement sera codé différemment par chaque sous-système : le sous-système économique se focalisera sur son impact sur les mécanismes de prix alors que le sous-système scientifique traitera de son impact sur la santé des populations exposées à la radioactivité. Le système social apparaît dès lors comme un moyen de réduire la complexité par la différenciation fonctionnelle.

Il est important de souligner les points suivants quant à la théorie des systèmes sociaux.

- Le système ne peut pas observer l'environnement. Ainsi, un système social se distingue tellement de son environnement qu'il n'arrive à l'observer que selon ses propres codes, par exemple dans des termes juridiques, politiques ou économiques. Quand le système

observe, il n'observe pas l'environnement « en soi » : il construit ses observations et observe ses observations codifiées.

- Un système n'arrive pas à constater qu'il n'observe pas ce qu'il n'observe pas : chaque système a un point aveugle. Le système politique n'arrive, par exemple, à observer des problèmes d'environnement que si ces problèmes sont traduits dans des codes politiques, surtout de gouvernement/opposition.
- Les sous-systèmes n'arrivent pas à communiquer ensemble puisqu'un système ne communique qu'avec lui-même et ne se comprend que lui-même.
- Il n'y a pas de recours à une vision ou à un système total.

Nous allons voir dans la section suivante comment les systèmes sociaux qui permettent de réduire la complexité et d'apporter des solutions communicationnelles peuvent rendre la prévisibilité des événements plus difficile et donc accroître l'incertitude.

2 - 1 3 2 RISQUE ET COMPLEXITE

Pour Luhmann (1993), le risque résulte de la grande complexité de notre société moderne et de la différenciation fonctionnelle. Cette complexité rend beaucoup plus difficile la prévisibilité des événements futurs au moyen de lois déterministes et des probabilités.

Considérons par exemple le cas du risque technique. Il est possible de déterminer ex post ce qui était à l'origine un dysfonctionnement et ce qu'il aura fallu faire pour l'éviter. Cependant, une telle analyse suppose que le système soit fondé sur une causalité linéaire et que l'analyste soit capable d'établir un lien clair entre une cause et tous ses effets.

Or, si l'on considère par exemple le système industriel, la grande complexité de certaines installations ne peut être appréhendée qu'au moyen d'un modèle qui la simplifie. La recherche d'une cause de dysfonctionnement est d'autant plus difficile que le système en question est complexe et suit rarement un schéma de causalité linéaire.

La complexité résulte du nombre de fonctions qu'un système doit remplir ainsi que sa taille : les interactions entre les sous-systèmes fonctionnellement différenciées ainsi que leurs effets deviennent plus incertains.

La complexité ne se limite pas au domaine technique et existe à chaque niveau de la société. Le risque est lié de façon inhérente à la société fonctionnellement différenciée. La société est fonctionnellement différenciée, c'est-à-dire composée de sous-systèmes sociaux (économique, légal, religieux, scientifique, ...) qui remplissent chacun une fonction spécifique afin de réduire

la complexité avec leur propre logique, programmes et codes de communication. Ainsi, le sous-système artistique ne remplit pas la même fonction que le sous-système juridique ou encore économique.

La modernité a amené une société « surspécialisée » et l'autonomie de chacun de ses sous-systèmes a créé plus d'incertitude sur les décisions. Les évaluations de risques faites au sein d'un sous-système en utilisant ses propres codes ne peuvent prendre en compte de façon efficace l'ensemble des effets qui peuvent résulter de ses décisions sur les autres sous-systèmes. Les conséquences indirectes du développement technologique sur l'homme et la nature illustrent bien cette idée.

2 - 1 3 3 LA DISTINCTION ENTRE RISQUE ET DANGER

Selon Luhmann, la complexité ne peut pas expliquer à elle seule notre sensibilité accrue face aux risques. Il développe l'idée selon laquelle les risques sont aujourd'hui plus importants du fait de notre mode d'observation qui a évolué.

En effet, selon Luhmann, les risques n'existent pas indépendamment de notre mode d'observation. Pour être capable d'observer, il nous faut procéder à une distinction. Si nous voulons désigner quelque chose comme étant un risque, nous devons le distinguer de ce qu'il n'est pas. Ce qui signifie que quelque chose ne peut pas être observé et désigné que s'il se distingue de quelque chose d'autre. Les systèmes sociaux n'ont pas de contact direct avec leur environnement car l'observation est une construction réalisée à partir d'un mode opératoire spécifique au système. Le système social ne peut pas communiquer avec son environnement mais ne peut que l'observer en communiquant à son sujet. Cette conception se différencie de l'approche positiviste qui considère que le risque peut exister indépendamment de l'observation.

Luhmann décrit deux modes pour établir une distinction. Le premier consiste à indiquer quelque chose comme étant distinct de tout le reste, sans spécifier ce qui est le reste. Dans ce cas, la distinction faite consiste à indiquer et désigner un objet. Le second mode consiste à procéder de la même manière tout en restreignant ce que peut être le reste (par exemple homme/femme, légal/illégal, ...). Cette distinction correspond non plus à un objet mais à un concept.

C'est sur cette base que Luhmann a introduit la distinction Risque / Danger pour pouvoir définir le concept de risque : *“ Cette distinction présuppose que l'incertitude existe en lien avec des pertes futures. Il y a dès lors deux possibilités. La perte potentielle est vue comme la conséquence*

d'une décision, c'est-à-dire qu'elle est attribuée à la décision. Nous parlons alors de risque. Ou bien, la perte possible est considérée comme ayant été causé par l'extérieur, c'est-à-dire qu'elle est attribuée à l'environnement. Dans ce cas nous parlons de danger” (Luhmann, 1993, p. 21).

L'accroissement de notre sensibilité aux risques peut être expliqué par la manière dont les événements sont observés dans notre société moderne et aussi attribués à nos décisions (plus qu'à des causes externes). Tout d'abord, la modernité nous a amené beaucoup plus de possibilités de décisions. Ainsi, le danger d'être mouillée par la pluie s'est transformé en risque avec l'invention du parapluie. Par ailleurs, notre mode d'observation a lui aussi évolué. Prenons le cas d'une catastrophe naturel, un tremblement de terre qui survient et détruit plusieurs bâtiments. Autrefois, cet événement était associé aux actes divins ou à la fatalité. Aujourd'hui, dans nos sociétés modernes, la cause ne sera pas uniquement recherchée dans l'évènement en tant que tel mais aussi dans les mauvaises décisions qui ont été prises par ceux qui ont décidé de construire dans cette zone. Ainsi, notre mode d'observation a changé.

La distinction Risque/Danger ne fait pas référence à une question de probabilité ou d'improbabilité. Le problème est de savoir si la possibilité d'une déception dépend de notre conduite préalable ou non.

Selon Luhmann (1993), l'évaluation des risques et la volonté à les accepter sont des problèmes avant tout d'ordre social. La prise de risque n'implique pas de communication entre ceux qui décident et ceux qui sont indirectement impactés par la décision prise. “Alter” n'est pas dépendant d'“Ego” lorsqu'il décide. Par ailleurs, il n'est pas possible d'avoir une évaluation objective du risque en l'absence de critères universellement acceptés par tous : ceux qui sont indirectement impactés auront une évaluation différente de ceux qui prennent la décision de prendre un risque. Cette différence ne résulte pas uniquement du fait que ceux qui sont indirectement impactés par la décision ne sont pas dans la situation de prise de décision, mais surtout du fait qu'ils ne bénéficient pas autant que les décideurs des avantages qui résultent de la décision. Cette distinction Risque / Danger crée alors une asymétrie sociale entre les décideurs et ceux qui sont indirectement impactés par leurs décisions. La particularité de cette asymétrie est de rechercher une solution communicationnelle. Or, dans la société différenciée, aucun sous système n'est dominant et ne permet d'y apporter une réponse satisfaisante.

La décision de prendre un risque – *par exemple technologique avec la construction d'une centrale nucléaire*– conduit à ce que d'autres soient exposés à un danger sans en avoir décidé.

Dans cette situation, la différenciation fonctionnelle ne permet pas de réduire la complexité et le problème posé reste intact. D'un côté, la décision engendrant directement le risque technologique se prend dans une organisation du système économique ; de l'autre, la contestation de la décision et de ses effets se développe dans le système politique. Or, puisque les systèmes sont opérationnellement clos les uns vis-à-vis des autres, autrement dit puisqu'ils ne communiquent pas entre eux, le système économique (les organisations à risques) ne peut *communiquer* avec son environnement externe : les entreprises n'ont pas à – et ne peuvent pas – communiquer avec une contestation qui, selon Luhmann, se trouve dans le système politique. Le risque se manifeste chez les contestataires par de l'angoisse, de l'anxiété (système psychique). Le sous-système politique ne peut pas les réguler avec le médium « Pouvoir », c'est-à-dire les rassurer. Il est alors improbable qu'Alter arrive à joindre Ego, qu'Alter se fasse comprendre d'Ego et qu'Ego accepte cette communication comme base de communication ultérieure. Pour que les deux sous-systèmes économique et politique puissent communiquer, il faut que les problèmes soient transformés en communication par les systèmes de média généralisés (le « médium »).

2 - 1 3 4 L'OBSERVATION DE SECOND ORDRE

« Les experts de la sûreté/sécurité, mais aussi ceux qui les accusent de ne pas en faire assez pour la sécurité, sont des observateurs de premier ordre. Ils croient dans les faits ; et lorsqu'ils croisent le fer ou négocient, cela se fait typiquement sur la base d'interprétations divergentes et des attentes en relation avec les mêmes faits. L'observateur de second ordre fait face au problème qui est que ce que les différents observateurs considèrent comme étant la même chose génère une information bien différente de la part de chacun d'entre eux » (Luhmann, 1993, p. 21).

L'observateur de premier ordre voit ce qu'il voit. Toute observation a une tache aveugle. Il n'est pas possible d'observer simultanément les deux faces d'une distinction, c'est-à-dire à la fois quelque chose qu'on distingue et tout ce qu'il n'est pas. Par ailleurs, il n'est pas possible d'observer quelque chose et de s'auto-observer en même temps. Il est possible de le faire mais en recourant une autre distinction. C'est ce que Luhmann nomme l'observation de second ordre.

L'observateur de second ordre voit comment l'observateur de premier ordre voit ce qu'il voit. Luhmann précise que la conscience du risque ne peut apparaître qu'au niveau de l'observation

de second ordre. Comme nous l'avons déjà vu, nous parlons de risque seulement si nous présumons que la personne qui perçoit un risque observe en recourant à une distinction.

Lorsqu'une personne agit de manière risquée, comme prendre des risques en conduisant en consommant de la drogue ou en utilisant une arme, il agit en tant qu'observateur de premier ordre. Dès lors que le même individu s'observe lui-même en train d'agir et se demande s'il prend un risque ou non, il devient un observateur de second ordre et prend conscience alors à ce moment-là conscience du risque. Enfin, l'observateur de second ordre voit les relations entre les caractéristiques personnelles de celui qui agit et la manière dont il appréhende une situation (sous pression, avec anxiété, ...).

Dans l'observation de second ordre, la question est de savoir quelles distinctions l'observateur de premier ordre réalise et comment il le fait. Au niveau de l'observation de second ordre, une action est observée comme une décision prise par les autres. La distinction Risque/Danger pour définir un risque se rapporte à une question d'attribution : qui décide de celle-ci ? La distinction entre les décideurs et ceux indirectement impactés par leurs décisions se rapporte à l'observation de second ordre. Les décideurs observent qu'ils sont observés.

2 - 1 3 5 LE « FUTUR » COMME RISQUE

Selon Luhmann (1993), l'idée selon laquelle il serait possible d'observer l'intégralité du temps de façon simultanée pourrait se faire qu'avec un observateur qui s'appellerait « Dieu » et où le temps serait l'éternité.

Nous devons, comme pour toute observation, procéder à des distinctions afin d'être en mesure d'observer. Ainsi, selon l'échelle de temps que nous considérerons pour appréhender le futur, les conséquences possibles associées à nos décisions seront sensiblement différentes. Luhmann souligne le fait que la manière dont le risque est évalué varie aussi au cours du temps.

Personne n'est en mesure de prétendre pouvoir connaître le futur : *« Ce qui va survenir ne dépend jamais d'un seul élément mais d'une somme de circonstances. En considérant l'horizon passé, nous savons ce qui s'est passé, même si les causes restent peu claires alors que pour un horizon futur, nous ne disposons pas de cette sécurité »* (Luhman, 1993, p. 41).

Le futur ne peut dès lors être appréhendé qu'au moyen du médium de la probabilité pour être en mesure de décider. Mais d'un point de vue social, cette idée se présente comme étant un échec. *« Même si l'on sait qu'une centrale nucléaire explose tous les douze millions d'années, cela peut arriver demain, mais aussi le surlendemain. Même si l'on sait qu'un accident de moto*

ne survient que tous les douze millions de kilomètres, la mort peut nous attendre au prochain virage. Dans l'évaluation sociale, le calcul laisse toutes les éventualités ouvertes au niveau individuel et l'évaluation du risque variera selon le fait que nous considérons que l'évènement peut survenir tôt ou probablement à un horizon lointain » (Luhmann, 1993, p. 49).

Conclusion :

La société est fonctionnellement différenciée et composée de sous-systèmes sociaux (économique, politique, scientifique...) qui remplissent tous des fonctions spécifiques en recourant à leurs propres programmes, modes opératoires et codes de communication. Les risques de la société moderne sont plus importants pour plusieurs raisons. Tout d'abord, du fait de la grande complexité de notre société qui rend la prévisibilité des événements plus difficile à travers les dimensions du temps et de l'espace. Ensuite, du fait de l'évolution de notre mode d'observation qui nous amène à associer les causes des incidents à nos propres décisions et non plus à la fatalité ou à des causes externes. Enfin, la modernité a considérablement augmenté les possibilités de décisions.

2 - 1 4 LA SOCIETE DU RISQUE D'ULRICH BECK

L'ouvrage d'Ulrich Beck intitulé *la société du risque* (1986) qu'il a écrit après la catastrophe de Tchernobyl traduit l'idée d'un changement radical qui s'est opéré avec le passage d'une société industrielle à une société (industrielle) du risque. Son ouvrage est composé de trois parties. La première partie précise les contours de la société du risque et la logique de répartition des risques, la seconde analyse le processus d'individualisation des inégalités sociales et enfin la dernière étudie les rapports entre la science et la politique et montre comment les frontières entre les deux tendent à s'effacer.

Ulrich Beck souligne à travers son livre la gravité des risques contemporains en précisant qu'ils sont de nature à pouvoir menacer l'existence de l'humanité. Qu'il s'agisse de catastrophes extrêmement rares (accident nucléaire) ou de pollutions diffuses (pollution industrielle, ...) qui empoisonnent l'air, l'eau et la terre, ces risques ont tous été créés par la science elle-même. Les risques ne résultent pas d'une incapacité technique humaine à faire face aux catastrophes naturelles mais plutôt du développement technologique lui-même.

Selon Beck (1986), nul n'est à l'abri : « la terre est devenue un siège éjectable, qui ne fait plus de distinction entre les riches et les pauvres, les noirs et les blancs, le nord et le sud ou l'est et l'ouest ». Pour échapper à la pollution, il faudrait ne plus boire, plus manger ni même respirer. Ces risques industriels se diffusent d'autant plus facilement qu'ils sont « invisibles ».

La société du risque résulte de deux phénomènes qui sont la « fin de la nature » impactée par les actions de l'homme et la « fin de la tradition ». Durant les siècles, l'homme s'est préoccupé des dangers que la nature faisait peser sur lui (tremblement de terre, inondation, ...) alors qu'aujourd'hui il se préoccupe de ce qu'il a lui-même fait à la nature.

2 - 1 4 1 LA SOCIETE MODERNE : UNE SOCIETE DU RISQUE

Le point de départ d'Ulrich Beck (1986) est la remise en cause de ce qu'il appelle « la religion moderne du progrès ». Il met l'accent sur une crise de légitimité des sociétés industrielles. En effet, les promesses de la modernité n'ont pas été tenues : la misère existe toujours, les inégalités sont plus importantes et le sous-développement d'une grande partie du monde n'a pas cessé. Mais surtout, le progrès a engendré en même temps que des richesses des maux et des dangers et donc des risques (pollution, catastrophe nucléaire, risques alimentaires, ...).

Il constate par ailleurs un changement dans la configuration de la société au sein de laquelle la question principale est la répartition des risques et non plus seulement des richesses. En effet, Les sociétés modernes ne produisent pas seulement des richesses mais aussi des risques qui ne sont pas maîtrisés.

Selon Beck (1986), le passage de la société de classe à la société du risque se caractérise par un changement de logique dans la production et la distribution sociale : on passe d'une société de classe avec production et des problèmes de distribution de la richesse à une société du risque avec la production de risques reliés à la science et des problèmes associés à leurs distributions. Il s'agit de risques globaux, qui dépassent leur territoire d'apparition et qui menacent l'ensemble de la vie sur terre. Le risque n'est plus une menace extérieure mais fait partie de la société.

Le mot risque est connoté d'une acceptation beaucoup plus large que l'idée d'un risque technologique majeur, mais il met alors sur le même plan, ce qui peut être critiquable, risques industriels (modernité réflexive), incertitudes scientifiques (risques scientifiques) et insécurité sociale (individualisation).

Ce passage est lié à la diminution de la véritable misère matérielle et la très forte croissance des forces productives. Les risques d'aujourd'hui sont attribuables à la surproduction industrielle.

Dans la société de classe, ou de pénurie, la possession de richesses par certains implique la non-possession de richesses pour d'autres. Dans la société du risque, le fait que certains soient touchés par les risques n'enlève rien à ceux qui ne le sont pas. Tout au plus pouvons-nous parler d'une opposition entre classe des exposés et classe de ceux qui ne sont pas encore exposés.

Dans la société de classe, on pouvait se demander comment répartir la richesse produite d'une façon qui soit à la fois légitime et socialement inégale. Dans le cas des risques, la question de la légitimité se pose plutôt dans les termes suivants : « comment les risques et les menaces [...] peuvent-ils être supprimés, diminués, dramatisés, canalisés et, dans le cas où ils ont pris la forme d'effets induits latents, endigués et évacués de sorte qu'ils ne gênent pas le processus de modernisation et ne franchissent pas les limites de ce qui est 'tolérable' ? Il est possible de légitimer l'existence des risques en affirmant qu'on ne les a pas vus et qu'on n'a pas voulu leur production, ce qui n'était pas possible dans une logique de répartition inégale de la richesse.

2 - 1 4 2 PERTE DE CONFIANCE DANS LA RATIONALITE SCIENTIFIQUE

Il met notamment l'accent sur la perte de confiance dans la rationalité scientifique et technique. Les risques échappent à la perception. Ils ne peuvent être appréhendés sans avoir recours à un organe de la science. Pour comprendre les risques, il faut par ailleurs établir des relations causales. Or, cette causalité n'est pas claire et échappe à la perception. Enfin, les risques ont une dimension normative : ils renvoient à la question de ce que nous sommes prêts à accepter.

Dans le système complexe du mode de production industrielle, il est presque impossible d'isoler des effets nocifs et des facteurs particuliers pour les mettre en relation. Il est facile pour les risques de prospérer en raison de l'écart qui existe entre réalité et perception. Alors que la richesse est perceptible, les risques, eux, ne le sont pas. C'est justement parce qu'ils sont considérés imperceptibles et qu'ils sont donc ignorés que les risques et menaces arrivent si bien à éclore, pousser et prospérer. C'est le caractère non perceptible des risques qui explique le rôle que tient la science dans cette société.

Ainsi, dans la modernité tardive, les risques ont ainsi changé de nature. Ils sont plus globaux, moins faciles à identifier et à gérer, plus anxiogènes. Les processus de calcul du risque utilisés dans la société moderne ne sont plus adaptés car les risques ne sont plus localisés et portent sur des échelles de temps plus longues. Les institutions ne sont plus capables de prévenir les risques ou d'en compenser les effets. Des causes uniques sont difficiles à identifier. Le risque ne peut pas être éradiqué mais juste être réduit.

Interpréter le risque comme un fait statistique donc traiter de la différence de perception du risque comme un déficit de rationalité entre le « risque réel » et le risque perçu » n'est pas très utile. Beck nous offre comme Luhmann une approche plus intéressante en établissant un lien entre la notion de risque et de décision. Les deux définissent le risque comme une menace, ou un dommage potentiel, comme une conséquence possible d'une décision ou d'un choix d'action. Les risques sont considérés comme pouvant être toujours évités, c'est-à-dire qu'il ne serait pas en l'absence de certaines décisions.

2 - 1 4 3 LA SOCIETE MODERNE : UNE SOCIETE INDIVIDUALISEE

La société devient de plus en plus une agrégation d'individus. Ces derniers sont libérés des certitudes et des rôles standards de la société industrielle (les hommes ne sont plus automatiquement des pères et les pères ne sont plus les seules sources de revenus, ...).

Alors que les institutions existantes perdent de leur sens et de leur influence, les individus gagnent plus de liberté de choix et d'autodétermination. Cette situation place les individus dans une chaîne de décision sans fin, transformant la liberté de choix en une contrainte institutionnalisée de devoir faire des choix. Les hommes et les femmes « modernes » doivent décider pour eux-mêmes et cela à maintes reprises. Le processus d'individualisation crée un besoin plus élevé de négociation : les valeurs communes, les attentes et les interprétations de la réalité seront toujours possibles, mais ils deviennent plus réflexifs, renégociables en permanence et valide seulement pour ceux qui sont directement concernés. La négociation devient un élément clé pour la prise de décision dans la société moderne.

2 - 1 4 4 LA MODERNITE REFLEXIVE

Beck (1986) a employé la notion de société du risque pour désigner « une phase de l'évolution de la société moderne dans laquelle les risques sociaux, politiques, écologiques et individuels engendrés par la dynamique du renouvellement, se soustraient de plus en plus aux instances de contrôle et de sécurité de la société industrielle ».

Il ajoute que notre société moderne se scinde en deux avec, d'un côté, les institutions, encore porteuses de « normes », de « modes de vie standardisés », et de l'autre, les modes de vie d'aujourd'hui qui sont de plus en plus diversifiés. Il y a un décalage institutionnel.

Beck établit une analyse critique de la modernisation à travers le passage d'une « modernité industrielle » à une « modernité réflexive ». Cette modernité réflexive devient elle-même l'origine de ses propres risques et détruit les cadres sociaux de la modernisation.

De la même façon que pour Luhmann (1993) et Giddens (1991), le concept de risque est construit autour de la décision. Le mot « risque » naît dans la modernité « avec la conscience que les résultats non anticipés [et indésirables] peuvent provenir de nos propres activités ou décisions » (Giddens, 1991). Dès lors, pour Beck (1986), la société industrielle assume des risques et essaye de maîtriser ou de compenser les dangers d'une quelconque manière (par des calculs de risque, des systèmes d'assurance, etc.).

Selon Beck, les nouveaux dangers industriels (surtout les dangers nucléaires, chimiques, écologiques ou reliés à la technologie génétique, etc.) sont qualitativement différents et se distinguent progressivement des anciens dangers par quatre caractéristiques :

- ils sont auto-générés par l'industrie ;
- ils ont une portée globale, sans être limitées ni dans le temps ni dans l'espace ;

- ils ne peuvent pas être facilement imputés à quelqu'un ou quelque chose avec les règles actuelles de la causalité ;
- ils ne peuvent pas être compensés ou assurés.

La modernité crée des nouveaux types de risques globaux, inconnus auparavant, issues du développement technologique et de la croissance économique. L'entrée dans la société du risque intervient lorsque le risque déjà déterminé et produit par la société industrielle nuit au système de calcul des risques et le système de sécurité établi jusqu'alors.

Beck insiste sur la difficulté à attribuer aux risques un responsable. Ceci découle notamment de la complexité du mode de production industrielle, de l'interdépendance des acteurs et de la difficulté de perception des risques. Tous peuvent être cause et effet mais personne ne peut être en particulier la cause de quoi que ce soit. Chacun peut donc continuer à faire ce qu'il fait, sans pour autant en être tenu responsable.

Giddens introduit la notion de réflexivité qu'il définit comme étant une auto-confrontation avec les conséquences d'une manière de vivre et des actions de l'homme. Il ne s'agit pas d'une contradiction mais une description de ce qui se passe lorsque les technologies se développent plus vite que les institutions qui les contrôlent. Les risques sont d'une nouvelle nature. Autrefois, ils étaient issus de l'extérieur. Aujourd'hui, ils sont engendrés par la société elle-même.

Les problèmes environnementaux, comme les autres risques qui découlent de notre société moderne deviennent des problèmes sociaux, ce qui induit que les gens se mobilisent pour les prendre en main. Beck nous montre que dans la société actuelle, la production sociale de richesse est systématiquement corrélée à la production sociale de risque. Ce qui ne signifie pas qu'aujourd'hui nous vivons dans un monde plus dangereux que dans le passé mais que l'on pense la société en anticipant les conséquences de ce qui est produit par les pratiques sociales. À ce stade, Beck nous parle de « modernité réflexive ». La société entre dans sa phase réflexive, c'est-à-dire que la société est obligée de penser et de se questionner.

Il prédit que les nouveaux risques vont avoir un impact social du fait de l'individualisation (qui a détruit les solidarités de classe ainsi que les normes et valeurs anciennes), la mondialisation, la prise de conscience et l'engagement des individus concernant les nouveaux risques. Nous sommes en train d'abandonner les modes de vie de la société industrielle.

Comme résultat de cette prise de conscience des risques modernes et l'incertitude des connaissances, combinée à une individualisation accrue, les individus deviennent réflexifs et s'engagent pour changer les politiques et réglementations. Cela signifie que les nouveaux risques ont le pouvoir de changer la société et donc la politique. Selon Beck, de nouveaux mouvements sociaux (« sub-politics ») vont alors émerger. Il met notamment en évidence l'avantage de la sub-politique technico-économique sur l'Etat. En effet, le premier a « l'autonomie des décisions prises sur les investissements et le monopole de l'utilisation de la technologie », ce qui lui confère son avance. Les transformations sociales ne sont alors plus décidées au sein des institutions politiques mais sont le résultat des innovations technologiques. Or, Beck envisage la politique comme « la construction et la transformation des conditions de vie ». Il explique comment la sphère politique a été dépolitisée et la sphère technico-économique politisée (devenue sub-politique). Il en résulte la fin du monopole de la politique sur la transformation sociale et du monopole de la science sur la maîtrise de la connaissance.

Conclusion :

Selon Beck, les risques ont changé de nature. Ils sont plus globaux, moins faciles à identifier et à gérer, plus anxiogènes. Les processus de calcul du risque utilisés dans la société moderne ne sont plus adaptés car les risques ne sont plus localisés et portent sur des échelles de temps plus longues. Les institutions ne sont plus capables de prévenir les risques ou d'en compenser les effets. Des causes uniques sont difficiles à identifier. C'est le caractère non perceptible des risques qui explique le rôle que tient la science dans cette société. Il met notamment l'accent sur la perte de confiance dans la rationalité scientifique et technique. Les risques échappent à la perception. Ils ne peuvent être appréhendés sans avoir recours à un organe de la science, qui est elle-même parfois à l'origine de certains risques. De la même façon que pour Luhmann et Giddens, le concept de risque est construit autour de la décision. Le mot « risque » naît dans la modernité « avec la conscience que les résultats non anticipés et indésirables peuvent provenir de nos propres activités ou décisions ».

Conclusion générale :

Comme nous avons pu le voir, de nombreuses approches ont été développées au sein de la sociologie du risque. L'ensemble de ces approches théoriques (la théorie culturelle de Douglas et Wildavsky, la théorie des systèmes sociaux de Luhmann, la société du risque de Beck et Giddens) contribue à mieux comprendre dans quelle mesure et de quelle manière le risque est un objet socialement construit. Leur étude permet de mettre en évidence à la fois des similitudes mais aussi des différences significatives.

Luhmann fournit dans le cadre de sa théorie une définition du concept de risque qui n'est pas explicité aussi précisément chez Giddens, Beck ou Douglas et qui constitue un apport fondamental de ses travaux. Luhmann (1993) définit le concept de risque en introduisant la distinction risque/danger. La distinction risque/danger ne fait pas référence à une question de probabilité ou d'improbabilité. Le problème est de savoir si la possibilité d'une déception dépend de notre conduite préalable ou non. L'accroissement de notre sensibilité aux risques peut être expliqué par la manière dont les événements sont observés dans notre société moderne et aussi attribués à nos décisions (plus qu'à des causes externes).

Nous allons aborder à la page suivante le choix de notre cadre d'analyse et les questions de recherche.

2 - 2 LE CHOIX DU CADRE D'ANALYSE ET LES QUESTIONS DE RECHERCHE

Nous allons voir dans cette partie comment nous avons mobilisé le cadre théorique afin de déterminer nos questions de recherche. Il est toutefois utile de rappeler au préalable notre problématique de départ qui porte sur l'activité des auditeurs internes en lien avec le thème du risque.

2 - 2 1 LA PROBLEMATIQUE

Selon les normes professionnelles qui régissent l'activité des auditeurs (IIA, 2014), ces derniers sont en charge d'évaluer les processus de gestion des risques au sein de leur organisation. Ils doivent pour cela mettre en œuvre une approche par les risques afin d'orienter leurs travaux afin de couvrir les risques de leur organisation. Il est notamment précisé que l'audit interne doit établir un plan annuel d'activité (IIA, 2014) ainsi que des plans de mission (IIA, 2014) en lien avec les risques de son organisation.

Or, le terme de risque qui constitue le cœur d'activité des auditeurs internes n'est pas précisément défini dans les normes. Il est simplement précisé que le risque représente tout type d'évènement qui, s'il se produit, peut compromettre l'atteinte des objectifs de l'organisation et qu'il faut l'apprécier en fonction d'un niveau d'appétence au risque.

Comment les auditeurs mettent en application les normes lorsqu'il est question de risque alors que ce concept traduit une certaine ambiguïté ? Le risque est traditionnellement représenté par une mesure (probabilité x impact) relative à la survenance possible d'un évènement et de ses conséquences.

En pratique, tous les risques ne sont pas mesurables au moyen de l'approche fréquentiste car les auditeurs internes ne disposent pas de statistiques pour tout.

Cette définition du risque en tant que mesure pose un autre problème pour étudier la pratique de l'audit. Notre objectif n'est pas d'évaluer le risque au niveau individuel mais organisationnel. Or, la conception du risque en tant que mesure ne permet pas de traiter véritablement de cette question dès lors que l'appétence au risque ne peut pas être mesurée sans ambiguïté.

La revue de la littérature nous a permis de mettre en évidence qu'il existait relativement peu de travaux sur l'approche par les risques de l'audit interne au regard de la planification de leurs travaux. Les recherches existantes ont essentiellement consisté à interroger les auditeurs internes pour savoir s'ils recouraient ou non à une approche par les risques. Toutefois, ces

travaux ne décrivent pas comment les auditeurs internes procèdent en pratique pour identifier et évaluer les risques au sein de leurs organisations.

Nous pouvons dès lors chercher à mieux comprendre comment ils procèdent pour passer des normes à la pratique pour évaluer les risques au sein de leur organisation.

2 - 2 2 LE CHOIX DU CADRE D'ANALYSE

La sociologie du risque nous permet d'avoir un éclairage particulier sur le concept de risque et de dépasser certaines limitations relatives à l'approche traditionnelle dite fréquentiste qui semble inopérante en l'absence de données abondantes.

Le risque y est défini non pas comme un objet et accessible et mesurable de façon objective mais comme un construit social. Cette construction résulterait alors des modes d'interactions entre les acteurs dans un contexte social et organisationnel particulier et des facteurs sociaux, culturels et politiques.

Vu sous cet angle, il apparaît essentiel de mieux comprendre le rôle que joue la fonction d'audit interne dans le processus d'identification et d'évaluation des risques au sein de son organisation et quelle est la nature de ses interactions avec les autres acteurs.

Notre objectif est d'étudier le processus de construction sociale des analyses de risque formelles réalisées au sein des organisations en mettant en relation les procédures mises en œuvre par les acteurs avec les résultats produits. C'est-à-dire analyser les heuristiques mises en œuvre au sein des organisations ainsi que les modes d'interactions des acteurs pour construire les objets de risque. Nous cherchons à comprendre comment les auditeurs internes évaluent les risques au niveau organisationnel et non pas individuel.

La théorie des systèmes sociaux et la sociologie des risques de Niklas Luhmann, que nous avons explicitée dans la partie précédente, nous apportent un cadre particulièrement riche afin d'étudier le phénomène de construction sociale du risque. Nous avons privilégié cette approche plutôt que d'autres puisque Luhmann fournit dans le cadre de sa théorie une définition du concept de risque qui n'est pas explicité aussi précisément chez Giddens, Beck ou Douglas. C'est la raison pour laquelle nous avons décidé de mobiliser ce cadre théorique.

C'est d'ailleurs le point que soulève Luhmann (1993) en soutenant que jusqu'à présent le problème de ce concept de risque est qu'il n'a jamais été clairement délimité. Un apport fondamental de ses travaux est d'avoir apporté une définition du concept de risque. Luhmann

(1993) précise qu'au plan de la méthode, la délimitation d'un concept nécessite de faire apparaître la différence par laquelle il se caractérise.

Luhmann (1993) cherche à répondre à une question fondamentale : pourquoi le risque est-il un problème ? L'évidence du problème tel qu'il se pose dans la démarche rationaliste (*les dommages doivent être évités même quand il n'est pas certains qu'ils se produiront*) dissimulerait une autre question, à savoir ce qu'il y a de problématique dans le problème. Ainsi, cette manière aveugle de poser le problème, confrontée à des préoccupations de tous les jours, explique qu'on ait négligé de traiter des questions conceptuelles alors qu'à l'inverse, on attend des calculs d'une certaine précision.

Afin de réussir à définir le concept de risque, Luhmann part de ce concept et cherche quel en est le concept opposé. Il nous précise que le premier concept qui nous vient à l'esprit n'est pas celui de danger mais plutôt de sécurité, le concept de danger paraissant être trop proche de celui du risque. Or, aucun système ni aucune situation ne peuvent se prévaloir d'être en mesure d'exclure la possibilité même infime d'un désagrément. Luhmann soutient que le concept de sécurité est une fiction sociale : la sécurité absolue n'existe pas. Il faut non pas s'intéresser aux conditions effectives de la sécurité mais plutôt à ce qui dans la communication sociale vaut comme étant sûr. Luhmann abandonne la distinction risque/sécurité qui dès lors fait apparaître un paradoxe lorsque nous nous projetons sur la société en ignorant volontairement la répartition des risques dans le temps et en fonction des couches sociales. Car selon Luhmann (1993), les tentatives de vouloir limiter ou réduire un risque comporte aussi un risque et que les seuls éléments qui peuvent varier sont l'occurrence dans le temps, l'impact et la répartition des avantages/dommages. Il est ainsi possible de ne pas souhaiter voir plusieurs centaines de personnes mourir lors d'un seul et même incident et préférer prendre des risques dont l'enjeu sera pourtant le même. Ces deux alternatives différeront quant aux moments, aux lieux et aux causes.

Luhmann abandonne ainsi la distinction risque/sécurité et propose de recourir à celui de risque/danger. Les deux côtés de cette différence ont un point en commun : on parle de risque et de danger dans la perspective de dommages et de préjudices possibles mais non certains. Cette différence ne peut être explicitée que par un processus d'attribution. Ainsi, en fonction de l'imputation, quelque chose peut s'avérer être soit un risque, soit un danger. La différence entre risque et danger dépend de la façon dont les dommages sont imputés et par qui ils le sont. Lorsque le préjudice est imputé comme une conséquence de sa propre décision, il s'agit de

risque. Lorsqu'il est imputé à causes (événements extérieurs, décisions des autres) que l'on juge en dehors de notre contrôle, il est question alors de danger. Ainsi, selon Luhmann (1993), ceux qui décident ne sont pas ceux qui en subissent les conséquences. Cette différence conceptuelle entre risque et danger présuppose un observateur. Cet observateur recourt à des distinctions qui lui permettent de distinguer ce qui est un risque de ce qu'il n'est pas. Sans distinction, il n'est pas possible d'identifier un risque.

Il nous faut alors établir ici les principaux attributs du concept de risque issus de notre cadre théorique afin de déterminer les questions que cela pose au regard de l'application des normes d'audit interne. C'est l'objet de la prochaine section.

2 - 2 3 LES ATTRIBUTS POUR ETUDIER LE PHENOMENE DU RISQUE ?

La théorie des systèmes sociaux et la sociologie des risques de Luhmann mettent en évidence un certain nombre de concepts pour traiter de la question du risque. Nous pouvons sur cette base établir les principaux attributs du concept de risque qui nous permettront d'élaborer nos questions de recherche.

Les risques varient selon le point et le mode d'observation. Selon Luhmann (1993), il n'est pas possible d'observer tout de façon simultanée et nous devons recourir à des distinctions pour pouvoir observer les objets au sein de notre environnement. Ainsi, un risque ne peut être identifié qu'en recourant à une distinction pour être en mesure de désigner ce qui est un risque de ce qu'il n'est pas. Ainsi, rien ne peut être observé sans établir de distinction, ce qui signifie qu'on ne voit jamais qu'une partie. Nous avons donc des taches aveugles qui résultent des distinctions auxquelles nous recourons pour observer un objet. Cette tache aveugle ne peut devenir visible que pour une autre observation, qui observe elle-même la première observation. C'est l'observation de second ordre. Luhmann distingue ainsi deux niveaux d'observation : l'observation de premier ordre et de second ordre.

L'observation de premier ordre permet au système de différencier ce qui lui appartient de ce qui appartient à son environnement. L'observation de second ordre n'est rien de plus que le redoublement de l'observation de premier ordre à un niveau supérieur.

L'observation de second ordre s'intéresse à la question des distinctions que l'observation de premier ordre utilise.

Selon Luhmann (1993), seule l'observation de second ordre permet de prendre conscience des risques. L'audit interne en tant qu'observateur de second ordre observe ce à quoi les managers

(observateurs de premier ordre) se fient, les structures et opérations qu'ils disent contrôler. L'audit interne a donc lui aussi recourt à des distinctions et donc des points aveugles.

Les distinctions que nous utilisons pour observer dans le temps et l'espace sont spécifiques à chaque sous-système social (légal, politique, économique, scientifique, ...) fonctionnellement différencié. Pour Luhmann, la société est fonctionnellement différenciée est composée de sous-systèmes spécialisés afin de réduire la complexité.

La complexité dépend du nombre de fonctions remplies ainsi que de la taille de chacun de ses sous-systèmes. Le risque résulte des conséquences des décisions prises au sein d'un système donné sans pouvoir envisager l'ensemble des conséquences sur les autres sous-systèmes. Les sous-systèmes sociaux sont opérationnellement clos et ne communiquent pas entre eux. Chaque sous-système social observe son environnement et communique à son sujet avec ses propres codes. L'audit interne constitue lui-même un système social avec sa propre sémantique issue des normes d'audit et donc de ses propres codes de communication et d'observation (risqué/non risqué).

Luhmann définit le futur comme risque, notamment du fait que celui dépend de nos décisions. Les risques ne sont pas les mêmes selon l'horizon temporel qui est considéré lorsque nous établissons des distinctions pour observer. Par ailleurs, les risques et leurs évaluations varient dans le temps. Enfin, pour Luhmann, ce sont les opérations au sein des systèmes sociaux qui diffèrent en termes de temporalité.

La notion de temps est donc essentielle pour la désignation des risques. Nous pouvons nous demander à quelles distinctions recourent les auditeurs internes lorsqu'il s'agit d'identifier les risques au sein de leur organisation ? La distinction risque/danger introduite par Luhmann (1993) soulève un certain nombre de questions. Dès lors que les risques des uns (au sein d'un sous-système social) constituent les dangers des autres, nous pouvons nous demander pour qui l'audit interne évalue les risques dans le but de mieux comprendre de quelle manière la méthodologie d'audit interne permet aux auditeurs d'être des observateurs de second ordre pertinents et de limiter le risque d'observation.

2 - 2 4 LA FORMULATION DES QUESTIONS DE RECHERCHE

Afin de préciser les questions de recherche relatives à notre sujet, il est essentiel de transposer les concepts de notre cadre théorique ainsi mobilisés aux normes professionnelles d'audit interne pour comprendre comment les objets de risques sont construits.

Nous posons comme hypothèse que chaque organisation représente en tant que tel un sous-système social avec ses propres codes de communication qui observe les risques avec des distinctions qui lui sont propres. Ces distinctions devant être mises en perspective de la dimension sociale et organisationnelle afin de mieux comprendre comment s'opère le processus de sélection des risques.

Notre question de recherche principale est la suivante : « *Comment les organisations construisent-elles leurs objets de risques et par quelles heuristiques ?* » en lien avec les activités de l'audit interne.

Ainsi qu'énoncé lors de l'introduction, cette question exige de répondre aux quatre questions suivantes pour être en mesure de comprendre *comment les directions d'audit construisent leurs objets de risque ... pour les rendre auditables* :

- *Comment les risques identifiés dans l'organisation (cartographie des risques) orientent-ils les travaux des auditeurs internes ?*
- *Comment sont évalués les risques de l'organisation lors de la construction du plan d'audit ?*
- *Comment sont définies les missions sur la base de l'évaluation préliminaire des risques ?*
- *Dans quelle mesure l'auditeur interne peut être un observateur pertinent des risques de l'organisation ?*

Conclusion :

Luhmann fournit dans le cadre de sa théorie une définition du concept de risque (1993) qui n'est pas explicité aussi précisément chez Giddens, Beck ou Douglas. C'est la raison qui justifie son choix comme cadre d'analyse. Selon Luhmann (1993), les risques n'existent pas indépendamment de notre mode d'observation. Il introduit quatre concepts fondamentaux qui sont mobilisés dans cette thèse : la distinction risque/danger, les codes de communication, l'observation de premier ordre et de second ordre et le futur comme risque. Notre question de recherche découle de ce cadre d'analyse et vise à répondre à la question suivante : « *Comment les organisations construisent-elles leurs objets de risques et par quelles heuristiques ?* » en lien avec les activités de l'audit interne. Nous allons aborder dans le chapitre suivant la méthodologie de recherche que nous avons établie afin de pouvoir répondre à cette question.

3^{EME} CHAPITRE : METHODOLOGIE

La méthodologie de recherche doit nous permettre de répondre aux questions de recherche posées. Rappelons que notre objectif est de comprendre comment les organisations construisent leurs objets de risques et quelles heuristiques elles mettent en œuvre pour y parvenir. Il ne s'agit donc pas d'expliquer pourquoi mais plutôt comment les membres d'une organisation, et plus particulièrement les auditeurs internes, font en pratique pour identifier et sélectionner les risques. Il nous faudra dès lors répondre aux questions suivantes : quelles sont les procédures mobilisées pour construire les plans d'audit et les plans de mission ? Quel est le lien entre ces éléments-là et les risques identifiés au sein de l'organisation.

Le cadre d'analyse de notre étude s'appuie sur deux assises théoriques, à savoir la théorie des systèmes sociaux (Luhmann, 1986) et la sociologie des risques (Luhmann, 1993) que nous avons développées dans le chapitre précédent.

Nous allons voir à dans ce chapitre les principales composantes de l'approche méthodologique que nous avons élaborée pour ce projet de recherche, à savoir : la stratégie de recherche adoptée, l'unité d'analyse, la stratégie de sélection des répondants, les types de données et leurs procédures de traitement et d'analyse. Nous aborderons ensuite les critères de validité qui ont été mis en œuvre. Enfin, nous traiterons des considérations éthiques associées à notre recherche compte tenu de la nature confidentielle et sensible de certaines données qui ont été recueillies. Il est essentiel dans le cadre de cette recherche d'assurer la protection de l'anonymat des sources de façon à prévenir d'un quelconque préjudice pour les participants et leur organisation respectives.

L'expérience du chercheur qui est un professionnel de l'audit est importante dans le cadre de cette recherche puisqu'elle lui a permis d'acquérir une très bonne connaissance de la dynamique du milieu et de ses codes spécifiques de communication. La distance qui est nécessaire pour aborder cette recherche a pu être assurée en décidant d'exclure son environnement de travail direct.

3 - 1 LA STRATEGIE DE RECHERCHE APPLIQUEE

Selon Eisenhardt (1989), la recherche qualitative est particulièrement enrichissante pour étudier un phénomène selon une approche qui est différente de l'approche théorique dominante et lorsque les données relatives à l'objet de recherche étudié sont soit insuffisantes, soit trop

fragmentaires pour réaliser une étude quantitative fiable. La revue de la littérature sur l'audit interne nous a montré que d'autres travaux de recherche sont nécessaires dans le domaine de l'approche par les risques et les pratiques de l'audit dans ce domaine, car les connaissances actuelles sont insuffisantes.

Selon Patton (2002), la méthodologie doit nous permettre de répondre aux questions de recherche et d'atteindre les objectifs. Notre recherche vise non pas à comprendre pourquoi mais comment les auditeurs internes procèdent en pratique pour identifier et évaluer les risques au sein de leur organisation et quelles heuristiques ils mettent en œuvre pour y parvenir. Nous nous intéressons aussi aux facteurs organisationnels, sociaux et culturels ainsi qu'aux systèmes de valeurs qui peuvent influencer ce processus de construction des objets de risque au sein des organisations. La recherche qualitative de type ethnographique permet de porter une attention particulière aux détails ainsi qu'au contexte du phénomène étudié. Les facteurs organisationnels et culturels représentent une dimension essentielle dans le cadre de notre projet de recherche.

Enfin, selon Miles et Huberman (2003), l'approche qualitative permet de développer une meilleure compréhension d'un phénomène du point de vue des personnes qui le vivent. Nous avons considéré dans le cadre de notre recherche que le risque est un construit social qui s'établit au sein des organisations par les membres qui en font partie. Il est dès lors primordial de s'intéresser à la manière dont ils se représentent le phénomène étudié qui est le risque.

C'est pour ces raisons que nous avons opté pour une étude qualitative avec comme méthode de recherche les entretiens. Le choix de la méthode découle des objectifs de notre projet de recherche.

3 - 2 L'APPROCHE METHODOLOGIQUE

L'approche méthodologique décrit l'approche et les choix que nous avons mis en œuvre pour collecter, traiter et analyser les données afin de répondre aux questions de recherche. Celui-ci est établi en cohérence avec notre stratégie et notre méthodologie de recherche basées sur les « entretiens ».

Tableau 6. Stratégie et méthodologie de recherche

Méthodologie	
Stratégie et type de recherche	Méthode qualitative / Entretiens
Unité d'analyse	Direction de l'audit interne
Sélection des entreprises et des répondants	Plusieurs critères de choix : <ul style="list-style-type: none"> - Grandes entreprises (Sociétés du CAC 40 et du SBF 120) - Secteur d'activité : Industriel et Commercial - Exclusion des banques, assurances et des PME
Collecte de données	<ul style="list-style-type: none"> - Réseau professionnel de proximité - Réseaux sociaux - Conférences
Sources des données	Entretiens <ul style="list-style-type: none"> - Entretiens individuels de type semi-directif avec guide d'entretien - « Focus group » avec les participants (volontaires) - Durée 1h30 par entretien individuel et 2h00 pour les focus group Documentation publique et non-publique relative aux risques et à l'activité des directions de l'audit interne des organisations qui ont été sélectionnées.
Procédures d'analyse de données	<ul style="list-style-type: none"> - Grille de codage initiale issue du cadre théorique et des normes d'audit - Grille initiale enrichie par un codage multithématique - Analyse de contenu
Expérience du chercheur	Directeur adjoint de l'audit d'un groupe industriel (15 ans d'activité en audit)

3 - 2 1 L'UNITE D'ANALYSE

L'unité d'analyse correspond à ce sur quoi le chercheur veut tirer des conclusions (Patton, 2002). On peut aussi la définir comme « un phénomène donné qui se produit dans un contexte délimité » (Miles et Huberman, 2003). L'unité d'analyse permet de traiter les données de façon à ce que le chercheur puisse conclure quant aux questions de recherche posées. Le choix de l'unité d'analyse est donc étroitement lié à l'objectif de la recherche (Patton, 2002).

Notre recherche vise à comprendre « *Comment les organisations construisent-elles leurs objets de risques et par quelles heuristiques ?* »

Il nous faudra dès lors répondre aux questions suivantes :

- *comment les risques identifiés dans l'organisation (cartographie des risques) orientent-ils les travaux des auditeurs internes ?*
- *comment sont évalués les risques de l'organisation lors de la construction du plan d'audit ?*
- *comment sont définies les missions sur la base de l'évaluation préliminaire des risques ?*
- *dans quelle mesure l'auditeur interne peut être un observateur pertinent des risques de l'organisation ?*

L'unité d'analyse retenue pour notre recherche est la direction de l'audit interne car elle nous permettra de répondre à l'ensemble de ces questions. La direction de l'audit interne n'agit pas indépendamment du contexte organisationnel dans lequel elle réalise ses activités. Il est dès lors essentiel de mieux comprendre la nature de ces interactions.

3 - 2 2 LE PROCESSUS DE SELECTION DES ENTREPRISES ET DES REpondANTS

En recherche qualitative, l'objectif n'est pas de pouvoir généraliser les résultats obtenus mais plutôt de comprendre en profondeur un phénomène étudié. La sélection ne repose donc pas sur une approche d'échantillonnage statistique mais se fait en fonction de critères prédéfinis par le chercheur en lien avec les questions de recherches qui sont adressées.

3 - 2 2 1 LES CRITERES DE CHOIX RETENUS

Selon Eisenhardt (1989), l'étude de terrain effectuée sur plusieurs sites présente l'avantage de permettre la comparaison des réponses des répondants qui travaillent dans des organisations différentes. Ce procédé permet d'acquérir des connaissances plus globales qu'au moyen d'une étude de terrain avec un site unique.

Notre projet de recherche a ainsi été conduit auprès de plusieurs directions de l'audit interne de grands groupes du secteur industriel, du secteur commercial et celui des services (CAC 40 et SBF 120). Les entreprises de ce secteur ne disposent pas, contrairement à celui des assurances, de données suffisantes pour appréhender le risque par une approche fréquentiste et probabiliste. Cette difficulté pratique soulève dès lors la question de savoir comment ces sociétés procèdent pour identifier et désigner les risques au sein de leur organisation.

Nous avons décidé de ne pas retenir pour notre étude le secteur financier (Banques et Assurances) qui est soumis à des obligations réglementaires particulièrement contraignantes qui de surcroît peuvent impacter la nature et le contenu du travail des auditeurs internes. Par ailleurs, l'application des outils traditionnels du risque (approche probabiliste ou fréquentiste) pose en règle générale moins de difficulté. Ont aussi été exclues de notre étude les Petites et Moyennes Entreprises puisqu'elle ne dispose souvent pas d'une direction de l'audit à part entière.

Afin de réaliser le choix des directions de l'audit, nous n'avons privilégié le chiffre d'affaires de la société plutôt que le critère de la taille de direction de l'audit interne. L'information relative aux ressources allouées pour les directions d'audit est rarement disponible. Par ailleurs, nous avons veillé à sélectionner des groupes qui sont issus principalement du CAC 40 et du SBF 120 puisqu'il s'agit de groupes qui sont soumis à des obligations de communication en matière de risques et de dispositif de contrôle interne dans le cadre des exigences réglementaires (lois de sécurité financière, 8^{eme} directive Européenne).

3 - 2 2 2 DETERMINATION DU NOMBRE D'ENTRETIENS

Après avoir précisé et délimité le périmètre de notre étude, il nous a fallu déterminer le nombre d'entretiens à réaliser pour répondre à nos questions de recherche.

Selon Pires (1997), il existe deux grandes manières de produire des preuves empiriques : les chiffres (méthodes quantitatives) ou les mots (méthodes qualitatives). Il insiste sur le fait qu'en matière de recherche qualitative, il n'est pas utile de faire la distinction entre échantillon probabiliste et non probabiliste. Selon Pires (1997), la distinction doit plutôt se faire entre l'échantillonnage par cas unique (une personne, un site, ...) ou bien par des cas multiples.

En matière de recherche qualitative, l'objectif n'est donc pas de respecter les techniques d'échantillonnage statistiques mais plutôt d'assurer l'adéquation de notre corpus empirique avec notre objet de recherche. Un critère essentiel de validité doit néanmoins être pris en compte en recherche qualitative : le principe de saturation.

Selon Thiétart et al. (2003), la taille adéquate d'un échantillon est celle qui permet d'atteindre la saturation théorique. Il relève à cet effet que « *cette saturation théorique est atteinte lorsqu'on ne trouve plus d'information supplémentaire capable d'enrichir la théorie. Par conséquent, il est impossible de savoir a priori quel sera le nombre d'unités d'observation nécessaire. La collecte des données s'arrête lorsque les dernières unités d'observations*

analysées n'ont pas apporté d'éléments nouveaux. Ce principe repose sur le fait que chaque unité d'information supplémentaire apporte un peu moins d'information nouvelle que la précédente jusqu'à ne plus rien apporter. Ce principe est observé empiriquement ».

Selon Pires (1997), il faut distinguer la saturation théorique de la saturation empirique. La saturation théorique s'applique à un concept et signifie que celui-ci émerge des données et est confronté par la suite à différents contextes empiriques, le but du chercheur étant de développer les propriétés du contexte et de s'assurer de sa pertinence théorique et de son caractère heuristique. Lorsque, après des applications successives, les données n'ajoutent aucune propriété nouvelle au concept, on peut dire que le concept créé est saturé (...).

La saturation empirique ou « de connaissance » (...) s'applique plus aux données elles-mêmes, ou aux aspects du monde empirique pertinents pour l'analyste, qu'aux propriétés des concepts en tant que telles. La saturation empirique désigne alors le phénomène par lequel le chercheur juge que les derniers documents, entrevues ou observations n'apportent plus d'informations suffisamment nouvelles ou différentes pour justifier une augmentation du matériel empirique.

Selon Griffin et Hauser (1993), le nombre d'informations additionnelles décroît avec le nombre de personnes interrogées selon une loi Bêta-binomiale. Les auteurs montrent dans leurs travaux qu'avec vingt entretiens, il est possible d'obtenir quatre-vingt-dix pourcents des informations collectées avec trente entretiens. Griffin et Hauser estiment qu'avec une trentaine d'entretiens, nous pouvons obtenir quatre-vingt-dix pourcents des informations qu'il est possible de collecter.

Dans notre cas, nous avons en pratique jugé avoir atteint le niveau de saturation théorique et empirique en ayant réalisé un peu moins d'une trentaine d'entretiens (27 entretiens d'une durée moyenne d'une heure trente). Nous avons décidé de poursuivre les entretiens afin de valider le fait que nous avons atteint le niveau de saturation. Nous avons décidé d'arrêter à l'issue du trente-deuxième entretien.

3 - 2 2 3 PROCÉDE EMPIRIQUE MIS EN ŒUVRE POUR CONSTITUER LA LISTE DES REpondANTS

L'accès aux données est particulièrement difficile dans le domaine de l'audit interne. Il s'agit de traiter lorsqu'il est question d'audit interne d'informations jugées confidentielles et potentiellement préjudiciables pour les organisations puisqu'il s'agit de leurs risques. Malgré le fait que les grandes entreprises communiquent sur ce thème dans le cadre des rapports

annuels, les informations restent le plus souvent très descriptives. Il n'est pas possible sur cette base de connaître les processus d'identification et d'évaluation qui sont mis en œuvre en amont.

Pour réussir à constituer la liste des répondants, le chercheur a dû mobiliser différentes ressources qui sont décrites dans cette section.

Comme nous l'avons précisé, le chercheur était au moment de l'étude lui-même salarié d'une Direction de l'audit interne d'un grand groupe industriel.

Le nombre de sociétés qui ont ainsi accepté de participer à ce travail de recherche représente un peu plus d'une trentaine de sociétés qui opèrent dans le secteur de l'Industrie, du Commerce et des Services. En recherche qualitative, la taille de l'échantillon est moins importante que la richesse des données collectées ainsi que la capacité d'observation et d'analyse du chercheur (Patton, 2002). Néanmoins, nous disposons d'un terrain de recherche particulièrement riche.

La première ressource que le chercheur a mobilisée a été son réseau professionnel. Étant praticien depuis plus d'une dizaine d'années et membre d'une association professionnelle (l'Institut Français de l'Audit et du Contrôle Interne), le chercheur avait accès à un réseau de professionnels de l'audit interne. L'association réunissait à diverses occasions ses membres dans le cadre soit de groupe de travail ou bien de conférences mensuelles et annuelles. C'est à l'occasion de ces réunions qu'il a pu établir un certain nombre de contacts avec plusieurs de ses homologues au sein des autres groupes de place. Il a donc décidé dans un premier temps de contacter une quinzaine de directeurs de l'audit ou manager d'audit dans le cadre de cette recherche. Il a veillé à bien préciser dans quel cadre s'insérait ce travail de recherche et qu'il s'agissait d'une démarche indépendante sans lien avec son activité professionnelle. Après s'être engagé sur un principe de confidentialité avec chacune d'entre elles, le chercheur a eu un accord de principe de 6 directeurs de l'audit (soit un peu moins de la moitié des personnes contactées).

Afin de pouvoir toucher plus de directeurs de l'audit, le chercheur a sollicité son hiérarchique afin de le mettre en contact avec son propre réseau professionnel. Le chercheur a ainsi pu obtenir 8 directeurs de l'audit supplémentaires. Le chercheur a ainsi pu constituer dans un premier temps une liste de 14 répondants dans le cadre de sa recherche.

La seconde ressource que le chercheur a décidé de mobiliser a été les réseaux sociaux (principalement le réseau « *LinkedIn* »). Le chercheur a établi dans un premier temps une liste des sociétés du CAC 40 et du SBF 120 sur un fichier Excel et élaboré un tableau de suivi. La stratégie retenue par le chercheur a été de simplement rentrer en contact avec les directeurs de

l'audit sans leur communication d'information relative à son projet de recherche. L'objectif était déjà d'envoyer un maximum d'invitation à rejoindre son réseau professionnel. Pour ce faire, le chercheur a procédé dans l'application à des recherches en tapant les mots-clés « Directeur audit interne », « VP audit », « SVP audit » associé au nom des groupes ciblés de sa liste de sociétés.

La copie d'écran qui figure ci-dessous met en évidence le profil que le chercheur a utilisé pour entrer en contact avec les directeurs de l'audit interne des entreprises au moyen du réseau social « *LinkedIn* ». Ce profil fait clairement apparaître sa double compétence en tant que professionnel de l'audit interne et de chercheur au sein d'une Université parisienne.

Figure 11. Collecte des données - profil du chercheur sur le réseau « *LinkedIn* »

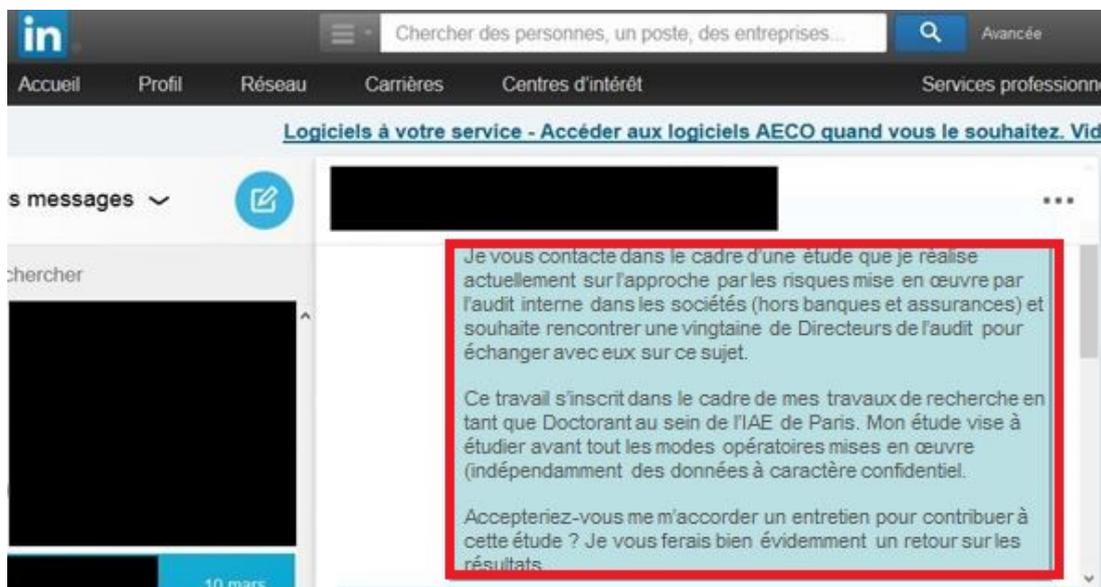


Une des difficultés qu'il a rencontrées est que le moteur de recherche ne lui a pas permis de retrouver un bon nombre de directeurs de l'audit pour les sociétés qu'il visait. Certains d'entre eux étaient inscrits mais sous un compte « premium » réservé à certains membres. Il a donc décidé de s'inscrire avec un nouveau profil pour lui permettre de rentrer en contact avec un plus grand nombre d'inscrits sur ce réseau. Il a par ailleurs réussi à identifier des auditeurs membres des sociétés ciblées qu'il a aussi contacté en vue de pouvoir être indirectement mis en contact avec leur hiérarchie. Cette dernière démarche ne s'est pas révélée efficace.

Cet exercice de prise de contact a été mis en œuvre par vague successive. C'est-à-dire que le chercheur une fois après avoir eu les premiers contacts a décidé de lancer la deuxième action de sa stratégie de collecte. Comme nous l'avons précisé, le premier message était une simple invitation à rejoindre son réseau professionnel sans faire référence au projet de recherche. L'application LinkedIn permet une fois que deux membres sont connectés de s'échanger des messages électroniques.

La deuxième étape a donc consisté à écrire à chacun des nouveaux contacts un courriel type que le chercheur a pris soin de rédiger. Le chercheur précisait dans ce message à quel titre il les contactait ainsi que l'objet de sa démarche, à savoir un travail de recherche doctoral sur l'audit interne et son approche par les risques. Le message précisait qu'il s'agissait d'une recherche universitaire sans lien avec son statut professionnel et que ce travail visait l'étude des pratiques sans accès aux données qui pouvaient être jugées comme étant confidentielles. Le chercheur précisait dans son message qu'il s'engageait d'ailleurs à assurer une stricte confidentialité sur le nom des répondants et à leur faire une restitution des résultats à une étape intermédiaire. Voici une capture d'écran du message qui a été transmis aux directeurs de l'audit.

Figure 12. Collecte des données – exemple de prise de contact – utilisation des réseaux sociaux



Cette démarche a été mise en œuvre de façon répétée jusqu'à pouvoir obtenir un accord de principe d'au moins une dizaine de directeurs. Au total, un peu moins de 50 invitations ont été envoyés avec un taux de réponse positif de 65% pour la première phase qui visait à faire partie du réseau de la personne contactée. Sur les 32 directeurs de l'audit qui ont accepté l'invitation,

le chercheur a réussi à obtenir un accord de principe pour 11 d'entre eux. Une personne s'est désistée en le motivant par un changement de poste.

Enfin la troisième ressource mobilisée a été la prise de contact direct lors de séminaires professionnels animés par le chercheur lui-même sur le thème de l'audit interne. Étaient présents à ce séminaire de nombreux praticiens de l'audit interne. Le chercheur qui a participé à deux de ces séminaires en tant qu'intervenant a pu prendre les coordonnées de plusieurs participants puis les a recontactés. Il a pu obtenir l'accord de 7 autres directeurs de l'audit pour participer à son étude.

Figure 13. Collecte de données – exemple de prise de contact direct

The screenshot shows the website for 'marcusevans France'. The main heading is 'Dispositif d'Audit et de Contrôle Interne' with the subtitle 'Maîtriser les risques et améliorer votre performance'. The event dates are '28-30 Jan 2015' in 'Paris, France'. A list of speakers is provided under 'Retour d'expérience de', including Emmanuel Pascal, Christopher Church, Andrew Bailey, Christophe Roger, and Coskun Cakar. A red box highlights 'Coskun Cakar' and a white box labeled 'Le chercheur' is connected to it by a line.

Le chercheur a ainsi réussi à constituer un groupe de 32 répondants dans le cadre de son travail de recherche.

3 - 2 3 LES REpondants

3 - 2 3 1 LES ENTREPRISES QUI ONT PARTICIPE A L'ETUDE PAR SECTEUR D'ACTIVITE

Le chercheur a pu réaliser des entretiens avec 32 directeurs de l'audit interne au sein de grands groupes du secteur Industriel, Commercial et des Services. Il s'agit de groupes pour la plupart cotés (26 sur 32) assujettis à des obligations de communication sur leurs dispositifs de contrôle

interne et processus de gestion des risques. Ils sont tous dotés d'une direction de l'audit interne dédiée. Le nom des sociétés qui ont participé à ce travail de recherche a été rendu anonyme pour des raisons de confidentialité compte tenu de la sensibilité des informations échangées. Les entreprises Industrielles représentent un peu moins de la moitié des répondants (15 entreprises). Elles font toutes parties du SBF 120. Parmi ces entreprises, sont notamment représentées celles qui sont spécialisées dans la chimie, le secteur automobile, l'énergie, l'alimentaire ou encore les matériaux de construction.

Tableau 7. Entreprises du secteur industriel

1	Batimodern	Equipements de construction
2	Chimica	Chimie
3	Chimicor	Chimie
4	Cimento	Ciment
5	Elec	Énergie
6	Equipauto	Equipements automobile
7	Fromago	Produits alimentaires
8	Gazeo	Chimie
9	LuxStore	Luxe
10	Micropix	Electronique
11	Petroleum	Énergie
12	RaceCar	Construction automobile
13	SanteForm	Chimie
14	Vehicar	Construction automobile
15	Voltage	Equipements électriques

Les entreprises commerciales sont des grandes entreprises (6 entreprises font partie du SBF 120) qui sont spécialisées dans la vente de produits de consommation (électroménager, multimédia, mode et habillement, ...).

Enfin, 8 entreprises du secteur des services (dont 6 cotées au SBF 120) ont participé à cette étude. Elles opèrent dans des domaines variés tels que le transport des personnes ou des biens de marchandise, l'ingénierie ou encore l'environnement.

3 - 2 3 2 NIVEAU DES EFFECTIFS DE L'AUDIT INTERNE PAR SOCIETE

Les effectifs des différentes directions de l'audit ont été recueillis lors des entretiens. Les données témoignent d'une grande hétérogénéité entre les entreprises aussi bien en termes de ratio du nombre d'auditeurs par Milliards de Chiffre d'affaires que du nombre d'auditeurs par rapport à l'effectif total exprimé en millier d'employés.

Tableau 8. Liste des sociétés qui ont participé à l'étude

		Effectif de l'audit (année 2015)			Effectif de l'audit (année 2015)
1	Restaulib	30	17	Petroleum	48
2	Chimica	7	18	Sportflex	12
3	Vestimod	2	19	Fromago	6
4	Bati-F	10	20	WallDistrib	50
5	DistriMart	137	21	Batimodern	80
6	Enginico	4	22	Baticosto	50
7	Gazeo	37	23	BeauMag	10
8	Voltage	20	24	LuxStore	7
9	Elec	90	25	ElectroStore	11
10	Chimicor	30	26	Cimento	27
11	Santeform	70	27	Naturelia	24
12	Vino	2	28	MultimedStore	3
13	Micropix	25	29	Vehicar	33
14	Autocar	5	30	Aéro	15
15	Mediacorp	15	31	RaceCar	26
16	Equipeauto	13	32	Voyago	50

3 - 2 3 3 DUREE DES ENTRETIENS REALISES

Les entretiens se sont déroulés entre le mois de février et la fin du mois de novembre 2015, soit une période de neuf mois avec en moyenne 3 entretiens par mois. Nous avons réalisé au total 47 heures d'entretiens. Les entretiens ont, à l'exception d'un cas, tous été réalisés avec les directeurs de l'audit interne au siège de chacune des entreprises, dans les locaux de la direction de l'audit concernée. La durée minimale des entretiens a été de 1 h 10 et la durée maximale de 2 h 20. La durée moyenne des entretiens représente 1 h 45. Les entretiens nous ont permis de constituer un volume significatif de données (près de 1 100 pages de transcription pour les

entretiens, complétées par de la documentation interne et externe qui ont pu être collectées par ailleurs).

La liste des entretiens figure à la page suivante.

Tableau 9. Liste des entretiens

		Date	Lieu	Fonction	Durée
1	Restolib	16/02/2015	Paris	Directeur de l'audit	1h15
2	Chimica	18/02/2015	Paris	Directeur de l'audit	1h45
3	Vestimod	23/02/2015	Région Parisienne	Directeur de l'audit	1h45
14	Autocar	24/02/2015	Paris	Directeur de l'audit	1h40
4	Bati-F	26/02/2015	Région Parisienne	Directeur de l'audit	1h25
24	LuxStore	27/02/2015	Paris	Directeur de l'audit	2h20
12	Vino	03/03/2015	Paris	Directeur de l'audit	1h35
10	Chimicor	09/03/2015	Région Parisienne	Directeur de l'audit	2h20
30	Aéro	17/03/2015	Paris	Directeur de l'audit	2h10
32	Voyago	31/03/2015	Région Parisienne	Directeur de l'audit	1h20
17	Petroleum	09/04/2015	Paris	Directeur de l'audit	1h45
27	Naturelia	14/04/2015	Région Parisienne	Directeur de l'audit	1h30
31	RaceCar	15/04/2015	Paris	Directeur de l'audit	1h10
25	ElectroStore	17/04/2015	Région Parisienne	Directeur de l'audit	1h40
26	Cimento	17/04/2015	Paris	Directeur de l'audit	1h40
6	Enginico	04/05/2015	Région Parisienne	Directeur de l'audit	2h15
21	Batimodern	04/05/2015	Région Parisienne	Directeur de l'audit	1h40
11	Santeform	05/05/2015	Paris	Directeur de l'audit	2h00
3	BeauMag	17/05/2015	Paris	Directeur de l'audit	1h50
16	Equipauto	18/05/2015	Paris	Directeur de l'audit	1h25
28	MultimedStore	18/05/2015	Région Parisienne	Directeur de l'audit	1h30
29	Vehicar	18/05/2015	Région Parisienne	Directeur de l'audit	1h10
8	Voltage	21/05/2015	Région Parisienne	Directeur de l'audit	1h30
9	Elec	21/05/2015	Région Parisienne	Directeur de l'audit	1h30
15	Mediacorp	29/05/2015	Paris	Directeur de l'audit	1h30
22	Baticosto	01/06/1995	Paris	Directeur de l'audit	1h30
7	Gazeo	25/06/2015	Paris	Directeur de l'audit	1h45
5	DistriMart	29/06/2015	Lille	Directeur de l'audit	1h20
20	WallDistrib	08/07/2015	Région Parisienne	Directeur de l'audit	1h15
19	Fromago	28/10/2015	Paris	Directeur de l'audit	1h45
13	Micropix	19/11/2015	Par téléphone	Directeur de l'audit	1h30
18	Sportflex	23/11/2015	Lille	Directeur de l'audit	1h30
					47h00

3 - 2 3 4 SPECIFICITES ORGANISATIONNELLES DES DIRECTIONS DE L'AUDIT

Les entretiens menés nous ont permis d'identifier plusieurs typologies d'organisation de la fonction d'audit interne au sein des groupes représentés dans cette étude. La direction de l'audit peut avoir des spécificités organisationnelles selon les organisations au regard de son rattachement hiérarchique, le périmètre et la nature des missions qui lui sont confiées et enfin son degré de décentralisation.

Tableau 10. Typologie d'organisation des directions de l'audit

Rattachement hiérarchique de l'audit	Périmètre couvert par l'audit	Organisation
Comité d'audit	Audit	Centralisée
Direction générale	Risque et audit Audit et contrôle interne Risque, audit et contrôle interne	Décentralisée

3 - 2 4 LES SOURCES DES DONNEES ET LES PROCEDURES DE COLLECTE

Selon Patton (2002), nous retrouvons souvent trois sources de données dans le cadre des recherches qualitatives : les entretiens, l'observation et enfin la documentation. Dans le cadre de notre projet de recherche, nous avons ainsi mis en œuvre la triangulation des outils de collecte de données ainsi que celles des sources. Pour ce qui concerne les entretiens, deux types d'entretiens ont été réalisés pour la collecte des données. Tout d'abord des entretiens individuels de plus d'une heure et demie en moyenne avec chacun des directeurs de l'audit identifiés puis des entretiens collectifs (focus group) avec une dizaine de volontaires parmi les répondants. Les entretiens ont été complétés par des sources documentaires à la fois publiques et non publiques.

Type d'entretien

Quatre types d'entretiens individuels sont répertoriés par Patton (2002) pour la recherche qualitative : l'entretien informel, l'entretien semi-structuré avec l'utilisation d'un guide, l'entretien standardisé avec des questions ouvertes et l'entretien avec des questions fermées.

Nous avons décidé d'utiliser les entretiens semi-structurés dans le cadre de notre recherche. Un guide d'entretien a été établi et comportait une liste de sujets à aborder au cours de l'entretien. Les sujets contenus dans cette liste portaient notamment sur le processus d'identification des risques, l'élaboration du plan d'audit interne et la réalisation des missions d'audit interne.

Le chercheur a pu ainsi conserver une grande liberté dans la formulation de ses questions et dans la séquence des sujets abordés, tout en s'assurant de traiter tous les sujets pertinents à la collecte de données.

Ce mode opératoire a permis d'obtenir des données sur chaque sujet en adaptant les questions à la durée de l'entretien. Le principal avantage de cette méthode est qu'elle conserve en grande partie le côté naturel de l'entretien et qu'elle permet au chercheur de rester centré sur ses questions de recherche dans le respect du temps imparti. Par ailleurs, le guide utilisé peut être plus ou moins détaillé selon la durée de l'entrevue.

Lors des entretiens, l'une des difficultés auxquelles a fait face le chercheur est que plusieurs personnes interrogées avaient tendance à formuler des réponses que l'on pourrait qualifier de génériques et difficile à exploiter. A titre d'exemple, à la question « comment procédez-vous pour l'évaluation des risques, la personne interrogée a répondu « mais c'est une démarche classique, avec probabilité et impact ». Si le chercheur s'en tient simplement à cette réponse, il sera certainement difficile pour lui de disposer pour la suite de son travail d'une information riche en contenu.

Le chercheur a donc pris une posture active lors de tous ces entretiens de façon à pouvoir avoir un regard vigilant sur le contenu et la valeur informative des données transmises. Le but étant de pouvoir relancer si besoin son interlocuteur pour pouvoir collecter une information la plus riche possible en contenu. Cette posture active a en partie été facilitée par le fait que le chercheur avait une bonne connaissance du milieu de l'audit et de certains de ces codes de communication.

Le chercheur a donc conduit les entretiens sur la base du guide qu'il avait établi et qui reprenait l'ensemble des axes qu'il souhaitait traiter. Ce guide est construit de telle manière qu'il permet au chercheur de ne pas se perdre dans le détail et de partir du général vers le particulier. La posture active du chercheur lui permet comme nous l'avons précisé de ne pas rester à un niveau de généralité mais d'interagir avec son interlocuteur pour approfondir les sujets.

Tableau 11. Guide d'entretien

1	Rappel de l'objectif de la recherche
2	Prise de connaissance générale sur l'entreprise
3	Organisation de l'audit Rattachement de l'audit Périmètre couvert par l'audit (Risque, contrôle interne, audit, conseil) Nombre d'auditeurs Profil des auditeurs Nombre de missions Type de mission
4	Processus de cartographie des risques Acteurs en charge d'animer le processus Processus mis en œuvre pour identifier les risques Outils d'identification des risques Sources d'identification des risques Méthode d'évaluation des risques Procédé de hiérarchisation des risques Procédé pour élaborer la synthèse Validation de la cartographie Processus de mise à jour
5	Élaboration du plan d'audit Processus d'identification des sujets d'audit Lien entre les risques et les missions du plan Autres critères que les risques pour le choix des missions Périmètre ou sujets non couverts Processus de hiérarchisation des sujets Processus de sélection des sujets Validation du plan d'audit Flexibilité du plan d'audit
6	Élaboration du plan de mission Préparation de la mission Analyse préliminaire des risques Choix des axes d'intervention (périmètre de revue) Allocation des ressources (durée, composition des équipes) Élaboration du programme de travail

Selon Patton (2002), le risque que court le chercheur en utilisant un guide d'entrevue pour sa collecte de données est d'omettre un sujet important lors de sa rencontre avec le répondant. Ce risque a néanmoins été limité par le fait que le guide d'entretien partait du général au particulier afin d'aider le chercheur à ne pas se perdre dans le détail. Le chercheur a veillé à couvrir de façon systématique l'ensemble des thèmes avec chacun des répondants pour ensuite approfondir certains thèmes en fonction du temps restants. Il a par ailleurs pu ajuster son guide pour l'enrichir au fil des entretiens afin de prendre en compte des problématiques spécifiques qui avaient émergé lors des premiers entretiens. Les sujets étant abordés dans une séquence pouvant être différente et au moyen de questions également différentes, il peut devenir difficile de comparer les réponses. Néanmoins, il nous a été possible d'assurer une certaine homogénéité des thèmes traités.

Enregistrement et transcription des entretiens

Tous les entretiens ont été enregistrés afin de pouvoir ensuite les retranscrire de façon la plus fidèle possible.

L'ensemble des entretiens qui représente 48 heures d'enregistrement a donc été intégralement retranscrit et nous a fourni un matériau brut de près de 1100 pages. Les transcriptions ont été complétées avec les notes prises par le chercheur durant l'entretien quant aux messages non verbaux.

3 - 2 4 2 LES ENTRETIENS COLLECTIFS (FOCUS GROUPE ET ATELIERS DE TRAVAIL)

Une seconde stratégie de collecte de donnée a été choisie dans le cadre de notre recherche. Il s'agit des entretiens collectifs. Ces entretiens ont été menés avec un nombre restreint de participants. Ils ont pris la forme des entretiens de groupe tel que décrits par Krueger et Casey (2002).

Constitution du Focus group

Selon Krueger et Casey (2002), certains critères de validité tels que la taille du groupe et sa composition doivent être respectés. Nous avons veillé à bien respecter ces critères lors de la constitution du groupe.

Nous avons ainsi constitué ce groupe sur la base du volontariat en proposant à l'ensemble des directeurs qui ont accepté de participer à notre étude de se joindre à une session spécifique de réunion de travail. L'acceptation par plusieurs directeurs de l'audit a été motivée par le fait que

le chercheur lors de sa première prise de contact avait proposé de faire une restitution des résultats de l'étude. Ainsi, le chercheur a saisi cette opportunité pour réussir à réunir un certain nombre de directeurs pour le focus group et à tenir l'engagement qu'il avait pris au départ auprès de chacun des répondants.

L'organisation des réunions de groupe

Selon Krueger et Casey (2002), la réalisation de groupes focalisés exige le respect de certaines règles méthodologiques afin d'assurer la validité et le caractère scientifique de la démarche. Cette technique d'entretien repose donc sur la dynamique de groupe, elle permet d'explorer et de stimuler différents points de vue par la discussion. Les échanges favorisent l'émergence de connaissances, d'opinions et d'expériences comme une réaction en chaîne grâce à la réunion de personnalités diverses favorisant l'expression et la discussion d'opinions controversées. Le chercheur est comme un explorateur, il peut connaître en partie le sujet mais qui va aussi découvrir des domaines inconnus. La méthode des focus groupes permet par l'expression directe des participants de faire émerger des idées diverses, parfois inattendues pour le chercheur, reflet des valeurs sociales, culturelles et/ou religieuses de chacun. L'entretien collectif permet de donner plus de poids aux critiques que dans les entretiens individuels. Cette méthode de recueil de données permet d'évaluer par exemple les expériences, les besoins, les attentes, les représentations des participants.

Les limites des focus groupes résultent des aspects « bloquants » de la discussion de groupe : les participants peuvent rester dans les idées considérées comme « socio culturellement correctes ». La présence d'un « leader » d'expression dans le groupe ou de relations conflictuelles entre les participants peut aussi entraver la libre expression. À charge du modérateur de canaliser ces différentes tensions afin d'optimiser le recueil des données et la richesse des débats.

Nous avons prévu d'appliquer cette méthode dans le cadre de plusieurs réunions spécifiques d'environ deux heures avec tous les membres du « focus group ». Toutefois, compte tenu des difficultés à réunir l'ensemble des participants plusieurs fois, nous avons finalement opté pour une réunion unique de deux heures avec l'ensemble des participants. Nous avons réservé pour cette occasion une salle de réunion équipée qui est située dans le centre de Paris. Ce dispositif nous a permis d'assurer à la fois une certaine neutralité du lieu et un environnement propice aux échanges. L'intégralité des échanges a été enregistrée avec un appareil numérique placé au milieu de la salle.

Le scénario du focus group

La spécificité du scénario de ce focus groupe réside dans le point d'amorce qui a été utilisé par le chercheur pour initier et alimenter les échanges. Le chercheur a veillé à rendre anonyme les sources de données dans le support qu'il a utilisé. Le focus groupe a démarré par une présentation sommaire des données issues des entretiens individuels réalisés en amont pour ensuite faire réagir et participer l'ensemble des membres. Ces derniers ont pu ainsi interagir sur la base des travaux et des synthèses établies par le chercheur et enrichir le matériau collecté lors des entretiens individuels.

L'animation du groupe

Le chercheur a dirigé l'ensemble des échanges sur la base du scénario préalablement établi. Il a eu recours lors de cet entretien à plusieurs outils : « approfondir, faire préciser, demander d'autres opinions, faire le tour de table ». La salle était équipée de deux tableaux « paper board » afin de noter les idées qui émergeaient et de permettre aux participants de les visualiser. Faute d'avoir pu disposer d'un observateur tiers comme cela avait initialement prévu, le chercheur n'a pas été en mesure d'assurer en parallèle de son animation la prise de notes pour relever les informations relatives à l'ordre d'intervention, aux messages non verbaux ainsi que les phrases clés. Il a cherché en priorité à faire réagir au maximum le groupe puisque le contenu des échanges était par ailleurs enregistré. Le chercheur a établi à la fin de la réunion une synthèse des idées et des opinions mais aussi des impressions qu'il avait lui-même ressenties ainsi que des difficultés rencontrées lors de la séance de travail.

3 - 2 4 3 LA DOCUMENTATION INTERNE ET LES RAPPORTS ANNUELS

Durant les entretiens, plusieurs directeurs de l'audit interne (30%) ont accepté de présenter et de commenter leurs documents internes relatifs à leurs activités d'audit interne. Le chercheur a ainsi pu voir des documents jugés particulièrement confidentiels tels que des cartographies des risques, des plans d'audit, des plans de mission et des rapports d'audit. Même si nous n'avons pas pu en prendre des copies, il nous a été possible de prendre des notes lors de l'entretien. Ces notes ont été reprises dans des mémos spécifiques afin de pouvoir être codés et donc exploités. Les répondants ont accepté d'échanger sur ces informations à condition que nous assurions une stricte confidentialité de ces données non publiques qui ne font pas partie des données présentées dans ce travail de recherche. Les informations recueillies ont néanmoins été

exploitées pour une meilleure compréhension du lien qui existe entre les éléments de la cartographie, la manière dont ils sont pris en compte dans le plan d'audit et le plan de mission. Nous avons également complété les entretiens avec la documentation publique présente dans les rapports annuels qui représentent une source d'information essentielle dans le cadre de notre recherche. En effet, suite aux scandales financiers et à la crise de confiance du début des années 2000, les États ont pour la plupart apporté une réponse réglementaire avec le vote des lois de sécurité financières. Ainsi, en France, la loi de sécurité financière impose depuis 2003 aux entreprises cotées de rendre compte dans leur rapport annuel des dispositifs de contrôle interne et de maîtrise des risques. Les rapports annuels présentent dans deux chapitres distincts les principaux risques de l'organisation et les dispositifs mis en œuvre pour les maîtriser. Nous avons rapproché ces éléments de ceux qui ont pu être recueillis durant les entretiens. Le recoupement des données publiques communiquées au travers des rapports annuels avec les informations collectées lors des entretiens nous a ainsi permis de trianguler les sources d'information.

3 - 2 4 4 LA RENCONTRE AVEC DES PAIRS

Le chercheur a été invité à participer à une réunion organisée par la direction des risques au sein du groupe BPCE. Étaient présents à cette réunion tous les « risk manager » ainsi que les responsables du contrôle permanent des antennes régionales (soit une quarantaine de personnes). Le chercheur a fait à cette occasion une restitution des principaux résultats auxquels il parvenait dans le cadre de ses travaux. La séance de discussion qui a eu lieu à l'issue de la présentation a mis en évidence que certaines des difficultés décrites par le chercheur pouvaient pour certains aspects concerner le secteur financier.

3 - 2 5 LA PROCEDURE DE TRAITEMENT ET D'ANALYSE DES DONNEES

3 - 2 5 1 L'ELABORATION DE LA GRILLE DE CODAGE

Dans une première étape, nous avons déterminé, à l'aide de notre cadre théorique et des normes d'audit interne, les principaux thèmes qui nous ont permis d'établir une grille de codage initiale. Ce travail a été réalisé préalablement aux entretiens.

Cette grille initiale a été enrichie et adaptée dans une seconde étape à l'aide des premiers entretiens individuels qui ont été réalisés. Afin de valider définitivement notre grille de codage, nous avons réalisé un double codage de nos premiers entretiens (4 entretiens sur 32) en faisant

appel à un deuxième chercheur qui était lui-même doctorant au sein de notre laboratoire de recherche. À l'issue de ce double codage la grille a été ajustée de façon à obtenir un taux de correspondance de 91% entre les deux chercheurs.

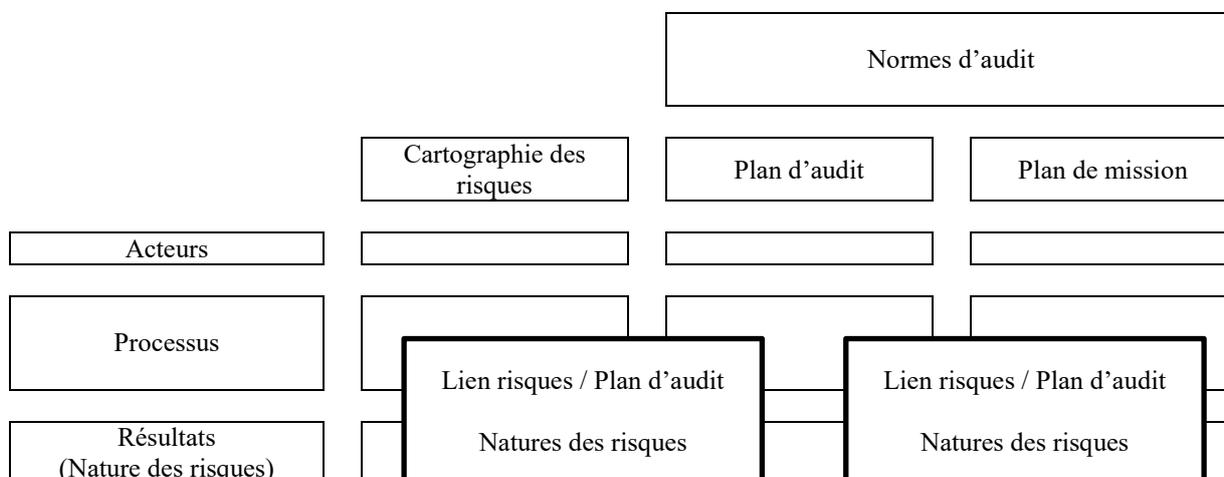
Nous devons répondre à deux questions de recherche spécifiques :

- Quelles sont les procédures mobilisées pour construire les plans d'audit et les plans de mission ?
- Quel est le lien entre ces éléments-là et les risques identifiés au sein de l'organisation ?

Notre grille de codage (représenté dans le schéma ci-dessous) a été établie de manière à pouvoir nous permettre d'y répondre en veillant à :

- recenser les acteurs impliqués, les processus de construction des objets de risques ;
- attacher ces données aux processus spécifiques couvertes dans notre étude en lien avec la construction des objets de risque (cartographie des risques, plan d'audit, plan de mission).

Tableau 12. Grille de codage – approche globale



La première étape pour élaborer cette grille de codage a été de reprendre les normes professionnelles pour la pratique de l'audit interne. Celles-ci décrivent chacune des étapes clés à respecter pour élaborer le plan d'audit et le plan de mission. La lecture attentive de ces normes a permis d'établir le processus d'élaboration associé. À titre d'illustration, les normes précisent que le plan de mission doit résultats d'une analyse préliminaire des risques afin d'établir les axes d'intervention et le programme de travail détaillé. La grille de codage a repris ces éléments.

Le tableau ci-dessous met en évidence la description du processus pour le plan d’audit ainsi que le plan de mission qui a résulté de ce travail. Il a été enrichi par les premiers entretiens.

Tableau 13. Processus d’élaboration du plan d’audit et du plan de mission

Plan d’audit
Construction de l’univers d’audit
Identification des sujets en lien avec les risques
Hierarchisation des sujets
Sélection des sujets
Validation du plan d’audit

Plan de mission
Analyse préliminaire des risques
Choix des axes d’intervention
Allocation des ressources à la mission
Élaboration du programme de travail

Nous avons dans un second temps établi le processus d’identification des risques sur la base du cadre de référence du COSO 2 – Entreprise Risk Management, enrichi par les premiers entretiens.

Tableau 14. Processus d’élaboration de la cartographie des risques

Cartographie des risques
Portage du processus
Identification des risques
Évaluation des risques
Hierarchisation des risques
Consolidation et synthèse des risques
Validation de la cartographie des risques
Mise à jour de la cartographie des risques

Une fois ces processus décrits, nous les avons croisés avec les concepts issus de notre cadre théorique. Ces concepts qui sont en lien avec les modes d'observation sont venus enrichir l'approche processuelle pour obtenir une grille de codage qui résulte de la combinaison du cadre théorique, des normes professionnelles de l'audit interne et du cadre de référence du processus de gestion des risques.

Tableau 15. Grille codage – méthode d'élaboration

Cartographie des risques		Cadre théorique	
Portage du processus			
Identification des risques	Processus d'identification des risques	Niveau d'observation	Observation 1 ^{er} ordre ou Observation de 2 ^e ordre
Évaluation des risques		Mode d'observation	Attribution des conséquences dommageables
Hiérarchisation des risques			Distinction temporelle
Consolidation et synthèse des risques			Code de communication
Validation de la cartographie des risques		Outils d'observation	Outils d'observation
Mise à jour de la cartographie des risques			

À titre d'exemple, l'étape identification des risques a été avec le cadre théorique de façon à retrouver les principaux concepts mobilisés dans le cadre de notre recherche ainsi que les étapes et les composantes du processus d'identification des risques. Ainsi, le risque est défini comme étant le futur selon Luhmann (1993). Une des questions qui est adressée lors des entretiens vise à voir quel est l'horizon de temps considérés par les acteurs en charge d'identifier les risques. Le fait de se projeter à un an est sensiblement différent d'une projection à dix ans et la nature des risques ainsi appréhendée sous le prisme du temps pourra être de nature différente. De la même manière, le processus de mise à jour de la cartographie fait intervenir une dimension temporelle puisqu'une cartographie remise à jours tous les deux ans dans un environnement particulièrement changeant ne sera pas forcément adaptée.

Nous avons ainsi procédé pour établir l'ensemble de notre grille de codage en nous interrogeant pour chacune des étapes des processus de cartographie des risques, de plan d'audit et de plan de mission afin d'établir un codage cohérent avec notre cadre théorique.

Nous avons complété les approches processuelles par une vision acteur. Notre objectif était de valider l’hypothèse selon laquelle l’audit interne était un observateur particulier au sein de l’organisation du fait de sa position d’observateur de second ordre. Au même titre que les autres fonctions expertes au sein de l’organisation.

Tableau 16. Grille de codage : codes relatifs aux acteurs impliqués

		Acteurs	
Qui attribue ?	Observateur de 1 ^{er} ordre	Gouvernance	Comité d’audit
			Président du conseil
		Management	PDG
			Directeurs fonctionnels
			Directeurs opérationnels
			Directeurs régionaux/pays
			Directeurs entités/opérationnels
	Observateur de 2 nd ordre	Audit interne	Rattachement de la direction de l’audit
			Compétences au sein de l’audit (spécialiste/généraliste)
		Autres fonctions contrôlantes	Experts internes/externes

La grille de codage par processus a été enrichie elle aussi sur la base des entretiens que le chercheur a menés. Notre cadre théorique nous a permis de mettre en lumière que le risque est fonction du point et du mode d’observation. La grille de codage permet de traiter des trois processus majeurs qui sont la cartographie des risques, le plan d’audit et le plan de mission.

La grille de codage reprend les concepts théoriques mobilisés.

Pour le point d’observation, nous avons distingué plusieurs niveaux organisationnels en distinguant des types d’approche (par fonction, par activité, par région, locale, transverse, ...) dans le but de voir quelles formes prennent les observations dites de premier ordre et de second ordre.

Le mode d’observation fait plutôt référence aux distinctions auxquels les acteurs ont recours lorsqu’ils identifient et sélectionnent les risques. Est-ce que les acteurs utilisent un langage

commun au sein de leur organisation ou bien des codes spécifique (à chaque sous-système) ?
 Quelle est l'échelle de temps auxquels ils se réfèrent lorsqu'ils cherchent à identifier les risques ?

Pour compléter cet aspect, il est essentiel de répondre à la question de savoir comment les acteurs évaluent le risque sur la base de la distinction risque/danger issue de notre cadre théorique. Les risques des uns étant les dangers des autres, que comprend l'évaluation du risque ? Est-ce que le processus d'évaluation des risques se limite à l'organisation ou bien envisage-t-elle les conséquences de ses décisions sur son environnement ?

Tableau 17. Grille de codage : codes relatifs au processus de cartographie

« Processus » de cartographie		
Acteurs	Portage du processus Validation de la carto	Portage du processus Validation de la carto
Type d'observation	Observation de 1 ^{er} ordre ou observation de 2 nd ordre	Observation de 1 ^{er} ordre Observation de 2 nd ordre
Mode d'observation	Point d'observation	Approche top-down/bottom-up/Mix
	Distinction risque/danger	Risque/danger – Externe (groupe vs. extérieur) Risque/danger – Interne (entité vs. groupe)
	Distinction temporelle	Historique (incidents survenus) Immédiat Prospectif
	Moment de l'observation	Multiple ou ponctuel
	Code de communication	Langage commun (de type proba/impact) Différents codes de communication
	Difficultés d'identification	Difficultés d'identification
Outils d'observation	Outils d'observation	Mapping des métiers/process Référentiel de risques existants Méthodologie d'identification des risques Sources d'information
Critères d'évaluation	Evaluation du risque	Modalités d'évaluation Difficultés d'évaluation
Critères de sélection	Critères de sélection	Sélection_ Comment Sélection_ Par qui
Résultats	Nature des risques	Natures des risques

Tableau 18. Grille de codage : codes relatifs à l'élaboration du plan d'audit

« Processus » du plan d'audit		
Type d'observation	Observation de 1 ^{er} ordre ou observation de 2 nd ordre	Observation de 1 ^{er} ordre Observation de 2 nd ordre
Mode d'observation	Point d'observation	Approche top-down/bottom-up/Mix
	Distinction risque/danger	Risque/danger – Externe (groupe vs. extérieur) Risque/danger – Interne (entité vs. groupe)
	Distinction temporelle	Historique (incidents survenus) Immédiat Prospectif
	Moment de l'observation	Multiple ou ponctuel
	Code de communication	Langage commun (de type proba/impact) Différents codes de communication
	Difficultés d'identification	Difficultés d'identification
Origine de la mission	Origine de la mission	Analyse des risques Autres que les risques
Critères de sélection	Critères de sélection	Sélection_Comment Sélection_Par qui
Critères d'exclusion	Critères d'exclusion	Sélection_Comment Sélection_Par qui
Résultats	Nature des missions	Natures des missions
Validation	Validation du plan	Validation_par qui

Tableau 19. Grille de codage : codes relatifs à l'élaboration du plan de mission

« Processus » du plan de mission		
Type d'observation	Observation de 1 ^{er} ordre ou observation de 2 nd ordre	Observation de 1 ^{er} ordre Observation de 2 nd ordre
Analyse préliminaire des risques : Mode d'observations	Point d'observation	Approche top-down/bottom-up/Mix
	Distinction risque/danger	Risque/danger – Externe (groupe vs. extérieur) Risque/danger – Interne (entité vs. groupe)
	Distinction temporelle	Historique (incidents survenus) Immédiat Prospectif
	Moment de l'observation	Multiple ou ponctuel
	Sources d'information	Sources d'information
	Difficultés d'identification	Difficultés d'identification
	Choix des axes d'intervention	Choix des axes d'intervention
Programme de travail	Élaboration du programme de travail	Programme standard Programme sur mesure
Critères d'exclusion	Critères d'exclusion	Exclusion_Comment Exclusion_Par qui
Résultats	Nature des missions	Natures des missions
Validation	Validation du plan	Validation_par qui

3 - 2 5 2 LE TRAITEMENT DES DONNEES

Le traitement et le codage des données

Nous avons établi dans le cadre de cette recherche une procédure spécifique de traitement des données avant de procéder à l'analyse. Celle-ci a consisté à définir un mode de traitement des données recueillies pour toutes les rendre anonymes du fait de leur caractère jugé hautement confidentiel et sensible par les participants de l'étude. La procédure qui a été mise en œuvre est décrite dans la section relative aux considérations éthiques.

Nous avons utilisé l'outil NVivo 10 afin de condenser et d'analyser l'ensemble des données collectées. Nous avons établi pour ce faire une grille de codage issue de notre cadre théorique et des normes d'audit interne. Cette grille de codage a été testée au moyen d'un double codage à l'issue des premiers entretiens réalisés afin de réduire le risque de circularité. Le double codage a été réalisé avec un autre chercheur qui n'était pas impliqué dans cette recherche.

Pour ce qui concerne le codage des données, nous avons appliqué le codage thématique (Miles et Huberman, 2003) pour identifier les thèmes récurrents, les éléments relatifs au contexte social, les événements (réunions, application de référentiels...) ainsi que les acteurs impliqués dans le phénomène étudié.

La méthodologie retenue a été établie afin de pouvoir répondre à la question de recherche tout en assurant les critères de validité (principe de saturation, triangulation des sources, authenticité des données...).

L'analyse des données

Une fois le codage des données terminé pour l'ensemble des entretiens, le chercheur a établi un premier travail de synthèse pour identifier toutes les catégories issues des données.

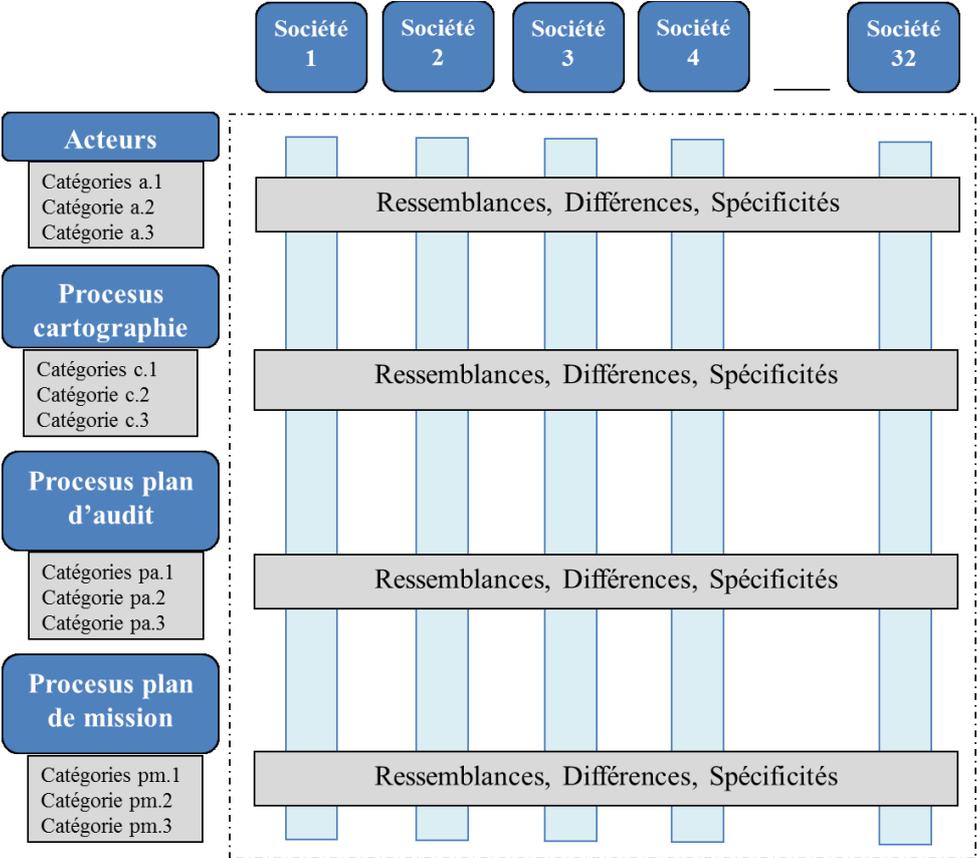
Un premier tableau de synthèse a été établi pour lister l'ensemble de ces catégories qu'il a identifiées à l'issue du processus de codage puis en colonne l'ensemble des entreprises qui ont participé à l'étude.

Un deuxième tableau d'analyse a été établi pour appliquer une approche matricielle qui permet de croiser chacune des catégories présentées en ligne avec les répondants présentés en colonne.

Le chercheur a procédé à une deuxième analyse détaillée qui a consisté à identifier pour chacune des catégories identifiées à l'issue de la première analyse, toutes les ressemblances et les dissemblances entre les différents répondants.

Le schéma qui figure à la page suivante représente la grille d'analyse matricielle qui a été appliquée par le chercheur.

Figure 14. Grille d'analyse des données codées – une approche matricielle



Cette méthode d'analyse des données a permis de faire ressortir toute la diversité des pratiques en fonction des organisations. Le chapitre 4 qui présente les données met en évidence toute la richesse du matériau qui a pu être traité en procédant ainsi.

3 - 3 LES CONSIDERATIONS ETHIQUES

Compte tenu de la nature des données collectées dans le cadre de cette recherche, nous avons décidé d'appliquer une procédure spécifique de traitement des données.

Cette procédure a été établie pour assurer l'anonymat de l'ensemble des répondants ainsi que la protection de leurs données jugées hautement sensibles et préjudiciables par ces derniers.

En pratique, cela a consisté à remplacer les informations d'origine qui pouvaient permettre d'identifier les sociétés concernées dans l'ensemble des transcriptions d'entretien. Chacune des sociétés s'est vue ainsi affecter un nom fictif. Les directeurs de l'audit ont été nommés avec un indicatif de type « DIRAUD 1 » qui signifie directeur de l'audit de la société 1 (RESTAULIB).

Tous les éléments spécifiques à un secteur d'activité potentiellement sensibles ont été par ailleurs retraités dans le contenu des retranscriptions d'entretiens afin de ne pas permettre de recoupement avec les sociétés qui ont accepté de participer. À titre d'exemple, le mot sûreté qui est spécifique à certaines activités aura été remplacé par le terme sécurité.

Enfin, l'ensemble des documents obtenus sous format papier ou électronique (hors documentation publique) ont aussi été retraités pour cacher le nom de la société concernée avant d'être scannés et importés dans le logiciel utilisé pour réaliser l'analyse des données (l'outil NVivo 10).

Seul le chercheur possédera in fine l'ensemble des documents originaux ainsi que les informations relatives aux répondants qu'il a pris soin de conserver en lieu sûr (sous coffre pour les documents papiers et sous format crypté pour les documents électroniques).

Conclusion :

Le statut professionnel du chercheur a joué un rôle clé dans le cadre de ce travail de recherche pour parvenir à collecter données extrêmement riches. Le chercheur a pu bénéficier d'une connaissance importante de la dynamique du milieu de l'audit et de ses codes de communication spécifiques pour les mettre à profit dans le cadre de cette recherche.

Le procédé empirique mis en œuvre pour établir la liste des répondants a mobilisé plusieurs ressources pour obtenir l'accord des directeurs de l'audit qui ont accepté de participer à ce travail de recherche. Le chercheur a notamment mobilisé avec une démarche originale les réseaux sociaux (principalement le réseau « *Linkedin* ») pour entrer en contact avec les directeurs de l'audit et réussir à les rencontrer. La stratégie retenue s'est avérée fructueuse puisque trente-deux directeurs de l'audit qui exercent au sein de grandes entreprises Françaises (principalement des sociétés cotées du CAC 40 et du SBF 120) ont accepté de participer à cette recherche.

La méthodologie de collecte des données repose sur les entretiens. L'originalité de la méthodologie repose sur la combinaison d'entretiens individuels et collectifs avec les répondants. Les entretiens réalisés représentent quarante-sept heures d'entretiens individuels et quatre heures d'entretiens collectifs. Les entretiens ont tous été enregistrés puis retranscrits de façon intégrale. La retranscription des entretiens représente près de 1 100 pages et constitue un corpus extrêmement riche.

Le chercheur réussi à collecter des données difficiles d'accès compte tenu de la sensibilité des informations. Il s'est engagé auprès de tous les répondants à respecter l'accord de confidentialité qui a été établi pour assurer un strict anonymat des sources.

La grille de codage a été établie en croisant les concepts du cadre d'analyse retenu avec les normes professionnelles de l'audit. La grille de codage initiale a été ensuite ajustée sur la base des premiers entretiens et fait l'objet d'un double codage.

La conduite d'une double analyse des données qui a consisté à identifier dans un premier temps les différentes catégories issues des entretiens puis dans un second temps à les recouper avec chacun des répondants a permis de mettre en évidence la grande diversité des pratiques en fonction des organisations et d'exploiter la richesse des données collectées.

Nous allons aborder dans la partie suivante la présentation des données.

4^{EME} CHAPITRE : PRESENTATION DES DONNEES

Préambule : chaque partie de ce chapitre comporte à la fois des données détaillées sous forme de verbatim issues des entretiens réalisés ainsi qu'une synthèse générale à la fin des différentes sections. L'objectif est de fournir au lecteur un accès aux données particulièrement riches qui ont pu être collectées dans le cadre de cette recherche tout en lui permettant de disposer d'une vision plus synthétique.

La présentation des données est organisée en trois parties de façon à suivre toutes les étapes du processus d'audit tel qu'elles sont décrites dans les normes professionnelles de l'audit interne. Il est donc important de rappeler quelques éléments clés sur ces normes d'audit.

Comme nous l'avons déjà vu dans le premier chapitre de ce travail de recherche, les normes d'audit interne sont centrées sur le concept de risque qui constitue le cœur du métier de l'audit interne.

La première étape consiste pour une direction de l'audit interne à identifier les risques au sein de son organisation. C'est à partir de ces risques qu'il devra bâtir son plan d'audit annuel ou pluriannuel.

La seconde étape vise à établir un plan de mission pour chacune des missions inscrites au plan d'audit qui repose sur une analyse préliminaire des risques.

4 - 1 LE PROCESSUS DE CARTOGRAPHIE DES RISQUES

Cette partie présente les données recueillies qui sont relatives au processus d'élaboration de la cartographie des risques. Nous traiterons successivement dans cette partie des éléments suivants :

- le portage du processus de cartographie des risques, c'est-à-dire qui anime le processus au sein de l'organisation ;
- l'identification des risques avec les modalités de collecte et d'observation qui sont mises en œuvre ;
- les méthodes d'évaluation des risques ;
- le processus de consolidation et de synthèse des risques de l'organisation ;
- la validation de la cartographie des risques qui résulte des étapes précédentes ;
- les modalités de mise à jour de la cartographie dans le temps.

4 - 1 1 LE PORTAGE DU PROCESSUS DE CARTOGRAPHIE DES RISQUES

Le portage du processus de cartographie des risques varie en fonction des spécificités organisationnelles des groupes qui ont été interrogés dans le cadre de cette recherche. Ainsi, certains de ces groupes se sont dotés d'une direction des risques dédiée pour animer le processus de cartographie des risques et de façon plus globale le processus de gestion des risques. D'autres groupes ne disposent pas d'une direction des risques en tant que telle.

Le processus de cartographie des risques porté par la direction des risques

Dans le cas des groupes qui disposent d'une direction dédiée à l'animation du processus de cartographie et de gestion des risques, il ressort que pour la plupart de ces directions ont été créés à partir du milieu des années 2000. Il s'agit de directions relativement jeunes qui ont au plus une dizaine d'années.

VEHICAR : « *Alors moi je n'ai pas les risques, il y a un directeur du management des risques, donc c'est lui qui établit la cartographie des risques. En fait il établit deux choses, donc ce qui vous intéresse ce n'est pas chez moi en tout cas, il établit une cartographie des risques et un univers des risques. Donc la cartographie des risques c'est la cartographie des risques groupe majeurs* ».

GAZEO : « *La maîtrise des risques elle a commencé à exister officiellement il y a cinq ans. Donc nous sommes deux directions séparées mais qui reportons tous les deux au contrôle général, lequel contrôle général reporte au Président-Directeur Général du groupe. Donc le fait que nous soyons dans la même direction favorise les interactions* ».

Néanmoins, pour certains groupes, le processus de cartographie des risques existait préalablement à la création de cette direction des risques. Il était notamment porté par la direction de l'audit interne (WALLDISTRIB) ou de la stratégie (AERO) qui ont été, avec la création de la direction des risques, dessaisies de cette mission.

WALLDISTRIB : « *À un moment donné, ici il n'y avait pas, il n'y avait pas de risk manager ici, il n'y avait rien. Et puis suite à différents problèmes, on a nous auditeurs mis en évidence des choses. On a dit c'est quand même scandaleux qu'il n'y ait pas ça. On m'a dit tient, à l'audit tu n'as qu'à faire ça. Donc j'ai mis en place un recensement, toute une méthodologie. Et puis tout ça nous a amené à avoir une cartographie des*

risques [...] La cartographie a été rebattue et il y a une direction qui a été créée et qui s'occupe un peu de ça et qui a changé fondamentalement l'approche ».

Le processus d'identification des risques porté par la direction de l'audit interne

Dans le cas des groupes qui ne disposent d'une direction des risques dédiée, l'animation du processus de cartographie des risques est assurée par l'audit interne (ELECTROSTORE, MULTIMEDSTORE, BATIMODERN, MICROPIX, EQUIPAUTO).

EQUIPAUTO : *« Donc en fait, ce qui est important de dire alors, moi quand je suis arrivée donc ça va faire 5 ans et demi. Donc on m'a nommé directrice de l'audit interne et on m'a dit "tu as également en charge la cartographie des risques ».*

MIRCROPIX : *« Moi, la difficulté que j'ai rencontrée quand je suis arrivé chez nous à la fin de l'année 2010, c'est qu'il n'y avait pas de dispositif ERM. Donc en fait, la première année, j'ai bâti un plan et j'ai fait du coup moi-même mon propre risk assessment, j'ai été moi-même interviewé vingt top executive et j'ai fait moi-même ma cartographie. Et comme j'étais nouveau dans la société, c'est vrai que c'était assez challenging ».*

L'audit interne peut pour ce faire soit prendre en charge l'activité de cartographie sans disposer de ressources dédiées, soit de doter d'une équipe dédiée (FROMAGO) qui n'intervient pas sur les autres missions de la direction.

FROMAGO : *« Ici dans ma direction, j'ai cinq personnels d'audit et j'ai deux personnes au Risk management. Donc, c'est un audit qui a dû être pensé les fonts baptismaux dans les années 2005-2007, bon peut-être encore avant, mais comme moi j'ai repris des armoires à moitié vides et qu'ils se sont étoffés au fur et à mesure. Et puis, de l'autre côté, il y a eu une Risk manager qui est arrivée, une vraie pro, dans les années fin 2012 ».*

Le processus de cartographie peut aussi être parfois co-animé entre l'audit interne et une autre direction du groupe. Cette co-animation prend différentes formes selon les organisations. Il peut par exemple s'agir de répartir les rôles selon les étapes du processus avec l'audit qui réalise la

cartographie et le contrôle interne la met à jour (LUXESTORE). Ou encore, cette co-animation peut consister à partager la supervision du processus de cartographie des risques entre l'audit et une autre direction (SANTEFORM).

SANTEFORM : « *Le risque management, c'est-à-dire la démarche ERM du groupe, c'est un département de deux personnes. Il rapporte à un Group Risk Committee et il y a deux chairman, le patron du corporate social responsibility et la patronne de l'audit interne. Et ils rendent compte régulièrement aussi au comité d'audit, et bien sûr à l'Executive committee* ».

Dans un cas (VESTIMOD), la cartographie des risques a été réalisée par la direction de l'audit interne mais n'a pas été maintenue. Elle n'a pas été mise à jour depuis plusieurs années.

Synthèse : selon les organisations, le processus de cartographie peut être soit porté par une direction des risques dédiée, soit par l'audit interne lui-même avec ou sans ressources spécifiques. Le processus de cartographie peut aussi être coanimé entre l'audit et une autre direction.

Tableau 20. Portage du processus de cartographie des risques

Direction des risques		Direction de l'audit		
Direction dédiée indépendante de l'audit	Direction dédiée coanimée par l'audit interne et une autre Direction	Par la Direction de l'audit (En l'absence de Direction des risques)		Direction des risques intégrée à la Direction de l'audit interne
		<i>Processus porté par les auditeurs internes au même titre que les autres missions</i>	<i>Processus porté par les auditeurs internes coanimé avec une autre Direction</i>	<i>Processus porté par des risk manager mais qui n'interviennent pas sur les missions d'audit.</i>

4 - 1 2 L'IDENTIFICATION DES RISQUES

Des modes d'observation doivent être définis pour être en mesure d'identifier les risques au sein de son organisation. Nous verrons dans cette section comment le résultat du processus d'identification des risques peut être influencé par ces modes d'observation.

4 - 1 2 1 LE POINT D'OBSERVATION DES RISQUES (DIMENSION SPATIALE)

La première caractéristique qui distingue les différents types d'approche concerne le point d'observation. Selon la méthode retenue, les niveaux organisationnels interrogés lors du processus d'identification des risques et ainsi que les procédés associés seront différents. Nous avons pu identifier trois formes d'approche : le « top down », le « bottom up » et l'approche « mixte ».

Le processus d'identification prend la forme d'une approche dite « Top Down ».

L'approche dite « Top Down » se caractérise par une méthode d'identification des risques descendante qui consiste à interroger les managers en partant du haut de l'organisation pour aller progressivement vers le bas. Ce procédé amène à obtenir une liste de risques dont la nature est différente de ceux obtenus avec une approche ascendante (Bottom Up).

VOLTAGE : « Alors on interviewe autour de soixante-dix personnes. Là-dedans, on a soixante-dix personnes, 70% qui sont au niveau du Comex ou à un cran sous le Comex. Tout le Comex systématiquement et pris individuellement. Et une partie assez significative de gens qui rapportent au Comex, donc notamment des patrons géographiques, de nos gros business. J'ai une vision tri dimensionnelle parce qu'on interviewe toutes les grosses géographies, donc les opérations. On interviewe tous les responsables de BU et en dessus de BU, un certain nombre de responsables de ligne de business ».

- **VOYAGO :** « Alors nous on est clairement pour l'instant Top Down. Donc les cartographies qu'on a faites, on les a faites surtout au niveau direction d'entité, direction de branches donc patron de branche, N-1 peut-être N-2 ».

La mise en œuvre du processus Top Down ou descendant peut varier en fonction des niveaux organisationnels qui sont couverts.

Le Top Down du « siège » (AERO)

L'approche siège consiste à interroger essentiellement des directeurs et des responsables au niveau du siège d'un groupe. C'est-à-dire la direction générale et les membres de son comité de direction puis quelques managers qui leur rapportent. Les entretiens se déroulent ainsi sur un périmètre relativement plus restreint par rapport à une approche ascendante et qui ne descend pas au niveau des opérations et des pays.

- **AERO** : le processus de cartographie des risques mis en œuvre consiste à s'entretenir avec une trentaine de directeurs opérationnels et fonctionnels du siège. Avec une approche Top Down, donc « à grosse maille » selon la directrice de l'audit qui précise l'approche Bottom Up aurait été difficile à mettre en œuvre compte tenu du nombre d'activités trop important au sein du groupe.

Le Top Down « siège » élargi aux pays (RACECAR, VINO)

A la différence d'une approche qui vise à interroger principalement les directeurs au niveau d'un siège, la méthode vise à prendre connaissance des risques spécifiques au niveau des pays.

- **RACECAR** : l'audit réalise une centaine d'entretiens avec le Comex, les cadres dirigeants, c'est-à-dire N-1 de Comex, les N-2 de Comex ainsi que les directions de région qui sont au nombre de six. Et puis quelques personnes qui ne sont pas forcément dans une situation direction mais qui ont l'expérience.
- **VINO** : 40 entretiens ont été réalisés avec les membres du Comex et les directeurs des grands départements du siège. Ces entretiens ont été complétés avec les directeurs des grandes filiales notamment aux Etats-Unis et en Chine. Au niveau des filiales, le contact privilégié étant le directeur financier.

Le Top Down « siège » élargi aux métiers/opérations (PETROLIUM)

À la différence d'une approche qui vise à interroger principalement les directeurs au niveau d'un siège et des membres du comité de direction de la direction générale et leur N-1, la méthode vise à prendre connaissance des risques spécifiques au niveau des directions « métier » (branche ou pôle d'activité, business unit, ...).

- **PETROLIUM** : soixante entretiens ont été réalisés avec les membres du COMEX, les différents directeurs corporate puis les membres des comités de direction des branches (exploitation production, raffinage chimie et marketing et service).

Le Top Down « siège » élargi aux métiers et aux régions (VOLTAGE)

- **VOLTAGE** : soixante-dix entretiens, dont 70% sont des personnes au niveau du Comex ou des N-1 des membres du Comex, ont été réalisés. Ils ont consisté à voir tous les membres du Comex, les directeurs régionaux et de BU. Et sous les BU, quelques responsables de lignes business. Et enfin toutes les fonctions globales et à l'intérieur quelques responsables de domaine fonctionnel.

La démarche Top Down a été parfois abandonnée chez certains groupes au profit d'une autre approche considérant qu'elle n'était pas adaptée.

Plusieurs groupes déclarent que la nature des risques identifiés dans le cadre de cette approche reste très macros ou bien que la culture du management ne s'y prête pas toujours.

Tableau 21. Cartographie des risques – les approches de type « top down »

Approche Top Down		
Siège	Siège élargi aux métiers / opérations	Siège élargi aux pays

Le processus d'identification prend la forme d'une approche dite « bottom up ».

L'approche « bottom up » ou ascendante comme son nom l'indique consiste à procéder de bas en haut pour recenser les risques au niveau de l'organisation. Il s'agit d'une approche qui vise à interroger en priorité les managers au niveau des entités opérationnelles puis de remonter progressivement vers le haut. La démarche ascendante peut être initiée à un niveau organisationnel plus ou moins bas et prendre fin à un niveau plus ou moins élevé de l'organisation. Les entretiens montrent que le nombre de risques collectés par ce procédé nécessite un important travail de traitement et de synthèse. Selon les groupes interrogés, il apparaît que la démarche « bottom up » ne prévoit pas d'interroger la direction générale qui est sollicitée lors de la validation de la cartographie des risques.

DISTRIMART : « *C'est une approche « bottom up » mais à partir d'un certain niveau parce que nous sommes un groupe quand on parle déjà de N-1, on parle je ne sais pas,*

on devait avoir plus de 600 interviews. Parce qu'on parle d'une trentaine de personnes en moyenne par BU. [...] Bon, on ne l'a pas fait dans toutes les BU etc. mais on parle entre 600 et 900 interviews. Donc, l'idéal c'était plus de mille mais à un certain moment, il faut s'arrêter sinon on se retrouve à 3 000 ou 4 000 ».

NATURELIA : *« Donc la direction des risques elle fait quoi ? Elle produit donc une cartographie des risques, enfin ça, ce n'est pas une grande nouveauté mais maintenant elle le construit de façon, enfin les règles se sont éclaircies. Parce que la première carto des risques 2006-2007 c'est un truc qui était conçu dans l'esprit des gens du siège et qui était censé représenter la réalité. Aujourd'hui on a quand même quelque chose qui part des entités et qui remonte par l'agrégation et qui est complété à chaque niveau ».*

L'approche « bottom up » ou ascendante repose sur des modalités de mise en œuvre qui différent selon les organisations.

Le « Bottom Up » orienté pays

Un pays regroupe souvent plusieurs entités, plusieurs métiers et activités. L'approche pays consiste non pas à interroger directement les managers en charge de ces activités mais les directeurs de pays. Le niveau managérial pays rendant souvent lui-même compte à une direction régionale ou bien de zone géographique. Il s'agit donc d'une approche transverse aux activités et aux métiers qui sont vus sous un angle pays/géographique. Cette approche privilégie, sans exclure les objets de risques relatifs aux métiers, une vision plutôt pays.

- **DISTRIMART** : chaque pays établit sa cartographie des risques. Cela consiste à réaliser des entretiens avec l'ensemble des membres du comité de direction pays, soit en moyenne dix entretiens par pays avec vingt pays, ce qui représente six cents entretiens. Chaque pays doit retenir et remonter à l'audit un nombre limité à 10 risques. Le management du siège n'est pas interrogé dans le cadre de cet exercice orienté pays.
- **SPORTFLEX** : les manager d'audit interne alimente la cartographie des risques du groupe sur la base des échanges qu'ils ont tout au long de l'année avec les directeurs pays et les directeurs de production (environ deux cents entretiens). L'objectif est de recenser les risques tels qu'ils sont perçus au niveau local. Cela permet d'alimenter une liste de risques standards par pays, par zone et par processus. Encore dans ce processus, les managers du siège ne sont pas interrogés.

Le « bottom up » orienté métier

Un métier peut opérer dans plusieurs pays ou zones géographiques. L'approche métier consiste à interroger en priorité les managers en charge des différents métiers (production, distribution, services, ...) ou pôle d'activités au sein de l'organisation.

- **LUXESTORE** : l'audit réalise des cartographies des risques pour chacun de ses métiers (cuir, prêt à porter, bijoux, ...) et aussi par filiale de distribution. Ces cartographies sont réalisées tout au cours de l'année au même titre que les autres missions d'audit interne. Cela consiste à interroger soit les directeurs de métier, soit les directeurs de filiale de distribution avec les membres de leur comité de direction. Chaque cartographie métier ou de filiale vient alors enrichir tout au long de l'année la cartographie des risques groupe. Il est à noter que la direction du siège n'est pas interrogée de manière à alimenter la cartographie établie par l'audit mais à régir dessus.

Le « bottom up » orienté pays / métier

Un pays peut regrouper plusieurs entités qui opèrent dans différents domaines d'activité. L'approche mixte orientée pays/métier consiste à interroger aussi bien les managers au niveau des zones géographies (responsables pays, régions, zones) que les managers métiers afin de recouper leur vision sans privilégier une vision plutôt qu'une autre.

- **MEDIACORP** : l'audit interne rencontre en moyenne quarante personnes pour chacune des deux activités qui sont « Musique » et « Médias » et termine le processus avec le Président-Directeur Général. Les entretiens sont réalisés avec les directeurs métiers (artistes et répertoires, digital, ...) et les directeurs fonctionnels, ainsi que les directeurs pays et les directeurs financiers pour les cinq pays majeurs du groupe. Dans la démarche il est important de noter que les entretiens sont réalisés en partant d'une synthèse des risques identifiés l'année précédente.
- **NATURELIA** : le pays est la maille de gestion sachant que les entités d'un pays peuvent opérer dans des activités différentes (énergie, propreté et eau). Chaque pays est supervisé par une zone géographique qui regroupe plusieurs pays. La cartographie des risques n'est pas établie par métier mais par pays. La zone à laquelle est rattaché un pays n'établit pas de cartographie et n'intervient pas non plus dans le processus de remontée des risques pays qui sont directement transmis à la direction des risques

groupe. La direction des risques groupe complète les cartographies pays avec des entretiens au niveau des directions métiers et fonctionnelles du siège afin d'établir la cartographie du groupe.

- **FROMAGO** : le processus consiste à recenser les risques en partant du bas de l'organisation, c'est-à-dire des patrons de pays, puis des patrons de zones avec éventuellement les fonctions supports de la zone. Ces entretiens sont ensuite complétés par les membres du comité de direction de la direction générale et leur N-1.

Tableau 22. Cartographie des risques – les approches de type « bottom up »

Approche Bottom Up		
Approche métier	Approche pays	Approche mixte

Le processus d'identification prend la forme d'une approche dite « Mixte ».

Ce processus d'identification des risques combine l'approche ascendante dite « bottom up » et descendante dite « top down ». Elle consiste ainsi à transmettre les risques du top management aux entités qui lui remontent leurs propres risques afin d'enrichir réciproquement les deux démarches.

CIMENTO : *« C'est un travail d'interview avec un peu toute la population, à peu près la même population que celle qu'on interview pour faire le plan d'audit annuel. Donc c'est COMEX du groupe, ce sont les têtes des fonctions Corporate, et c'est une sélection des patrons des plus grands pays. Ce qui fait une cinquantaine ou une soixantaine de personnes et avec une itération. Alors l'idée étant d'avoir des personnes qui à la fois ont une vision un peu « Top-down » et « Bottom-Up » et de confronter le regard d'un 'SVP' opération avec celui d'un patron de pays, de confronter la vision du contrôle interne qui se bat parfois avec des niveaux de maturités hétérogènes et puis celle du directeur financier. Et ce qui fait que là on sort avec un premier jeu de matrice ».*

MULTIMEDSTORE : « Et depuis deux ans, on fait une approche « Top-Down » / « Down-Down ». C'est-à-dire qu'on fait redescendre vers les filiales, les grandes directions, les risques identifiés dans la carto des risques stratégiques ».

Vision de l'audit confrontée à la celle des entités (RESTAULIB)

L'audit confronte sa vision des risques qui est établie au travers d'un référentiel de risques. Ce référentiel comporte un inventaire des processus de l'entreprise (achat, vente, ...) et des risques théoriques associés à chacun de ces risques. Ce référentiel a été construit par l'audit puis souvent validé avec les responsables des processus concernés et des experts au sein du groupe. Cette vision des risques de l'audit est ensuite confrontée aux risques qui lui remontent lors des entretiens avec les entités.

- **RESTAULIB** : l'audit réalise des entretiens avec une centaine de managers qui sont les directeurs pays et les directeurs financiers pays puis les directeurs de zone géographique. Le registre des risques établi par l'audit est enrichi sur la base de ces entretiens qui sont menés sans imposer de cadre aux personnes interrogés.

Vision du Top management confrontée à celle des entités

Dans cette approche, l'audit peut avoir, selon les organisations, recourt à des référentiels de risques pour cadrer la démarche.

Approche cadrée par un référentiel de risque

- **ELECTROSTORE** : l'audit mène des entretiens (dix-douze personnes) avec l'ensemble des directeurs du Comex et les directeurs généraux des deux Filiales étrangères. Puis il soumet aux entités le référentiel de contrôle interne (RCI Framework) qu'il a établi avec les experts du groupe. Ce référentiel permet aux entités opérationnelles d'évaluer leurs risques au regard des règles applicables validées par le Top Management.
- **BATI-F** : Le processus vise à faire remonter au comité de revue des engagements les risques liés aux offres commerciales et aux projets. Cette grille d'évaluation standard (axes financiers, opérationnels, techniques, ...) est transmise par les directeurs des différentes branches métier aux membres du comité qui se réunit régulièrement. Le directeur de l'audit recoupe ces risques avec ceux identifiés à l'issue d'une série d'entretiens au niveau du top management au siège.

Approche non cadrée par un référentiel de risque

Cette approche mise en œuvre par plusieurs groupes (ELEC, MICROPIX, BATICOSTO, LUXESTORE, MULTIMEDSTORE, CIMENTO) consiste à combiner une approche ascendante et descendante telle que décrite dans les sections précédentes. Néanmoins, nous avons pu identifier quelques spécificités dans les modalités de mise en œuvre.

- **LUXESTORE, MICROPIX, BATICOSTO, ELEC, CIMENTO** : la démarche consiste à interroger les entités (bottom up) sans leur donner la vision des risques du groupe (top down). Les risques identifiés par les entités peuvent venir enrichir la synthèse du groupe.
- **MULTIMEDSTORE** : la démarche consiste à interroger les entités (bottom up) sur leurs risques en leur communiquant la vision des risques du groupe (top down) qui résulte des risques identifiés dans le cadre du plan d’actions stratégique. Le but étant que les entités puissent illustrer les risques groupe en lien avec leur activité puis remonter des risques spécifiques qui n’étaient pas identifiés au niveau du groupe.

Tableau 23. Cartographie des risques – les approches de type « mixte »

Approche « Mixte » (Top-Down et Bottom-Up)		
Vision de l’audit (top) confrontée avec celle des entités (bottom)	Vision du management (top) confrontée avec celle des entités (bottom)	
	Approche cadrée par un référentiel de risque	Approche non cadrée par un référentiel de risque

4 - 1 2 2 LE MODE D'OBSERVATION DES RISQUES (DIMENSION SPATIALE / TEMPORELLE)

Suivant les modalités de sa mise en œuvre, le processus d'identification des risques peut amener à exclure certains types d'événements en fonction de leur nature (internes ou externes à l'organisation) et en fonction de l'échelle de temps considéré.

Dimension spatiale :

Selon les groupes interrogés, la nature et l'origine des événements sont des critères qui peuvent influencer sur le processus d'identification et de sélection des risques.

Le processus d'identification des risques vise à recenser exclusivement des événements internes à l'organisation.

Certaines organisations (VINO) excluent dans le cadre du processus de cartographie des risques les événements externes en considérant qu'ils sont le plus souvent subis et difficiles à maîtriser.

VINO : « *Vous allez rester six mois parce que vous allez déjà passer quatre mois à leur expliquer que ce que c'est un risque. Le tremblement de terre qui peut raser la ville de Tokyo, il est le numéro un mais personne ne va vous le citer, et c'est quelque chose d'innée. C'est accepté mais dans le sens c'est fataliste, ça va arriver, il n'y a rien à faire* ».

Le processus d'identification des risques mise en œuvre retient les événements qui sont externes à l'organisation mais qui constituent des facteurs de risque.

Certaines organisations (MEDIACORP) considèrent que les dysfonctionnements dont l'origine est interne à l'organisation relèvent de problèmes opérationnels courants qui ne sont pas repris dans la cartographie. Leur cartographie vise à recenser plutôt des événements externes qui sont susceptibles d'avoir un impact significatif sur leur organisation.

MEDIACORP : « *Non, mais les risques internes, on considère que c'est de l'opération [...] Ce sont les risques exogènes qui sont les plus forts parce que ce sont ceux-là qui sont les moins maîtrisés, qui ont un impact sur le business* ».

Le processus d'identification des risques prend en compte aussi bien les facteurs externes qu'internes à l'organisation dès lors qu'ils sont sources de dysfonctionnement.

Parmi les groupes interrogés, la plupart intègrent tout type d'événement dès lors que ceux-ci peuvent avoir un impact sur les activités de l'organisation et être source de dysfonctionnement.

Ainsi, il est possible de voir dans certaines cartographies des risques liés au changement climatique, aux catastrophes naturelles, aux menaces externes qui peuvent peser sur la sécurité des personnes, etc.

VEHICAR : « *C'est-à-dire que même pour le séisme, il y a quelqu'un qui traite. Parce que si séisme au Chili, donc globalement il y a une liste de traitements à savoir, dans ce cas-là est-ce qu'on fait la production en Roumanie, je ne sais pas où* ».

Parmi tous ces groupes, l'un d'entre eux fait formellement une distinction dans sa matrice des risques afin d'identifier l'origine des événements.

CIMENTO : « *Donc si on prend les risques qu'on a, ils se croisent sur un double axe. Un, c'est le risque exogène du type bouleversement politique, pandémie, changement climatique, enfin vous voyez. Ce genre de changement alors dont on peut se dire que c'est extrêmement macro. Avant qu'Ebola n'impacte le business on sait que ça peut prendre du temps. La géopolitique, bon on est en Syrie, on est en Irak, on est en Égypte, bon on l'a un petit peu senti mais voilà ça, c'est un premier axe. L'autre, c'est beaucoup plus les risques qu'on a, ce sont les conséquences de non-efficience de nos processus* ». *Donc un même sujet peut être éclaté en fonction de sous éléments dans les différentes liasses. Dans un sujet, si on prend un sujet qui est moitié interne/moitié externe, la sûreté des employés actifs c'est un mélange des deux. Quand Boko Haram fait intrusion dans notre usine du Nigeria, il y a une part d'externe. En revanche la façon dont on a déployé les politiques de sûreté avec des systèmes d'alerte, de coopération avec les autorités fait qu'on peut être dans des pays dangereux tout en ayant un sentiment de sûreté* ».

Tableau 24. Cartographie des risques – origine des événements « risqués »

Identification des risques	
	Événements internes
Sources de risque	Événements externes
	Événements internes et externes

Dimension temporelle :

Au vu des entretiens, les groupes interrogés se distinguent par en fonction de l’horizon de temps avec lequel ils se projettent pour envisager les événements futurs et les risques.

Nous avons pu identifier trois groupes d’acteurs parmi les répondants qui ont participé à ce travail de recherche.

Les groupes qui envisagent les risques plutôt à court terme

Les groupes (CIMENTO) qui envisagent les risques plutôt à court terme excluent les risques susceptibles de les impacter à plus long terme.

CIMENTO : *« Et puis essayer de les mettre un peu en prospective, qu’est ce qui peut se passer mal, qu’est ce qui peut les surprendre, qu’est ce qui peut faire qu’ils ne font pas ce qu’ils pensaient faire l’an prochain ».*

Les groupes qui envisagent les risques à moyen terme

La plupart des groupes interrogés déclarent qu’ils envisagent les risques avec un horizon de temps qui va de deux à cinq ans. Le choix de cet horizon (RACECAR, BATICOSTO, DISTRIMART, CHIMICA, RESTOLIB, MULTIMEDSTORE, SPORTFLEX, MEDIACORP, MICROPIX) est fait afin de s’aligner avec les objectifs de leur plan moyen terme ou bien d’actions stratégiques. De surcroît, les risques au-delà cet horizon de temps ne sont pas envisagés. Selon plusieurs directeurs de l’audit, il est difficile de se projeter au-delà de cinq ans.

BATICOSTO : *« Donc l’échelle de temps, si on voit une échelle de temps lointaine en général ça rend les choses floues. Si on se met à dix ans. C’est pour cela que nous, on a eu un parti pris, on a mis à trois ans. Parce que ça c’est concret. C’est mesurable. À dix ans le monde sera différent. Prédire quels seront mes risques dans dix ans, on partirait sur des élucubrations qui n’intéressent personnes ».*

Les groupes qui envisagent les risques à beaucoup plus long terme

Les entretiens réalisés ont permis d’identifier deux groupes (AERO et PETROLIUM) qui adressent les risques avec un horizon de temps au-delà de l’exercice du plan d’actions stratégiques.

- **AERO** : la cartographie identifie fait apparaître clairement une échelle de temps afin de positionner les risques. Cette échelle va d'une période inférieure à 1 an jusqu'à 10 ans et supérieure à 10 ans. Il s'agit d'un cadre formalisé au regard de la dimension temps.
- **PETROLIUM** : l'horizon considéré est variable selon les activités. Il peut aller en de 2-3 ans jusqu'à 10 ans compte tenu de la culture et de l'activité du groupe qui engage à long terme.

Par ailleurs, il apparaît que les groupes recourent à différentes échelles de temps pour envisager les risques à venir. Il est important de souligner qu'aucun de ces modes d'observation n'est utilisé de façon exclusive au sein des groupes qui ont été interrogés mais qu'ils sont souvent complémentaires.

Les acteurs envisagent les risques en partie à partir d'événements connus qui sont issus soit du passé, soit du présent.

La prise en compte du passé

Les risques peuvent être envisagés (*CIMENTO, MULTIMEDSTORE*) en partie, mais non exclusivement, à partir des événements passés pour pouvoir envisager les événements futurs.

CIMENTO : « *C'est des questions ouvertes sur leur appréciation des risques, sur qu'est-ce qui a changé. Les plus grandes surprises qu'ils ont pu avoir, enfin c'est les faire réagir, c'est les faire s'ouvrir, les faire parler de ce qui a pu les surprendre sur le passé* ».

La prise en compte du présent

Les risques peuvent être envisagés (*SANTEFORM, NATURELIA, DISTRIMART, PETROLIUM*) en partie mais non exclusivement en fonction des préoccupations ou bien de l'actualité du moment.

SANTEFORM : « *Ça dépend aussi de la culture de la gestion des risques. Je prends un patron de site par exemple, à chaque comité de direction ils ont un sujet risque qui est à l'ordre du jour. Parce qu'ils vont être HSE, parce qu'ils vont suivre leurs accidents, parce qu'ils vont suivre leurs ruptures, parce qu'ils vont suivre un certain nombre de choses et donc il traite quelque part des sujets sont très opérationnels* ».

NATURELIA : « *Honnêtement la préoccupation, elle est quand même de court terme dans une boîte qui est vraiment en restructuration, voilà c'est contextuel* ».

Les acteurs se projettent dans le futur à plus ou moins long terme pour envisager les risques comme des événements qui ne sont pas encore survenus.

Les risques peuvent être envisagés (PETROLIUM, RACECAR, BATICOSTO, DISTRIMART, CHIMICA, RESTOLIB, MULTIMEDSTORE, SPORTFLEX, MEDIACORP, MICROPIX) à partir de scénarios d'événements futurs qui sont de nature à constituer des risques pour l'organisation.

PETROLIUM : « *Quand on interpelle sur les grands risques et de la manière la plus ouverte possible dans un entretien le moins directif possible, on arrive à des choses qui sont parfois étonnantes. Je me souviens du patron de la chimie de l'époque qui me dit "bah moi je vois un risque que peut-être un jour les plastiques soient interdits, sont plus acceptables". Bon effectivement on ne dit pas ça quand on pense à ses risques opérationnels à un moment donné. Il faut avoir le temps de se projeter, de parler de vision* ».

GAZEO : « *On s'est dit, on s'est posé la même question finalement est-ce qu'on ne va pas passer à côté de quelque chose, un peu le Black Swan, qui va nous arriver, et qu'on n'aurait pas vraiment imaginé parce que précisément on est sur du long terme. Donc depuis cette année on réfléchit à des scénarios combinatoires qui pourraient bah nous aider à penser différemment* ».

Tableau 25. Cartographie des risques – dimension temporelle

Identification des risques	
Echelle de temps	Evénements connus
	Passé
	Présent
	Futur
Evénements envisagés	Envisagé à court terme, moyen terme ou long terme

Synthèse : Le processus d'identification des risques est fonction du point d'observation et du mode d'observation.

- Le point d'observation varie selon qu'il s'agit d'une approche « top down », « bottom up » ou bien « mixte ».
- Le mode d'observation porte tout d'abord sur la nature des événements pris en compte, à savoir s'ils sont internes ou bien externes à l'organisation. Cette dimension est complétée par l'échelle de temps considérée par les acteurs pour identifier les événements réputés risqués pour leur organisation.
- Les codes de communication utilisés par les différents acteurs mobilisés.

Tableau 26. Cartographie des risques – synthèse des modes d'observation par type d'approche

Identification des risques					
Dimension spatiale (point d'observation)	Type d'approche	Top-Down	Dimension temporelle	Passé	
		Bottom-Up		Présent	
		Mixte		Futur	
	Sources	Evénements internes			
		Evénements externes			
		Tout type			

4 - 1 2 3 LES MODALITES PRATIQUES DE RECENSEMENT

Les modalités de collecte des données mises en œuvre pour identifier et les recenser les risques sont de différentes natures. L'un des principaux moyens reste la conduite d'entretiens qui est ensuite plus ou moins complétée par d'autres sources.

Les entretiens individuels réalisés aux différents niveaux de l'organisation pour recenser les risques

Nous avons développé dans la section précédente (*4-1 2 1 points d'observation*) les différents types d'approche qui pouvaient être mis en œuvre dans le cadre des entretiens d'élaboration de la cartographie des risques.

Les guides d'entretien utilisés dans le cadre des entretiens traduisent des différences d'approches selon les organisations.

Nous avons pu identifier que les personnes en charge de mener les entretiens pouvaient parfois recourir à des guides d'entretiens. Nous avons pu constater que les questions posées ou bien l'orientation même de ces guides pouvaient être variables selon les groupes.

BATIMODERN : « *Donc on s'est senti un peu obligé de faire une étude en juillet dernier, ça a duré trois mois en fait c'était de septembre à novembre, une étude top down où donc là c'était sur la base d'entretiens de tout le top management du groupe. Ça faisait quand même une soixantaine de personnes donc c'était quand même assez large [...] Et on a demandé à chacun quelle était son évaluation de ses risques selon un guide d'entretien qu'on a refait nous-même, on a inventé notre mission au lieu de la confier à des consultants* ».

Ces guides d'entretiens témoignent d'une certaine hétérogénéité en termes de contenu et donc sur la nature du questionnement qui vise à identifier les risques.

- **VINO, MEDIACORP et VOLTAGE** : le guide d'entretien vise à identifier les risques à partir de l'historique existant. Le point de départ de l'échange est la liste des risques identifiés lors de l'exercice précédent.
- **ELECTROSTORE** : l'entretien a pour but d'identifier dans un premier temps les changements intervenus au cours de la période ou ceux qui sont envisagés. Puis dans un second temps de s'interroger sur ceux qui pourraient impacter l'activité de façon soit

positive soit négative. Les changements dont il est question lors de ces entretiens portent aussi bien sur des éléments internes à l'organisation qu'externes (changements organisationnels, changements de marché, organisationnels, d'infrastructure).

- **LUXESTORE** : les entretiens sont menés avec un guide d'entretien qui porte directement sur le thème du risque avec deux questions posées à chacune des personnes rencontrées. « *Quels sont les risques au sein de votre métier ?* » puis « *Quels sont les risques des autres métiers ?* ».

Des difficultés liées à l'absence de langage commun au sein de l'organisation

Les entretiens ont mis en évidence une difficulté exprimée quant à l'absence d'un langage commun sur la notion de risque. Parmi les difficultés, figure notamment la différence entre le langage de l'audit et des autres membres de l'organisation.

RESTAULIB : « *Pour faire court, on a quand même encore un gap entre ce qui descend je dirais, qui vient beaucoup de l'audit par le biais du contrôle interne : la vision des risques et ce qui remonte des entités qui chacun a son langage, sa méthode, sa technique. On a des entités qui vont faire des cartos à deux axes, d'autres à trois axes, d'autres ne vont pas faire de cartographie, ils vont faire une identification des dix plus gros sujets à risque. Donc chacun y va de son langage machin* ».

BATIMODERN : « *Ça faisait partie des notions délicates à manipuler parce que quelque part le risque financier en soi est un risque, le risque d'image est en soi et le risque sur la sécurité des personnes est un risque en soi. Donc c'était à la fois l'échelle et la mesure, ça faisait partie des problèmes qu'on a avec la gestion du mot « risque » qui est un problème presque philosophique ou de sémantique en tout cas* ».

Les questionnaires destinés au recensement des risques

Nous avons pu identifier que certains groupes (ENGINICO, CHIMICOR, VINO, LUXESTORE, MULTIMEDSTORE) ont recouru à des questionnaires afin d'évaluer les risques.

CHIMICOR : « *Bon, sur les risques groupe ce qu'on a fait, on a envoyé un questionnaire au top 40, eux, on leur a dit vous nous donnez les risques principaux groupe. Donc on leur demande - il y aura une petite variante au niveau des BU et des fonctions - on leur demande de nous remonter les principaux risques, on ne donne pas*

de nombre, on leur donne une indication, voilà environ cinq pas plus de dix et pas moins de trois quoi, les cinq tops risques selon vous. Il y a un petit fichier qu'on leur demande de renseigner on a un petit outil qui permet ensuite de consolider les réponses, en disant soyez relativement clair, explicitez, donnez les causes, les conséquences, si possible un commencement d'évaluation pour qu'on comprenne bien de quoi il s'agit ».

Ces questionnaires sont sensiblement différents d'une organisation à une autre. Ils peuvent être établis avec des questions de type ouvertes ou bien fermées, porter sur des thèmes spécifiques, etc.

Questions ouvertes

- **ENGINICO** : le questionnaire d'auto-évaluation du contrôle interne structuré par cycle (achat, vente, finance, ...) a été complété avec un volet risque dans lequel il était demandé aux personnes interrogées de citer cinq risques majeurs dans leur domaine de responsabilité et de les évaluer sur une échelle de probabilité et d'impact. Cela a fourni une liste de plus de 500 risques.
- **RACECAR** : un petit questionnaire est envoyé en amont des entretiens en vue de les préparer avec des questions qui portent distinctement sur les risques et les missions d'audit. Pour les risques deux questions sont posées : « *quels sont selon vous les risques majeurs auxquels est exposée votre direction* ». Et « *quels sont selon vous les tops risques auquel est confronté le groupe* ».
- **VINO** : l'audit a établi un questionnaire en deux parties. La première rappelle les risques de la dernière mise à jour de la cartographie (N-2) et pose un certain nombre de questions : le risque est-il toujours d'actualité, oui/non ? Pourquoi ? Quelle est votre évaluation du risque ? etc. La seconde est une partie vierge pour lister les nouveaux risques (limités à vingt) survenus durant la période.
- **CHIMICOR** : il est demandé aux directeurs fonctionnels et aux directeurs de Business unit (une quarantaine de managers) d'établir une synthèse des risques de leur organisation. La demande ne repose pas sur un format spécifique et la synthèse demandée peut être faite sous format libre.

Questions fermées

- **MULTIMEDSTORE** : l'audit transmet un fichier aux directeurs pays et leur N-1 (directeur commercial, directeur marketing, directeur d'exploitation en charge des magasins et directeur logistique). La structure de ce questionnaire est la même que celle du questionnaire d'auto-évaluation du contrôle interne (14 cycles standards). Le fait de recourir à des questions fermées permet selon le directeur de l'audit de remonter des risques alors que la question ouverte ne le permettait pas vraiment.

Le réseau des correspondants contrôle interne peut constituer une source d'information spécifique

LUXESTORE : « La distribution, une filiale, elle peut avoir trois magasins. Si elle fait 100 de CA, mon prédécesseur avant il voulait couvrir 80, mais il n'y avait pas ce réseau de correspondants de contrôle interne. Moi, j'ai des gens, j'ai des petits gars qui arpentent les magasins en vérifiant qu'ils bossent bien selon les critères que j'ai déterminés ».

Le réseau de contrôleurs internes, lorsqu'il existe, peut alimenter le processus d'identification et d'évaluation des risques. Ce réseau est plus ou moins développé selon les organisations et il adresse de différentes manières les risques.

- **SPORTFLEX** : le contrôle interne établit un document intitulé diagnostic de passation à chaque fois qu'un Directeur de magasin change. Il s'agit d'une évaluation sur le volet sécurité des personnes. L'audit interne se procure l'ensemble de ces rapports.
- **CIMENTO** : la société qui était cotée aux Etats-Unis a mis en place un système d'auto-évaluation du contrôle interne non limité aux processus financiers avec 350 points de clés. Le résultat de cette auto-évaluation fournit une matrice de maturité des pays par processus.
- **LUXESTORE** : les correspondants « contrôle interne » qui représentent une cinquantaine de personnes sont mobilisés par la direction de l'audit pour suivre les plans de remédiation des risques de la cartographie. L'avantage est qu'ils sont au plus proche du terrain.

Les comités spécialisés mise en œuvre pour compléter les entretiens

En complément des entretiens, plusieurs groupes (CHIMICA, NATURELIA, AERO, ont créé des instances spécifiques pour échanger sur le thème du risque. Elles prennent la forme de comités spécifiques dont le rôle est notamment de suivre les risques au sein de leur organisation.

BATI-F : « Là-dessus, notre nouveau patron est arrivé, moi je suis arrivé et on était complètement en phase d'un point de vue opérationnel en disant ça sert à rien ce truc-là, on va identifier le risque à partir du cœur de métier. Le cœur des métiers c'est de faire des chantiers, donc on va monter un comité des risques pour chaque grosse affaire. Donc, c'est une revue d'engagement mais qui va traiter de l'ensemble des risques. Voilà et ça, ça couvre 80% des risques du groupe. Et les vingt qui restent, on a fait pour la bonne forme un comité des risques groupe qui se réunit une fois par an et qui liste les vingt gros risques majeurs qui sont au niveau groupe quoi, risque de liquidité, risque d'image, risque machin ».

Ces comités sont de natures différentes en fonction des organisations au regard des champs et des sujets qu'ils adressent.

- **BATI-F**, il s'agit d'un comité qui est orienté exclusivement sur les risques associés à la prise d'affaires qui se réunit soixante fois par an. L'évaluation des risques associée aux futurs projets de construction du groupe est réalisée sur la base d'une grille standard.
- **GAZEO** : un comité des risques a été créé. Il est composé essentiellement des directions fonctionnelles (finance, RH, juridique, communication, contrôle général avec l'audit, les risques, et l'éthique) du groupe. Ce comité organise des ateliers sous forme de « remue-ménages » pour établir des scénarios d'événements risqués.
- **MUTLIMEDSTORE** : un comité contrôle interne a été institué afin d'établir des échanges durant l'année (deux à trois fois par an) avec chacune des grandes entités et les directions fonctionnelles. Le but de ces échanges est de faire remonter les éléments qui peuvent être source de risque (incidents, litiges en cours, ...). Il est complété par un comité de la sécurité informatique qui a établi une cartographie des risques spécifiques à ce domaine.

La cartographie des processus et des activités qui permet de construire l'univers des risques de l'organisation.

Plusieurs directions, en charge d'animer le processus d'identification des risques, ont mis en œuvre un travail spécifique pour établir ce qu'elles nomment leur univers des risques. L'univers des risques correspond à un inventaire des risques théoriques qui découlent directement de la nature même des activités. Par exemple, le vol est un risque inhérent pour l'activité de vente en magasin tout comme l'intoxication d'un client pour un restaurant. L'univers des risques représente les risques liés aux activités.

AERO : *« En fait ce qui fait l'univers des risques c'est les grands domaines d'activité de l'entreprise. C'est là, où potentiellement il peut y avoir des risques, si vous voulez ça couvre, c'est au niveau du groupe, ça y est, je crois l'avoir encore perdu, je vais demander à quelqu'un parce que si je commence à chercher ça va (Elle part chercher un document interne). Donc en fait l'univers des risques, c'est la décomposition de toutes les activités du groupe qui sont toutes évidemment porteuses de risques ». « Elle a bâti cet univers de à peu-près cent dix risques. Alors comment, parce qu'elle-même arrivait de, avait eu tout un parcours dans le passé dans la direction de la stratégie, et avait une très bonne connaissance de l'entreprise et donc elle a procédé par interview, par travail de manière très transversale avec l'ensemble des directions ».*

MICROPIX : *« On a un dispositif d'Enterprise Risk Management, qui a été mis en place maintenant depuis quelques années. Un des outputs de ce dispositif, c'est une cartographie des risques qui est basée sur un univers de risques qui a été défini à l'origine avec un certain nombre de risques génériques qui sont propres à l'activité de la société ».*

Synthèse : les risques recensés peuvent correspondre soit à des risques qui sont induits par les membres de l'organisation sous forme déclarative, soit à des risques qui sont déduits (risques « théoriques ») par la direction en charge de réaliser la cartographie. Les risques déduits résultent d'une cartographie des processus et des entités.

Tableau 27. Modalités de recensement mis en œuvre lors du processus de cartographie des risques

Risques recueillis auprès des membres de l'organisation (induits)	Risques recueillis auprès des membres de l'organisation (induits)
Entretien individuels	Cartographie des processus et des activités considérés comme étant toutes porteuses de risques
Comités des risques	
Questionnaires	
Réseau des correspondants contrôle interne	

4 - 1 3 L'ÉVALUATION DES RISQUES

Les entretiens nous ont permis d'identifier une multitude d'approches en matière d'évaluation des risques sensiblement différentes entre les groupes interrogés.

L'énumération des risques sans y associer une évaluation

Le groupe **PETROLIUM** a réalisé un premier exercice de cartographie en 2011 qui a permis d'énumérer un certain nombre de risques sans y associer une méthodologie d'évaluation. Dans le cadre de la mise à jour de la cartographie lancée en 2014, le groupe était lors des entretiens au stade de la réflexion pour déterminer le mode d'évaluation et de hiérarchisation.

Le groupe **ELECTROSTORE** a établi un référentiel de contrôle interne et de risque sans y associer non plus d'évaluation.

L'évaluation du risque prend en compte uniquement l'impact de l'événement (sans probabilité d'occurrence).

BATIMODERN : « *Le truc qu'on ne voulait surtout pas faire vis-à-vis de ce qui est écrit dans les normes, il y a quand même un endroit où on ne voulait surtout pas aller, c'était de rajouter la notion de probabilité. Ça, on a fait exprès de la supprimer partout où on pouvait ou de ne pas l'introduire. Et ça, on est très résistant, finalement on n'est pas d'accord avec les normes. [...] Parce que le niveau de probabilité on l'a trouvé très dangereux dans le sens où on n'est pas des experts en assurance. Pour nous c'était mettre le doigt dans l'engrenage justement d'une gestion externe. Et donc les probabilités, voilà on n'a pas voulu rentrer dedans en considérant que c'est vrai c'est un peu une porte ouverte sur l'extérieur et on a voulu rester sur notre évaluation interne à nous, et en considérant qu'on n'était pas capables de donner des probabilités trop fines, voilà ».*

Le groupe **BATIMODERN** a établi une méthodologie d'évaluation de ses risques qui portent sur l'impact du risque mais a décidé de ne pas retenir la notion de probabilité. Selon la méthode établie, l'impact se mesure sur une échelle de un à quatre en prenant en compte distinctement trois dimensions : le financier, l'image et la sécurité des personnes. Chaque risque est alors évalué sur ces trois dimensions en fonction de critères prédéfinis. Sur le financier, la gravité est fonction du montant en jeu (très grave pour supérieur à 500 MEUR, Grave entre 200 et 500 MEUR, Important de 100 à 200). Sur l'image, l'impact est fonction de la durée et de l'étendue

de l'exposition dans les médias (courte durée, longue durée / locale à internationale) et pour la sécurité des personnes, elle n'a pas été explicitée (le niveau 4 étant associé à un accident mortel). La règle étant de prendre pour chacun des risques évalués l'impact le plus élevé parmi les trois dimensions.

L'évaluation du risque prend en compte à la fois l'impact potentiel d'un événement et sa probabilité d'occurrence sans prise en compte des dispositifs de maîtrise existants.

AUTOCAR : « *Le brut, c'est le risque sur lequel on donnait une évaluation impact occurrence, puis on mettait les mesures de maîtrise mises en œuvre qui nous donnait le risque résiduel impact occurrence. Voilà, du coup, maintenant, ce n'est plus ça. Donc on met juste le risque qu'on estime avec l'impact et l'occurrence et après on voit ce qu'on met en plan d'actions* ».

Le risque est évalué sans avoir de précision sur la nature du type d'impact à évaluer.

Plusieurs groupes (MUTLIMEDSTORE, DISTRIMART, FROMAGO) mettent en œuvre une évaluation du risque qui associe une échelle de probabilité et une échelle d'impact (échelle de 1 à 4). Toutefois, la nature du type d'impact à prendre en compte n'est pas précisée contrairement au cas précédent (BATIMODERN).

Le risque est évalué avec une notion d'impact qui est limité à la dimension financière.

BATICOSTO : « *C'est-à-dire que n'importe quel risque, si vous n'arrivez pas à le traduire en montant financier, c'est que ce n'est pas un risque. Ce n'est pas un filtre dans la mesure où on ne regarde pas que les sujets financiers. Bien évidemment on regarde aussi les sujets de terme réputationnel, image de marque. Ce n'est pas facile à traduire en matière financière, mais on s'oblige à le faire. [...] Comme on quantifie tout c'est plutôt monétaire. Sauf qu'on intègre quand même la notion de probabilité. C'est-à-dire un risque extrêmement peu probable a peu de chance de rencontrer. Un Boeing qui s'écrase sur ce site ne remonte pas. Pour nous ça n'est pas un risque* ».

Les entretiens nous ont permis d'identifier plusieurs approches dans la mise en œuvre.

- **BATICOSTO :** l'évaluation des risques se fait par le produit de l'impact et de la probabilité. L'impact est uniquement évalué en terme financier. A titre d'illustration, le risque image sera évalué soit par la perte de chiffre d'affaires potentielle ou bien le coût

envisagé pour restaurer son image. L'impact financier correspond à un montant (et jamais à une fourchette).

- **ENGINICA** : en 2013, l'échelle de mesure retenue comportait 3 niveaux : High, Medium, Low. L'impact était apprécié en fonction du % de perte de Chiffre d'affaires (High si supérieur à 15 %, Médium entre 10 et 15%. Et faible en dessous de 10%).
- **CHIMICA** : le directeur de l'audit applique une règle qui consiste à ne retenir comme étant un risque que les éléments qui pourraient avoir un impact financier égal ou supérieur à 10 MEUR.

L'évaluation du risque prend en compte l'impact potentiel de l'événement, sa probabilité d'occurrence ainsi que le degré de maîtrise associé aux contrôles existants.

Cette méthode d'évaluation complète la précédente en y ajoutant la notion de degré de maîtrise.

MICROPIX : *« C'est la combinaison sur un axe de l'impact et de la probabilité, c'est ce qu'on appelle l'exposition et sur l'autre axe, on a ce que l'on appelle la marge d'amélioration. Cela veut dire : quelles sont les mesures de réduction du risque en place ? Et est-ce que la marge d'amélioration est faible ou bien est-ce qu'elle est élevée ? Et, bien évidemment, plus elle est élevée, plus le risque est lui-même élevé et plus le risque a des chances d'être un risque prioritaire.*

- **GAZEO** : l'échelle de probabilité est faible, moyen ou élevé. Pour ce qui est de l'impact, trois niveaux ont été définis : A, B et C. Les impacts sont appréciés selon plusieurs typologies : industriels, financiers, ressources humaines, juridiques, opérationnels et transverses. Pour l'impact financier, un critère spécifique a été établi : A = 50 Millions, B= 100 Millions et C : Au-delà de 100 Millions. La maîtrise est évaluée par la fonction sponsor du risque (sauf pour le transverse) sur une échelle de 1 à 4, en référence à un référentiel de risque qui récapitule les risques standards et les contrôles associés pour les maîtriser.

Pour certains groupes, il apparaît que même si des échelles sont fournies pour évaluer les différentes dimensions, elles ne reposent pas toujours sur des critères explicites ou détaillés.

- **MULTIMEDSTORE** évalue le risque en utilisant des échelles de probabilité, d'impact et de niveau de maîtrise mais restreint l'impact à la dimension financière.

- **ELEC, SANTEFORM et MICROPIX** ont défini des échelles de mesure sans toutefois préciser la nature des impacts à prendre en compte.

Dans certains cas, l'évaluation faite doit être documentée afin de justifier l'évaluation.

- **VINO** : Il est demandé aux personnes d'évaluer sur une échelle de 1 à 5 la probabilité, l'impact et le degré de maîtrise. A cette évaluation, il est aussi demandé aux personnes de fournir des exemples concrets quantitatifs ou descriptifs afin de justifier leur évaluation. Il en est de même pour le niveau de maîtrise. Il est demandé de décrire les dispositifs en place. (En pratique, le degré de maîtrise est plus facile à appréhender que la probabilité selon le directeur de l'audit).
- **CIMENTO** : la matrice des risques est représentée avec l'impact en ordonnée et en abscisse "ça dépend de nous ou pas". L'évaluation faite par les personnes rencontrées lors des entretiens est au final re-pondéré par l'audit au vu des éléments factuels, c'est-à-dire l'existence ou non de dispositifs de contrôle.

L'évaluation du risque prend en compte pour un événement donné sa probabilité d'occurrence et ses impacts potentiels (qui peuvent recouvrir plusieurs dimensions).

VOYAGO : « *Donc qu'est-ce qu'on a fait, on a essayé de définir une méthode sur la base d'entretiens, on a essayé de définir ce qu'on appelle une métrique. On va dire donc un risque voilà comment on le quantifie. Donc on a défini différents critères suivant lesquels on apprécie un risque. Donc bien sûr on a la partie financière mais on a défini aussi des impacts humains, des impacts image, des impacts sociaux. Voilà donc on a toute une grille d'analyse de risque* ».

VOLTAGE : « *Alors on n'est pas très content de la matrice. On l'a fait évoluer l'année dernière. Avant on avait une dimension très, très simple qui était la dimension probabilité d'occurrence et impact avec une vision très financière de la chose sur le compte de résultat. L'impact financier avec toutes les difficultés qui vont avec pour l'apprécier. C'était par vraiment revu, c'était vraiment en résultat net ou en EBIT. Et on se disait, alors moi je suis en poste depuis Novembre 2013, donc ce qu'on s'est dit c'est que quand on essaye de convertir en euros des risques qui touchaient beaucoup plus à la réputation, à l'image, à la santé des personnes, etc. on a vu un tableau de conversion qui ne voulait pas forcément dire grand-chose. Donc, il y avait plein de*

choses qui se retrouvaient de facto' sur un axe en abscisse d'impact financier, c'était trop conventionnel quoi. Donc on a rajouté deux dimensions. On a rajouté une dimension « Image et réputation », une dimension « Humaine, environnement et ou organisationnel. Ce n'est pas parfait évidemment ».

- **VOLTAGE** : Il est à noter qu'au final l'évaluation est re-pondéré par l'audit sur la base de sa connaissance et des échanges contradictoires avec les fonctions expertes comme la R&D.
- **RESTAULIB** : la probabilité est évaluée sur une échelle de 1 à 5 en fonction des occurrences de réalisation survenues ou bien envisagées pour un événement donné comme l'intoxication alimentaire (arrive chaque semaine = 1, chaque mois = 2, chaque année = 3, une fois sur ces trois dernières années = 4, une fois sur ces dix dernières années= 5). L'impact est aussi évalué sur une échelle de 1 à 5 par rapport à cinq axes : stratégique, opérationnel, finance, RH, image. Des critères d'évaluation ont été définis pour chacun de ces 5 axes (par exemple, pour l'image l'impact sera gradué en fonction du niveau d'exposition médiatique, avec une couverture locale, nationale, ...).
- **SPORTFLEX** : l'évaluation de la probabilité se fonde sur la fréquence de survenance constatée lors des missions d'audit (de 1 à X fois). L'évaluation de l'impact s'effectue par rapport à 2 axes pour l'ensemble des risques (Finance, Sécurité des personnes) et un axe complémentaire (image) pour les risques associés à la production.
- **EQUIPAUTO** : l'évaluation est mise en œuvre à partir d'une échelle de 4 pour la probabilité et l'impact. Pour l'impact, il s'agit de plusieurs dimensions : image, financier, production, juridique et RH. L'impact qui sera retenu sera le plus fort de ces différentes natures d'impact. L'utilisation de ces critères permet de remonter des risques qui ne seraient pas forcément remontés par les interlocuteurs compte tenu de la diversité des natures de risques. La difficulté de l'évaluation réside dans le manque de documentation associé à l'évaluation.

L'évaluation du risque prend en compte la probabilité d'occurrence et ses impacts potentiels (sans se limiter à la dimension financière) et le degré de maîtrise.

Parmi les groupes interrogés, nous avons pu identifier le groupe AERO qui est le seul à avoir introduit une dimension temporelle dans son évaluation.

- **AERO** : Les risques sont évalués en termes de probabilité et d'impact sur une échelle de 1 à 4. L'impact est considéré selon 5 axes : opérationnel, financière, juridique, clients, image. Pour chacune de ces dimensions, des critères ont été définis (pour le financier en % du chiffre d'affaires, pour l'image en fonction du niveau d'exposition c'est-à-dire locale, nationale, ...). Une autre dimension a été introduite : l'échelle de temps qui précise à quelle échéance le risque peut survenir (une période inférieure à 1 an jusqu'à plus de 10 ans). Plus l'évènement est lointain et moins il pèsera.

Synthèse : l'évaluation des risques telle que mise en œuvre au sein des organisations témoigne d'une très grande diversité des pratiques mais aussi des difficultés de mise en œuvre lorsqu'il s'agit d'appréhender les notions d'impact, de probabilité et de maîtrise. Seule une entreprise a introduit la dimension temporelle dans son évaluation des risques.

Tableau 28. Cartographie des risques – modes d'évaluation du risque

Méthode d'évaluation	Enumération sans évaluation	
	Impact sans probabilité (impact = 1 dimension)	Financier
		Autres
	Probabilité × Impact (impact = 1 dimension)	Financier
		Autres
	Probabilité × Impact (impact multidimensionnel)	
	Probabilité × Impact × Maîtrise (impact = 1 dimension)	Financier
Autres		
Probabilité × Impact × Maîtrise (impact = 1 dimension)		

4 - 1 4 LE CLASSEMENT PAR CATEGORIE ET LA SYNTHESE DES RISQUES

À l'issue du processus d'identification et d'évaluation des risques, un travail de synthèse est réalisé. Celui consiste à regrouper des risques spécifiques sous des catégories plus génériques et englobantes par souci de simplification. Une autre manière de procéder est de soumettre les risques recensés à un processus de sélection. Dans ce cas, la sélection nécessite de hiérarchiser les risques.

4 - 1 4 1 HIERARCHISATION DES RISQUES

Le processus de hiérarchisation peut être basé sur la prise en compte des impacts financiers potentiels.

BEAUMAG : « Pendant un moment, on s'est dit « allez tout ce qu'on estime qu'on peut perdre ne fait pas plus de 500.000 on va le mettre dans telle classe, plus d'un million dans telle classe, plus de 3 millions mais finalement ça ne donne rien. Enfin, ça rend invisible des risques opérationnels qui existent et qui doivent être gérés et ça les rend complètement invisible à la direction ».

CHIMICA : « Dans les listes de risques qu'ils m'ont fournis, moi j'ai dit « écoutez, on va faire un seuil à 10 Millions ». Souvent, ils ont en tête des risques très opérationnels parce que ça leur pourrit la vie au quotidien. Et puis en réfléchissant un peu ensemble, on s'aperçoit que l'enjeu est bien inférieur. Je dis « Et bien, tu vois, il ne figure pas dans la cartographie des risques ». Alors, on va le mettre pour mémoire mais [...] Et ça, c'est un exercice qui les aide énormément parce qu'ils n'ont pas l'habitude de le faire. Ils vont souvent surestimer un risque, en tout cas mentionner un risque dont l'enjeu est beaucoup plus faible que ce qu'ils croyaient ».

Le processus de hiérarchisation et de sélection peut reposer sur des approches quantitatives non limitées à l'impact financier.

- **FROMAGO :** Le critère retenu pour les risques groupe est de ne retenir que les risques communs au plus grand nombre. Les risques groupe sont des risques que tout le monde remonte où qu'ils soient (réputation, sécurité, supply chain, ...).

- **DISTRIMART** : l'audit quant à lui ne retiendra que les risques évalués par le produit de la probabilité et de l'impact comme étant supérieur ou égal à 8 (1x8 ou 2x4 par exemple) une fois les risques remontés par les BU
- **BATIMODERN** : la hiérarchisation des risques est réalisée sur la base de l'impact en considérant l'impact le plus significatif qui peut résulter soit de la dimension financière, soit du risque d'image ou bien de la sécurité des personnes. Cette hiérarchisation a été présentée à la direction financière et à la direction juridique afin de les apprécier au regard des dispositifs de contrôle en place et donc du degré de maîtrise.
- **BATICOSTO** : la hiérarchisation des risques s'opère sur la base de l'importance de l'impact financier et de la probabilité. Un événement peu probable ne remontra pas (par exemple la chute d'un avion sur le site). De même, pour la cartographie groupe, il a été demandé aux métiers de remonter 10 risques majeurs. L'impact est variable selon les métiers. Seuls les risques métiers les plus importants remonteront au niveau de la cartographie corporate.
- **CIMENTO** : le nombre de fois qu'un risque est cité, c'est-à-dire l'occurrence est un critère. Le second est la matérialité. Mais aussi le recoupement des informations remontées lors des entretiens avec le résultat des audits, du contrôle interne qui permet d'évaluer la pertinence des éléments issus des entretiens. La difficulté est plutôt d'appréhender les risques de façon plus prospective.
- **AERO** : la hiérarchisation est mise en œuvre sur la base de l'évaluation des risques à savoir le produit de l'impact et de la probabilité. Ainsi, un risque coté 16 (avec une probabilité de 4 et un impact de 4 sera prioritaire). A cela s'ajoute la dimension temps puisqu'un risque éloigné pourra être traité plus tard. Par ailleurs, le groupe a identifié un certain nombre de risques inacceptables indépendamment de leur évaluation. Il s'agit des risques éthiques, déontologie-fraude, sécurité des personnes et des biens, protection de l'information et la sécurité aéroportuaire, la sûreté et la satisfaction client.

Le processus de hiérarchisation et de sélection peut reposer sur des approches plus qualitatives

ENGINICO : « Vous voyez ça c'est en termes de risque inhérent et de risque résiduel limité. Quand ils ont la caisse, c'est 500/600 euros. Donc le risque en lui-même si on se faisait juste l'analyse en termes de poids des risques inhérents ou résiduels, le petty

cash ne devrait pas y apparaître. C'est parce qu'il y a une règle groupe et que notre CFO, Président dit « non, je ne veux pas de petit cash » que du coup ça remonte ! Et donc c'est mou comme matière. C'est pas du tout se dire on prend cap et on se tient à son cap. Même si effectivement la logique est celle-là hein. Maintenant effectivement, je vous dis c'est mou parce qu'on doit intégrer des dimensions, des données qui ne résultent pas d'une analyse par risque ou par poids du risque ».

ELEC : *« Les risques élémentaires de division, des business units, dans leur méthode, il y a une grille impact/probabilité, qualité du contrôle, etc. Il essaye de quantifier mais bon, ce qui fait qu'on va les reprendre au niveau groupe ou pas, c'est un peu plus subjectif. L'idée de toute façon, c'est d'arriver à quelque chose de l'ordre de 75, gérable quoi. C'est gérable même si ça peut paraître comme étant beaucoup mais c'est gérable, on est nombreux, on arrive sans problème ».*

Synthèse : le processus de hiérarchisation peut s'établir selon les organisations soit au moyen d'une approche quantitative, soit plus qualitative et cela indépendamment des évaluations quantitatives qui peuvent exister ou non.

Tableau 29. Cartographie des risques - processus de hiérarchisation des risques

Approche quantitative		Approche qualitative
Impact financier potentiel	Autres critères	Critères hétérogènes

4 - 1 4 2 CLASSEMENT DES RISQUES PAR CATEGORIE

Le classement des risques par catégories peut se faire soit en utilisant des catégories de risques définis a priori, soit définis a posteriori.

La cartographie est la somme des risques : regroupement et agglomération des risques spécifiques sous forme de macro-risque défini « a priori ».

CIMENTO : « Les risques qui sont décrits là sont assez génériques pour être assez large. On aurait un problème de sélection si on descendait sur une granulométrie plus fine. Et quand vous prenez par exemple « health and environment concerns » c'est très large. Donc, si vous commencez à ségréguer entre santé et santé qu'est ce qui est lié à, enfin on pourrait à la limite saucissonner la santé, l'environnement mais si on recommençait à saucissonner, faut se dire « Ok, à un niveau groupe, est-ce que c'est un sujet ?! [...] Ce qui fait qu'il n'y a pas de débat sur « Ah oui mais vous avez quand même oublié quelque chose de matériel ».

MUTLIMEDSTORE : « Donc qui les a triés ? C'est moi. Et en fait dans le boulot que je fais avec mon boss, ce que j'essaye de faire, on a nos macros risques au niveau groupe, il y en a une vingtaine. Et en fait j'essaye de voir dans ce qui me remonte des questionnaires ou des entretiens si ces macros, si c'est les risques terrains opérationnels ou pays se raccrochent à ces macros risques. Et c'est aussi pour moi un autre contrôle, parce que s'il y a des choses qu'on m'a remontées et qu'on n'avait pas je dirais le risque générique ou macro c'est que j'aurais un trou dans la raquette ».

La cartographie n'est pas la somme des risques : mise en œuvre d'un tri sélectif par strate afin de ne retenir que certains risques définis « a posteriori ».

- **ENGINICO :** en 2013, une fois la liste des 750 risques a été établie, puis l'audit l'a réduit à 150 risque en réalisant un brainstorming au sein de l'équipe d'audit, sur la base de sa connaissance des activités et de l'impact financier sur le groupe. Cette nouvelle liste de 150 risques a été soumise aux 7 membres du COMEX en leur demandant de choisir chacun 10 risques majeurs. Chaque directeur ayant choisi des risques différents, le PDG a sélectionné lui-même les 20 risques majeurs en excluant tous les sujets opérationnels.

NATURELIA : « Aujourd’hui on a quand même quelque chose qui part des entités et qui remonte par l’agrégation et qui est complétée à chaque niveau parce que la carto centrale ce n’est pas juste la somme des cartos. Les risques enfin vous savez mieux que moi ce n’est pas la simple addition des risques. Voilà, il y a d’autres choses qui se produisent au fur et à mesure de l’agrégation et aujourd’hui ce problème-là est à peu près bien géré. [...] Et il y a des risques, si je prends, on peut avoir tout un tas de pays qui nous disent que le risque principal, c’est l’insolvabilité de certains gros clients. Ça ne peut pas être un risque majeur pour le groupe. En tout cas, c’est justement la diversité de ses clients qui fait que ce n’est pas un risque important, voilà. Donc on ne peut pas les additionner simplement. Et puis effectivement les fonctions peuvent avoir aussi une vision un peu différente ».

Synthèse : A l’issue du processus d’identification et d’évaluation des risques, un travail de synthèse est réalisé. Celui consiste à regrouper des risques spécifiques sous des catégories plus génériques et englobantes par souci de simplification. Une autre manière de procéder est de soumettre les risques recensés à un processus de sélection.

Tableau 30. Cartographie des risques – consolidation des risques

Simple agglomération (création de catégorie génériques)	Regroupement, Elimination, Sélection
Défini a priori	Défini a posteriori

4 - 1 4 3 NATURE DES RISQUES

Les risques recensés dans le cadre de l'élaboration de la cartographie de natures multiples au regard des pratiques.

Les risques de direction et les risques transverses

Les risques dits de direction sont des risques isolés dont les conséquences ne concernent qu'une partie de l'organisation. Il peut s'agir soit d'une entité, soit d'une direction, soit d'un département, d'une fonction ou bien d'une activité. Les risques transverses sont par définition transverses à l'organisation.

RACECAR : *« Les Top risques dits de direction, ceux qui sont bien circonscrits au niveau d'une direction et dont les plans d'action sont effectivement à la main des directions. Et puis des Top risques transversaux qui impactent plusieurs directions et où il y a potentiellement, on va nommer à la fin de la fin un sponsor pour gérer le plan d'actions transversal mais potentiellement il y a plusieurs acteurs impactés ».*

BEAUMAG : *« On va les classifier par ordre de priorité, enfin d'enjeux, d'enjeux métier et ça va nous permettre d'avoir nos fameux risques, alors après vous en avez qui se recoupent bien évidemment etc. Alors là où j'ai, où ça a une limite et je trouve que c'est compliqué pour moi, c'est tous les process transverses. Par exemple les projets, la question que je me suis posée c'est est ce que je mets les projets dans chacune des (parce que vous avez les projets RH vous avez des projets na, na, na, na et puis vous avez des projets aussi qui touchent la DAF, la DRH) ou est-ce que finalement je fais, j'ai fait un dernier pavé qui s'appelle l'activité transverse ».*

Les risques génériques et les risques spécifiques

Les risques génériques sont des risques qui du fait de leur nature peuvent englober plusieurs risques spécifiques.

ELECTRO STORE : *Voilà, sachant qu'on a de la chance, c'est que nos 3 sociétés opèrent quasiment selon le même standard. Et ce qui était vrai déjà avec les autres filiales si vous voulez. Donc ça simplifie un peu. Après ce qui change c'est effectivement tout ce qui est lié à l'infrastructure, donc cette partie « Bottom-Up » où là les risques*

sont spécifiques, donc plus du tout de caractère générique et inhérent aux marchés, aux juridictions dans lesquels les filiales opèrent ».

MICROPIX : *« Donc maintenant, si on passe sur les risques, donc on a un dispositif d'Enterprise Risk Management, qui a été mis en place maintenant depuis quelques années. Un des outputs de ce dispositif, c'est une cartographie des risques qui est basée sur un univers de risques qui a été défini à l'origine avec un certain nombre de risques génériques qui sont propres à l'activité de la société et je dirais que cet univers de risques, c'est un élément clé aussi pour structurer le risk assessment de l'audit interne ».*

Risques stratégiques et opérationnels

Les risques stratégiques se distinguent des risques opérationnels par leur portée et leur impact jugé plus significatif dans le temps.

FROMAGO : *« On a des risques stratégiques, on a des risques opérationnels. Sur les risques opérationnels, il y a des plans d'actions. Et du coup, l'audit, moi, je pioche à travers les plans d'actions. C'est très clair : j'en avais 19, il y en a 9 qui sont partis en risque opérationnel, il y en a 10 qui sont partis en risque stratégique ».*

Les risques inacceptables

Les risques inacceptables représentent des risques jugés comme étant majeur à gérer et maîtriser et cela indépendamment de leur probabilité de survenance.

AERO : *« On a six risques inacceptables. Il y a le risque éthique, déontologie-fraude, on a la sécurité des personnes et des biens. On a la protection de l'information, on a la sécurité aéroportuaire ce qui n'est pas la même chose que la sécurité des personnes et des biens [...] mais tout ce qui est accident aérien, et puis la sûreté. Il manque quoi, la satisfaction client, qui a été mise, alors ça, c'est le seul qui pourrait sortir de l'inacceptable, à un moment où il y a le directeur général qui est maintenant parti, délégué, et qui a crié parce qu'il trouvait qu'on ne faisait pas assez d'effort en matière de satisfaction client et qui a voulu que ce soit dans les inacceptables ».*

Les risques bruts et les risques nets

Les risques bruts sont les risques avant la mise en œuvre d'actions spécifiques pour réduire le niveau de risque. Les risques nets correspondent aux risques résiduels une fois les actions de maîtrise du risque mis en œuvre.

AUTOCAR : « *Et là, on a simplifié puisqu'avant, on faisait les risques bruts, les risques nets. Maintenant, on est directement passé sur le net. Si vous préférez, le net, le résiduel, c'est le risque et ce qui subsiste malgré tout ce qui est déjà mis en place* ».

Tableau 31. Synthèse sur la nature des risques recensés lors du processus de cartographie

Nature des risques
De direction (limité à la Direction) ou transverse
Générique ou Spécifique
Stratégique ou Opérationnel
Brut ou net
Inacceptable

4 - 1 5 LA VALIDATION DE LA CARTOGRAPHIE DES RISQUES

Une fois la cartographie des risques établie, celle-ci est soumise à la validation. Les acteurs en charge de la validation varient en fonction des spécificités organisationnelles.

Instances de gouvernance uniquement

Il s'agit des cas où la direction de l'audit (RESTAULIB, VINO, MICROPIX, MULTIMEDSTORE) est hiérarchiquement et fonctionnellement rattachée aux instances de gouvernance.

VINO : « Ça peut être discuté au niveau du DG ou du DAF ici mais en général, c'est directement le comité d'audit. En fait, là ici, moi ici je reporte directement au conseil d'administration et au comité d'audit [...]. J'ai eu une discussion avec le DG et avec le DAF, j'ai un rôle d'animation mais je n'ai aucun lien hiérarchique ».

Management et instances de gouvernance (conseil d'administration ou comité d'audit)

Il s'agit des cas où la direction de l'audit est hiérarchiquement rattachée au management et fonctionnellement aux instances de gouvernance, ou bien l'inverse.

AUTOCAR : « Le Comex et le comité d'audit. Ça passe en Comex et ça passe en comité d'audit ».

Synthèse : la validation du plan suit les deux modalités suivantes. Dans le cas où l'audit est hiérarchiquement rattaché aux instances de gouvernance, le plan d'audit est directement validé au niveau du comité d'audit. Lorsque l'audit est rattaché hiérarchiquement au management, le plan d'audit est soumis à une double validation : celle de sa hiérarchie puis celle du comité d'audit.

Tableau 32. Cartographie des risques – instances de validation

Validation
Uniquement Comité d'audit
Instance de gouvernance et Management

4 - 1 6 LA MISE A JOUR DE LA CARTOGRAPHIE DES RISQUES

La cartographie des risques une fois établie, peut être mise à jour selon une certaine périodicité qui diffère selon les organisations.

4 - 1 6 1 MISE A JOUR DE LA CARTOGRAPHIE DES RISQUES ET SUIVI DES PLANS D' ACTIONS

Le processus de mise à jour de la cartographie s'effectue à des fréquences et des modalités qui diffèrent en fonction des organisations.

La cartographie n'est pas mise à jour

- **VESTIMOD** : la cartographie n'a pas été mise à jour depuis 2009

La cartographie des risques est établie sur une période supérieure à l'année

- **PETROLIUM** : la dernière mise à jour de la cartographie des risques de 2011 a été engagée en 2014 et est toujours en cours.
- **CIMENTO** : La cartographie des risques est mise à jour tous les deux ans avec un "light update" qui se fait avec les entretiens du plan d'audit l'année où elle n'est pas réalisée.
- **VINO** : la mise à jour est faite tous les deux ans.

La cartographie est mise à jour de façon annuelle

- **GAZEO** : l'exercice de cartographie se fait une fois par an. L'objectif est de valider les évaluations de risque associées aux risques standards et de voir s'il faut ou non rajouter de nouvelles catégories de risque.
- **BATICOSTO** : la cartographie est mise à jour de façon annuelle, à l'exception du métier Télécom et Multimédia. La cartographie est mise à jour trois fois par an au sein des métiers Télécom et Multimédia compte tenu de leur environnement extrêmement soumis à des changements rapides dans le temps.
- **AERO** : le processus de mise à jour est annuel. Il s'agit non pas d'identifier de nouveaux risques mais plutôt de valider le positionnement des risques existants.

La mise à jour est semestrielle

Il s'agit des groupes **ELEC** et **AUTOCAR**.

La mise à jour repose sur un processus d'actualisation régulier

- **LUXESTORE** : le processus de cartographie est un processus permanent avec six missions de cartographie réalisées chaque année. L'objectif est de couvrir progressivement l'ensemble du périmètre du groupe et d'enrichir progressivement la cartographie du groupe. Pour les entités dont la cartographie a déjà été réalisée, la mise à jour n'est pas une mise à jour des risques mais du suivi des plans d'action, sauf en cas de changement significatif.
- **EQUIPAUTO** : la direction de l'audit réalise des missions d'analyse de risque durant l'année de façon récurrente afin de s'assurer qu'il n'y a pas de risque majeur non identifié. Ce processus couvre les pôles et les Régions.
- **SPORTFLEX** : la direction s'est dotée d'un outil qui permet à ses auditeurs d'alimenter à l'issue de chacune des missions d'audit la liste standard des risques qu'elle a établie. Ceci permet d'avoir une mise à jour quasi-continue des risques par entité, pays, process et sous-processus.

Synthèse : la fréquence ainsi que les modalités de mise à jour de la cartographie des risques varient en fonction des organisations. De façon plus spécifique, certains groupes ont établi des mises à jour plus en fonction du type d'activité ou bien de réaliser des missions de cartographie tout au long de l'année. La mise à jour peut consister à modifier à la marge la liste des risques en fonction des changements intervenus durant la période ou bien à refaire l'exercice sans référence à la cartographie précédente. Certains groupes ne mettent à jour que l'évaluation des risques sans actualiser la liste des risques, d'autres uniquement l'avancement des plans d'actions associés aux risques.

Tableau 33. Cartographie des risques – modalités de mise à jour

Mise à jour		
Ponctuel (moins de 1 fois/an)	Ponctuel (1 fois/an)	Multiple (au moins 2 fois/an)
Exercice complet		
Mise à jour de la liste des risques (cartographie précédente)		

4 - 2 L'ELABORATION DU PLAN D'AUDIT

Les normes d'audit internes (norme 2010) précisent que « le responsable de l'audit interne doit établir un plan d'audit fondé sur les risques afin de définir les priorités cohérentes avec les objectifs de l'organisation. Cette même norme précise que « le plan d'audit doit s'appuyer sur une évaluation des risques documentés et réalisée au moins une fois par an ».

Nous allons voir dans cette partie que **l'élaboration du plan d'audit repose sur plusieurs étapes** :

- La construction de l'univers d'audit,
- L'identification des missions d'audit que la direction de l'audit pourrait retenir en lien avec les risques de la cartographie,
- L'identification des missions d'audit en fonction de critères spécifiques (autres que les risques),
- La présélection des missions d'audit parmi la liste des missions « possibles » identifiées en amont,
- La présentation et la validation du plan d'audit,
- Le degré de flexibilité retenu dans le plan d'audit.

4 - 2 1 LA CONSTRUCTION DE L'UNIVERS D'AUDIT

L'univers d'audit comprend l'ensemble des objets d'audit qui pourront une fois recensés venir alimenter le plan d'audit et cela en lien avec les risques de l'organisation tels qu'exigé par les normes d'audit interne (norme 2010). Il s'agit d'un travail de recensement de l'ensemble des objets d'audit. L'élaboration de l'univers d'audit consiste à procéder au découpage de l'organisation sous forme de segment d'audit (processus, entités, ...) et à établir un inventaire des entités, des activités et des processus.

Le niveau de description des éléments qui composent l'univers d'audit peut être hétérogène au sein d'un même groupe.

La démarche de construction de l'univers d'audit telle que décrites par les directeurs de l'audit consiste à inventorier les entités aussi bien légales que de gestion au sein de leur organisation. Une fois cet inventaire réalisé, les entités sont ensuite découpées en objet d'audit en fonction de leur taille et de leur spécificité en termes d'activité. Ainsi, il est possible d'avoir un pays qui représente un objet d'audit équivalent à une activité au sein d'un grand pays. En procédant ainsi,

l'univers du périmètre « auditable » peut être établi avec des objets d'audit jugés équivalents dans le but de pouvoir ensuite dimensionner les ressources d'audit à allouer en fonction du nombre d'objets d'audit à couvrir.

RESTAULIB : « *La deuxième chose, ça va être ce que j'appelle chez moi l'univers d'audit. Je ne sais pas si ça vous parle quand je dis ça. L'univers d'audit, ça va être quoi ? Ça va être de construire qu'est-ce qu'il y a d'auditable chez Restaulib, c'est des segments d'audit. Je vais prendre un exemple. Restaulib Pérou, ce n'est pas gros, ça fait 40 Millions d'Euros de chiffre d'affaires par an. On ne va pas aller faire une approche par process. On va aller, si on fait un audit chez eux, en trois semaines, en faisant un bon risk assessment à la base comme vous disiez, on doit être capable de couvrir le Pérou. On va aller voir les achats, les ressources humaines, la finance [...] trois auditeurs, trois semaines. On parle de segment d'audit un peu similaire en taille. Et on est en train de, on réfléchit dans ce document en disant quel est le nombre de segments d'audit que j'ai. Et donc, soit on met un en disant c'est un segment, Restaulib Pérou. Par contre, quand je vais aller au Brésil qui est énorme pour nous, aux Etats-Unis, en France, à Londres, on ne peut pas dire j'arrive en France et je fais un audit en deux semaines, je couvre pas la France, il faut que j'attaque par process. Donc en fait la France, on va découper la France en processus. On va faire un audit des achats, on va faire un audit des RH. Et à l'intérieur des RH, on va peut-être même découper en sous-process tellement c'est gros ».*

Les entretiens ont mis en évidence une certaine difficulté liée à cet exercice qui suppose de disposer d'un inventaire fiable et à jour des entités, des activités et des processus.

CHIMICOR : « *Là on va plutôt avoir une approche par usine ou par unité de contrôle donc on a une base de données, un univers d'audit qui est juste un cauchemar parce que la maille dépend de la Legacy. Sur Chimicor, vous avez quasiment une entité juridique par BU, par pays. Chez Chimi-R (filiale), on va être obligé de redescendre sur une unité de contrôle plus bas, parce que si vous vous arrêtez au niveau de l'entité du pays, d'abord vous dupliquez et vous n'allez rien voir, vous allez être sur une entité qui est tellement énorme, qui couvre tous les Etats-Unis, les BUs vous ne voyez rien. Vous êtes obligé de descendre au niveau de l'usine et vous allez découper l'usine, plus vous allez faire aussi les plateformes purchasing, les plateformes customers services, les*

plateformes payroll etc. et tout ça c'est un univers d'audit. L'esprit, c'est qu'on repart, on réconcilie tout ce qui est entité juridique avec la conso, pour s'assurer qu'on a bien les mêmes entités, qu'on prend même les AS et qu'ensuite quand une entité consolidée, une entité juridique n'est pas à un degré de d'organisation suffisamment fin, c'est un peu l'expérience on l'a vraiment construit, ça fait 3 ans qu'on est dessus et chaque fois on rajoute, on va descendre à un niveau plus fin ».

Synthèse : La construction de l'univers d'audit consiste à établir la liste des entités et des processus afin de recouper ces deux dimensions pour établir des segments d'audit « équivalent ». L'univers d'audit n'est pas figé puisqu'il peut évoluer dans le temps.

Tableau 34. Plan d'audit – construction de l'univers d'audit

Univers d'audit
Recensement des entités
Recensement des processus et sous processus
Croisement entités et processus

4 - 2 2 L'IDENTIFICATION DES SUJETS (POTENTIELS) D'AUDIT EN LIEN AVEC LES RISQUES

La direction de l'audit doit établir la liste des missions d'audit (sujets et missions potentielles) dans le cadre de la planification annuelle de ses activités afin de la soumettre pour validation à sa hiérarchie. La liste des missions d'audit découle d'une analyse des risques recensés dans la cartographie des risques.

4 - 2 2 1 LES ENTRETIENS PREPARATOIRES POUR ETABLIR LE PLAN D'AUDIT

Des entretiens spécifiques pour préparer le plan d'audit

Toutes les directions de l'audit, à l'exception de celle du groupe EQUIPAUTO, réalisent des entretiens spécifiques dans le cadre de l'élaboration du plan d'audit. L'objectif de ces entretiens est d'identifier les sujets d'audit potentiels à inscrire au plan d'audit.

BATIMODERN : *« Le plan c'est sur la même base en fait, le plan c'est sur la base d'entretiens donc quelque part, on va revoir les mêmes personnes, séparément de l'analyse de risques en leur demandant quelles sont les missions qu'ils nous demandent d'auditer, voilà. Et on le fait exprès de le faire en deux fois, c'est un peu bizarre mais c'est vrai que ça ne se prête pas trop à [Euh...] comment dire ? Les sujets sont assez disjoints en fait, l'évaluation d'un risque pur et le fait que l'on ait besoin d'auditer ou pas et on n'est pas encore trop capable de le mener dans un même entretien et sachant qu'en durée on est quand même un peu limité, on peut pas prendre les gens plus de 2 heures. Et en fait 2 heures on en a bien besoin pour l'évaluation du risque donc sinon il n'y aurait plus de temps pour les demandes d'audit en fait, donc c'est pour ça qu'on fait 2 entretiens en fait ».*

Une identification des sujets d'audit en fonction du niveau organisationnel interrogé

La nature des sujets d'audit (potentiels) qui sont identifiés lors de ces entretiens est liée en partie aux personnes que la direction de l'audit interroge lors de la préparation du plan d'audit. Le recoupement par l'audit des informations recueillies lors des entretiens permet d'identifier un certain nombre de sujets potentiels d'audit.

VEHICAR : *« C'est Région Métier, c'est Fonctions et Régions. Puisque VEHICAR a à la fois à une organisation fonction et une organisation région. Donc il faut qu'on couvre les deux. Une fonction peut très bien, dans sa fonction, si je prends par exemple*

la fonction achat, elle ne va pas forcément me remonter à un truc pour la région Maroc par exemple. Alors que la fonction achat, elle peut dire voilà sur les achats voilà ce que je sens et la région parce qu'elle est quand même plus au courant de ce qui se passe typiquement sur le Maroc va dire moi je veux voir ce qui se passe sur les achats Maroc. Donc on croise à chaque fois Fonction/Région ».

Pour les directions de l'audit qui sont en partie décentralisée (ELECTROSTORE, BATICOSTO, BATIMODERN, MEDIACORP, MICROPIX, SANTEFORM, CHIMICOR, ELEC, GAZEO, DISTRIMART, RESTAULIB) les entretiens sont menés en cohérence avec le périmètre couvert par les directions d'audit décentralisée.

- **GAZEO** : le groupe dispose d'équipe d'audit en pays, en zone géographique puis au siège. Pour le plan d'audit groupe adressé par l'équipe du siège, les entretiens sont réalisés avec la direction générale, le COMEX et ses N-1 afin de confronter la vision de l'audit avec la leur. Une centaine de sujets sont identifiés. Pour le plan d'audit des zones, des entretiens sont réalisés avec le management de la zone (directions fonctionnelles de la zone, directeurs de filiale). Pour le plan d'audit entités, les entretiens sont réalisés avec les opérationnels des différentes activités.

Une identification des sujets d'audit en lien avec la dimension temporelle

Le processus d'identification des sujets d'audit nécessite comme celui de la cartographie de se donner pour les auditeurs un horizon de temps afin d'identifier les problématiques à couvrir. Ils peuvent pour ce faire identifier des sujets à partir des incidents passés, des sujets d'attention en lien avec le contexte et l'actualité de leur groupe ou bien traiter des sujets à plus long terme. Les enjeux du moment peuvent peser sur ces choix.

PETROLIUM : *« Tout le monde a son agenda et un DG qui doit partir l'année d'après, il ne va pas s'embêter avec un sujet qui peut attendre ».*

NATURELIA : *« Honnêtement la préoccupation, elle est quand même de court terme dans une boîte qui est vraiment en restructuration, voilà c'est contextuel. Après je vous dis il y a quelques départements dont c'est la vocation de travailler et d'avoir une vision un peu plus lointaine. Mais dans ces départements-là, on a rarement retenu des sujets soit par compétence, soit par ce que ça a été déjà traité, soit parce qu'on n'avait pas la même appréciation aussi de l'importance quoi ».*

Synthèse : la nature et le contenu des missions d’audit sont impactés par le niveau organisationnel interrogé ainsi que la dimension temporelle retenue pour appréhender les sujets réputés être porteurs de risque.

Tableau 35. Plan d’audit – modes d’observation pour l’identification des missions

Identification des missions d’audit			
Type d’approche	« Top-down »	Dimension temporelle	Passé
	« Bottom-Up »		Présent
Dimension spatiale (point d’observation)	« Mixte »	Sources	Futur
	Directions Pays/Régions		Directions métier
	Directions fonctionnelles		

4 - 2 2 2 LA PRISE EN COMPTE DES RISQUES DE LA CARTOGRAPHIE

La prise en compte de la cartographie des risques lors de l’élaboration du plan prend plusieurs formes en fonction des organisations.

Un degré variable de couverture des risques

Certaines directions de l’audit considèrent que leur rôle consiste à auditer en priorité les risques couverts par des dispositifs de maîtrise. Elles considèrent que les risques non couverts par des dispositifs sont connus et qu’une mission n’apporterait pas de valeur ajoutée si ce n’est de confirmer effectivement qu’il s’agit de risque. Alors que d’autres directions de l’audit estiment devoir prendre en compte l’ensemble des risques au travers du plan d’audit.

CHIMICOR : « On se disait où est le rôle de l’audit, ce n’est pas sur des risques critiques où il n’y a rien en face. Notre rôle c’est des risques critiques où on dit le degré de maîtrise est très élevé, parce que j’ai mis ça et ça, c’est là que l’audit doit regarder, est-ce que je ne me suis pas planté sur mon évaluation de degré de maîtrise en imaginant que tout était en

œuvre et fonctionnait bien. Donc il faut que je regarde à la fois la mise en œuvre mais aussi est-ce que ça répond à mon risque ».

ELEC : *« Ce que l'on fait c'est qu'on prend en compte ces cartographies des risques, c'est une donnée d'entrée pour notre programme d'audit, sachant que ce que l'on veille à faire, c'est à couvrir, c'est être capable de donner un avis sur chacun des risques du groupe à travers d'un ou plusieurs audits, les soixante-quinze ».*

Des missions d'audit qui adressent les risques selon différentes modalités

Plusieurs directions de l'audit ont procédé à une sélection de risques à partir soit de la cartographie, soit de l'univers d'audit et les adressent selon des modalités différentes. L'audit peut soit réaliser des missions d'audit sur certains de ces risques, soit faire des missions de suivi des plans d'actions établis par le management, soit les couvrir indirectement sous un prisme spécifique.

- **LUXESTORE** : l'audit couvre au travers de ses missions essentiellement les risques liés à la protection et la sécurité du patrimoine. Les autres risques donnent plutôt lieu à un suivi des plans d'actions définis par les manager dans le cadre du processus de cartographie.
- **VINO** : l'audit identifie à partir des 5 risques majeurs des thèmes (1 ou 2) qu'elle va traiter de façon transverse sur toutes ses missions en lien avec les dispositifs de contrôle qui peuvent exister.
- **ELECTROSTORE** : les risques majeurs identifiés dans le registre des risques donnent lieu à des missions sur le bon suivi des plans d'action. Les risques standards donnent plutôt lieu à des audits de conformité sur le respect des principes de conformité.
- **AERO** : l'audit identifie un certain nombre de sujets en lien avec le TOP 10 des risques du groupe qui donne lieu à des audits thématiques.
- **MUTLIMEDSTORE** : le risque est appréhendé par le prisme des processus et du contrôle interne, c'est-à-dire des risques couverts par des dispositifs. Sont donc exclus les risques de la cartographie dont le plan d'action reste à être définis tout comme le dispositif de contrôle associé.
- **EQUIPAUTO** : 40% des missions d'audit sont en lien avec les risques de la cartographie. Le moyen de les traiter a consisté à rapporter les risques à des processus

et donc aux sous-catégories définies dans la cartographie. Ce qui les rend auditables selon la directrice de l'audit.

Synthèse : les missions d'audit en lien avec les risques peuvent porter sur tout ou partie des risques de la cartographie. En l'occurrence, lorsqu'il s'agit de couvrir les risques à travers les audits, l'approche peut être différente selon les organisations. Elle peut consister à opérer à une sélection de certains risques (risques couverts par des dispositifs de maîtrise, risques spécifiques, ...) ou bien à les traiter indirectement sous le prisme des processus sous-jacents.

Tableau 36. Plan d'audit – Choix des missions en fonction du niveau de risque de la cartographie

Identification des sujets en lien avec les risques

Le risque sous un prisme particulier

Les risques à fort impact et maîtrisés

Les risques à fort impact et peu maîtrisés

4 - 2 3 L'IDENTIFICATION DES SUJETS (POTENTIELS) EN FONCTION DE CRITERES SPECIFIQUES

Les entretiens nous ont permis d'identifier un certain nombre de critères spécifiques, autres que les risques de la cartographie, pour identifier les missions d'audit.

Les missions qui découlent d'objectif de rotation

Certaines directions d'audit ont établi des objectifs de rotation dans le but de pouvoir couvrir leur périmètre d'audit selon une périodicité prédéfinie qui peut être supérieure à l'année. Cette périodicité qui rythme la fréquence de passage de l'audit au sein des entités peut varier en fonction de critères spécifiques tels que la taille des entités, le type d'activité, le type de pays ou de région, etc.

WALLDISTRIB : *« Donc d'abord j'ai ça, donc je vais partir de ça et puis je vais mécaniquement installer un certain process de rotation classique. Alors pour que cette rotation elle soit efficace, je vais rajouter quand même des principes. Donc au moins un passage par pays par an ».*

PETROLIUM : *« Alors sur les grandes filiales on a une logique un peu différente. On y va chaque année. Mais on audite 1 ou 2 processus spécifiques parce que sinon il faudrait rester 6 mois quoi si on voulait tout voir. Donc on a quand même une approche différenciée. [...] Et celles qui sont de taille plus moyennes ou petites, on a un taux de rotation. Donc si elles sont moyennes tous les 3 ans, si elles sont petites sans risque particulier tous les 4/5 ans ».*

Objectif de rotation des entités basé sur la fréquence de passage

Certaines directions de l'audit ont établi des objectifs de rotation en termes de fréquence de passage sur un niveau organisationnel donné.

- **BATI-F :** l'audit vise à couvrir chaque direction régionale qui est rattachée à une branche métier au moins une fois tous les 4-5 ans. Cet objectif de rotation porte sur un niveau organisationnel relativement élevé qui regroupe un nombre beaucoup plus important d'entités. Chaque direction régionale est composée de plusieurs agences qui regroupent quant à elles plusieurs chantiers.

- **VINO** : l'audit s'est donné pour objectif de revoir toutes les filiales au moins une fois tous les 2-3 ans. Une filiale correspond à un pays. Le niveau défini est relativement élevé puisqu'un pays peut regrouper une multitude d'activités et d'entités.
- **SPORTFLEX** : 25% des missions d'audit d'entités sont établies par l'audit sur la base du principe de rotation. Les filiales doivent être couvertes tous les 4 ans.
- **FROMAGO** : des objectifs de rotation ont été définis pour couvrir les entités du groupe sur 3 ans. L'audit a établi un tableau de suivi qui permet d'identifier toutes les entités qui lui restent à couvrir sur un cycle de 3 ans.
- **RESTAULIB** : l'audit s'est donné comme objectif pour couvrir tous les ans chaque pays (même si le nombre de processus qui sont revus au sein d'un pays peut être plus ou moins limité).

Objectif de rotation des entités basé sur la fréquence de passage et des critères spécifiques (taille de l'entité, type de pays, type d'activité).

Plusieurs directions de l'audit ont défini des objectifs de rotation complétés par des critères spécifiques afin d'adapter la fréquence de revues des entités en fonction de leur nature. Les entretiens ont mis en évidence une multitude d'approches en matière d'objectif de rotation.

- **SANTEFORM** : l'audit s'est donné des objectifs de rotation par typologie de pays et par taille d'entité. Pour les 5 plus gros pays qui constituent le "Brick M" (Chiffre d'affaires supérieur à 10 milliards), ainsi que les sites industriels majeurs, ils doivent être audités chaque année. Pour les pays émergents, l'objectif est de les voir tous les 5 ans.
- **MEDIACORP** : le groupe est présent dans 70 pays dont 5 qui sont de taille significative dans l'activité de la musique. L'audit a déterminé 3 catégories les pays (tiers 1, tiers 2 et tiers 3) et s'est fixé comme règle de visiter au moins une fois par an les 5 gros pays qui représentent le tiers 1, au moins tous les cinq ans les autres pays, c'est-à-dire les pays tiers 2 et tiers 3. Les pays tiers 3 sont les petites entités qui feront l'objet d'une revue standard et plus courte.
- **RACECAR** : l'audit a défini des objectifs de rotation en fonction de la taille, des zones géographiques et du type d'activité. Les grandes entités (comme le commerce France)

doivent être suivies de façon quasi continue, les grands pays dénommés du G5 doivent être couverts tous les 3 ans, l'activité pièces de rechange tous les x années.

- **PETROLIUM** : les grandes entités (Exploration et Production, Marketing et Services) sont couvertes tous les ans. La revue consiste non pas à revoir tous les processus mais un nombre limité. Pour les entités moyennes, il est prévu de les revoir tous les trois ans. Et enfin les petites entités sans risque particulier, tous les quatre cinq ans.
- **ELECTROSTORE** : pour les audits d'entité pour la partie RCI Framework (contrôle interne), l'audit a défini des objectifs de rotation. Par exemple, tous les magasins doivent être revus tous les dix-huit mois. Tous les sites ne seront pas couverts avec la même profondeur. Il va y avoir les audits standards de cinq jours et des audits d'une journée pour être en mesure de respecter l'objectif de rotation.
- **BATICOSTO** : l'objectif de rotation ne concerne qu'une partie du groupe. Ainsi, seuls trois métiers au sein du groupe appliquent ce principe qui détermine 50% de leurs missions (Baticosto-Route, Baticosto-Const et Baticosto-Immo). L'objectif de rotation ne vise pas à couvrir toutes les entités mais à cibler les entités risquées avec des activités risquées et qui ont un résultat inférieur aux prévisions financières.
- **CIMENTO** : l'audit s'est donné un objectif de couverture de 4 ans maximum et a établi des objectifs spécifiques en fonction de la taille des activités : tous les quatre ans pour les plus petites, tous les deux ans pour les intermédiaires et tous les ans pour les plus grands (avec la couverture d'une activité majeure par an. Soit 1 le ciment, 2 le béton, 3 le granulat, 4 l'organisation de pays et les fonctions supports).

Objectif de rotation basé sur la fréquence de revue des entités ainsi que des processus

Certaines directions de l'audit ont défini des objectifs de rotation qui portent à la fois sur une approche par entité et une approche par processus.

- **WALLDISTRIB** : des objectifs de rotation ont été définis par l'audit en termes de couverture pays et de processus. La règle est de couvrir un pays au moins une fois par an. Pour ce qui concerne, les processus, des objectifs plus spécifiques ont été définis par type de processus avec certains qui devront être revus tous les deux ans, d'autres entre deux et quatre ans. Et enfin certains de 4 ans à plus.

- **ELEC** : l'audit s'est donné des objectifs de rotation qui varie de trois à cinq ans pour couvrir des entités puis des processus transverses aux entités qui représentent la moitié des missions du plan d'audit.
- **AERO** : L'audit a défini des objectifs de rotation. Pour les audits d'entité, les entités doivent être couvertes tous les trois à cinq ans. Pour les audits d'activité, le principe va être le même sauf qu'il va y avoir vingt-cinq métiers déclinés par régions. Il y a ainsi un nombre d'activités à couvrir avec un taux de rotation par région.
- **RESTAULIB** : l'audit s'est donné pour objectif couvrir l'univers d'audit en 4 ans. L'univers d'audit étant constitué d'entités et de processus.
- **ENGINICO** : l'audit s'est donné pour objectif de couvrir en trois ans le processus gestion de projet sur l'ensemble des entités du groupe.

Objectif de rotation basé sur la fréquence de revue des risques de la cartographie

- **GAZEO** : des objectifs de rotation ont été établis pour couvrir certains risques de la cartographie groupe. Il s'agit de risques qui seront couverts de façon récurrente chaque année mais sous des angles différents, en fonction des enjeux du moment. Les autres risques de la cartographie devront être couverts tous les trois ans.

Synthèse : les objectifs de rotation prennent une multitude de formes au sein des organisations. Certaines directions de l'audit se sont donnés des objectifs de rotation pour couvrir avec une périodicité donnée des entités. Les critères associés à ces objectifs peuvent être plus ou moins détaillés. D'autres groupes combinent cette approche par entité avec des objectifs de revue par processus ou bien encore des thèmes associés aux risques de la cartographie.

Tableau 37. Plan d'audit – typologie des objectifs de rotation retenue pour le choix des missions

Objectif de rotation
Entités
Entités + critères spécifiques (taille, pays, activité)
Entités et Processus
Risques de la cartographie

Les missions qui découlent d'objectifs de couverture

L'objectif de couverture se distingue de l'objectif de rotation. Il consiste à déterminer le périmètre que l'audit doit couvrir sur une durée déterminée. Alors que l'objectif de rotation vise à définir une fréquence de passage pour couvrir un périmètre donné. Les deux objectifs peuvent se compléter.

VINO : « C'est là où il y a un défaut qu'on essaye un peu de corriger c'est très dur, je pense que partout c'est pareil, c'est qu'entre guillemet les grosses sont sur-auditées. Et d'expérience je sais qu'en général ce n'est pas les gros qui vous plantent méchamment, c'est les plus petit. Parce qu'on dit toujours « oui, mais telle filiale, elle fait un million et demi d'euros de chiffre d'affaires cumulé ». Je vois le chiffre et je dis « oui, sauf qu'elle peut vous planter de 15 millions ».

GAZEO : « Donc moi j'ai des enjeux de couverture. Voilà donc y a plusieurs choses qui interviennent, il n'y a pas que l'environnement de risque. C'est qu'il faut aussi avoir une rotation de couverture de mes différentes entités. Donc sur une période de 3 ans, je veux avoir une couverture d'environ 90% du chiffre d'affaires. Voilà, donc je l'ai par zone géographique. Donc, globalement au niveau du groupe on a 80%. On peut avoir des différences, et on le voit d'une région à l'autre, qui peuvent s'expliquer, d'une façon ou d'une autre. Et on identifie aussi les entités qui ne sont pas couvertes. Parce que ça ne suffit pas là, la règle des 80-20 est parfois bien défailante. [...] Donc ça, c'est l'approche couverture géographique. J'ai mon approche par processus clés, par activité ».

Approche entité (indépendante de leur poids économique)

Certaines directions de l'audit se sont donné un objectif de couverture sur une durée déterminée indépendamment du poids économique des entités revues.

- **SANTEFORM :** l'audit s'est donné pour objectif de couvrir les entités du groupe sur une période de cinq ans. Le document univers d'audit qui liste les entités par pays et par métier a été complété avec la liste des audits réalisés depuis les cinq dernières années afin d'identifier le périmètre qu'il reste à couvrir. Tous les pays qui n'ont pas été couverts depuis cinq ans deviennent prioritaires. Le corporate est peu couvert (seulement 3%).

Couverture en termes de poids économique

La direction de l'audit se focalise dans ce type d'approche sur les grandes entités.

- **CIMENTO** : l'audit a un objectif de couverture des pays au regard de l'importance du montant de ses actifs et de son chiffre d'affaires.
- **MEDIACORP** : l'audit vise à couvrir en priorité les entités significatives en termes de contribution au chiffre d'affaires. Cet objectif est complété par celui qui vise à couvrir un certain nombre de petites entités.

Approche petits pays

L'approche petit pays vise à couvrir des pays qui échapperaient à une approche économique alors qu'ils pourraient être une source de dysfonctionnement.

- **VINO** : l'audit s'est donné un objectif pour couvrir les petites entités qui sont malgré leur taille potentiellement source de dysfonctionnement et de risque de perte.
- **ENGINICO** : l'audit s'est donné pour objectif de couvrir un certain nombre de petites entités éloignées

Approche combinée grandes entités et petits pays

- **GAZEO** : des objectifs de couverture ont été définis afin de couvrir en trois ans environ 90% du chiffre d'affaires du groupe. Et un objectif spécifique a été défini pour les petites entités supérieures à 10 MEUR. Elles doivent être couvertes sur une période de cinq ans.

Approche entités et processus

- **RESTAULIB** : l'audit s'est donné pour objectif de couvrir en 4 ans l'univers d'audit.

Approche en lien avec les risques de la cartographie

- **EQUIPAUTO** : l'objectif de couverture porte sur les risques de la cartographie. L'audit doit couvrir l'ensemble des risques en trois ans. Même si la mission ne couvre pas l'ensemble du risque, l'objectif est d'adresser des thèmes associés aux risques.

Synthèse : les objectifs de couverture sont établis sur la base d'orientation sensiblement différentes selon les organisations. Certains vont privilégier de couvrir essentiellement les grandes entités ou pays. D'autres vont chercher à assurer un contrôle plutôt des petites entités qui peuvent être aussi sources de dysfonctionnement. Certaines correspondent à des approches qui permettent de couvrir aussi bien les petites que les grandes entités ainsi que des processus. Une approche plus rare ressort des entretiens. Il s'agit pour l'audit de se donner des objectifs de couverture des risques de la cartographie.

Tableau 38. Plan d'audit – typologie des objectifs de couverture retenue pour le choix des missions

Objectif de couverture
Approche économique : entités significatives
Approche petite entité / petit pays
Approche entité mixte (petite taille / grande taille)
Approche mixte entités / processus
Approche par les risques

Les missions décidées à l'issue des missions d'audit réalisées dans le passé

Certaines missions peuvent découler de risques identifiés lors d'audits précédents.

Les risques identifiés lors d'une mission d'audit peuvent donner lieu à des missions transverses pour traiter de la zone à risque identifié.

BEAUMAG : « *Et donc il y avait ça comme input, il y avait les fameuses zones de risques qu'on avait identifiées quand on faisait un audit et qu'on voyait qu'à côté ça n'allait pas* ».

Par ailleurs, l'audit peut réaliser des missions de suivi pour s'assurer que le niveau d'avancement des plans d'actions établi par le management en réponses aux recommandations de l'audit à l'issue de sa mission.

RACECAR : « *Mais en gros on avait affiché avec une logique d'effectifs de structure 34 audits sur 75 qui sont des Tops risques et puis après vous aviez quand même 26*

suivis. Les suivis, c'est des audits qui sont faits 1 an maximum après et sur des missions qu'on avait vues avec des feux rouges ou orange. Voilà ».

Les missions qui découlent de demandes spécifiques du management lors de la préparation du plan d'audit.

Les directions de l'audit peuvent répondre à des attentes spécifiques du management en réponse à leurs sujets de préoccupation. Elles peuvent parfois représenter un poids relativement important dans le choix des missions du plan pour certains groupes (SPORTFLEX)

SPORTFLEX : *« Dans ces 50 % d'audits récurrents, il y a la moitié qui viennent des pays. C'est-à-dire que c'est eux qui nous sollicitent en disant : « Nous, on aurait besoin de ça. Que vous iriez sur telle zone, parce qu'on n'est pas très secure là-dessus ».*

EQUIPAUTO : *« Mais eux, souvent quand on leur demande à quoi vous pensez, ils nous parlent d'entité, ils ne nous parlent pas de processus. Et c'est en ça que je vous dis que je n'apprends pas grand-chose parce que les entités ! Voilà il faut aller les voir pour leur demander qu'est-ce que vous voulez, en fait il faut aller vendre un peu l'audit interne et leur dire qu'est-ce que vous aimeriez ».*

Les missions qui découlent de demandes spécifiques du comité d'audit

Certaines missions sont inscrites au plan à la demande des membres du comité d'audit.

MICROPIX : *« Ce qui est important, je ne l'ai pas mentionné mais dans les personnes que nous interviewons, j'ai mentionné le management mais moi j'interview aussi le comité d'audit. Donc chaque membre du comité d'audit est interviewé individuellement, et a aussi la possibilité de fournir des inputs sur la planification de l'année à venir. Souvent les membres du comité d'audit sont dans d'autres boards, donc ils peuvent voir un peu des choses qui sont faites dans d'autres sociétés : alors ils disent qu'est-ce que tu en penses ? C'est quelque chose que tu as prévu ? Et puis voilà, c'est un dialogue que je juge vraiment bénéfique ».*

Les missions qui découlent des résultats d'auto-évaluation du contrôle interne

Depuis le vote des lois de sécurité financière depuis le début des années 2000, il est demandé aux sociétés cotées de rendre compte sur leur dispositif de contrôle interne. Pour ce faire, les grands groupes se sont pour la plupart dotés d'outils d'auto-évaluation du contrôle interne afin

de répondre à cette exigence. Ces auto-évaluations prennent le plus souvent la forme de questionnaires sur des points de contrôle attendus et réputés couvrir des risques sur des processus clés de l'entreprise. Les directions de l'audit disposent ainsi, lorsque ce dispositif est en place, d'informations spécifiques qui peuvent constituer des données d'entrée lors de l'élaboration du plan d'audit.

MULTIMEDSTORE : « *Donc soit ça n'a jamais été fait ou ça fait très longtemps, soit l'auto-évaluation qui a été faite par les opérationnels montre qu'il y a des points de vigilance, ça sert à ça aussi l'auto-évaluation d'accord, c'est les signaux faibles* ».

BATICOSTO : « *Oui, même les autres, parce que typiquement on peut avoir des sujets transverses sur lesquels telles ou telles entités se sont très mal notées en termes de contrôle interne. C'est un critère qui va inciter à y aller* ».

Les missions en lien avec des alertes

Plusieurs directions de l'audit alimentent leur plan d'audit en prenant en compte les alertes ou les suspicions de fraude ainsi que les incidents qui ont pu survenir durant la période. Ces informations peuvent constituer des données d'entrée pour les missions du plan d'audit.

MICROPIX : « *Après, s'ajoutent encore à ce chiffre toutes les missions liées à l'évaluation de cas de fraude ou de suspicions de fraudes et là, les cas, ce n'est pas facile de les quantifier d'une année à l'autre. Je dirais, un ordre de grandeur, entre 10 et 20 cas à traiter par année. En sachant que chaque cas n'amène pas forcément une investigation formelle. Nous, notre processus d'investigation, il a deux phases : il a une première phase d'évaluation du cas durant laquelle on évalue si on a des éléments suffisants, suffisamment précis, suffisamment crédibles, pour ensuite lancer une investigation formelle. Si à l'issue de cette phase d'évaluation, on conclut qu'on n'a pas assez d'éléments, on ferme le cas* ».

NATURELIA : « *On a un reporting fraude, donc tout ce qui a été signalé, il y en a quand même un paquet puisque les gens remontent sans montant minimum. Donc on a, je ne sais pas, une centaine de fraudes qui remontent par an, ça aussi c'est un signal d'attention* ».

L'identification des incidents et des cas ou suspicions de fraude s'effectue selon des modalités différentes selon les organisations. Certains disposent de reporting spécifiques, d'autres sont

dotées de département en charge de traiter ces sujets (compliance, auditeur fraude), etc.

- **SANTEFORM** : l'audit se rapproche du département compliance pour obtenir la liste des alertes et le statut des investigations réalisés ou en cours.
- **MICROPIX** : la direction de l'audit recense les différents cas de fraude qui ont pu être identifiés lors des missions d'audit classiques ou bien des investigations suite à des dénonciations. Elle inclut dans son programme d'audit des thématiques en lien avec le risque de fraude (corruption, états financiers, détournement) qu'elle évolue sur 3 ans afin d'établir une cartographie du risque de fraude.
- **EQUIPAUTO** : le manager d'audit en charge des missions de fraude est une source d'identification des failles en termes de contrôle interne.
- **LUXESTORE** : l'audit dispose d'une base historique des incidents qui sont survenus. En plus des incidents, le réseau contrôle interne remonte des dysfonctionnements qu'il constate sur le terrain.
- **NATURELIA** : un reporting fraude est établi et permet de remonter une centaine d'alertes. Il n'y a pas de limite de montant.

Les missions qui découlent de certaines contraintes réglementaires

Plusieurs groupes (SANTEFORM, MICROPIX, PETROLIUM) parmi les répondants sont soumis à la loi Sarbanes Oxley (ou l'étaient jusqu'à une date récente comme NATURELIA). Un certain nombre de missions d'audit doivent être réalisées pour répondre aux exigences réglementaires. Il s'agit de missions d'évaluation du niveau de contrôle interne relatif aux processus financiers.

NATURELIA : « Nous on a été coté aux Etats-Unis jusqu'à la très récemment, en fait jusqu'au mois de Mars dernier. Donc il y avait des obligations réglementations assez fortes liées à l'évaluation du contrôle interne ta, ta, ta. Et plus les responsabilités qui pesaient sur les dirigeants, ce qui a fait que le domaine financier était privilégié à l'intérieur de l'équipe. Donc si on a en arrière-pensée la gestion des risques, enfin on s'est très focalisé quand même sur les risques financiers ».

Les missions de suivi des plans d'action établis dans le cadre des processus de gestion des risques.

Dans le cadre du processus de gestion des risques, une fois la cartographie établie, des plans d'actions sont fixés par le management afin de réduire l'exposition aux risques. L'audit peut réaliser des missions de suivi de ces plans d'actions pour traiter des risques de la cartographie.

RACECAR : « *Ou alors vous avez à faire à un niveau de maturité où on a bien identifié le risque, on a identifié ses composantes, on sait le décrire, etc. Et là vous avez une série de plans d'action qui sont à la main d'une direction ou des directions et là on nomme un sponsor et on suit l'avancement de ça* ».

Les changements liés à l'organisation et/ou au processus

Les changements d'organisation et de processus (la mise en place d'un service partagé, la mise d'un nouveau système d'information) sont décrits par les directeurs de l'audit comme étant potentiellement sources de dysfonctionnement. Lors du processus d'élaboration du plan d'audit, ces changements peuvent motiver l'inscription de missions d'audit au plan. Le recensement de ces changements pour la majorité des groupes interrogés lors des entretiens de préparation du plan d'audit. Un directeur de l'audit (NATURELIA) complète les entretiens avec les informations issues du questionnaire d'auto-évaluation du groupe qui prévoit de les remonter.

Changements internes à l'organisation susceptibles impacter le bon fonctionnement des activités

FROMAGO : « *Non, les audits pays, c'est indépendamment des risques. On a, si vous voulez, dans tous nos métiers d'audit, on couvre l'activité normale. Là c'est, j'avais mon plan, j'avais tout à l'heure mon Excel de plan. J'ai une colonne avec des missions pays. Donc là, c'est l'historique, celle de 3 ans. Enfin bon, plus, je rajoute la Turquie qui l'an dernier est passée sous SAP. Je rajoute les US où on a ouvert une usine, il y a un an et demie. Enfin, voilà, vous voyez un peu d'opérationnel et puis, ma bonne Angleterre qui n'a pas été visitée, ma bonne Allemagne qui a un changement de GM et qui en plus, n'a pas été visitée depuis un certain temps, bref. Donc là, il y a de l'historique, il y a de l'intelligence. Je veux dire, là encore, je n'ai pas tous les moyens* ».

Changements internes comme externes à l'organisation susceptible d'impacter le bon fonctionnement des activités

MICROPIX : « *S'il y a eu ou si on est au courant de changements organisationnels qui pourraient impacter l'activité* ».

Les activités cœur de métier qui sont jugées comme incontournables

Le cœur de métier est identifié par certaines directions de l'audit comme devant être audité indépendamment du niveau de risque.

MULTIMEDSTORE : « *Donc et puis autre chose même si je n'ai pas des risques significatifs au niveau du groupe dans les magasins, dans mes incontournables du plan d'audit, je ferai toujours des audits magasins. Je ne peux être une direction de l'audit d'un groupe de retail et ne plus faire d'audit de magasins. Même si j'ai un vol ou un risque qui est faible, je dois continuer* ».

LUXESTORE : « *Une vingtaine de maroquineries, je dis que moi je vais en faire deux chaque année pour savoir comment ça se passe. Et pour moi en termes de directeur de l'audit et des Risques sur un métier principal du groupe, je ne peux pas dire je ne suis pas allé, donc j'y vais quand même* ».

Les outils spécifiques d'analyse et de reporting

Parmi les groupes interrogés, plusieurs directions de l'audit se basent sur l'exploitation d'indicateurs de gestion spécifiques afin d'identifier des entités à auditer.

- **DISTRIMART :** l'audit s'est doté d'un outil d'analyse de données (de type « data mining ») qui lui permet de ressortir sur une base annuelle des indicateurs d'anomalies sur certains processus transactionnels (RH, achats et ventes). Il s'agit par exemple du nombre de commandes reçues sans facture ou qui ont fait l'objet d'une commande de régularisation. Ces données sont destinées à identifier des écarts types importants par rapport à la moyenne et donc à les investiguer.
- **NATURELIA :** l'audit exploite les reportings financiers ainsi que le reporting juridique qui retrace les contentieux. Selon le directeur, une entreprise qui présente des résultats financiers difficiles à comprendre combinés à des contentieux est un mauvais signal.
- **MULTIMEDSTORE :** l'audit identifie les magasins à couvrir notamment sur la base des indicateurs et des résultats (perte importante, performance opérationnelle, vol, sécurité, ...).

Synthèse : les missions identifiées par la direction de l’audit sont issues pour partie de la cartographie mais aussi de critères spécifiques qu’elle a définis. Parmi ces critères les objectifs de rotation et de couverture sont communs à la majorité des groupes interrogés. Il est important de noter l’application de ces critères se traduit par des spécificités au sein de chacune des organisations.

Tableau 39. Plan d’audit – principaux critères de choix des missions d’audit

Missions d’audit	
Issues des risques de la cartographie	Issues d’autres critères
	Rotation (entités, processus, thème)
	Couverture
	Demandes spécifiques du management
	Demandes spécifiques du Comité d’audit
	Résultats de l’auto-évaluation du Contrôle interne
	Contraintes réglementaires
	Cœur du métier : les incontournables
	Changements organisationnels / processus
	Analyse d’indicateurs spécifiques
	Alertes

4 - 2 4 LA SELECTION DES MISSIONS D'AUDIT ET L'ELABORATION DU PLAN D'AUDIT

La sélection des missions d'audit parmi la liste des missions d'audit « possibles » identifiées en amont suppose de mettre en œuvre un processus de hiérarchisation des sujets. Cette hiérarchisation et cette sélection se font à l'aide de critères spécifiques aux organisations.

4 - 2 4 I LE PROCESSUS DE HIERARCHISATION DES MISSIONS

Présélection des sujets sur la base des échanges avec le management avant de le soumettre pour validation finale.

GAZEO : *« Et du coup on arrive à voir un champ possible comme ça, et on doit le réduire comme ça. On doit faire une sélection. Donc ça passe par un tamis. Donc on a cent sujets, en sachant qu'on a au niveau Corporate une trentaine de missions par an, donc du coup on réduit déjà de cent à oui peut être quarante ou cinquante quand on passe au niveau du Comex. On rencontre individuellement chaque membre du Comex en disant « bon bah voilà, sur votre zone ou sur votre activité, voilà ce qu'on vous propose ». Et c'est là où ils nous disent « oui, d'accord ! Mais moi j'aurais bien aimé ça. Ou en termes de priorité ça c'est trop tôt, je vois plutôt l'année prochaine parce que notre problématique elle n'est pas encore mûre donc vous allez arriver trop tôt ».*

WALLDISTRIB : *« Alors et là vous voyez, juste avant que vous arriviez, j'étais en train de regarder les discussions avec les Exec que je vais réaliser, que je vais faire dans les jours qui viennent. Alors il y en a un certain nombre je vais leur dire « tiens, j'ai pensé à ça chez toi », ils vont me dire « ah c'est super merci ! » Et puis d'autres pour me suggérer des pistes, des pistes peut-être sur des choses nouvelles, sur des morceaux d'activité qui sont en train d'évoluer qu'on n'aura peut-être pas vu ou peut-être pas pondérés comme eux le voient. Donc c'est un mélange et je ne peux pas vous dire je pondère ça comme ça, comme ça. C'est à un moment donné il y a une réflexion qu'on essaye de faire la plus honnête possible et la moins entre guillemet politique possible pour avoir cette liste. Et puis après bah on s'organise en fonction ».*

Le degré de choix donné aux managers lors de ce processus de présélection est variable selon les groupes. Il peut consister à soumettre en partie ou intégralement le choix des missions potentielles identifiées par l'audit.

Liste intégrale des missions d'audit identifiées soumise au choix du management

- **VEHICAR** : les managers de Régions et/ou de Métiers qui expriment des demandes de missions doivent les classer par ordre de priorité de trois à un. L'audit ne retient que les missions notées 3 (prioritaires). Chaque membre du Comité Exécutif Groupe (DRH, Finance, ...) priorise de nouveau la liste des missions qui remonte de leur équipe, c'est-à-dire qu'il en supprime et en rajoute de nouveaux qu'il note de 3 à 1 pour constituer la liste finale.

Liste des missions d'audit identifiées partiellement soumise au choix du management

- **CIMENTO** : deux listes sont présentées successivement aux CFO puis au CEO pour la sélection des missions d'audit. La première est la liste des missions d'entité qui découlent des objectifs de rotation. La seconde est la liste des missions de processus ou de projets qui résultent des entretiens. Cette dernière contient un nombre plus important que la capacité de l'audit afin de permettre un choix. La liste présentée au CFO est mise à jour avant d'être soumise au CEO.
- **GAZEO** : pour le plan d'audit corporate, l'audit fait une présélection des 100 sujets identifiés lors des entretiens pour arriver à une cinquantaine de sujets à soumettre au COMEX. Une fois cette liste établie, l'audit rencontre individuellement chaque membre du COMEX afin d'arriver sur la base d'un échange à la sélection de 30 sujets d'audit pour le plan annuel.
- **FROMAGO** : le choix des missions thématique fait l'objet d'un échange lors des entretiens. Le critère retenu reste le taux d'avancement des plans d'action en lien avec la cartographie des risques opérationnels.

Présélection des sujets en fonction des ressources limitées de la direction de l'audit

RACECAR : « *Sauf que nos effectifs, comme vous voyez la tendance un peu partout, se réduisent aussi, l'audit n'est pas épargné. Donc on est obligé d'ajuster cette année et puis l'année qui arrive, on va être obligé d'ajuster cette proportion d'audit Top risques parce que c'est consommateur d'avantage de ressources vu qu'ils sont plus compliqués. Certes plus intéressants pour la direction générale, aussi plus consommateur de ressources intelligentes. Les ressources sont rares donc on doit faire*

des audits autrement pour aussi couvrir l'autre composante, l'autre donnée d'entrée qui se base sur l'univers d'audits récurrents, c'est-à-dire le truc classique ».

VINO : *« Bon gré mal gré, ce n'est pas parfait si j'avais cinquante personnes à ma disposition avec des avions, ça serait faisable ».*

La limitation des ressources est un élément qui impacte le nombre de missions que l'audit peut réaliser au cours de l'année.

- **AUTOCAR :** le nombre de mission est induit par la capacité en jours homme de l'équipe d'audit (à savoir cinq personnes). L'année précédente, le plan prévoyait 10 missions, cette année il en prévoit huit, compte tenu du fait qu'il manque une ressource.
- **VEHICAR :** la liste des missions notées qui est présélectionné par le Comité Executif Groupe, une fois établie, est soumise aux deux directeurs généraux du groupe qui doivent sélectionner 8 missions par secteur d'audit et les classer de nouveau par ordre de priorité. Les secteurs d'audit qui sont au nombre de six ont chacun une capacité de 8 missions par an.
- **MULTIMEDSTORE :** il est difficile selon le directeur d'assurer un niveau de couverture satisfaisant avec des ressources limitées (trois personnes).
- **VESTIMOD :** l'audit ne compte que deux personnes pour couvrir un réseau de plus de 4000 magasins.

Présélection des sujets en fonction du niveau de maturité des dispositifs et des référentiels de contrôle.

MULTIMEDSTORE : *« Alors comme moi je suis parti de zéro il y a cinq ans et tu vois et tu vois la première version c'était avril 2012, il a fallu construire les règles, après il a fallu les faire auto évaluer, puis après j'ai commencé à les auditer. Donc il a fallu que je construisse des programmes de travail. Les premiers datent de début 2013, donc maintenant on a des programmes de travail. Mais la logique est la même, on part de ces règles qui ont des risques sous-jacents et puis à l'intérieur on a des tests, et où on a, oui des tests, des demandes de documents qui justifient que les contrôles sont bien en place ».*

Présélection des sujets au regard de la couverture des risques par les autres fonctions contrôlantes de l'organisation.

L'audit se coordonne avec les autres fonctions contrôlantes au sein de son organisation ainsi qu'à l'extérieur (commissaires aux comptes notamment). Ceci dans le but en principe d'assurer une meilleure couverture des risques et de limiter les doublons.

SANTEFORM : « *Et vous verrez que l'on a aussi une approche qui est propre à l'audit et qui vient compléter la partie qui sort de l'ERM. Donc, j'avais dit que je faisais un mapping entre les risques génériques et notre process model et les organisations. Après, dans cet exercice de mapping, il y a une autre dimension maintenant que j'ai intégré récemment, c'est que j'identifie quelles sont les fonctions au sein de la société qui donnent de l'assurance par rapport à ces risques. En fait, on est dans une société où, en plus de l'audit interne, il y a d'autres fonctions qui donnent de l'assurance par rapport à certains risques. Pour les nommer, on a notre département Qualité, on a notre département Environnement Santé Sécurité, on a le département qui a la responsabilité du programme SOX, on a le département Sécurité (mais là, plus la sécurité physique, où Sûreté si j'utilise le terme français), et puis on a l'auditeur externe aussi. Donc là, ce que l'on fait avec cet exercice, c'est d'identifier quelle fonction fournit de l'assurance par rapport à quel risque ».*

L'influence du rattachement de l'audit sur les orientations du plan d'audit

Le niveau hiérarchique auquel est rattachée la direction de l'audit peut avoir une influence sur le choix et la nature des missions d'audit.

MICROPIX : « *Je pense que le rattachement, il a définitivement un impact. Moi, je veux dire avant que j'arrive ici, le rattachement a été à la compliance et avant le rattachement était à la Finance. Donc, depuis que j'ai repris, le focus il a changé de manière significative. Alors que dans le passé le département était avant tout concentré sur des thématiques plutôt finance ou conformité, là on est parti sur des domaines beaucoup plus opérationnels voire stratégiques ».*

GAZEO : « *Donc aujourd'hui j'ai un plan d'audit qui est construit à trois niveaux. Donc le plan groupe qui traite des enjeux, des systèmes de maîtrise des risques, donc ceux-là. Donc je vais auditer tous ces sujets-là. Voilà ce qui remonte dans la Carto et*

ce sont les sujets qui intéressent évidemment la direction générale, le comité d'audit et le Comex. Au niveau des zones et des entités locales, je suis essentiellement focalisée sur des enjeux de contrôle interne. Et des processus qui sont généralement des grands processus clés par activité, qui eux, sont revus sous pilotage du Corporate. Donc finalement, j'ai une fusée à plusieurs étages, que je spécialise par niveau en fonction de mon client. Où est mon client, à qui je dois rendre compte et à qui ça va être utile ? Si je devais faire un audit de mon activité en Thaïlande depuis Paris, il va falloir que j'interface avec la zone Asie Pacifique basée à Shanghai, avec le cluster d'Asie du Sud Est qui est basé à Singapour, tout ça piloté depuis ici, ce n'est pas très efficace ».

Synthèse : dans le cadre du processus d'élaboration du plan d'audit, une liste de missions est établie. Celle-ci fait l'objet d'une hiérarchisation pour déterminer les missions qui seront finalement retenues au plan d'audit. Nous avons identifié un certain nombre de facteurs qui impactent ce processus de hiérarchisation.

Tableau 40. Plan d'audit – critères de hiérarchisation des sujets

Hiérarchisation des sujets d'audit avant de les soumettre à validation

- Avis du management (entretiens intermédiaires)
 - Ressources et capacité de la Direction de l'audit
 - Niveau de maturité des dispositifs de contrôle
 - Niveau de couverture du risque par autres fonctions contrôlantes
 - Niveau de rattachement de la Direction de l'audit
-

Une fois que la direction de l'audit interne dispose de son univers d'audit et de l'évaluation des risques, elle met en œuvre un processus de présélection afin d'identifier une liste de mission qui sera soumise à la validation du management pour le plan d'audit. Le processus de sélection amène ainsi à retenir certains types de sujets et en exclure d'autres. Parmi les critères de sélection, nous avons notamment noté le critère d'auditabilité. Nous verrons donc dans cette section quels peuvent être les différents facteurs qui peuvent amener à exclure certains sujets.

Le critère d'auditabilité est un filtre qui amène à exclure certaines missions et certains risques du plan d'audit

Les directeurs de l'audit identifient des risques qu'ils qualifient de non auditables. Cette notion d'auditabilité se traduit sous différentes formes.

VEHICAR : « Voilà donc il y a beaucoup de sujets vous voyez qui ne s'auditent pas. [...] Vous voyez, la baisse de profitabilité des pièces de rechange, je veux dire, ça ne s'audit pas, c'est un sujet de performance. Clairement, bon on sait bien qu'il y a une perte aujourd'hui chez VEHICAR du business après-vente qui était très fort. Ça ne s'audit pas je veux dire. Pourquoi ça baisse parce que je veux dire c'est vraiment une analyse économique. Ça baisse parce que de toute façon les voitures, il y a moins de pannes, parce qu'on est chers, il y a plein de gens qui passent à la concurrence. Le diagnostic il est réel, le sujet il est réel, maintenant ce n'est pas un sujet d'audit tel qu'on saurait le faire de, de regarder la perte du business après-vente quoi. A la limite, ça peut être une mission de conseil ou une mission d'organisation mais ce n'est vraiment pas une mission d'audit un peu à la mode contrôle interne de ce qu'on sait faire ».

MEDIACORP : « On va en parler sur des cas concrets, ce qui est toujours très compliqué c'est que l'exercice de cartographie d'identification des risques, c'est toujours très intéressant mais c'est toujours le grand écart entre le risque et le plan d'audit parce que. En tout cas, nous la manière dont on l'a positionné, on va le voir sur des cas concrets, c'est souvent des risques auditables ou facilement transcriptibles dans des plans d'audit ».

Le critère d'auditabilité se traduit de différentes façons mais le point commun à de nombreuses directions d'audit est qu'un risque non couvert par un dispositif de contrôle s'avère difficile à auditer.

Les risques non couverts par des dispositifs de contrôle peuvent être considérés comme non auditables

- **GAZEO** : les scénarios identifiés pour lesquels des dispositifs de contrôle ou des plans d'action n'ont pas encore été établis ne seront pas couverts par l'audit.
- **SANTEFORM** : certains sujets de la cartographie des risques (image et réputation, nouvelles technologies,) sont exclus momentanément du plan. L'audit considère que ces risques ne pourront être adressés qu'une fois que les plans d'action mis en œuvre dans le cadre du processus de management des risques donneront lieu à des objets auditables. Un autre moyen de traiter ces risques est de faire une mission de conseil et non pas d'audit.
- **EQUIPAUTO** : l'audit considère qu'il ne peut pas auditer les risques en soi mais qu'il vise à vérifier que les dispositifs de contrôle existent et s'ils sont appliqués.
- **LUXESTORE** : l'audit arbitre entre des missions de cartographie des risques et des missions d'audit. Lorsqu'elle considère que le sujet est relativement difficile à auditer en lien avec la nature des dispositifs de contrôle, elle décide de faire un suivi des plans d'actions de la cartographie. Il s'agit notamment des thèmes tels que la qualité, la création artistique.
- **CIMENTO** : les risques groupe sont gérés par les membres du COMEX et donnent lieu à des plans d'actions qui pourront être auditables une fois les dispositifs de contrôle en place. C'est notamment le cas pour les grands projets d'investissement inscrits à la Cartographie des risques.

Les risques qui ont comme source des facteurs externes peuvent être considérés comme non auditables

- **MEDIACORP** : les risques de la cartographie qui sont à long terme et des facteurs externes sont difficilement auditables.
- **BATICOSTO** : Un certain nombre de risques de la cartographie ne sont pas couverts par l'audit du fait de leur nature jugée comme étant des risques non auditables. Il s'agit

notamment de risques externes tel que la baisse du marché de l'immobilier, un crédit crunch, etc. Selon le directeur, il est difficile d'auditer ces sujets compte tenu de la difficulté à anticiper les évolutions dans le temps.

- **VEHICAR** : deux tiers des risques de la cartographie des risques sont exclus du fait de leur nature jugée comme étant non auditable (séisme dans tel pays, ...). L'audit estime qu'il n'est pas en mesure de l'auditer. Ces missions ne relèvent pas selon l'audit d'une évaluation du contrôle interne.
- **AERO** : Certains sujets de la cartographie ne sont pas retenus car ils sont considérés comme non auditables. Il s'agit par exemple de l'évolution du trafic aérien, environnement naturel (changement climatique, ...), innovation technologique.

L'univers d'audit qui représente les objets auditables

Le groupe **RESTAULIB** souligne que l'univers d'audit ne comprend que les objets auditables.

Exclusion de certaines missions en raison des compétences des membres de l'audit

LUXESTORE : *« J'ai une limite dans l'exercice de cet audit parce qu'on est censé être la maison qui vend les produits de qualité avec la qualité la plus élevée au monde dans son domaine. Et donc je n'ai pas un auditeur qui serait capable d'auditer le dispositif de qualité de cette nature. Mon critère c'était, oui ça peut être la compétence ».*

VESTIMOD : *« Concrètement, nous, on ne sait pas auditer vraiment du process métier. Je pense par exemple des achats. Les achats tels que c'est fait chez nous, on ne sait pas, on ne saurait pas par quel bout le prendre. On était très, très finance au tout début quand moi j'ai repris le département parce que j'avais cette culture là et que j'avais traité du processus financier et petit à petit on est plus allé sur du logistique et la supply chain. On a appris ça ici. C'est ce qui nous a permis d'aller voir l'entrepôt. On l'aurait pas pu le faire il y a quatre ans par exemple. Après, je ne suis pas [...] on apprend sur le tas ».*

Certains sujets peuvent ne pas être adressés du fait de ses compétences au sein de la direction de l'audit. Ils peuvent néanmoins être couverts par d'autres fonctions contrôlantes ou bien être pris en charge par le management.

- **BATI-F** : l'audit ne fait pas d'audit des projets et des chantiers alors qu'ils représentent les risques majeurs au sein du groupe. Les missions portent sur revues de contrôle interne limitées à sept familles de processus standards.
- **VESTIMOD** : les auditeurs ont un profil d'auditeur financier et n'ont par ailleurs pas de compétences informatiques. Ils font donc peu d'audits métiers et opérationnels.
- **VOLTAGE** : l'audit peut exclure certaines missions pour des raisons de compétence mais s'assure qu'elles sont couvertes par d'autres fonctions expertes.
- **LUXESTORE** : certains sujets sont exclus pour des raisons de compétence. A titre d'exemple la qualité est un sujet sur lequel l'audit considère qu'il n'a pas la compétence. Il s'agit d'un thème couvert à travers les plans d'action de la cartographie.

Exclusion de certaines missions qui sont jugées comme sources de tension au niveau de l'organisation.

BEAUMAG : *« Il y a eu des projets avec des restructurations et tout chez nous ou j'ai dit « bah ça je l'annule parce que un, on est trop avancé dans le projet de restructuration pour que nous on vous apporte une vision supplémentaire et deux, il y a un vrai enjeu social c'est-à-dire que c'est déjà hyper tendu là, c'est sûr que les gens vont se foutre en grève. Donc celui-là je l'ai carrément annulé en disant peut être qu'on le remettra en plan d'audit quand ce sera 100% restructuré et voir si ça marche bien. Mais comme il est à l'heure actuelle, il ne faut plus y aller ».*

Exclusion de certaines missions qui sont jugées comme ne relevant pas du métier de l'audit

BATICOSTO : *« Mais ceci étant, si on considère qu'on ne sait pas faire la mission on va tout de suite lui dire « je ne vois pas bien en quoi est-ce qu'on peut vous aider là-dessus, je ne vois pas ce qu'on peut regarder, etc. ». Si l'audité demande une analyse stratégique d'un marché potentiel on va lui dire ce n'est pas notre métier ».*

Exclusion de certaines missions par l'audit en raison de la difficulté à apporter de la valeur ajoutée et de la crédibilité sur certains sujets.

LUXESTORE : « *Mais même en s'obstinant, à supposer qu'on ait de la compétence, par exemple le processus artistique, non, je n'irais pas auditer ça parce que, comment dire ? Je trouve que pour l'emploi de nos ressources dans un exercice coût/valeur ajoutée. Je ne trouve pas que ça serait le meilleur placement que je puisse faire, avec un gros risque de se faire arakiri au passage, d'accord ?! Avec quelle valeur ajoutée ? Qui je vais mettre là-dessus ? Et en plus encore une fois c'est la maison qui a été classée par Forbes comme la plus innovante, je veux dire. On audite là où on peut avoir une valeur ajoutée sur les sujets où on n'est pas tranquille et où on veut s'assurer qu'il y ait des plans d'actions ». [...] Après il y a la relation que vous avez avec votre Comex et la crédibilité que vous pouvez avoir ou pas sur certains sujets. Est-ce qu'on est prêt à prendre le risque d'aller se vautrer. Donc oui ce n'est pas des mauvaises questions mais ».*

VEHICAR : « *Voilà donc il y a quand même quelques sujets qu'on sait qu'on ne pourrait rien en dire de pertinent. Par contre, que ce soit un sujet de préoccupation et qu'ils aient mis des patrons derrières pour surveiller ça, ce n'est pas choquant ».*

Exclusion de certaines missions en considérant que les risques sont couverts par des plans d'action et des dispositifs existants.

VEHICAR : « *Donc en fait quand on prend ça, soit le directeur des risques nous dit bon là ça sert à rien, il y a un bon plan de traitement, ce n'est pas la peine d'aller voir. Soit de toute façon, c'est un sujet sur lequel nous, on ne sait pas, on ne sait pas traiter ».*

MEDIACORP : « *Après le lobbying vis-à-vis des autorités, du juge, de la réglementation parce qu'il faut se donner les moyens de lutter etc, ce n'est pas nous, enfin on l'audite pas, on en discute et c'est des dispositifs de la carto, on les écrit mais on ne va pas aller jusqu'à auditer est-ce que vous faites bien votre travail quoi. On considère qu'il y a des dispositifs ».*

Exclusion de certains sujets couverts par d'autres fonctions « contrôlantes »

Les autres fonctions contrôlantes sont des fonctions expertes qui prennent en charge l'évaluation de certains risques spécifiques tels que l'environnement, la sûreté, la qualité.

SANTEFORM : « *Donc quand on fait l'élaboration du plan, on partage avec la qualité, HSE et là je donnais l'exemple de ma compliance, ou les commissaires aux comptes aussi car on interagit avec eux plusieurs fois par an dans le cas de la construction du plan pour partager des zones de risques identifiées, avoir une planification des missions. S'il y a une investigation compliance, on ne va pas aller sur le truc et donc on la postpone et on va se coordonner sur l'approche et le planning de ce qu'on doit couvrir* ».

Exclusion de certaines missions « opérationnelles » et qui sont jugés comme relevant de l'expertise

AUTOCAR : « *Alors, son expertise, elle est une bonne généraliste aussi. C'est plutôt des gens qui ont une capacité de réflexion et autre mais effectivement, j'essaie de faire au mieux dans le planning pour voilà, mais à la direction de l'audit aussi, on n'attend pas de nous une expertise poussée, on ne va pas aller regarder particulièrement les graphicas, enfin, nous, on ne fait pas des audits non plus purement opérationnels* ».

Exclusion de certaines missions à la demande du management

FROMAGO : « *Le management dit ça c'est des risques stratégiques, c'est nous qui les prenons. Parce que c'est le moment de la définition du plan strat, on s'en occupe. [...] C'est pour ça que le fait d'avoir des risques opérationnels et des risques stratégiques, les risques stratégiques, globalement, on ne va pas aller faire un audit, pas plus qu'on n'audite pas la [...], on peut auditer la mise en œuvre d'une stratégie mais ne nous mentons pas, en général, c'est la mise en œuvre d'une politique* ».

VESTIMOD : « *En fait, ce qu'il faut savoir sur la Chine, c'est qu'il y a encore trois, quatre ans, je pense que les gens ici ne savaient même pas qu'on avait une entité en Chine, c'était très nébuleux. Ça appartenait, c'était le pré carré de mon chef, donc le fils du patriarche, et on avait aucune visibilité, et quand je dis aucune, on n'en parlait pas, que ce soit la com aux salariés c'est vraiment aucune. Nous, on le savait parce*

qu'on était rattaché là-haut, on savait qu'il y avait quelque chose, mais même nous, on ne nous demandait pas d'aller regarder ».

Exclusion de certains périmètres qui sont liés aux facteurs externes

AERO : « *C'est la notion de couverture, enfin la couverture des risques grâce aux audits, sachant qu'il y a des audits qu'on va jamais faire non plus, parce qu'il y a des sujets qui ne se traitent pas. Pour l'évolution du trafic aérien, c'était en externe ».*

Synthèse : les missions d'audit peuvent être exclues soit à la demande du management, soit à l'initiative de l'audit selon plusieurs critères. Un des critères qui ressort de ces entretiens est la notion d'auditabilité qui renvoie à l'existence ou non de dispositif de maîtrise pour couvrir le risque. Le critère de compétence peut y est indirectement associé.

Tableau 41. Plan d'audit – critères d'exclusion des missions

Critères d'exclusion des missions	
Missions exclues à la demande du management	Missions exclues par la Direction de l'audit
	Critère d'auditabilité
	Compétences
	Climat et tension sociale
	Missions distinctes de l'audit
	Crédibilité
	Capacité à apporter de la valeur ajoutée
	Certains risques couverts par des plans d'actions
	Risques couverts par d'autres fonctions contrôlantes
	Missions d'expertise
	Missions liées à des facteurs externes

4 - 2 5 LA VALIDATION DU PLAN D'AUDIT

La direction de l'audit doit, une fois la liste des missions d'audit établie, la soumettre pour validation à sa hiérarchie mais aussi éventuellement recueillir ses demandes spécifiques.

4 - 2 5 I NIVEAU D'INFORMATION COMMUNIQUEE SUR LES MISSIONS D'AUDIT LORS DE LA VALIDATION DU PLAN D'AUDIT.

Le niveau d'information communiqué pour la validation du plan d'audit peut être plus ou moins détaillé selon les organisations.

WALLDISTRIB : *« Alors après au croisement de cette matrice, on va donner un titre pour que tout le monde le comprenne. Mais ce titre il est suffisamment générique pour nous laisser la main, pour après dimensionner les choses comme on le souhaite. [...] Donc on veille à avoir une intervention centrée sur quelque chose qui a de la consistance par rapport à nos yeux. Ce que je vends dans ces processus-là, ce que je vends reste assez macro. Il y a une idée, il y a une idée derrière mais je ne vais pas trop loin dans le détail. Moi je suis quand même groupe, je ne suis pas contrôleur interne. Si j'étais au niveau d'un pays, je le ferais d'une façon plus fine ».*

MICROPIX : *« Oui, dans mon plan d'audit en fait, je présente quand même après comment les ressources sont déployées et quels blocs organisationnels on va couvrir. Donc, il y a une synthèse de la couverture de la société où je dis on va dédier tant de % aux organisations régionales, tant de % aux organisations « manufacturing », etc. Donc ça, je veux dire cette indication-là, ils l'ont. Après, s'ils veulent aller plus dans le détail, ils l'ont aussi mais c'est plutôt une annexe du document et, en règle générale, on ne le discute pas trop. On n'a pas le temps de le discuter ».*

Le niveau de couverture des risques par le plan d'audit est plus ou moins documenté

VEHICAR : *« Non, on présente tel que je vous l'ai montré, à chaque fois on met la carto et jamais on ne nous a questionnés. Parce que durant les comités d'audit, on le présente toujours rattaché à ça mais ils n'ont jamais dit pourquoi il y en a qui ne sont jamais sélectionnés ».*

BATICOSTO : « C'est-à-dire que vous avez la cartographie, nous on leur explique assez au profondément notre cartographie sur tous les risques, comment ils sont scénarisés etc. Il y a un bon niveau de transparence avec nos administrateurs sur le sujet. Derrière ils ont le plan d'audit. On leurs fait le lien entre les deux. Il n'est pas exhaustif puisqu'il y a plein de risques qui ne sont pas audités. Mais ils ont connaissance des risques, ils ont connaissance des risques audités, et comment on va faire l'audit, sur quel périmètre, sur quel délai puisque qu'on leur dit aussi que sur tel type de risque on va le faire sur 3 ans. Ils savent qu'on s'en occupe, mais ils ne connaissent pas les résultats et pas tout de suite. Est-ce qu'il y a d'autres risques qui ne sont pas adressés par nous ? Probablement. Après c'est vrai qu'il n'y a pas de demandes particulières des administrateurs sur d'autres sujets ».

Certaines directions de l'audit communiquent sur les risques qu'elles n'adressent pas.

Parmi les groupes interrogés, nous avons relevé que certains groupes (**VOLTAGE** et **NATURELIA**) communiquaient explicitement sur les risques qui n'étaient pas couverts par l'audit interne avec les justifications associées.

D'autres directions de l'audit établissent un lien plus implicite entre les risques et les missions d'audit.

- **VEHICAR :** l'audit rattache les missions aux risques de la cartographie afin de créer un lien mais qui est a posteriori. Ce lien est possible car les risques de la cartographie sont suffisamment génériques.
- **AERO :** l'audit présente dans son plan les risques couverts par les missions d'audit. Une présentation est faite l'année suivante en montrant le nombre de recommandations émises par grande catégorie de risques en lien avec l'univers des risques.

L'influence des membres du comité d'audit et du management sur les orientations du plan d'audit.

EQUIPAUTO : « Et puis après donc qu'est-ce qui joue, après j'ai des demandes, par exemple processus en bout de ligne, ça le comité d'audit a demandé puisque c'est arrivé dans une discussion, il y avait eu un problème qualité, des impacts importants, le

directeur général dit voilà, en plus on a une direction qui a mis en place un nouveau processus. Ça serait bien si l'audit interne s'assurait qu'il est bien mis en place etc. ».

CHIMICOR : *« Assez peu, ils ont quelques marottes certainement par référence à ce qu'ils voient ailleurs, ce qu'ils lisent dans la presse etc. d'un coup ils ont une espèce d'impulsion, et ça je le capte. Alors les plans d'audit passent comme une lettre à la poste, à chaque fois j'ai 0 remarque ni du Comex, ni du Comité d'audit. Sur 80 missions c'est presque frustrant, c'est à se demander s'ils le regardent. Les nouveautés que je vais introduire cette année c'est que je vais faire le tour individuel de chacun des membres du Comex pour les obliger à ».*

La validation du plan d'audit par le management et le comité d'audit

Le plan d'audit est soit validé uniquement par l'instance de gouvernance lorsque l'audit lui est hiérarchiquement rattaché ou bien par le management puis le comité d'audit dans les autres cas.

AUTOCAR : *« Le plan d'audit je le fais, je l'élabore à partir du mois de septembre, je le passe en Comex au mois d'octobre et il est validé au comité d'audit de fin octobre, début novembre, ça dépend des années ».*

VEHICAR : *« Oui, après que le CAR se soit adressé au comité d'audit pour approbation, il le valide de façon formelle. Par exemple, c'est ce que je vous montrais tout à l'heure. Donc on lui présente toujours le projet de plan, le bilan, bon maintenant ce n'est plus le projet, en fait c'est le plan parce qu'on voit le comité d'audit avant. Le Comité d'audit est vu deux fois, en amont du PDG ».*

4 - 2 5 2 LIEN ENTRE RISQUE ET PLAN D'AUDIT

Le lien qui existe entre les risques de l'organisation et les missions inscrites au plan d'audit est affiché comme étant plus ou moins fort par les répondants des différentes organisations.

La nature des risques adressés par les missions du plan d'audit peut différer avec celle de la cartographie des risques.

MULTIMEDSTORE : *« On peut dire les missions d'audit, c'est plutôt des risques de contrôle interne ou des risques entité, process qui font partie de notre référentiel de contrôle interne, pratiquement très opérationnel, donc des risques liés aux entités, aux*

responsables des entités qu'on audite ou des responsables de process et des porteurs de process. Mais pas forcément j'allais dire ceux de la direction générale ou ceux d'actionnaires qui pourraient demander des comptes ».

GAZEO : *« On a une autre thématique sur les achats. Donc là, on peut le traiter à plusieurs niveaux. C'est-à-dire que moi je vais traiter les enjeux entre guillemets stratégiques, c'est-à-dire est-ce que j'ai des organisations d'achat entre les niveaux, globales, la fonction globale, les plateformes d'achat zonales, qui s'interfacent bien, qu'elles sont les missions des uns et des autres etc. Moi je le vois d'un point de vue stratégique. D'accord ? Au niveau zone, ils vont aller regarder comment fonctionner les plateformes d'achats en zonale. Et au niveau local, ils vont faire des revues de contrôle interne sur les achats. Et donc du coup je vais traiter ma thématique achat à travers les différents plans. Et j'aurais toutes les couches finalement, qui vont être abordées sur la thématique achat et qui vont répondre aux attentes de mes interlocuteurs à chaque niveau ».*

Un lien faible entre la cartographie des risques et les missions du plan d'audit

VESTIMOD : *« Mais qui est assez macro. En gros, il y a [...] c'est un fichier Excel, il y a 15 lignes. C'est vraiment très, très macro en termes de risque, c'est risque fournisseur. C'est vraiment le plus macro qu'on puisse être, est-ce qu'on a quelques contrôles au-dessus, on est à risque ? on l'accepte ou pas, voilà [...]. C'est une vue d'avion et on ne s'en sert pas aujourd'hui. Elle n'est pas à la base du plan d'audit. Ça fait partie des, des missions de cette année de la mettre à jour et d'avoir un truc un peu plus robuste ».*

VEHICAR : *« Donc la cartographie des risques c'est la cartographie des risques groupe majeurs. Bon c'est des risques très macros, il doit y avoir une vingtaine de risques et comme c'était justement trop macro on avait beaucoup de mal à s'en servir dans, dans les audits. Il a élaboré ce qu'on appelle un univers des risques. L'univers des risques en gros est un peu plus micro et c'est ce qu'on utilise nous dans nos rapports d'audit, voilà. Donc en fait on fait un lien artificiel entre la cartographie des risques groupe et les audits. Artificiel parce que sincèrement je vous dis la cartographie des risques groupe elle est beaucoup trop macro. Et finalement les missions d'audit*

correspondent très peu, on peut rapprocher très peu de missions d'audit à la cartographie des risques ».

Un lien fort entre les missions d'audit tel qu'affiché au plan d'audit et la cartographie des risques.

ELEC : *« Alors nous, ce que l'on fait à la direction de l'audit, on est associés à ces discussions pour la cartographie des risques mais ce n'est pas nous qui décidons là. Par contre, ce que l'on fait c'est qu'on prend en compte ces cartographies des risques, c'est une donnée d'entrée pour notre programme d'audit, sachant que ce que l'on veille à faire, c'est à couvrir, c'est être capable de donner un avis sur chacun des risques du groupe à travers d'un ou plusieurs audits ».*

Un lien partiel entre les missions d'audit tel qu'affiché au plan d'audit et la cartographie des risques.

RACECAR : *« On va dire 25/30 Top risques. En face de ça on a comme donnée d'entrée le plan d'audit, les audits axés Top risques. Une fois de plus pour éclairer une composante du Top risque, pas le Top risque. On ne prétend pas couvrir le Top risque avec l'audit (rire) mais une composante. Et là, sur les années dernières on devait être à, alors après ça dépend comment l'on compte, on était dans les 60% d'audits qui étaient axés un peu Top risque ».*

Des plans d'audit qui sont établis par niveau organisationnel afin de disposer d'un lien plus fort entre des cartographies locales et des plans d'audit locaux.

DISTRIMART : *« Chaque pays élabore le plan d'audit en fonction de ses risques. Là, on voit un peu s'il y a quelque chose a été oublié mais bon, les choses fonctionnent normalement bien. Après l'équipe ici sert à faire les audits qui ne sont pas faits dans les pays parce que ça ne justifie pas, ce sont les métiers spécialisés. Par exemple, il n'y a d'audit informatique dans la plupart des BU parce qu'on fait une ou deux audits informatiques par BU par an, Ce n'est pas nécessaire d'avoir des auditeurs pour faire une ou deux missions, donc on a des auditeurs pour les achats, la finance. Les pays se concentrent plus dans la partie opérationnelle ».*

PETROLIUM : « *Oui parce qu'en fait vu que c'est une organisation par branche qui est bien marquée par des plans d'audit par branche etc. Quelque part on est prestataire de services entre guillemet pour les branches et donc ils s'attendent à ce que on pourrait dire on a un budget d'actions d'audit à leur disposition. Et ils l'attendent et ils comptent quelques fois même sur nous pour faire du contrôle de deuxième ligne de défense sur certain sujet. Regarder le déploiement d'une directive sécurité, regarder des choses assez classiques* ».

Synthèse : le lien entre la cartographie des risques et le plan d'audit est déclaré comme étant plus ou moins fort selon les organisations interrogées.

Tableau 42. Plan d'audit – intensité du lien entre les risques de la cartographie et le plan

Lien entre la cartographie des risques et le plan d'audit		
Lien faible	Lien partiel	Lien fort

Or, les informations communiquées lors des réunions de validation peuvent varier d'une organisation à une autre pour être en mesure d'apprécier le contenu du plan d'audit en lien avec la cartographie des risques.

Tableau 43. Plan d'audit – nature des informations communiquées lors de la validation du plan

Informations relatives à la couverture des risques et de la cartographie		
Non disponible	Peu détaillée	Détaillée
Informations relatives au contenu de la mission		
Peu détaillée		Détaillée
Influence du comité d'audit et/ou du management sur le contenu du plan d'audit final.		
Très faible		Faible

4 - 2 6 LA FLEXIBILITE DU PLAN D'AUDIT

Le plan d'audit une fois validé conserve malgré un certain degré de flexibilité.

Le plan d'audit permet tel qu'il est établi d'intégrer a posteriori un quota de missions non planifiées.

Ce quota varie entre 5 et 20% selon les directions de l'audit.

CIMENTO : *« Alors on se prévoit un peu moins parce qu'on se prévoit une marge de manœuvre pour des sujets non prévus. Donc on prévoit la possibilité de faire 4-5 missions non planifiées. [...] S'il y a un feu qui surgit quelque part, comme on a gardé la flexibilité de. Vous voyez la semaine prochaine on va en Ukraine, ce n'était pas prévu mais on avait gardé cette flexibilité ».*

LUXESTORE : *« C'est-à-dire que si j'ai un business, si j'ai un sujet en particulier qui remonte comme étant particulièrement problématique, je peux déclencher, ajouter un audit parce que mon plan d'audit, il est mobile et je peux l'ajuster ».*

Le plan d'audit permet tel qu'il est établi permet une flexibilité sur le choix du périmètre qui sera revu lors de la réalisation de la mission.

Le niveau d'information associé aux missions lors du processus de validation du plan permet d'avoir de la flexibilité sur le choix du périmètre qui sera effectivement revue.

LUXESTORE : *« Tous les ans en Novembre, je présente au comité d'audit et des risques mon projet de plan d'audit. Alors par rapport à d'autres groupes, j'ai noté que j'étais quand même assez high level. [...] Je leur dis, je leur avais dit voilà il y aura contrôle de fin de ligne, il y aura projet de R&D, tout ça. Et puis après pour les entités, c'est là où je dis on fait un focus, voilà les zones géographiques qu'on voudrait faire, je leur dis on fera tant de services partagés finance, tant de. Voilà mais je ne rentre pas, je ne dis pas c'est telle et telle entité. Je ne donne pas la liste des entités parce que ça, ça peut être amené à bouger ».*

Le plan d'audit peut être réactualisé en cours d'année

ELEC : *« Donc là, on a notre programme d'audit et chaque fois qu'on refait le programme, tous les six mois qu'on passe au comité d'audit, on vérifie que l'on a bien*

une couverture correcte de la cartographie des risques. En fait, c'est ce document-là, vous voyez. On dit : « Ben voilà, les méta risques couverts par nos audits sur la période 1^{er} vague 2012 jusqu'à 4^{eme} vague 2014 ».

Synthèse : le plan d'audit est construit de façon à conserver un certain degré de flexibilité.

Tableau 44. Plan d'audit – nature de la flexibilité du plan d'audit

Flexibilité du plan d'audit
Quota de missions pour mission non planifiées
Périmètre générique (latitude pour le choix des entités/processus)
Réactualisation durant l'année

4 - 3 L'ELABORATION DU PLAN DE MISSION

Rappel sur les normes :les normes professionnelles pour la pratique professionnelle de l'audit interne requièrent (norme 2210.A1) que les auditeurs internes procèdent à une évaluation préliminaire des risques liés à l'activité soumise à l'audit. Les objectifs de la mission doivent être déterminés en fonction des résultats de cette évaluation.

4 - 3 1 LA PREPARATION DE LA MISSION ET L'ANALYSE PRELIMINAIRE DES RISQUES

Cette section présente les modalités de recueil d'information des auditeurs internes en durant la phase de préparation de leur mission.

Les entretiens constituent une première source d'information afin de préparer l'analyse des risques. Ces entretiens sont réalisés à différents niveaux et selon différentes approches en fonction des organisations.

Une approche de type « Top Down » pour recueillir les préoccupations du management

Les entretiens préparatoires qui sont menés avec une approche top down visent à interroger le management du siège ainsi que la hiérarchie de l'entité auditée.

PETROLIUM : « *La plupart du temps il s'agit d'évaluer les dispositifs du pilotage. Donc en fait on va s'appuyer sur ce qui existe au niveau du siège et des sièges de branche comme dispositif de maîtrise du sujet. Et quelle remontée d'information ils ont ? Qu'est-ce qu'ils en font ? Est-ce qu'ils ont une mécanique qui permet de faire progresser les gens par des plans d'action, enfin comment c'est. Et on va rendre compte de tout ça de manière à ce qu'on voit déjà les secteurs où ça va bien ou pas. Mais aussi permettre aux uns et aux autres de prendre des idées en regardant des choses intéressantes qui ont été mises en place dans la branche d'à côté, c'est le côté un peu positif* ».

BATIMODERN : « *Non parce que ça, on doit avoir une confidentialité avec eux. Donc les entretiens préalables c'est plutôt avec le management ici. Alors quand je dis « siège » j'exagère en fait c'est les sièges de tous les métiers, parce que quelque part on n'audit pas souvent un métier* ».

Une approche de type « Bottom Up » pour recueillir les risques du terrain

Les entretiens préparatoires qui sont menés avec une approche bottom up visent à interroger le management de l'entité auditée ainsi que ses collaborateurs.

BATI-F : « *Donc on va plutôt s'attacher à partir, à faire du bottom up quoi mais dire mais vous dites-moi vous ? Parce que quand on va faire les entretiens, on va voir des ouvriers, on va aller voir des conducteurs de travaux, on va aller voir des secrétaires comptables. On ne va pas aller voir la tête qui va nous dire tout va bien. On va dire, c'est quoi vos risques, qu'est qui vous empêche de dormir. [...] Et je ne vois pas comment je peux savoir parce que même si je travaille plus de temps à préparer, à un moment ça reste, on est dans un métier faut bien comprendre, il faut bien comprendre ça, dans un métier de BTP, un métier d'homme. Il n'y a pas d'outils industriels, donc tous les reportings, les indicateurs ils ne traduisent pas forcément la réalité quoi. On est vraiment dans un métier de management où entre deux résultats, on ne peut pas savoir s'il y en a un qui est plus à risque que l'autre. Donc il faut aller sur le terrain, il faut voir, c'est compliqué quoi ».*

EQUIPAUTO : « *Alors ce qu'il y a, c'est entité mais c'est quand même entité au sens large. Parce que pour un audit, là vous voyez par exemple pour le processus de fin de ligne, on est quand même allé au cœur du groupe, au siège de chaque Produit Groupe pour demander comment vous avez fait pour déployer. Notre audit il a quand même deux niveaux : on va à l'entité, mais on va un peu au-dessus de l'entité, c'est comment le processus est supervisé. Ça, on l'oublie quand même jamais lors de nos audits. Donc ça, l'entité toute seule indépendante, c'est l'entité et le processus de supervision qu'a mis en place le groupe sur un audit transverse ».*

Une approche de type « Mixte » pour recouper la vision du management avec celle des membres de l'entité auditée.

Les entretiens qui reposent sur une approche mixte consistent à interroger le management du siège ainsi que la hiérarchie de l'entité auditée. Afin de compléter ces entretiens, l'audit peut interroger le management et les membres de l'entité auditée.

RESTAULIB : « *La première journée, en fait on fait la première journée, dans les autres livrables, il y a l'opening meeting. On a carrément des slides où on vient*

présenter notre vision des risques telle que discutée dans le RPM (Risk Planning Memo) en rencontrant les managers au-dessus. C'est la question que vous posez. Là, on la confronte à l'entité qu'on audite et souvent les gens vont changer leur vision, notre vision, rajouter des choses, en enlever. Et donc, vous avez raison, la première semaine, on va un peu s'adapter et modifier des choses. Pas couvrir des choses et en rajouter, parce qu'on a une demande qui est finalement extrêmement risquée que personne n'avait vu jusqu'à maintenant et que les locaux voient bien ».

GAZEO : *« Il y a des regards croisés. C'est-à-dire que pour définir, pour cadrer la mission, ce n'est pas qu'avec le directeur général de l'entité que l'on va aller auditer. On va aussi interviewer le contrôleur de la zone, donc des points d'entités, par exemple. On va interviewer peut-être la fonction globale qui sera revue donc soit les achats ici, soit la finance groupe. Alors vous voyez, il va y avoir des regards croisés ».*

En complément des entretiens, les auditeurs mobilisent d'autres ressources afin de réaliser leur analyse de risque spécifique à la mission.

Les informations qui remontent par le contrôle interne

L'audit mobilise les résultats des auto-évaluations du contrôle interne et des tests de revue réalisés dans le cas de sociétés soumises aux exigences de la loi Sarbanes Oxley. Dans d'autres cas (LUXESTORE), certains groupes disposent d'un réseau important de contrôleurs internes qui peuvent alimenter l'analyse de risque du fait de leur proximité avec le terrain.

CHIMICA : *« Alors, pourquoi j'y ai pensé, pourquoi ? Parce que c'est des problématiques qu'on a par ailleurs détectés par le contrôle interne ou détecté, principalement détecté par les contrôles interne en termes de fiscalité, de prix de transfert ».*

SANTEFORM : *« Sur la finance, ce que je voulais ajouter c'est qu'on a aussi le dispositif 'SOX', un dispositif continu de tests avec des remontées des tests dans une seule, enfin ici tout est centralisé. Ils ont accès à tous les tests des filiales ».*

L'historique des audits passés

L'audit peut se baser sur les conclusions et les recommandations d'audit émises ainsi que sur le suivi des plans d'action associés s'il s'agit d'une entité ou d'un thème qui a déjà été audité.

PETROLIUM : « On a des informations sur l'entité, on est déjà souvent passé quelque temps avant. Donc on a un historique d'audit, on a Sarbannes Oxley. Et l'historique d'audit nous donne l'historique du suivi, la façon dont la mise en œuvre des plans d'action s'est déroulée. Parce que c'est tout ça, On a ça chez nous donc on a des connaissances ».

Les indicateurs issus des systèmes d'information

Les auditeurs peuvent recourir à un certain nombre d'indicateurs de gestion.

VESTIMOD : « Alors là, on a un outil de reporting qui s'appelle « Store Loss Prevention », qui est une espèce de « requeteur » informatique. Donc en fait ça va piocher dans notre système d'information un certain nombre de data et ça va les agréger dans des indicateurs financiers par magasin, type le nombre d'écarts de caisse par magasin, le nombre de remise en banque par mois. Et là-dessus, on a sélectionné les magasins qui ressortaient en rouge, donc avec des indicateurs mauvais ».

Une direction de l'audit (WALLDISTRIB), des outils spécifiques à l'audit ont été mis en place afin d'exploiter les données relatives aux transactions sur les cycles achat, vente et comptabilité. Cet outil permet aux auditeurs de disposer pour chacune des entités auditées d'informations relatives aux transactions identifiées comme étant en anomalie.

Les informations et rapports établis par les autres fonctions contrôlantes

L'audit peut disposer d'un certain nombre de rapports établis par des fonctions contrôlantes qui peuvent être soit internes à l'organisation ou bien externes (commissaires aux comptes notamment).

SANTEFORM : « Six semaines avant la partie fieldwork, je suis en charge en tant que global coordination d'envoyer des demandes d'information officielles et formelles à toutes les 2eme lignes de maitrise que je vous évoquais tout à l'heure. Je peux vous montrer un exemple. J'envoie à HSE, à la qualité, à la sécurité, aux assurances, à la compliance, aux internal control, en disant voici les missions que nous allons nous vous remercions de revenir vers nous avec pour ce qui ont un département d'audit expert leurs derniers rapports et les plans d'action. Et pour les autres fonctions que ça soit les achats ou autres, les éléments qui les concernent, la dernière business review qui a été fait et les points d'attention qui leurs semblent importants pour nous de regarder ».

La collecte de documents type à des fins d'analyse

BATI-F : « On a une trentaine de documents type. C'est des documents financiers, des organigrammes, des reportings. C'est des reportings sur les accidents du travail, sur toutes ces thématiques-là. Les statistiques sur les prises d'affaires, sur les départs, les licenciements sur les RH, tout un tas de choses quoi ».

L'échelle de temps considéré par les auditeurs dans le cadre de leur analyse de risque est variable selon les organisations.

Une prise en compte des enjeux à court terme

PETROLIUM : « Dans les audits d'entité généralement on est quand même sur un horizon de temps limité. On ne parle pas de restitution des sites. Par contre la restitution des sites, elle se posera bien un jour. Donc la question c'est de savoir s'il y a des choses à documenter aujourd'hui fondamentalement et qui seront nécessaires plus tard. Auquel cas on pourra faire une remarque sur le sujet mais je dirais que c'est assez rare quand même je trouve que les auditeurs raisonnent en se projetant dans le temps comme ça ».

ELECTROSTORE : « Pour le moment oui puisque si vous voulez le problème du retail, c'est 10% de stratégie, 90% d'exécution. Donc si vous voulez, voilà on reflète à travers nos ressources cette problématique-là. Donc on ne va pas auditer, on ne change pas tous les jours l'organisation des fonctions transverses. En revanche tous les jours on va se préoccuper de savoir si nos magasins font correctement le boulot quoi ».

Une prise en compte des enjeux à court et moyen terme

DISTRIMART : « C'est trois ans. Après, c'est de la futurologie ».

RESTAULIB : « On est vraiment sur des maximums de deux ans à venir. Du coup, on va lui redemander, on refait un risk assessment mais à niveau beaucoup plus bas. Et on va leur demander quels sont les risques identifiés de ne pas atteindre ses objectifs que vous vous êtes fixés. Soit on le fait par le biais des entretiens, soit on le fait par le biais nous-même de notre connaissance ».

GAZEO : « *Oui, mais ça dépend. C'est intéressant comme exemple parce que vous pouvez certes évaluer en interne à court terme mais en interne moyen terme. Dans l'analyse de risque, ce que je demanderai à mes auditeurs, c'est de réfléchir si la performance d'efficacité qui est donnée à court terme n'a pas d'impact sur le moyen terme. Alors ça, si vous voulez, quand je dis que je veux qu'ils me fassent de l'audit au-delà de la conformité, c'est ça, c'est qu'ils réfléchissent bien à leur environnement global et qu'ils ne se focalisent pas que sur du contrôle interne classique pour dire vous voyez j'ai manqué le match et voilà* ».

La dimension savoir-faire en matière d'analyse des risques se traduit à travers plusieurs dimensions

La connaissance des métiers de l'entreprise

La connaissance des métiers et des activités est citée par plusieurs directeurs comme un élément nécessaire pour le bon accomplissement des missions d'audit.

PETROLIUM : « *Sur l'analyse des risques en semaine de préparation on a à progresser, ça on ne peut pas se le cacher, on met l'accent, l'IFACI (l'Institut Français de l'Audit et du Contrôle Interne) qui nous le met à chaque évaluation, etc. Donc j'ai l'impression que c'est mieux fait, j'ai vu M. X qui m'a dit oui, on trouve ça sur vos analyses de risque, on trouve que ça progresse. Ceci dit, on a prévu au mois de Mai de faire un petit atelier pour reformer tout le monde sur comment on s'y prend pour faire une analyse des risques pertinente en semaine de préparation. Mais c'est un mix. Moi je ne me sentirais pas confortable d'avoir des managers qui ne connaissent pas du tout la Branche. Parce que quelque part le fait d'avoir vécu, on voit quand même bien les risques* ».

SANTEFORM : « *C'est d'avoir des nouveaux managers expérimentés avec plus de dix ans d'ancienneté. Quand je parle d'ancienneté ce n'est pas de l'audit, c'est pharma, métier, business accument on appelle ça chez nous, et du coup la séniorité. On essaye d'avoir comme vous pouvez le voir un truc séniorité qui est à près de 60% [...]. Et enfin on gère quatre choses : professionn background et comme vous allez le voir il y a les anciens external auditors, j'ai 21% d'opérationnels. Qu'est-ce qu'un opérationnel. C'est un gars qui a fait de la supply chain, de l'industriel, du commercial, des achats,*

un certain nombre de choses. J'ai 12% qui ont une expérience financière avant, d'internal audit, et j'ai 7% pour consulting ».

La connaissance du métier de l'audit interne

FROMAGO : *« On leur demande d'abord de sélectionner par rapport à une approche risque. Et effectivement, bah après, de toute façon, c'est toujours pareil dans tous les métiers. Quand on change de fonction, il faut se former à sa nouvelle fonction. Et ce n'est pas cinq jours de stage à l'IFACI qui vont changer la personne ». Et en plus, il faut se poser la question quand on recrute les personnes : est-ce qu'ils ont vraiment envie de faire de l'audit interne.*

La mise en œuvre d'une approche par regards croisés au sein de l'équipe d'audit.

GAZEO : *« Donc ce que l'on a c'est quand même des regards croisés. C'est-à-dire que les auditeurs ils travaillent à plusieurs. Il y a un minimum de 2 auditeurs par mission. Il y a un superviseur, un directeur de mission et puis il y a moi. Donc en fait, ils préparent d'abord entre eux les auditeurs, ils sont challengés par le directeur des missions et enfin par moi. Puisqu'avant de partir en mission, ils viennent me voir et ils me disent " bah voilà ce qu'on va regarder, voilà les grands enjeux". En fait moi je ne leur demande pas leur programme de travail, ça c'est le rôle du directeur de mission. Mais je veux qu'ils me disent au-delà du standard qu'on connaît tous "quelles sont les spécificités que vous avez rencontrées dans votre préparation " et c'est ça que je challenge. Donc voilà je ne vais pas me tromper bien évidemment (rire). Je peux en laisser passer bon. Mais c'est pour ça que je dis qu'on a des regards croisés parce qu'il y a plusieurs niveaux de challenge ».*

AUTOCAR : *« Je suis plutôt favorable au double regard et on sait très bien, voilà, une mission déjà, côté risque et autres ne sont pas toujours évidentes. Et parce que vous l'avez vu ce n'est pas des auditeurs pour bon nombre à l'origine donc voilà, et du coup, puis on sait très bien que sur certains types d'entretiens à deux, on entend mieux qu'à un. Parce qu'il y en a qui vont capter certaines choses, on a tous notre sensibilité et puis voilà. Et puis pendant deux heures d'entretien, on ne peut pas être au taquet tout le temps ».*

L'exploitation et le recouplement des informations recueillies

Le recouplement d'informations permet d'identifier des incohérences soit dans les propos recueillis, soit dans les documents produits à l'audit.

FROMAGO : *« Un expert va connaître les process. Il va ouvrir la porte sur les process aux auditeurs et après l'auditeur avec son côté, à cette heure-ci, je dirais chien de chasse, il y va. Mais le chien de chasse, si vous ne le mettez pas sur une piste, il ne va rien sentir ».*

ELEC : *« C'est pour ça que je pense qu'on n'est pas très handicapé par le fait de ne pas avoir d'expertise sur tout. Parce qu'effectivement, c'est plus soit la sincérité de ce qui remonte, soit l'incohérence entre les valeurs sur des choses que l'on va récupérer sur le terrain ».*

Synthèse : l'analyse préliminaire des risques repose sur des approches qui diffèrent selon les organisations.

Tableau 45. Plan de mission – mode d'observation des risques

Analyse préliminaire des risques				
	Type d'approche	« Top-down »	Dimension temporelle	Passé
		« Bottom-Up »		Présent
Dimension spatiale (point d'observation)	Sources	« Mixte »		Futur
		Historique des audits		
		Indicateurs et KPI		
		Analyse documentaire		
Savoir-faire et méthodologie		Connaissance métiers de l'entreprise		
		Connaissance métiers de l'audit		
		Recoupement/Regards croisés		
		Exploitation des informations recueillies		

4 - 3 2 LE CHOIX DES AXES D'INTERVENTION (PERIMETRE DE REVUE)

4 - 3 2 1 CHOIX DES AXES D'INTERVENTION POUR LA MISSION

Le choix des axes d'intervention consiste à sélectionner les processus et sous-processus qui seront revus ainsi que les entités qui seront soumises à l'audit.

Choix des axes d'intervention en fonction du niveau de risque

FROMAGO : *« Attendez, risque sûreté people, moi, je l'affine. Je vais tomber sur les 5 usines qui sont Iran, Turquie, Égypte, Algérie et Maroc. Ça devient concret et ça veut dire que ces 5 missions, c'est 5 fois 3 jours avec une check-list montée avec le presta, trouver un presta qui serait efficace et puis, on y va. Donc, moi, j'ai sélectionné ces zones-là parce que par rapport au risque de sûreté, on a quelques rapports locaux et c'est là que pour l'instant c'est le plus chaud. On pense tous que quand là ça va péter en décembre ou en janvier en France, allez discuter avec votre directeur de sûreté. Bon là à ce moment-là, on se posera peut-être la question sur la France ».*

SPORTFLEX : *« Là, par exemple, on a audité les appels d'offres sur les zones géographiques les plus à risque et sur les business unit les plus à risque. Le Brésil, centre immobilier brésilien, des choses comme ça, pour en faire une traduction en disant : c'est quoi le degré de maturité du process d'appel d'offres au Global Groupe. Ça venait d'où ? Ça venait de travail d'interview. Ça venait des cas de fraude qui étaient principalement sur cette thématique d'appel d'offres donc voilà c'était justifié de pouvoir l'auditer »*

Les risques sélectionnés par l'audit peuvent être différents de ceux qui étaient à l'origine de la mission.

SANTEFORM : *« Ce que je ne vous ai pas dit, c'est que les entretiens de plan qui étaient à la fin, certains on les retrouve quand on fait la préparation de la mission et donc s'il y a un an il nous a dit qu'il faut absolument aller en Chine pour voir tel sujet. Parfois on se dit, non voici ce qui s'est passé depuis 6mois, ça c'est bon ça a été résolu, on a ce problème-là. Du coup, parfois on adresse des risques qui n'étaient pas ceux du plan ».*

BEAUMAG : « *Et là c'est tout l'enjeu de votre sujet qui m'a semblé intéressant, c'est-à-dire que par rapport à une thématique que l'on réfléchit en amont bah finalement les auditeurs quand ils sont sur le terrain des fois il y a tout à refaire. Alors les grands tests sont là mais il n'empêche que oui il y a tout à refaire parce que le risque qu'on identifie sur la phase terrain, au bout d'un moment il m'appelle, il me dit qu'il faut qu'on se voie, qu'on fasse un point. Et on découvre des trucs et ce n'est pas du tout les trucs et ce n'est pas du tout ce qu'on avait pu imaginer* ».

Choix des axes d'intervention qui découlent des demandes du management

BATI-F : « *On demande au DR (Directeur Régional) où il veut qu'on aille pour voir quoi. La DR est parfois au-dessus. Parfois, c'est la Branche qui dit bah tiens quand tu iras en Normandie, j'irais bien à telle agence parce que j'ai des doutes sur tel et tel sujet. Donc tout ça, c'est empirique si vous voulez, ce n'est pas formalisé dans une grille*».

DISTRIMART : « *Aujourd'hui, dans la plupart des cas, ce sont les gens qui viennent me demander, me dire j'ai des problèmes, et nous quelques fois on a des vrais problèmes, des problèmes de moyen pour les aider* ».

AERO : « *Là je vous parlais des processus de pilotage de l'UO, unité opérationnelle, après sur leurs processus opérationnels, et ça c'est UO par UO, c'est eux qu'ils nous disent, en ce moment je me fais du souci sur tel ou tel sujet, est-ce que vous voulez les regarder* ».

Choix des axes d'intervention pour permettre de réaliser des comparaisons entre plusieurs entités

L'objectif dans ce cas-là est de fournir au management une vision non faussée qui pourrait résulter du fait de n'avoir sélectionné que des entités ou des processus faibles. Le fait de couvrir des périmètres réputés être bien gérés et d'autres qui le sont moins permet aussi d'identifier les bonnes pratiques qui pourront être étendues.

BATIMODERN : « *Bah la sécurité à ce moment-là, on va faire systématiquement un mix de configurations différentes, c'est-à-dire on va prendre une grande, une moyenne et une petite typiquement* ».

CHIMICA : « *Et on avait le choix entre on le fait à l'International mais que sur 2/3 BU ou au contraire on le fait qu'en Europe mais sur toutes les BUs. Et on a décidé de le faire sur toutes les BUs en Europe. Et puis probablement du coup que l'année prochaine, on fera les US. Pourquoi on a choisi ça, c'est à l'analyse. On s'est dit les 12 BUs risquent d'avoir des pratiques très différentes et il y aura une grosse valeur ajoutée à les comparer* ».

Choix des axes d'intervention aléatoire

En l'absence d'éléments d'information, le choix ne peut s'opérer que de façon aléatoire.

ELEC : « *Non mais quand on a fait une filiale par exemple avec 280 entités, on n'est pas allé voir 280 entités mais on est allé voir au niveau global. Alors on est allé dans certaines entités qu'on a choisies un peu au hasard et on a regardé globalement comment la filiale était pilotée, qu'est-ce qui faisait le résultat de la filiale* ».

VINO : « *S'il y a des méthodes pour dire ça va merder là, là, là et là et les autres c'est nickel, je ne sais pas si ça existe mais je suis très preneur* ».

Choix des axes d'intervention établi sur la base des moyens que l'on souhaite allouer et dont on dispose.

FROMAGO : « *C'est une question de moyen. Vous faites, par exemple, au niveau de la sûreté, ce sont des débats. Est-ce que je prends un petit bout ou est-ce que je passe carrément par une société qui va me faire un diagnostic de cyber-vulnérabilité entre 20 et 40 jours en payant 2 gars à peu près à 750 euros la journée. Et on passe le truc et après ça débouche sur des plans d'actions* ».

CHIMICOR : « *Je reviens sur ce que j'ai dit au début. Penser qu'on couvre un risque, c'est prétentieux. Parce que on va choisir, on a 130 entités dans le groupe, et là on en choisira 10 quoi. Donc voilà mais bon moi je fais avec les effectifs que j'ai* ».

Le processus de sélection amène les auditeurs à exclure certains axes d'intervention de leurs missions en fonction de certains critères.

Des axes d'intervention exclus de la mission d'audit en lien avec les compétences disponibles.

SPORTFLEX : « *En fait, ce qui nous manque c'est beaucoup les risques liés à la supply. Quand je vous disais que ça manque cruellement dans notre staffing et dans notre Scope, on ne l'audite pas vraiment. On fait un peu d'audit thématiques mais ce n'est pas suffisamment précis. On n'a pas l'expertise donc voilà. Qu'est-ce qui peut nous manquer ? Je ne sais pas, c'est une bonne question. J'ai l'impression qu'on a une couverture qui nous correspond plutôt pas trop mal* ».

CHIMICOR : « *Après je pense qu'il y a des choses qu'on ne sait pas, la corruption on ne sait pas l'auditer en tant que tel. Mais de fait je pense qu'on s'est libéré du fait qu'on ne peut pas tout regarder à chaque fois et donc ce qu'on fait, nous dans les rapports d'audit on va mettre les points qu'on va remonter, les points d'audit, et quand on va donner notre opinion on va dire qu'il y a des choses, soit ce n'est pas applicable qu'on ne va pas auditer c'est-à-dire qu'on va rappeler qu'il y a des choses qu'on n'a pas regardées* ».

Des axes d'intervention exclus du fait qu'ils sont couverts par d'autres fonctions contrôlantes et expertes.

SANTEFORM : « *J'ai de la latitude. Je vais vous donner un exemple. S'il y a un expert audit qui est passé trois mois avant moi, deux options. Soit je veux refaire, c'est possible ou alors je fais confiance et je ne traite pas du tout ou alors je vais me limiter, on va faire une limited review, une limited review qui va consister à vérifier la mise en place des plans d'actions. C'est les trois options que j'ai. Mais ça, en revanche, on demande aux auditeurs avant de partir de bien avoir listé « in scope, out of scope » et les étapes que je me mets en P1 (priorité 1). C'est le seul moyen, sinon c'est une approche par le temps* ».

MICROPIX : « *Si on fait une General Review typiquement, là on a une matrice standard, qu'on a définie avec les 6-8-10 domaines que l'on revoit. Après ces domaines, suivant les entités, ils sont applicables ou pas applicables. Après, suivant les entités, ces domaines sont soumis à du testing SOX, donc si ça a déjà été soumis à des contrôles SOX des fois, on ne va pas le revoir encore une fois. Même si l'angle n'est pas exactement le même mais, je veux dire, c'est encore une fois une question d'allocation des ressources* ».

Le choix des axes d'intervention peut être impacté par le moment d'observation qui est choisi par les auditeurs.

BATI-F : « *C'est le principe de l'échantillonnage parce qu'on serait venu la veille ou le lendemain, on n'aurait pas vu la même chose. Donc, à partir du moment où on accepte qu'il y ait une part d'échantillonnage, bon bah autant pousser la logique jusqu'au bout* ».

Synthèse : les données ont permis de mettre en évidence plusieurs critères de choix mobilisés par les auditeurs internes pour identifier les missions susceptibles de constituer une mission d'audit du plan. Ces critères ne sont pas en lien direct avec les risques de la cartographie.

Tableau 46. Plan de mission – critères de choix des axes d'intervention

Choix des axes d'intervention	
Issues des risques du moment (pouvant être différents de ceux de la cartographie des risques)	Issues d'autres critères
	Demandes spécifiques du management
	Pouvoir réaliser des comparaisons entre entités
	Choix aléatoires
	Contraintes de ressources
	Compétences
	Couvert ou non par autres fonctions expertes
	Contraintes réglementaires
	Cœur de métier : les incontournables
	Changements organisationnels/processus

4 - 3 3 L'ALLOCATION DES RESSOURCES ET LA DUREE DE LA MISSION

Les ressources allouées à la mission ainsi que la durée de réalisation et donc d'observation varient en fonction des organisations.

Une durée de mission en fonction du type de mission d'audit

DISTRIMART : *« Même voire une semaine parce qu'on a beaucoup d'opérationnelles. Les missions qui sont demandées par le haut ou plus stratégiques prennent deux, trois semaines. Mais des missions plus récurrentes, c'est une semaine ».*

RACECAR : *« Pour simplifier je vous fais grosse maille, vous avez des audits qui sont dits plus 'spot' vous voyez ou flash, chez Vehicar ils disaient flash, nous, on dit spot. Donc c'est un truc c'est entre 15 jours et 3 semaines. Voilà, Et puis « bon an, mal an » vous êtes à et puis vous avez d'audit d'univers récurrent qui sont de 6 à 8 semaines aussi mais c'est des trucs tellement rodés que, c'est plutôt 6, moi je veux toujours les ramener à 6 semaines, j'ai eu du mal avec les équipes parce que bon les plans de travail c'est toujours les mêmes, on perd moins de temps à la préparation ».*

Une allocation des ressources internes en fonction des expertises

SPORTFLEX : *« Moi, je ne peux pas me permettre que quelqu'un qui est IT aille faire de la sécurité, c'est ça et inversement. Ce n'est pas responsable, c'est vraiment inenvisageable, il ne va pas être crédible quoi. C'est déjà suffisamment compliqué comme ça. Chacun doit être sur sa zone de force sur les audits récurrents ».*

Des équipes dédiées pour traiter de missions spécifiques (SI, Fraude, ...).

- **GAZEO :** l'audit dispose d'une équipe spécialisée qui est dédiée aux audits industriels.
- **BATICOSTO :** pour les audits sur les systèmes d'information, l'audit dispose d'auditeurs spécialisés qui ne font que des missions sur ce thème.
- **MICORPIX :** il y a deux équipes d'audit spécialisées par thématique : les auditeurs IT et les auditeurs qui traitent des missions d'investigation de la fraude.

Des affectations en fonction des expertises métiers suivant les missions

- **PETROLIUM :** Les directeurs sectoriels et les managers viennent des branches qu'ils auditent. Cela permet d'aller plus vite dans l'analyse des risques.

- **SPORTFLEX** : sur les audits récurrents, chaque auditeur reste sur sa zone de force et d'expertise (sécurité, ...).
- **ELECTROSTORE** : les auditeurs opérationnels sont dédiés aux audits cycliques de magasin pour couvrir les risques du référentiel de contrôle interne (RCI framework).
- **NATURELIA** : sur les audits de sites industriels, l'équipe comprend un ancien opérationnel qui selon le directeur de l'audit sera plus apte qu'un financier à identifier des dysfonctionnements liés à la production.
- **VEHICAR** : seuls les directeurs de secteurs sont spécialisés. Ainsi, chaque directeur de secteur traitera des missions liées à son périmètre (commerce, qualité, ingénierie, ...)
- **RACECAR** : pour les audits, il existe des responsables de secteur qui sont affectés à leur domaine d'expertise Il s'agit des secteurs suivants : systèmes d'information, amont (conception, achat et production, logistique), fonctions support (finance, RH, commerce).

Une allocation des ressources qui n'est pas directement liée à des expertises métiers

FROMAGO : *« Parce qu'au fur et à mesure, ils muent au fur et à mesure de leur parcours dans l'entreprise. C'est tout le travail du chef de service de, on prend un désosseur de bilan et de P&L et puis on en fait un homme ou une femme d'audit de process ».*

BEAUMAG : *« Ils sont quand même assez généralistes mais justement je trouve qu'ils se complètent très très bien, d'ailleurs j'en ai un qui est très process, j'en ai un est très donc financier, l'autre qui est est très process IT et la troisième qui est process ».*

La possibilité de faire appel à des ressources externes

Les auditeurs ont la possibilité de recourir à des ressources externes à l'organisation pour réaliser des missions pour lesquelles ils estiment ne pas disposer des compétences ou bien des ressources suffisantes.

NATURELIA : *« Il y a des choses pour lesquelles on n'a pas les compétences, ça c'est clair. Quand on n'a pas les compétences, on peut se les attacher. Donc nous, ça arrive qu'on fasse des audits en emmenant des gens du siège ou des gens de l'externe, des spécialistes je ne sais pas quoi sur des produits financiers sophistiqués ou des experts*

techniques pointus ou des choses comme ça. Donc ce type de compétences qui sont facilement intégrables, on le fait ».

BATICOSTO : *« Dans des missions, on embarque des experts sur la phase terrain, sur certains types. Je ne sais pas, je dirais 20 % des missions, on a un expert avec nous en full-time ou part-time ».*

4 - 3 4 L'ELABORATION DU PROGRAMME DE TRAVAIL

4 - 3 4 I ELABORATION DU PROGRAMME DE TRAVAIL

Le programme de travail des auditeurs liste le travail que l'équipe d'audit interne a prévu de mettre en œuvre dans le cadre de la mission. Les normes précisent que ce programme doit être établi sur la base d'une analyse préliminaire des risques afin de cibler en priorité les zones à risques. Nous avons recensé plusieurs types de programmes de travail au sein des organisations.

Programme de travail « standard » de type systématique pour des audits de processus récurrents

Les programmes de travail standards de type systématique sont des programmes qui présentent peu de flexibilité. L'ensemble des tests prévus au programme doivent être appliqués.

ELECTRO STORE : *« Ah oui-oui c'est long. C'est long parce que c'est des tests qui sont très ritualisés et ce n'est pas du journalisme, on fait vraiment du Testing. Je crois qu'on doit avoir à peu près 300 tests et 90 thématiques de tests. On couvre toute la partie revenue, encaissements, retour produit, etc. toute la partie stock et toute la partie sécurité et administration du magasin. Donc voilà. Et là, là c'est important puisqu'on couvre des sujets qui sont quand même un peu clés pour nous. Sujet encaissement naturellement avec tout ce qui est lutte contre la fraude, etc. Enfin bon là l'optimisation des stocks, vous voyez ».*

CHIMICA : *« Alors que les 20 autres vont être plus mécaniques et des audits d'entités, et encore une fois très généraliste. C'est-à-dire qu'on passe de l'organisation générale aux achats, à la compta, à la logistique, à la production, à la vente, à la R&D. Donc on balaye l'ensemble des processus de manière générale. On a un référentiel qui comme toujours n'est pas parfait mais qui couvre l'ensemble de ces 12 cycles ».*

Les groupes interrogés disposent pour la plupart de programmes standards à appliquer de façon systématique.

- **MULTIMEDSTORE** : pour les audits magasin, l'audit a établi une liste de quatorze cycles qui sont revus de façon systématique sur 600 points de contrôle (dont une partie est traitée en phase de préparation de la mission). L'ensemble des tests sont réalisés sans exception. Les variables d'ajustement portent sur la période de transactions revue (1 mois ou 3 mois, ...) et le nombre de documents testés.
- **AERO** : l'audit dispose de programme de travail standard pour la revue des unités opérationnelles et des filiales. Il s'agit d'un document nommé grille de contrôle interne qui couvre des processus standards (achats, ventes, RH, SI...). Cette grille permet d'avoir une base de comparaison entre entités. Ce programme est appliqué de façon systématique avec des cycles qui peuvent donner lieu à plus de travaux en fonction de risques spécifiques (montants des achats significatifs, ...). Ce programme est complété par un processus opérationnel demandé par l'entité auditée.
- **MEDIACORP** : sur les audits de petites entités, le programme de travail est standard. Il couvre essentiellement les cycles transactionnels qui donnent lieu à des paiements dans une optique trésorerie, paiement, fraude et conformité et respect des délégations.
- **SPORTFLEX** : pour les audits récurrents, le programme de travail est entièrement appliqué une fois le périmètre établi. Si un autre risque est identifié durant la mission, le programme de travail n'évoluera pas. Une autre mission pourra être inscrite au plan d'audit.
- **ELECTROSTORE** : pour les audits opérationnels, il s'agit d'un programme standard ritualisé composé de 300 points de contrôle regroupés sous 90 thématiques (encaissement, stocks, sécurité et administration du magasin, ...). Les programmes de travail sont mis à jour au regard des nouveaux risques qui apparaissent avec le temps.

Programme de travail « standard » sous forme de guide en complément d'une approche par les risques.

GAZEO : « On a des programmes de travail par grand cycle mais on se laisse une partie de préparation d'analyse de risques spécifiques pour adapter le programme de travail à la problématique. C'est-à-dire que l'audit interne chez Gazéo n'est pas un audit de conformité à la SOX. C'est un audit qui oblige les auditeurs à réfléchir. Et

quand j'embauche quelqu'un je dis aux candidats, si vous êtes venu ici pour le confort et appliquer des procédures comme ça et les déployer, voilà on va gagner du temps vous et moi ».

BATI-F : *« C'est des tests standards absolument, et qu'on a formalisés, donc ce sont les mêmes et qu'on va sortir. Alors, c'est là où on est, moi je suis en train de réfléchir mais je n'arrive pas à voir comment on pourrait améliorer le système. On est à la merci de la personnalité ou éventuellement de la sensibilité de l'auditeur, du contexte, de je ne sais pas trop quoi qui fait qu'il va plutôt faire le test sur les notes de frais, ou plutôt faire le test sur la LME, plutôt faire un test sur les créances clients ».*

Les directions de l'audit peuvent disposer de programme de travail type qui constitue des guides d'audit. Le choix et le nombre des thèmes sont sensiblement différents selon les organisations.

- **CHIMICA :** pour les audits d'entités (80%), l'audit applique un programme de douze business cycle qui sont tous revus de façon quasi standard (avec ajustement si besoin mais uniquement dans le cadre qui existe)
- **BATI-F :** l'audit applique un référentiel de contrôle intitulé maîtrise des risques avec **7 processus clés** : l'organisation, la prise d'affaire, les Ressources Humaines, la prévention, les achats, environnement et compta/gestion
- **ENGINICO :** l'audit utilise le programme standard qu'elle a établi sur la base du questionnaire d'auto-évaluation. Ce programme liste les risques standards par processus pour 4 thèmes clés : les achats, le reporting financier, les RH, et gestion de projets. Pour chacun des risques, il liste les activités de contrôles attendues et les tests standards. Ce programme est ajusté de façon à pouvoir traiter des risques spécifiques qui ressortent lors des entretiens de préparation de la mission. Certains axes sont supprimés pour pouvoir en traiter d'autres.

Certains thèmes restent néanmoins des « incontournables ».

- **ELEC :** pour les audits d'entités, de nombreux guides d'audit ont été établis pour constituer un référentiel pour les auditeurs. Les programmes ont été complétés avec les programmes des commissaires aux comptes. Les auditeurs n'appliquent pas l'intégralité du programme d'audit mais sélectionnent certains thèmes (organisation, achats, SI, RH,

stratégie, pilotage, ...). Il subsiste néanmoins des thèmes qui sont considérés comme incontournables et qui sont revus de façon systématique (achats, sécurité, ...).

- **LUXESTORE** : l'audit a établi des programmes de travail détaillés qui sont appliqués sous forme de guide lors des missions. Ces programmes sont orientés sécurité des actifs et couvrent moins les aspects performance, notamment sur le périmètre de la gestion des stocks et de la production.
- **ELECTROSTORE** : pour les audits opérationnels dits quick scan (audit en 1 journée) à, l'objectif est de couvrir des risques "incontournables" plus des risques spécifiques en fonction des magasins. Cette approche est en cours de développement.

La priorisation des thèmes doit notamment reposer sur une approche par les risques ou des spécificités liés à l'activité.

- **GAZEO** : l'audit dispose de programmes de travail standards pour les grands cycles. Les auditeurs devront réaliser une analyse préliminaire des risques afin d'ajuster le programme en fonction des spécificités de l'entité auditée.
- **EQUIPAUTO** : l'audit dispose de programme de travail standard. A titre d'exemple, sur l'axe investissement, il est prévu de regarder un certain nombre de thèmes comme la sélection des fournisseurs, la conduite de projet. Ces programmes peuvent être ajustés pour tenir compte des spécificités liées aux entités auditées.
- **BATIMODERN** : il existe des programmes de travail standards. Les auditeurs choisissent des modules parmi les cycles du programme (achats, RH, comptabilité, ventes, ...). Cette sélection s'opère sur la base de l'analyse de risque. Les objectifs de rotation permettent de choisir les entités, alors que le risque permet de choisir les cycles.

Le choix des thèmes à couvrir au sein du programme de travail peut être déterminé en fonction des demandes des audités.

- **BATICOSTO** : pour les audits d'entité liés aux critères de rotation, des programmes standards ont été établis. Ils couvrent des thèmes standards tels que le commercial, la finance, les processus opérationnels, la gestion des stocks, etc. Il s'agit notamment des cycles couverts par le processus d'auto-évaluation du contrôle interne. Le choix des thèmes abordés résulte des entretiens réalisés par les auditeurs en phase de préparation

mais aussi ceux réalisés sur le terrain avec les audités. L'audit demande toujours au patron de l'entité audité ce qu'il souhaiterait que l'audit couvre.

- **VEHICAR** : la direction de l'audit a développé de nombreux programmes de travail standards. Ces programmes sont appliqués tout en pouvant être ajusté si besoin. Ce n'est pas très souvent le cas en pratique. Les programmes évoluent peu.

Programmes de travail sur des nouveaux processus qui seront amenés à être standardisés

RACECAR : *« Vous voyez, là on parlait du positionnement prix, c'est des thématiques très à la mode dans l'automobile, allez savoir pourquoi mais vous le lisez dans les journaux. Bah l'année dernière, on l'avait fait sur l'Europe et puis nous on a une exposition Chine qui est en train de monter comme ça ! Mais cette année on est en train de le faire sur la Chine vous voyez bon. Par contre j'aurai été très mal à l'aise de proposer un audit sur la Chine directement sans avoir fait alors sur l'Europe parce que je n'avais pas encore les gammes de travail. Mais ça c'est un audit qui est compliqué, il ne nous a pas pris 8 semaines, en fait il a plutôt pris 10, 11 semaines, vous voyez, au détriment d'autres. Et maintenant que j'ai la gamme de travail sur la Chine bon là vous voyez c'est un audit Top risque mais quelque part c'est une gamme de travail récurrent ».*

MULTIMED STORE : *« Ça c'est pour les magasins. Par contre lorsqu'on est sur les thématiques plutôt des directions pays et fonctionnelles. Alors comme moi je suis parti de zéro il y a 5 ans et tu vois et tu vois la première version c'était avril 2012, il a fallu construire les règles, après il a fallu les faire auto évaluer, puis après j'ai commencé à les auditer. Donc il a fallu que je construisse des programmes de travail. Les premiers datent de début 2013, donc maintenant on a des programmes de travail. Mais la logique est la même, on part de ces règles qui ont des risques sous-jacents et puis à l'intérieur on a des tests, et où on a, oui des tests, des demandes de documents qui justifient que les contrôles sont bien en place ».*

Programme de travail « sur mesure »

PETROLIUM : *« Moi, j'ai des thématiques qui sont validées au niveau du Comex, je n'ai aucune idée de la façon dont je vais le traiter. Et donc je commence à discuter avec les uns les autres, à réfléchir. Bon je vais prendre un exemple concret parce qu'il*

est d'actualité : contrôle des fournisseurs et des chaînes de sous-traitance par rapport à la conformité sociétale (rire). Bon, sujet intéressant, sujet qui comporte des risques majeurs. Comment on traite ça ? On ne peut pas faire des audits chez les fournisseurs, enfin voilà on ne peut pas avoir une méthodologie d'audit standard. Donc là moi, mon réflexe c'est déjà de documenter ce qui existe en termes de pilotage et de dispositif de maîtrise au niveau des branches, des activités. Et je vais essayer de documenter ça. Ça va être le but de cet audit ».

CHIMICOR : « *Typiquement là, cette année on a attaqué un sujet, on ne sait pas trop comment l'aborder, c'est business continuity plan que vous pouvez décliner à tous les niveaux. Au niveau d'une usine ça peut être le fait que le fournisseur ne fournit pas les produits requis, ça peut être le fait que casse des équipements, il y a plusieurs sources possibles, ça peut être aussi le fait que l'IT ne fonctionne plus au niveau d'un Shared services, donc là on tâtonne complètement. On s'est dit c'est une thématique qu'on aimerait comprendre cette année, regarder cette année donc on l'attaque sur toutes les usines. [...] Ce n'est pas une mission spécifique, on a dit comme on ne sait pas l'aborder en particulier, qu'on va plutôt essayer de l'aborder de façon empirique mission par mission et de demander systématiquement ce qui est en œuvre et construire notre propre expertise sur le sujet ».*

Ces programmes sont établis par l'audit avec l'aide d'experts ou en se basant sur des guides de bonnes pratiques.

Les programmes bâtis en référence aux référentiels de bonnes pratiques

- **DISTRIMART** : pour les audits transverses de type achat, marketing qui sont adressés par le corporate et la partie stratégie et management des audits récurrents, les programmes sur mesure sont établis en référence aux bonnes pratiques recensé dans un book qui a été réalisé par l'audit avec les experts métier. Il résulte de l'analyse des causes de dysfonctionnement récurrent identifiés dans les pays.

Les programmes établis avec l'aide des experts

- **VOLTAGE** : pour les audits transverses de type R&D, gestion stratégique, transformation d'un business, les programmes de travail sont sur mesure en mobilisant les experts du groupe.

- **MICROPIX** : sur les missions thématiques moins standards, l'audit établira une matrice de risque et de contrôle sur mesure. Ce travail est réalisé en rencontrant des experts, en utilisant des bases externes spécialisées, afin de recenser les risques inhérents liés à un nouveau thème et les types de contrôles pouvant être établis.
- **FROMAGO** : sur les audits thématiques issus des risques groupe, l'audit établit des programmes de travail sur mesure. Néanmoins, il sera important de mobiliser des experts soit en interne soit en externe.

Synthèse : Il a été possible d'identifier principalement deux types de programme de travail. Le premier « standard » et le second que nous appellerons « sur mesure ». Le programme standard à des processus que l'audit évalue de façon récurrente mais aussi des sujets plus ponctuels. Dans ce cas-là, l'audit construit un référentiel de contrôle standard sur la base des premières missions, ce qui donnera lieu par la suite à un programme de travail standard. Le programme de travail sur mesure se distingue du précédent dans la mesure où le programme est adapté, complété, enrichi à chaque mission.

Tableau 47. Plan de mission – types de programme de travail

Programme de travail	
« Standard »	« Sur mesure »
Processus récurrents	Nouveaux processus

Conclusion :

Ce chapitre consacré à la présentation des données montre combien les données collectées auprès des répondants se sont avérées riches en contenu sur l'objet de notre recherche.

Les données collectées mettent en évidence une très grande diversité des pratiques en matière de construction des objets de risques au sein des organisations.

Nous pouvons être étonnés à ce stade de cette diversité malgré l'existence de cadres normatifs en matière d'évaluation des risques pour mettre en œuvre les processus d'identification, d'évaluation et des sélections des risques au sein des organisations.

Ce constat permet de montrer combien la notion de risque peut être riche et donner lieu à une multitude d'approches qui traduit aussi dans une certaine mesure la difficulté à l'appréhender.

Nous allons aborder dans la partie suivante les principales contributions de ce travail de recherche.

5^{EME} CHAPITRE : CONTRIBUTIONS

Cette thèse apporte trois contributions principales. La première est de démontrer les différentes dimensions de l'écart décrit par Power (1999) entre le système abstrait de l'audit et sa pratique et d'explorer les causes potentielles qui permettent de l'expliquer. La seconde est de mieux comprendre le processus d'auditabilité, c'est-à-dire le processus mis en œuvre par l'audit interne pour transformer les risques en risques auditables. Enfin, ces travaux permettent de porter un regard renouvelé par rapport à la littérature existante sur le lien entre audit interne et gouvernance ainsi que sur l'appréciation de la qualité de l'audit.

Il est utile de rappeler en préambule de ce chapitre la théorie de la société de l'audit de Power (1999) à partir de laquelle sont établies les principales contributions de cette thèse.

Selon l'auteur, l'audit est présenté au travers des normes comme une pratique objective pour répondre aux attentes sociétales. Or, la pratique de l'audit reste « obscure » et n'exclut pas une dimension subjective. Il distingue d'une part le savoir abstrait et d'autre part la pratique concrète de l'audit. Il existe selon Power un écart entre le système abstrait de l'audit qui correspond au cadre normatif et sa pratique qui reste « obscure ».

Lorsque de nouvelles demandes sont adressées à l'audit pour fournir de nouveaux types d'informations « objectives », l'audit accepte d'y répondre et les intègre dans ses normes qui représentent son savoir abstrait. L'écart qui apparaît entre les normes et la pratique de l'audit résulte du maintien des pratiques d'audit qui restent inchangées alors que les normes évoluent avec la prise en compte de nouvelles demandes.

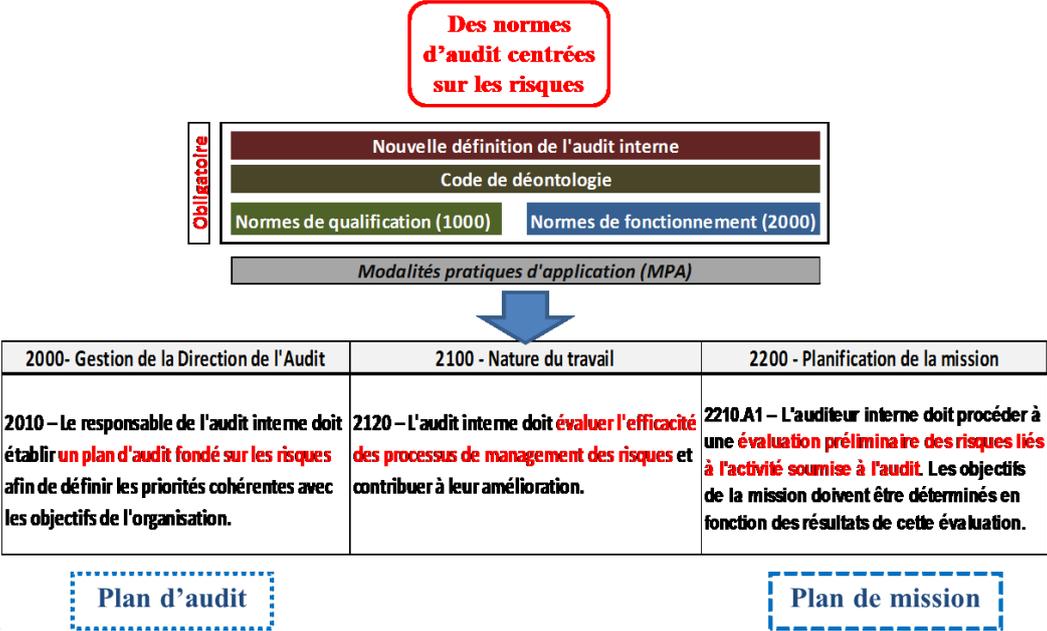
Comme le caractère « obscur » de l'audit est caché derrière son savoir abstrait, Power affirme qu'aucun non-auditeur n'est en mesure de vérifier l'étendue de cet écart et que la profession d'audit peut dès lors poursuivre l'intégration de nouvelles demandes sociétales dans son savoir abstrait. Selon Power, la nature obscure des pratiques d'audit constitue une ressource qui lui permet de se développer et de maintenir son statut.

5 - 1 L'ECART ENTRE UNIVERS DES RISQUES ET UNIVERS D'AUDIT

La première contribution de cette thèse démontre les différentes dimensions de l'écart décrit par Power (1999) entre le système abstrait représenté par le cadre normatif de l'audit et les pratiques des auditeurs. Il est dès lors important de rappeler en préambule de cette partie les principales exigences normatives auxquelles est soumis l'audit interne.

Les normes précisent que l’audit interne est en charge d’évaluer la robustesse des processus de gestion des risques au sein des organisations et qu’il doit planifier ses travaux de façon à traiter en priorité des risques majeurs auxquels est exposée son organisation. Le fait d’avoir fondé les pratiques de l’audit sur les risques permet à l’audit d’intégrer dans ses normes les nouvelles attentes sociétales dans un contexte de crise de confiance.

Figure 15. Normes d’audit : exigences en matière de planification

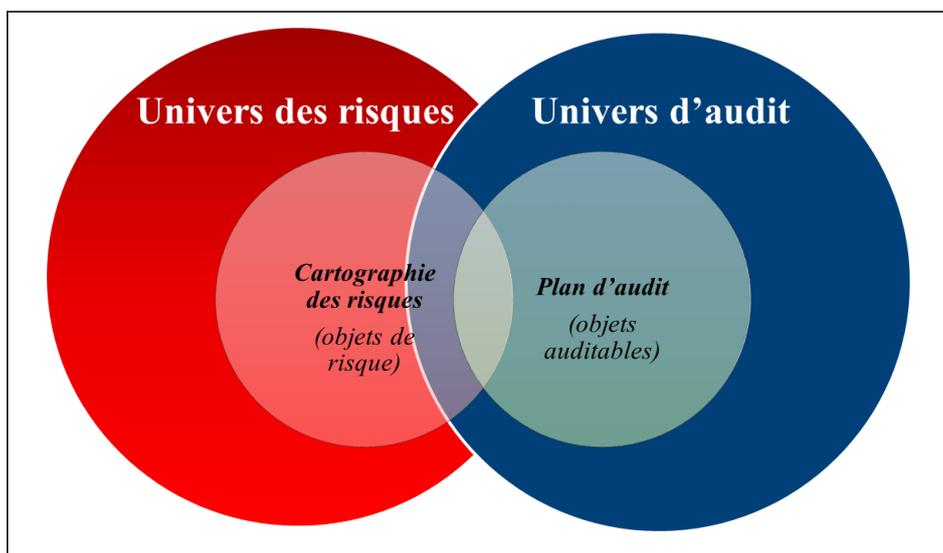


La norme 2010 relative à la planification annuelle des travaux de l’audit précise que « le responsable de l’audit interne doit établir un plan d’audit fondé sur les risques afin de définir les priorités cohérentes avec les objectifs de l’organisation ». La norme 2210 précise que « l’auditeur interne doit réaliser une analyse préliminaire des risques liée à l’activité soumise à l’audit. Les objectifs de la mission doivent être déterminés en fonction des résultats de cette évaluation ». L’audit interne doit pour chacune de ses missions réaliser une analyse de risque spécifique pour déterminer le périmètre qui sera revu par l’audit.

Les résultats issus de l’analyse de nos données mettent en évidence que le taux de couverture des risques de la cartographie par les missions d’audit peut être plus ou moins important selon les organisations. Le plan d’audit contient des missions qui ne sont pas en lien direct avec la cartographie des risques et qui reposent sur des critères spécifiques à l’audit interne. La décision de réaliser ces missions permet à l’audit interne d’appréhender d’autres sources de risques qui

n'apparaissent pas dans la cartographie. Il en résulte dès lors par un écart entre l'univers d'audit et l'univers des risques tel que représenté dans le schéma ci-dessous.

Figure 16. Ecart entre univers d'audit et univers des risques



Selon Power (1999), il existe un écart entre le système abstrait de l'audit représenté par les normes et la pratique effective des auditeurs.

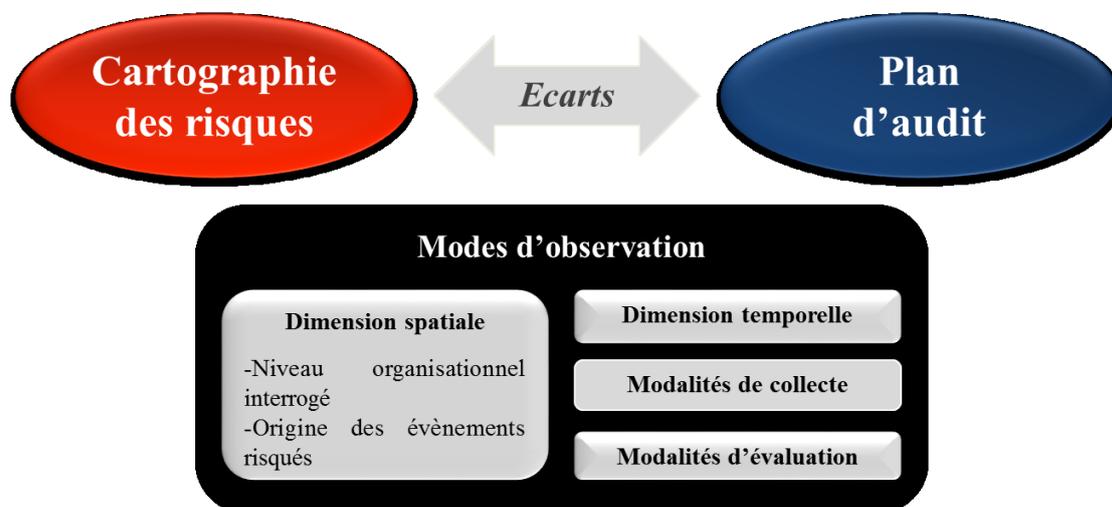
Ce travail de recherche confirme l'existence de cet écart mais va au-delà en spécifiant les différentes dimensions qu'il revêt et en explorant les causes potentielles qui permettent de l'expliquer.

5 - 1 1 LES DIFFERENTES DIMENSIONS DE L'ECART ENTRE UNIVERS DES RISQUES ET UNIVERS D'AUDIT

Le processus d'élaboration du plan d'audit tel que décrit par les directeurs de l'audit met en évidence que le plan est bâti à partir de la prise en compte de certains risques de la cartographie mais aussi d'autres types de risque. Il en résulte que les risques sur lesquels se fondent les opérationnels ne sont pas forcément les mêmes que ceux retenus par l'audit interne.

Il est dès lors important de comprendre en quoi l'approche retenue par l'audit ainsi que ses modes d'observation spécifiques nous informent sur la nature des risques qui ne sont pas représentés dans la cartographie.

Figure 17. Dimensions de l'écart entre univers des risques et d'audit



L'écart entre univers des risques et univers d'audit résulte des modes d'observation qui sont spécifiques à chacun de ces processus. La comparaison du processus d'élaboration de la cartographie des risques avec celui de l'élaboration du plan d'audit permet de mettre en évidence les différentes dimensions que revêt l'écart entre univers des risques et univers d'audit tel que décrit dans le schéma ci-dessus.

5 - 1 1 1 L'ANALYSE DU PROCESSUS DE CARTOGRAPHIE DES RISQUES

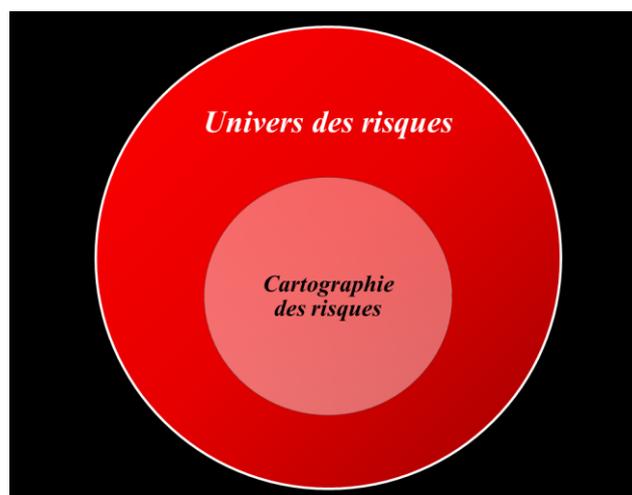
Le résultat de la cartographie des risques est conditionné par les modes d'observation retenus pour appréhender les risques. Cette section permet de voir dans quelle mesure chacune de ces dimensions peut influencer sur le résultat du processus de recensement des risques au sein d'une organisation.

Le niveau organisationnel interrogé :

Les risques qui figurent dans la cartographie correspondent à ceux que la direction générale a décidé de retenir comme étant les risques majeurs pour son organisation et ceux à partir desquels le plan d'audit sera en principe établi.

La cartographie représente une sélection de risques parmi un ensemble de risques potentiels qu'il est nécessaire de recenser au préalable. Cet ensemble peut être défini comme étant l'univers des risques qui regroupe l'ensemble des risques potentiels. De surcroît, il est important de distinguer « univers des risques » et « cartographie des risques ».

Figure 18. Cartographie et univers des risques



D'après notre cadre d'analyse les risques n'existent pas indépendamment de notre mode d'observation. Pour être capable d'observer, il faut procéder à une distinction. Pour désigner quelque chose comme étant un risque, il faut le distinguer de ce qu'il n'est pas. Rien ne peut être observé sans établir de distinction, ce qui signifie qu'il n'est pas possible de tout observer mais juste de voir qu'une partie. L'observateur est dès lors soumis à des points aveugles.

L'univers des risques peut être plus ou moins accessible en fonction des choix méthodologiques et donc des distinctions qui sont retenues par les acteurs pour identifier les risques au sein de leur organisation. Ces derniers seront soumis à des points aveugles lorsqu'ils chercheront à observer et à reconstituer leur univers des risques. Plusieurs types d'approche ont pu être identifiés dans le cadre des entretiens : l'approche « top down », l'approche « bottom up » et l'approche « mixte ». Les modalités de mise en œuvre pour chacune de ces approches ont un impact sur la représentation de l'univers des risques puisqu'ils impliquent des points aveugles spécifiques.

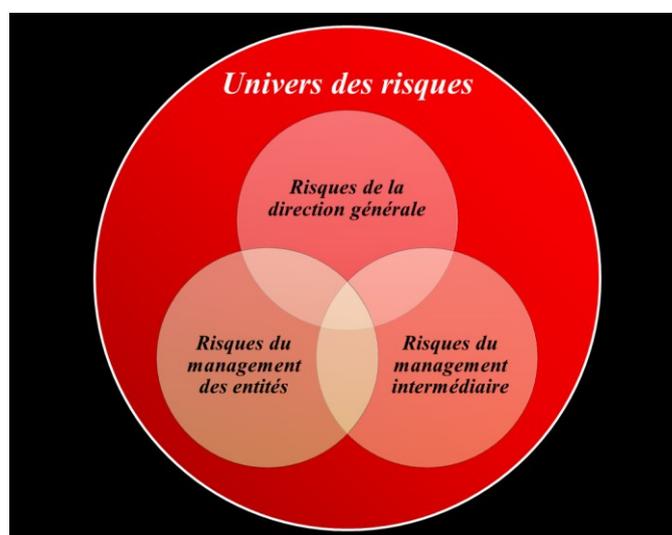
A titre d'exemple, dans l'approche « top down », lorsque seule la direction générale est interrogée sur ses risques, la cartographie des risques établie traduit les risques de la direction générale et exclut les risques des entités.

VINO : « Alors le mode opératoire à l'heure actuelle donc on a la cartographie, il a plutôt une approche qui était d'une part c'était fait en collaboration avec des Big Four, Price ou Ernst qui donnaient un coup de main on va dire plutôt humain, pas vraiment methodo mais clairement humain. Et on avait une approche qui était essentiellement

Top Down, c'est-à-dire cartographie qui reposait sur une identification d'un certain nombre de top management Parisien, on va dire Français, quelques filiales significatives et on estimait des très grands risques ».

Le schéma ci-dessous traduit cette idée que l'univers des risques est constitué de l'ensemble des risques potentiels mais que le résultat du processus de recensement est conditionné par le niveau organisationnel interrogé. Les risques de la direction générale pourront de surcroît être différents de ceux d'un directeur de zone géographique, d'un directeur de ligne de produit ou bien d'une unité opérationnelle.

Figure 19. Univers des risques en fonction des personnes interrogés

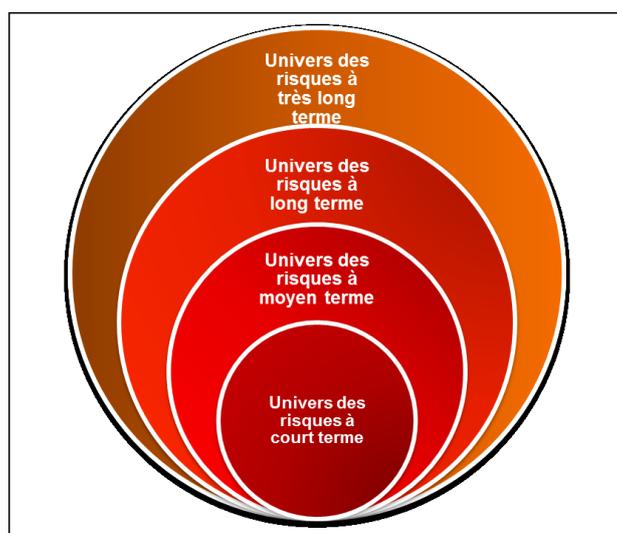


Au sein d'une même organisation telle qu'une entité opérationnelle, les risques détectés du point de vue du directeur général de l'entité pourront être différents de ceux des autres membres de son organisation. Les risques identifiés par les directeurs opérationnels (production, maintenance, logistique, ...) pourront être différents de ceux des fonctions support (finance, commercial, ...).

L'horizon de temps :

Une seconde dimension clé qui peut conditionner le résultat de la cartographie est l'horizon de temps retenu pour identifier les risques. Selon l'horizon de temps retenu, la nature des risques sera sensiblement différente avec d'une part des risques « opérationnels » qui portent sur le court terme et des risques « stratégiques » qui portent sur le moyen et long terme.

Figure 20. Univers des risques en fonction de l'horizon de temps

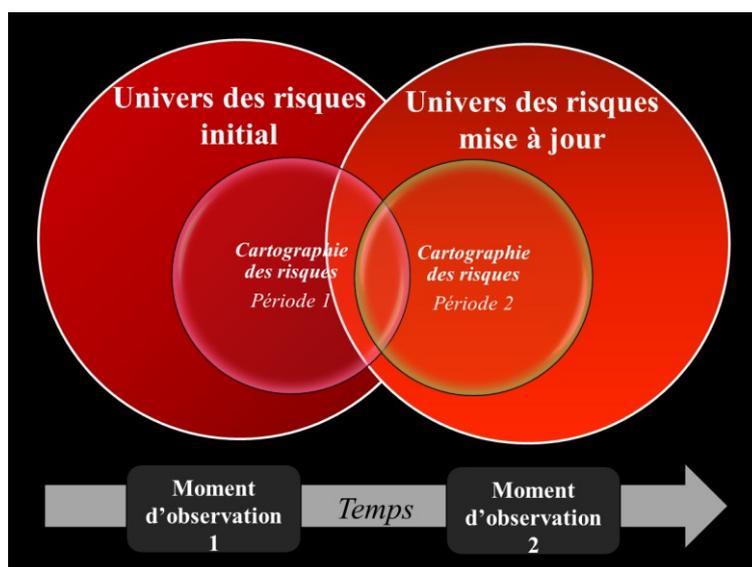


PETROLIUM : « *Quand on interpelle sur les grands risques et de la manière la plus ouverte possible dans un entretien le moins directif possible, on arrive à des choses qui sont parfois étonnantes. Je me souviens du patron de la chimie de l'époque qui me dit "bah moi je vois un risque que peut-être un jour les plastiques soient interdits, sont plus acceptables". Bon effectivement on ne dit pas ça quand on pense à ses risques opérationnels à un moment donné. Il faut avoir le temps de se projeter, de parler de vision* ».

SANTEFORM : « *Ça dépend aussi de la culture de la gestion des risques. Je prends un patron de site par exemple, à chaque comité de direction ils ont un sujet risque qui est à l'ordre du jour. Parce qu'ils vont être HSE, parce qu'ils vont suivre leurs accidents, parce qu'ils vont suivre leurs ruptures, parce qu'ils vont suivre un certain nombre de choses et donc il traite quelque part des sujets sont très opérationnels* ».

La dimension temporelle intervient aussi au regard du moment d'observation des risques. L'univers des risques pourra ainsi varier en fonction du moment auquel il sera établi car le futur tel que nous l'envisageons aujourd'hui sera certainement différent au moment de sa réalisation. Le fait de retenir comme principe de mettre à jour la cartographie avec une périodicité relativement éloignée peut amener à ne pas observer des nouveaux risques.

Figure 21. Univers des risques en fonction du moment d'observation

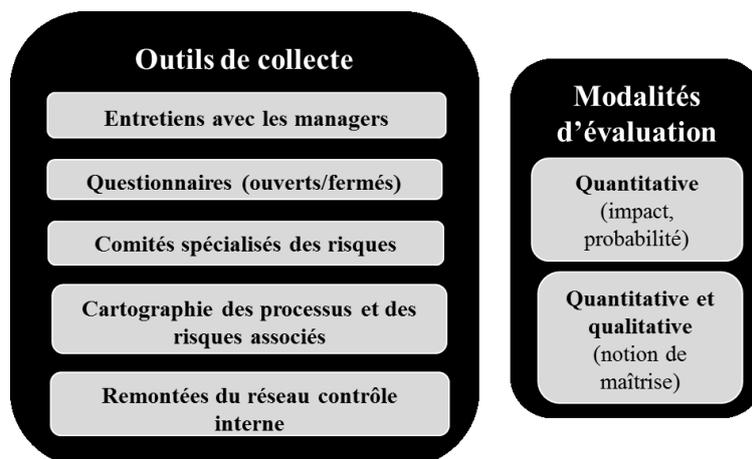


Les outils de collecte et les modalités d'évaluation :

Les entretiens ont permis d'identifier un certain nombre d'outils de collecte pour recenser les risques ainsi que différentes modalités d'évaluation (décrits dans le quatrième chapitre). Au-delà de leur diversité, il est essentiel de saisir l'impact que peut avoir le mode d'observation associé à chacun d'entre eux sur le résultat de la cartographie des risques.

Le schéma qui figure à la page suivante est une synthèse des principaux outils de collecte mobilisés lors du processus de cartographie et des modalités d'évaluation.

Figure 22. Outils de collecte et d'évaluation des risques de la cartographie



Les modalités d'évaluation des risques peuvent amener à exclure certains risques lors du recensement des risques en raison de règles ou de critères restrictifs. Pour certains, seuls les risques pouvant être traduits en impact financier sont retenus alors que pour d'autres, le risque revêt d'autres dimensions mais qui sont eux-mêmes restreints par souci de simplification. Les modalités d'évaluation appliquées par les organisations sont multiples et amènent dès lors à retenir certains risques plutôt que d'autres en fonction des règles qui sont définies.

CHIMICA : « Et d'ailleurs, dans les listes de risques qu'ils m'ont fournies, moi j'ai dit écoutez, on va faire un seuil à 10 Millions. Souvent, ils ont en tête des risques très opérationnels parce que ça leur pourrit la vie au quotidien. Et puis en réfléchissant un peu ensemble, on s'aperçoit que l'enjeu est bien inférieur. Je dis et bien, vous voyez, il ne figure pas dans la cartographie des risques ».

Les outils de collecte doivent aussi être considérés sous le prisme des modes d'observation qui peuvent influencer sur le résultat de la cartographie des risques. A titre d'exemple, le fait de soumettre un questionnaire aux managers pour recenser les risques donnera certainement des résultats sensiblement différents suivant qu'il s'agit d'un questionnaire ouvert ou bien fermé. Dans le cas de questions fermées qui vise à évaluer des risques prédéfinis, les risques émergents ou bien ceux qui ne font pas partie du registre des risques prévus dans le questionnaire ne seront pas appréhendés.

Les modes d'observation associés aux outils de collecte ainsi qu'aux méthodes d'évaluation sont de nature à conditionner les résultats de la cartographie des risques.

L'origine des évènements considérés comme risqués :

Les organisations se distinguent dans leur approche par la nature des évènements qu'elles prennent en compte lors de l'élaboration de la cartographie. Pour certaines d'entre elles, les risques ont pour origine les facteurs internes à l'organisation alors que pour d'autres il s'agit principalement de facteurs externes. La nature des risques sera de surcroît sensiblement différente selon les approches retenues.

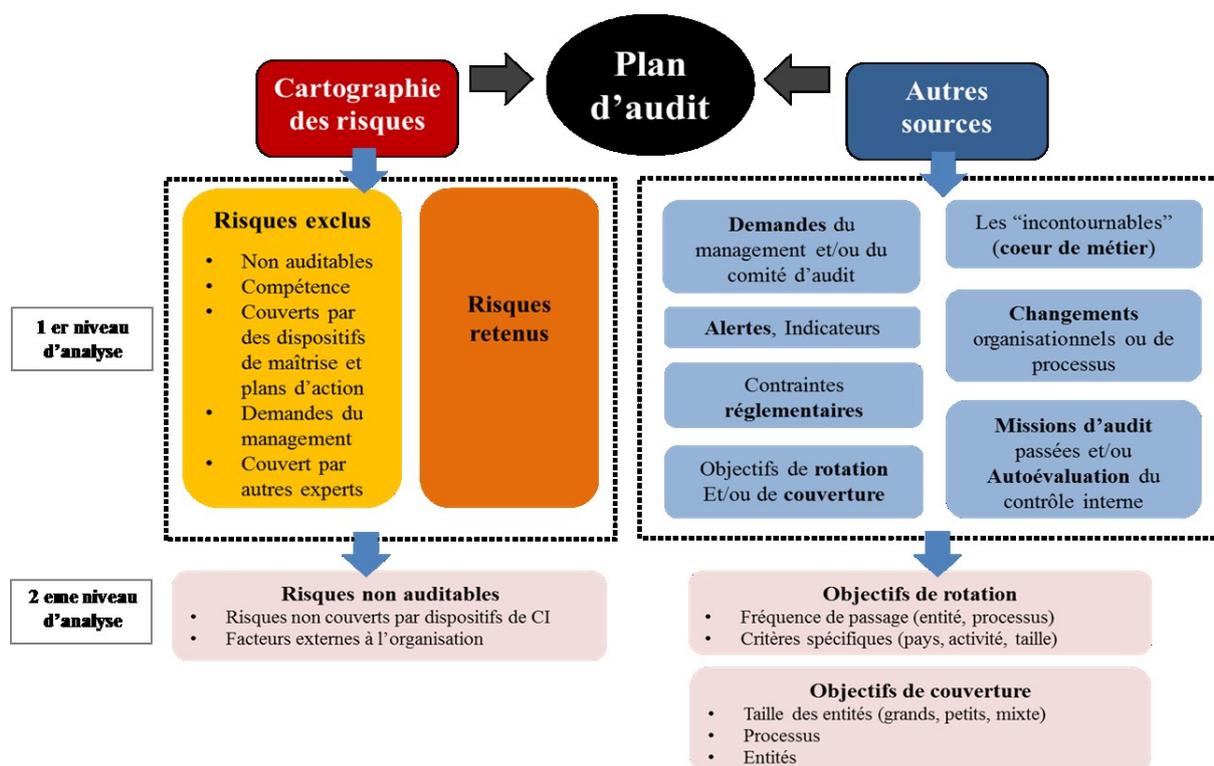
Le résultat de la cartographie des risques est conditionné par les modes d'observation qui sont mis en œuvre et des variables associées (niveau organisationnel interrogé, horizon de temps considéré, ...). De surcroît, l'accès à l'univers des risques ne peut être que partiel et dépend des approches méthodologiques retenues. La question qui se pose dès lors est de savoir dans quelle mesure l'approche retenue par l'audit permet de compléter cette vision partielle des risques.

5 - 1 1 2 L'ANALYSE DU PROCESSUS D'ELABORATION DU PLAN D'AUDIT

Le processus d'élaboration du plan d'audit tel que décrit par les directeurs de l'audit met en évidence que le plan est bâti à partir de la prise en compte de certains risques de la cartographie mais aussi d'autres sources de risque.

Ainsi que l'illustre le schéma qui figure à la page suivante, le lien entre le plan d'audit et la cartographie n'est que partiel puisque l'audit interne s'appuie également sur d'autres sources pour élaborer le plan d'audit et exclut certains risques de la cartographie.

Figure 23. Origine des missions inscrites au plan d'audit



Un premier niveau d'analyse des données collectées a permis d'identifier les principaux facteurs qui justifient l'inscription d'une mission au plan d'audit ainsi que les critères d'exclusion appliqués par l'audit pour certains risques. Un second niveau d'analyse a permis d'observer pour chacun de ces critères la diversité des pratiques.

A titre d'illustration, l'objectif de rotation est un critère spécifique de l'audit pour alimenter le plan d'audit en complément des risques identifiés dans la cartographie. Cet objectif peut être défini selon les organisations soit par entité, soit par processus et être complété par des critères plus spécifiques tels que le type de pays, la nature des activités ou encore la taille de l'organisation.

Il est important de comprendre en quoi les critères spécifiques appliqués par l'audit interne pour élaborer le plan d'audit peuvent nous informer sur les autres types de risque au sein de l'organisation.

Les événements considérés comme risqués :

Les risques considérés par les auditeurs se rapportent à des processus d'entreprise et se distinguent des risques de la cartographie qui peuvent pour certains avoir comme origine des facteurs externes à l'organisation. Les risques ne sont donc pas appréhendés de la même manière par les opérationnels et les auditeurs internes.

Les auditeurs se basent pour le plan d'audit sur les risques qui sont en lien avec les processus internes à l'organisation qui sont considérés comme étant tous porteurs de risques. Les risques appréhendés par l'audit sont les risques inhérents aux activités réalisées, c'est-à-dire qui sont indissociables des activités. A titre d'exemple, le risque d'avoir des produits périmés est inhérent à l'activité de la grande distribution tout comme le risque d'avoir des pannes de machine est inhérent à l'activité de production pour une usine.

VESTIMOD : « *On sait que dans notre métier (mode, textile, bijoux), il y a forcément des défectueux. L'activité, enfin, c'est inhérent à notre activité. Un magasin qui ne nous déclare jamais de défectueux, c'est tout aussi louche qu'un magasin qui nous en déclare cent cinquante* ».

Puisque les risques inhérents découlent directement des activités, l'audit recense les entités, les métiers, les activités, les processus et sous-processus qui existent au sein de son organisation. Une fois ce travail réalisé, il peut rattacher aux différentes entités de son organisation des risques inhérents en lien avec leurs activités et donc leurs processus. Ce travail d'inventaire constitue l'univers d'audit.

WALLDISTRIB : « *Donc je fais ma liste d'activités en quelque sorte au sens entité avec une certaine autonomie économique. Et puis je mets l'ensemble de mes process. D'ailleurs je n'ai pas qu'un seul tableau, j'en ai plusieurs parce qu'en fonction des activités j'ai plusieurs tableaux. Et puis là on se dit qu'est ce qui est important à couvrir ? Alors bah ça c'est important, ça ce n'est pas important, ça ce n'est pas chez moi donc là j'enlève. Donc je fais une espèce de Mapping qui me sert à définir déjà quel est potentiellement mon périmètre auditable* ».

En complément de cette approche processuelle mis en œuvre par l'audit pour déterminer les risques inhérents, le plan d'audit se fonde aussi sur les risques de la cartographie. De nouveaux, l'audit s'attache à établir un lien entre les risques de la cartographie et des processus de l'organisation qui constitueront les objets d'audit.

EQUIPAUTO : « *« La difficulté c'est qu'un risque, il a plus d'un processus, et c'est pour ça que c'est difficile. Mais justement dans un risque on choisit, aujourd'hui dans le groupe quel est le processus clé, la direction fonctionnelle rattachée, enfin il y en a plusieurs mais c'est quoi leurs sujets du moment, il faut aller là en fait. Nous on part du risque, on demande à la personne, aux personnes interviewées, c'est quoi le dispositif de contrôle que vous avez en face du risque. Et c'est comme ça qu'en faisant la synthèse, parce que sur le même risque on a pas mal d'interviews, qu'on arrive à identifier les processus, quelle est la direction fonctionnelle qui là le gère majoritairement, parfois, il y en a plusieurs ».*

CIMENTO : « *Ce qu'on fait en fait c'est que quand on inscrit une entité, par exemple Ciment du pays lambda dans le plan d'audit 2015. Au moment où on l'inscrit on ne sait pas, en tout cas on ne dit pas quel processus on va regarder. Plusieurs semaines avant le début de la mission qu'on a démarre un travail de préparation qui commence par un travail lourd d'interview. On va voir si un certain nombre de fonctionnels, on discute avec le pays. Et entre les thèmes de l'année globalement pour l'audit et ce qui ressort comme étant les sujets les plus potentiels ou les plus prioritaires au moment où on va faire l'audit, c'est là où on sélectionne les processus. Et alors un autre élément qui est important c'est le croisement avec le contrôle interne. Parce que le contrôle interne nous donne une vision assez juste des processus qui sont robustes et qui ne sont pas robustes ».*

Une des difficultés rencontrées par les auditeurs concerne la tenue à jour de cet univers des risques afin de pouvoir tenir compte des changements qui interviennent dans le temps au niveau de l'organisation et des processus d'entreprise. Une deuxième difficulté est le choix du niveau de détail avec lequel l'univers d'audit doit être décrit.

CHIMICOR : « *L'esprit, c'est qu'on repart, on réconcilie tout ce qui est entité juridique avec la conso, pour s'assurer qu'on a bien les mêmes entités, qu'on prend même les AS et qu'ensuite quand une entité consolidée, une entité juridique n'est pas à un degré de d'organisation suffisamment fin, c'est un peu l'expérience on l'a vraiment construit, ça fait trois ans qu'on est dessus et chaque fois on rajoute, on va descendre à un niveau plus fin ».*

L'audit est dès lors lui-même soumis au risque inhérent de ne pas avoir un univers d'audit correctement défini pour déterminer son périmètre auditable.

Modalités d'évaluation des risques :

Le risque inhérent est considéré comme un événement pouvant avoir des conséquences négatives sur les processus et donc sur l'atteinte des objectifs de l'organisation. Dès lors qu'il est inhérent à une activité, il devient possible. Il n'est pas appréhendé comme dans la cartographie des risques de façon quantitative en termes d'impact ou de probabilité mais comme une source de dysfonctionnement potentielle.

L'audit introduit une autre dimension pour apprécier le risque. Il s'agit du degré de maîtrise. Pour faire face à ces risques inhérents, les organisations mettent en place des dispositifs de contrôle interne dont le but est d'assurer le correct fonctionnement des processus. Un risque inhérent qui n'est pas couvert par un dispositif de maîtrise apparaît dès lors comme plus important. Cette évaluation ne peut pas être réalisée en amont de la mission puisque l'audit doit l'apprécier dans le cadre de ses missions.

Le fait de rattacher les risques de la cartographie à des processus est fondé sur l'idée que les risques inhérents aux processus sont bien liés aux risques de la cartographie. En procédant ainsi, cela suppose d'accepter l'hypothèse que si les risques inhérents liés aux processus audités sont maîtrisés, alors le risque identifié dans la cartographie le sera aussi.

BATI-F : « *On n'audit pas un chantier, on audite des processus de contrôle interne sur un chantier* ».

VINO : « *J'ai un système d'auto-évaluation et de contrôle interne dans la partie contrôle interne qui me permet d'évaluer via une grille X thématiques, X contrôles thématiques sur toutes les filiales et de dire bon bah je vois que sur une base déclarative ? on peut commencer à évaluer en termes de contrôle interne pur telles filiales* ».

Les risques qui sont considérés par les auditeurs sont donc en priorité les risques de défaillance des processus et des dispositifs de maîtrise. Les programmes de travail de l'audit sont dans cette logique établis par processus.

CHIMICOR : « *On a des programmes de travail sur les process gérés dans nos usines, on va avoir tout ce qui est investissement, tous les Capex, les immos, les stocks ça c'est vraiment les deux incontournables. On a manufacturing, la maintenance, on va voir l'HSE [...]. C'est nos 13 macroprocess ça, c'est nos macroprocessus et Finance on a divisé en deux, la partie vraiment trésor et puis la partie taxe qui est un peu séparée* ».

SANTEFORM : « Ça oui c'est le G(eneral) A(udit) methodology, on est based on global process and standard model. Et donc on explique que quand on fait une mission industrielle, on fait ça, quand on fait une mission commerciale on fait ça, et quand on fait une mission shared service par exemple, on regarde ça ».

Le choix des missions :

Parmi les principaux critères retenus par l'audit, il convient de retenir les objectifs de rotation et de couverture, les résultats des missions d'audit passés, les auto-évaluations du contrôle interne, les alertes et les incidents, les changements organisationnels puis les demandes du management. Chacun de ces critères nous informe sur la manière dont l'audit appréhende le risque.

Des faiblesses qui ont donné lieu à des plans d'actions correctifs à l'issue d'une mission d'audit peuvent faire l'objet d'audit de suivi pour s'assurer que les actions ont bien été mises en œuvre. Le risque inhérent appréhendé par l'audit est la non mise en œuvre des plans d'actions.

NATURELIA : « On a les audits précédents, le suivi des recommandations, enfin les gens qui ne suivent pas les recommandations sur les trucs un peu graves, de toute façon on va y retourner ».

Pour ce qui concerne les changements organisationnels ou de processus qui interviennent au sein de l'organisation, l'audit considère qu'ils sont de nature à pouvoir générer des dysfonctionnements faute de réviser et d'adapter les dispositifs de contrôle existants. Un processus qui évolue sans adapter les dispositifs de contrôle interne est source de nouveaux risques inhérents.

MICROPIX : « Typiquement, une restructuration, une annonce de fermeture d'usine pourraient amener à une démotivation de certains employés et accentuer le risque de fraude. Donc là, on conduit cette évaluation-là, et après on regarde ce qu'on peut en ressortir ».

VEHICAR : « Typiquement, les notes de frais c'est nous qui les avons proposés. Ça n'a pas été demandé par quiconque mais nous on a estimé que, maintenant comme il n'y avait plus de contrôle a priori mais a posteriori, on a décidé de le proposer, ça a été validé ».

Faute de disposer d'indicateurs de risque fiables pour déterminer quelles sont les entités les plus à risque au sein de l'organisation, l'audit se donne des objectifs de couverture des entités et des processus de son organisation sur la base d'une fréquence de passage prédéfinie.

NATURELIA : « *Et après j'essaye quand même d'équilibrer, pas d'équilibrer mais de pas laisser des zones complètement vierges. Il pourrait se produire que sur une zone donnée, si on a beaucoup travaillé les années d'avant, il se peut que mais en général j'essaye de garder au moins un ou deux sujets par zone* ».

La cartographie des risques reste déclarative et l'audit intègre le risque lié à la non-déclaration de certains risques par les entités interrogées.

BEAUMAG : « *Les magasins ce que j'ai fait, c'est que j'ai été voir la direction de la filiale, je lui ai dit « quels magasins tu veux que j'audite et pour quelle raison tu veux que je les rentre ? » donc elle m'a donné une liste, donc je les ai pris et j'en ai pris 5 en plus en aléatoire que j'ai choisi moi-même. Et j'ai un côté auditeur qui ne fait pas forcément confiance. Moi j'ai tendance à ne pas leur faire confiance parce qu'ils vont faire comme avec les contrôleurs fiscaux ils vont nous donner un os à ronger et ils ne vont pas vouloir aller ou ça peut les mettre en porte-à-faux politiquement, nous il y a un vrai enjeu politique chez nous* ».

ELEC : « *Enfin, bon on a un certain nombre de tests un peu incontournables. Bon puis après on est plutôt, nos auditeurs ne pourront pas trouver un problème que les gens ne connaissent pas, ça c'est sûr, ça c'est sûr ! Par contre, et ça on le fait, ils trouvent des problèmes qui sont connus pour certains mais qui ne remontent pas. Et c'est ça qu'on va chercher. En gros, quelque part, quand on se ramène au Coso, c'est plus la fiabilité des reporting* ».

L'audit dispose par ailleurs d'outils de collecte afin d'identifier des zones à risque qui sont susceptibles de ne pas figurer dans la cartographie des risques. Il s'agit de risques envisagés sur la base de recoupement d'informations qui sont potentiellement contradictoires et peuvent constituer des risques.

BATICOSTO : « *On a une méthode, effectivement on fait beaucoup d'entretiens, on pose beaucoup de questions à ce moment-là, on vérifie, on recoupe, on demande les dysfonctionnements, les anomalies, les exceptions qui ont été rencontrées, on essaye d'analyser, on prend des avis un peu à la périphérie. C'est pour ça que j'insistais tout*

à l'heure sur un point qui est fondamental. Ici les directeurs d'audit ont plus 20 ans de groupe. Tout simplement parce qu'ils ont un réseau, moi c'est la même chose, j'ai 25 ans de groupe. On a un réseau qui nous permet d'appeler directement des gens qui ne sont pas directement sur le sujet mais qui sont autour et qui peuvent nous alerter ».

Enfin, un certain nombre de missions découlent directement de l'audit sur la base d'autres critères tels que les incidents survenus, les activités cœur de métier, les enjeux du moment.

MEDIACORP : *« On part quand même des cartographies précédentes, cet exercice il est mené maintenant depuis la sortie de la bourse de New York, donc depuis 2007, on a 8 ans d'historique de cartographie qu'on met d'ailleurs en place quand on a racheté GVT, en un an et demi, on a mis la cartographie d'ailleurs en place etc. Donc c'est une méthode rodée et avec un peu d'historiques donc on sait, on regarde les risques réalisés qui n'étaient pas identifiés, voir l'évolution, on ne part pas de zéro donc on a une certaine connaissance historique de ces risques plus les missions d'audit ».*

L'audit exclut du plan d'audit un certain nombre de missions, et ce indépendamment du critère de limitation de ses ressources puisqu'une partie des missions adressées par l'audit ne découle pas de la cartographie des risques. Ces exclusions peuvent résulter des initiatives propres de l'audit ou bien découler de décisions managériales. Parmi les critères d'exclusion, nous avons notamment identifié le critère d'auditabilité. L'audit considère que certains risques ne sont pas auditables, notamment du fait de l'absence de dispositifs de contrôle. Il est ainsi possible d'avoir un risque évalué comme important au niveau de la cartographie et qui est exclu du plan d'audit s'il est considéré comme non auditable.

SANTEFORM : *« Je vous donne un exemple, le risque groupe Image and Réputation, je veux bien aller l'auditer, mais où, comment, pourquoi je ne sais pas le faire. Emergence de nouvelles technologies ou regulatory intelligence, je ne sais pas faire »..*

L'audit peut exclure certains sujets qui sont soit couverts par des plans d'actions du management, soit pris en charge par d'autres fonctions expertes que l'audit pour leur évaluation.

ELECTROSTORE : *« Oui, ça, on n'y va pas. Et enfin "other risks not currently converted in audit topics " sur lequel il y a un sponsor potentiel [...]. On veut rationaliser relativement précisément notre ségrégation, et en particulier effectivement faire ressortir clairement la dimension compétence. Et aussi la dimension raison d'être. C'est-à-dire qu'on considère qu'il y a des natures de risque qu'on a aucune raison*

d'aborder parce que ça ferait une duplication de savoir-faire, de métier et autre. Et que dans cette logique de troisième ligne défense et autre, on ne se positionne pas là-dessus ».

Enfin, la décision d'exclure certains risques du périmètre de revue de l'audit peut résulter d'une décision managériale.

ENGINICO : *« Parce que je ne sais pas non plus si, quand je vois à peu près aujourd'hui, les quinze tops risques, je m'aperçois que, soit je les couvre dans le programme standard, soit je ne les couvre pas. Mais c'est une volonté de management qu'on ne les couvre pas. Le Président avait une vision de dire : Voilà, dans la gestion de projet interne, pas de projet client, mais il y a une partie gouvernance qui est chargée de faire cette partie risque, même si ce n'était pas le cas mais bon. Donc, il y a une partie que je ne couvrais pas parce qu'on ne veut pas que je la couvre ».*

Le management qui mandate l'audit peut ainsi décider de ne pas le missionner sur certains risques.

Les résultats montrent que le plan d'audit exclut un certain nombre de risques de la cartographie au profit d'autres missions d'audit. Le lien entre le plan d'audit et la cartographie n'est que partiel.

Les travaux de Mikes (2009, 2011) mettent en évidence l'existence de deux styles de management des risques. Le premier caractérisé par un "enthousiasme quantitatif" orienté vers la mesure des risques, le second par un "scepticisme quantitatif" basé sur des méthodologies peu quantitatives, non formelles, et orientée vers les incertitudes stratégiques. Mikes (2011) utilise la notion d'*envisionnement* par opposition à celle de *measurement*. La matière dont traite la cartographie est de l'ordre de la représentation et non pas de l'ordre du réel objectif représenté par l'univers d'audit. L'écart entre l'univers d'audit et celui des risques confirme que différentes conceptions de l'ERM peuvent exister mutuellement au sein d'une même organisation.

5 - 1 2 LES CAUSES POTENTIELLES DE L'ECART ENTRE L'UNIVERS DES RISQUES ET L'UNIVERS D'AUDIT ?

Notre cadre d'analyse et les principaux concepts mobilisés par Luhmann (1993, 1995) apportent un éclairage particulièrement riche pour étudier les pratiques d'audit interne. Il permet

notamment de mieux comprendre l'écart que nous avons pu identifier entre l'univers des risques et l'univers d'audit.

5 - 1 2 1 LA DISTINCTION RISQUE/DANGER ET SA PRISE EN COMPTE DANS LES PROCESSUS DE CARTOGRAPHIE DES RISQUES ET SES CONSEQUENCES SUR LE PLAN D'AUDIT.

Selon Luhmann (1993), les risques n'existent pas indépendamment du mode d'observation. Pour être capable d'observer, il nous faut procéder à une distinction. Si nous voulons désigner quelque chose comme étant un risque, nous devons dès lors le distinguer de ce qu'il n'est pas.

Il est utile de rappeler la définition du risque telle qu'elle est établie par Luhmann (1993) en introduisant la distinction risque/danger. « *Cette distinction présuppose que l'incertitude existe en lien avec des pertes futures. Il y a dès lors deux possibilités. La perte potentielle est vue comme la conséquence d'une décision, c'est-à-dire qu'elle est attribuée à la décision. Nous parlons alors de risque. Ou bien, la perte possible est considérée comme ayant été causé par l'extérieur, c'est-à-dire qu'elle est attribuée à l'environnement. Dans ce cas nous parlons de danger* » (Luhmann, 1993, p. 21). Le choix de l'une des deux faces de cette distinction risque/danger dépend du mode d'attribution des conséquences.

L'absence de distinction entre risque et danger dans les cartographies des risques

Les entretiens réalisés avec les directeurs de l'audit montrent que la distinction risque/danger est absente des approches mises en œuvre dans le cadre des processus de cartographie des risques. Pour certains, les risques sont liés principalement aux dysfonctionnements internes alors que pour d'autres, ce sont les éléments externes à l'organisation qui constituent des risques. Les organisations concernées établissent des cartographies des risques qui incluent aussi bien des risques que des dangers sans faire de distinction entre ces deux notions.

Le fait de considérer des dangers comme étant des risques n'est pas neutre car elle conduit à envisager les dangers comme étant des éléments maîtrisables et gérables au même titre que les risques.

AERO : « *C'est évident que nous le désordre climatique, pour nous c'est un vrai-vrai sujet, et jusqu'à présent ce n'était pas du tout dans la cartographie des risques. Ce qui fait que ça sort c'est les cyclones, c'est le dérèglement climatique, on se paye des tempêtes, toute la répercussion c'est sur le transport aérien, on a quelque chose d'ailleurs et ça, ça avait été prévu déjà, ça rentre dans l'univers des risques [...]. Donc on est bien sur un truc environnement naturel, et qui ne figurait pas dans la cartographie*

des risques, donc ce qu'a demandé le directeur de l'environnement, c'est que maintenant, et ça a été accepté d'ailleurs, c'est dans la cartographie ».

CIMENTO : *« Donc si on prend les risques qu'on a, ils se croisent sur un double axe. Un, c'est le risque exogène du type bouleversement politique, pandémie, changement climatique, enfin vous voyez. Ce genre de changement alors dont on peut se dire que c'est extrêmement macro. Avant qu'Ebola n'impacte le business on sait que ça peut prendre du temps. La géopolitique, bon on est en Syrie, on est en Irak, on est en Egypte, bon on l'a un petit peu senti mais voilà ça c'est un premier axe. L'autre c'est beaucoup plus les risques qu'on a, c'est les conséquences de non efficacité de nos processus ».*

Les dangers sont plus difficiles à auditer

Certains dangers qui sont qualifiés de risque dans les cartographies des risques sont exclus du plan d'audit par les auditeurs internes qui les considèrent comme des objets non auditables.

AERO : *« C'était en risque, c'est clair que si demain il n'y a plus de trafic aérien, bah on sera mal. Mais quand on ferme les aéroports, on est très mal mais en même temps que j'aille auditer ce n'est pas auditable ce sujet, ce n'est pas auditable, donc voilà ».*

BATICOSTO : *« Donc on va définir un plan d'audit qui intègre la cartographie des risques mais ça ne veut pas dire qu'il intègre tous les risques de la cartographie. De risque pas auditable, par exemple des risques liés à une baisse d'activité forte dans l'immobilier, on considère que ce n'est pas un risque auditable parce que c'est extrêmement exogène ».*

Ainsi, l'écart entre l'univers d'audit et l'univers des risques résulte en partie de l'absence de distinction entre risque et danger dans le processus de cartographie des risques. Les cartographies peuvent soit recouvrir uniquement des dangers (comme le cas de MEDIACORP) ou bien des dangers et des risques (comme c'est le cas pour la majorité des organisations interrogées). Les facteurs externes sont aux dires des directeurs de l'audit plus difficiles à auditer dès lors qu'ils ne sont pas couverts par des processus, d'où la décision de les exclure du plan d'audit.

La théorie des systèmes sociaux de Luhmann (1995) nous apporte un éclairage particulier pour mieux comprendre le fonctionnement de l'audit interne au sein des organisations. Il est néanmoins important d'en rappeler les quelques éléments fondamentaux.

La société que nous décrit Luhmann est fonctionnellement différenciée, c'est-à-dire composée de sous-systèmes sociaux (économique, légal, scientifique, artistique, politique...) qui se distinguent de leur environnement. Les systèmes sociaux surgissent à partir des problèmes de double contingence qu'ils permettent d'affronter avec leurs opérations pour réduire la complexité. Chaque sous-système remplit des fonctions spécifiques avec ses propres modes opératoires et ses propres codes de communication.

La complexité du système est toujours inférieure à celle du milieu. En effet, comme beaucoup de relations du milieu sont inutiles pour la survie du système, celui-ci réduit la complexité au sens réduction de l'image qu'il se fait du milieu. Par la réduction, le système fixe ce qu'il pourra percevoir (le reste deviendra invisible) et une stimulation externe n'a de sens pour le système que si elle est traduite dans son propre langage.

Dès lors, les sous-systèmes sont opérationnellement clos, c'est-à-dire qu'ils ne peuvent pas communiquer entre eux mais juste traiter et interpréter les signaux extérieurs. Les sous-systèmes ne peuvent pas communiquer avec leur environnement mais juste communiquer à son sujet en utilisant leurs propres codes. Il existe dès lors un filtre appliqué par chaque sous-système à la résonance extérieure au moyen du son propre mode opératoire.

Il est important de souligner les points suivants quant à la théorie des systèmes sociaux :

- Le système ne peut pas observer l'environnement. Ainsi, un système social se distingue tellement de son environnement qu'il n'arrive à l'observer que selon ses propres codes, par exemple dans des termes juridiques, scientifiques ou économiques. Quand le système observe, il n'observe pas l'environnement « en soi » : il construit ses observations et observe ses observations codifiées ;
- Le système n'arrive pas à constater qu'il ne voit pas ce qu'il n'observe pas : chaque système a un point aveugle. Le système économique n'arrive, par exemple, à observer des problèmes d'environnement que si ces problèmes sont traduits dans des codes économiques.

- Les sous-systèmes n'arrivent pas à communiquer ensemble puisqu'un système ne communique qu'avec lui-même et ne se comprend que lui-même.
- L'absence de recours à une vision ou à un système total.

Il en résulte des implications significatives sur les pratiques d'audit interne dès lors que l'audit est considéré comme étant lui-même sous-système social. Dans cette perspective, la fonction principale de l'audit interne est de fournir une assurance sur la maîtrise des risques au sein des organisations, ce qui lui confère une fonction spécifique.

L'absence de codes de communication communs pour traiter du risque au sein de l'organisation.

Selon Luhmann (1995), tout sous-système social dispose de sa propre sémantique et de ses modes opératoires. La sémantique du système audit est fondée sur le médium sens du « risque auditable ». La distinction à laquelle il recourt est un code binaire de type « risqué/non risqué ». Le système s'observe avec ses codes et observe lui-même les opérations de ses codes, uniquement par ses codes. L'audit en tant que sous-système opérationnellement clos ne peut les observer qu'au travers de ses propres codes de communication. C'est la raison pour laquelle les risques de la cartographie des risques qui sont énoncés par le sous-système management représentent pour l'audit des « bruits » émis par son environnement. Les entretiens menés au sein des directions d'audit mettent en évidence que l'audit interne ne partage pas les mêmes codes de communication lorsqu'il est question de risque au sein de l'organisation.

FROMAGO : *« Et en fait, ce que je m'aperçois maintenant, par expérience, ce n'est pas nouveau, je suis formatrice au niveau du CIA, j'ai vu les normes passer, j'ai été à suffisamment de conférences. Globalement, on va dire, on parle souvent de risque, c'est un même mot mais qui recouvre des choses tout à fait différentes même en termes de maille ».*

RESTAULIB : *« Pour faire court, on a quand même encore un gap entre ce qui descend, je dirais qui vient beaucoup de l'audit par le biais du contrôle interne : la vision des risques et ce qui remonte des entités qui chacun a son langage, sa méthode, sa technique. On a des entités qui vont faire des cartos à deux axes, d'autres à trois axes, d'autres ne vont pas faire de cartographie, ils vont faire une identification des dix plus gros sujets à risque. Donc chacun y va de son langage machin ».*

EQUIPAUTO : « *Mais eux, souvent quand on leur demande à quoi vous pensez, ils nous parlent d'entité, ils ne nous parlent pas de processus. Et c'est en ça que je vous dis que je n'apprends pas grand-chose [...]. Oui, oui c'est vrai, ou il donne une vision parce qu'ils sont quand même très aussi reporting, résultats, et les Reporting, résultats ils ne sont pas remontés par processus en fait* ».

Le sous-système audit est opérationnellement clos, c'est-à-dire qu'il ne peut pas communiquer avec son environnement mais juste traiter et interpréter les bruits extérieurs. Les informations issues de son environnement sont dès lors traduites pour lui permettre d'établir un sens aux signaux extérieurs par ce que Luhmann nomme le processus de « re-entry ». Il s'agit pour le sous-système audit de traduire dans ses propres codes les informations qui lui parviennent de son environnement. C'est d'ailleurs pour cette raison que les risques de la cartographie sont rattachés à des processus et des risques inhérents que l'audit connaît.

CHIMICOR : « *Non il n'est pas intégré (le terme de risque), c'est pour ça qu'on essaye de donner des exemples quand on les fait voter ou qu'on présente même une fiche, on leur donne un exemple, on dit voilà [...] alors nous on prend souvent safety parce que ça leur parle, on dit voilà ce qu'il faut y retrouver* ».

LUXESTORE : « *Quand ils s'expriment (les managers interrogés par l'audit), ils disent une chose et nous on leur dit "eh bien si j'ai bien compris, ce que vous voulez dire c'est ça". Et nous on en a en tête une formulation qui a été déjà été patiné. Et Eux ils disent "oui c'est exactement ça". Donc le "ça" en question on le prend et on le met voilà en risque macro. Oui ça nous arrange nous parce que ça nous permet de raccrocher à des choses qu'on connaît. Mais ça leur correspond aussi, ça répond à ce qu'ils voulaient dire. Et par contre la déclinaison et le contenu détaillé est traduit et adapté à chacun des métiers* ».

PETROLIUM : « *On a parlé de risques en fait et c'est moi qui ait requalifié en évènement parce que on s'est aperçu que tous n'étaient pas des risques en fait. Il y a beaucoup de gens qui parlent de facteur déclenchant et qui voilà, qui ne pensent pas que c'est des risques* ».

L'audit interne : un sous-système social autopoïétique qui peut s'autoalimenter

Selon Luhman (1995), le système social est autopoïétique. L'autopoïèse signifie « se faire soi-

même ». Ainsi, un système autopoïétique est un système qui gère lui-même sa reproduction, c'est-à-dire capable de produire ses propres éléments et ses propres structures. Il précise par ailleurs que chaque système autopoïétique est caractérisé par ses opérations spécifiques. Il en résulte la mise en œuvre d'un certain nombre d'opérations qui sont propres au sous-système social qu'est l'audit interne pour communiquer à propos du risque et établir le plan d'audit et les plans de mission qui y sont associés.

Par conséquent, lors de l'élaboration du plan d'audit, l'audit interne recourt à un certain nombre de critères spécifiques pour déterminer les objets de risques au sein de l'organisation. Il s'agit notamment des objectifs de rotation et de couverture, des résultats des évaluations réalisées par l'audit au cours de ses missions passées ou encore la prise en compte des changements intervenus au sein de l'organisation. Ces éléments constituent les codes spécifiques au sous-système audit et nous renseignent sur la manière dont celui-ci appréhende différemment les risques de l'organisation par rapport à la démarche de cartographie.

MICROPIX : *« Le quatrième domaine c'est les résultats du programme de conformité SOX, où là on revoit les résultats des tests, et puis s'il y a des défaillances qui sont identifiées. Si oui, est-ce qu'il y a des points particuliers qui doivent en être ressortis pour alimenter notre planification d'audit ».*

Le plan d'audit ainsi établi permet à l'audit d'identifier des sujets et de s'auto-alimenter sans avoir à établir un lien direct avec les risques énumérés dans la cartographie des risques. Le lien qui est établi par l'audit n'est un lien indirect entre les risques de la cartographie et des processus.

NATURELIA : *« On a eu un sinistre important dans une filiale aux Etats-Unis qui traitait d'activités très marginales pour le groupe. [...] Et cette boîte-là a complètement disjoncté et au moment de la fuite de BP, son activité s'est écroulée et puis je ne sais pas, par amour-propre elle a falsifié ses résultats pour faire croire que l'activité continuait. Ça nous a coûté 100 millions d'euros, à l'échelle de Naturelia c'est important. Donc le résultat de Naturelia cette année, c'est 300 millions et on est plutôt en phase de remontée. Quand vous prenez 100 millions sur 300 c'est beaucoup. Et du coup on s'est posé la question de se dire voilà des entités qui gèrent, ce ne sont pas des grosses entités, qui gèrent des activités loufoques, enfin il y en a quand même un paquet dans le groupe. Donc il y a une année, c'était il y a trois ans, on a regardé toutes ces*

activités-là. En termes de risque sur une cartographie ça n'apparaît pas. Et à partir du moment où ça vous arrive, celle qui fait de l'éclairage d'aéroport, peut-être que je vais aller regarder ».

L'audit interne en tant que sous-système social couvre partiellement les risques de la cartographie qu'il perçoit comme des « bruits » externes qu'il observe avec ses propres codes afin de pouvoir les traduire en mission d'audit. Cette difficulté résulte en partie du fait que l'audit ne dispose pas des codes de communication des autres sous-systèmes au sein de l'organisation. Ce constat explique en partie l'écart entre l'univers d'audit et l'univers des risques. Les objets de risque considérés par l'audit portent non pas sur tous les risques mais uniquement sur ceux qui correspondent à ses codes de communication.

5 - 1 2 3 DES MODALITES D'OBSERVATION DES RISQUES QUI DIFFERENT ENTRE L'AUDIT ET LES AUTRES MEMBRES DE L'ORGANISATION.

Selon Luhmann (1993) les risques n'existent pas indépendamment de notre mode d'observation. Pour être capable d'observer, il nous faut procéder à une distinction. Si nous voulons désigner quelque chose comme étant un risque, nous devons le distinguer de ce qu'il n'est pas. Ce qui signifie que quelque chose ne peut pas être observé et désigné que s'il se distingue de quelque chose d'autre. Luhmann (1993) distingue par ailleurs deux niveaux d'observation : l'observation de premier ordre et l'observation de second ordre. L'observateur de premier ordre voit ce qu'il observe. Toute observation a une tache aveugle car il n'est pas possible d'observer simultanément les deux faces d'une distinction, c'est-à-dire à la fois quelque chose qu'on distingue et tout ce qu'il n'est pas. Par ailleurs, il n'est pas possible d'observer quelque chose et de s'auto-observer en même temps. Il est possible de le faire mais en ayant recourt à une autre distinction. Luhmann décrit l'observation de second ordre qui consiste à redoubler l'observation de premier ordre afin de voir ce qu'il voit et ce qu'il ne voit pas. Dans l'observation de second ordre, la question est de savoir quelles distinctions l'observateur de premier ordre réalise et comment il le fait. Dès lors, l'observateur de second ordre peut voir ce que l'observateur de premier ordre observe grâce aux distinctions auxquelles il recourt ainsi que les points aveugles qui en découlent.

L'audit interne comme observateur de second ordre ?

La méthodologie d'audit repose sur plusieurs actions qui contribuent à observer différemment les risques et confère à l'audit interne une position d'observateur de second ordre.

Les auditeurs n'observent pas directement les risques mais demandent à ceux qui sont en charge de les gérer aux différents niveaux organisationnels. Puisque les risques ne sont pas les mêmes en fonction du point d'observation, les auditeurs interrogent à la fois le management et les différents membres de l'organisation. En procédant ainsi, l'audit est en mesure d'identifier les risques retenus au sein de chacun des sous-systèmes sociaux de l'organisation et les points aveugles qui en découlent. Les points aveugles portent notamment sur les conséquences des décisions prises au sein d'un sous-système sur les autres sous-systèmes. Ces conséquences ne sont pas appréhendées dès lors que chaque sous-système observe avec ses propres codes. L'audit procède en pratique par recoupement lorsqu'il interroge les différents niveaux de l'organisation.

VEHICAR : « Bah c'est région métier, c'est fonctions et régions. Puisque Véhicar a à la fois à une organisation fonction et une organisation région. Donc il faut qu'on couvre les deux. Une fonction peut très bien, dans sa fonction, si je prends par exemple la fonction achat, elle ne va pas forcément me remonter à un truc pour la région Maroc par exemple. Alors que la fonction achat, elle peut dire voilà sur les achats voilà ce que je sens et la région parce qu'elle est quand même plus au courant de ce qui se passe typiquement sur le Maroc va dire moi je veux voir ce qui se passe sur les achats Maroc. Donc on croise à chaque fois fonction/région ».

GAZEO : « Alors là aussi, y a des regards croisés. C'est-à-dire que pour définir, pour cadrer la mission. Ce n'est pas qu'avec le directeur général de l'entité que l'on va aller auditer. On va aussi interviewer le contrôleur de la zone, donc des points d'entités, par exemple. On va interviewer bah peut-être la fonction globale qui sera revue donc soit les achats ici, soit la finance groupe. Alors vous voyez, il va y avoir des regards croisés. Donc on va déjà dans le plan d'audit, une thématique qui est choisie, mais on la vérifie dans cette période de cadrage, avec d'autres personnes. Donc on ne dépendra pas que de la filiale auditée en question ».

L'audit appréhende les risques selon un autre point de vue qui est le dispositif de contrôle interne mis en place par chacun des managers pour les risques dont ils sont en charge.

Enfin, l'indépendance apparaît comme une des conditions nécessaires pour permettre aux auditeurs internes de se positionner en tant que tel. « Le Cadre de Référence International pour la Pratique Professionnelle de l'Audit Interne (CRIPP) précise que l'indépendance est une

exigence des normes (normes sous la référence 1100) ». L'audit est indépendant jusqu'à son niveau de rattachement qui doit être le plus haut au sein de l'organisation selon la même norme.

MICROPIX : « *Je pense que le rattachement, il a définitivement un impact. Moi, je veux dire avant que j'arrive ici, le rattachement a été à la compliance et avant le rattachement était à la Finance. Donc, depuis que j'ai repris, le focus il a changé de manière significative. Alors que dans le passé le département était avant tout concentré sur des thématiques plutôt finance ou conformité, là on est parti sur des domaines beaucoup plus opérationnels, voire stratégiques. C'est un choix délibéré* ».

GAZEO : « *Et aussi nous sommes indépendants. Donc le fait d'être indépendant nous permet d'avoir cette ouverture d'esprit. Alors que si on devait dépendre uniquement de la finance, elle va nous orienter la finance vers, avec un certain angle de vue. Si je dépends que de la RH (rire)* »

Les limites de la méthodologie d'audit

Une première limite de la méthodologie d'audit est que l'auditeur interne doit lui-même faire certaines distinctions pour pouvoir observer les risques. Puisqu'il n'est pas possible de tout observer, les auditeurs doivent définir pour chacune de leurs missions un périmètre de revue qui se traduit par des objets d'audit. Ils doivent dès lors établir des distinctions qui consistent à sélectionner et à observer certains objets de risque et à en exclure d'autres. L'audit ne peut donc pas voir ce qu'il n'observe pas et il est lui-même soumis à des points aveugles qui découlent des distinctions qu'il mobilise.

EQUIPAUTO : « *Et c'est toute la difficulté du lien entre auditer les risques et l'audit. C'est-à-dire que pour auditer de façon approfondie un risque, il faudrait de telles ressources, de tels moyens que finalement on en aurait jamais qu'une [...] enfin on en donnera qu'une vue qui reste quand même assez générale. D'abord on n'est pas non plus des experts du domaine* ».

Le fait de choisir de couvrir une entité plutôt qu'une autre ou bien un processus plutôt qu'un autre amène l'audit à exclure de son observation certains objets d'audit et donc de risque.

SANTEFORM : « *Jamais tous, non on ne fait pas tout. Je vous donne un exemple, dans Insure and Secure, j'ai le report management, qu'est-ce que je vais aller tester qu'ils les ont bien détruits étant donné qu'ils ont plus de 10 ans ! On vérifie d'un point de vue gouvernance que c'est en place et que la procédure est connue. Après, aller voir que*

[...] on sait qu'on n'a pas la capacité, donc nous on le fait pas. On sait qu'il y a des choses qu'on ne voit jamais ».

BATI-F : *« C'est le principe de l'échantillonnage parce qu'on serait venu la veille ou le lendemain, on n'aurait pas vu la même chose. Donc, à partir du moment où on accepte qu'il y ait une part d'échantillonnage, bon [bah] autant pousser la logique jusqu'au bout. Après, c'est moi qui, quand je fais un point avec lui, je le challenge un peu dans l'équipe pour pas qu'il fasse du copier-coller dans les domaines où il est confortable et je peux très bien dire, là-dessus, quand on planifie un programme de travail, ça fait longtemps qu'on n'a pas vu ce truc-là, vous allez me regarder ce truc-là ».*

ELEC : *« Non mais quand on a fait une filiale par exemple avec 280 entités, on n'est pas allé voir 280 entités mais on est allé voir au niveau global. Alors on est allé dans certaines entités qu'on a choisies un peu au hasard et on a regardé globalement comment la filiale était pilotée, qu'est-ce qui faisait le résultat de la filiale ».*

Ces choix se matérialisent au moment de l'élaboration du plan ainsi que celui des plans de mission. Les points aveugles auxquels sont soumis les auditeurs peuvent s'avérer plus ou moins importants en fonction du type d'approche retenue par ses derniers pour appréhender les risques dans le cadre des plans de mission. Nous avons pu identifier deux approches principales. Une première qui consiste à appliquer des programmes de travail standardisés et une seconde qui consiste à établir des programmes de travail sur mesure. Les programmes de travail trop standardisés qui consistent à revoir systématiquement les mêmes processus sans tenir compte des risques spécifiques qui peuvent exister par ailleurs sont sources de points aveugles plus importants.

CHIMICA : *« On a un référentiel qui comme toujours n'est pas parfait mais qui couvre l'ensemble de ces douze cycles. On a douze cycles et puis ça marche comme ça. Et systématiquement sur ces audits transverses, on fait les douze business cycles ».*

GAZEO : *« Je vais vous dire. Nous ne sommes pas SOX, nous ne l'avons jamais été et c'est un avantage. C'est que finalement, les auditeurs n'ont pas une pile de références comme ça chez nous et donc ils sont obligés de se poser des questions. Je pense que c'est beaucoup plus difficile pour un auditeur qui a une pile de guidelines de contrôle de sortir de cette mécanique qui pour moi est de la mécanique de type SOX pour se*

poser justement des questions sur la perspective, l'environnement. Donc ça, c'est que j'attends de mes équipes, c'est qu'elle réfléchisse out of the box : ne soyez pas focalisés sur vos enjeux de conformité et réfléchissez au-delà de ça ».

La seconde limite de la méthodologie est inhérente à la durée limitée et aux ressources affectées pour réaliser la mission. L'observation nécessite du temps et l'auditeur interne doit donc définir des priorités car il ne peut pas tout observer. Le risque d'audit qui correspond au risque de non-détection par l'audit de risques significatifs ne peut pas être entièrement éliminé.

DISTRIMART : *« Ce n'est pas facile, ce n'est pas du tout évident sachant que si on fait un audit pendant trois mois, on va découvrir plus de choses que si on le fait en deux semaines. Donc ça dépend de la qualité de l'auditeur, du contexte, de la durée, ça peut dépendre de beaucoup de choses ».*

BEAUMAG : *« Non, elles ne restent pas cantonnées au programme, pour le coup elles élargissent vachement mais il y a un moment où je suis obligée de, vous voyez on en a parlé pas plus tard que cette semaine-là, où il y a un de mes auditeurs qui me dit il faut qu'on se voie parce que là j'ai tel problème, si je veux aller vraiment jusqu'au bout de la démarche, il faut que j'aïlle sur tel process. Mais là on rentrait dans tout le process de pub et de com de Beaumag, je ne sais pas si vous voyez et sinon bah j'en vois qu'un petit bout. Et là vous êtes obligé de lui dire attends, sinon la mission elle dure 6 mois ».*

Enfin, Luhmann (1993) développe aussi l'idée que notre société réduit la complexité au moyen de la différenciation fonctionnelle. La difficulté des auditeurs est de savoir comment appréhender et faire face à une complexité croissante avec des risques qui ne sont plus isolés mais tous interdépendants dans une société de plus en plus fonctionnellement différenciée. Ainsi, la méthodologie d'audit ne permet pas de répondre entièrement à une limite inhérente à la complexité des organisations et des activités qui sont auditées. Ce constat est d'autant plus vrai si l'on reconnaît que les auditeurs internes ne peuvent pas être des experts dans tous les domaines.

CHIMICOR : *« La procédure elle vous dit que vous devez identifier vos pièces critiques mais c'est vrai qu'on aura pas nous par rapport à ça un regard critique en disant est-ce que les pièces que j'ai mises dans ma liste sont les bonnes, ça on ne peut pas juger là-dessus alors nous on va regarder s'il y a un inventaire des pièces critiques et s'il n'y en a pas on va remonter le point et on ne sera pas à même de juger. Mais*

après quand vous rentrez dans ce niveau d'expertise là c'est un peu les fonctions spéciales qui s'en chargent parce qu'on a des programmes manufacturing etc. nous ça reste assez [...] ».

Le mode d'observation des risques mis en œuvre par les auditeurs confère une position unique pour observer les risques en tant qu'observateur de second ordre au sein de l'organisation. En effet, l'auditeur n'observe pas directement les risques mais observe comment les managers observent les risques, c'est-à-dire ce que les managers observent et ce qu'ils ne voient pas. L'écart qu'il peut y avoir entre l'univers des risques et l'univers d'audit s'explique par la différence de mode d'observation.

5 - 1 2 4 DES TEMPORALITES MULTIPLES LORSQU'IL S'AGIT D'APPREHENDER LES RISQUES

Luhmann (1993) définit le futur comme risque, notamment du fait qu'il dépend de nos décisions. Les risques ne sont pas les mêmes selon l'horizon temporel qui est considéré lorsque nous établissons des distinctions pour les observer. Or, les temporalités au sein de l'organisation sont multiples selon le niveau organisationnel interrogé et donc les sous-systèmes sociaux.

PETROLIUM : *« Mais vous avez raison de poser la question parce qu'on a une filiale dans le solaire qui s'appelle "SP" qui est aux Etats-Unis, qui fait des cartographies des risques depuis pas mal de temps. Quand vous les regardez, effectivement ce sont des risques qui sont maximum à deux, trois ans parce qu'ils se focalisent sur leurs risques opérationnels. C'est pas du tout la même logique que nous ».*

EQUIPAUTO : *« Alors nous finalement, on mène un peu une réflexion là-dessus et on fait un peu une présentation au comité des risques jeudi prochain. Donc on a décidé d'augmenter notre horizon de temps. Donc, nous on est plus dans une activité ou une culture qui est quand même très court-termiste. Si vous voulez, on travaille sur la production automobile mondiale, on fait des 'forecast', enfin vous voyez ce que je veux dire, bon. Et en fait, il nous apparaît important aujourd'hui que notre horizon de temps devienne vraiment celui du plan à moyen terme 3 à 5 ans. Donc justement on lance notre cartographie, enfin notre mission d'analyse de risque, cartographie dans un de nos pôles. Et là clairement on va poser qu'on est à trois ans. Voilà, cinq ans c'est peut-être un peu loin parce qu'il est quand même difficile aussi pour les gens de [...] On veut quand même balayer plus loin, parce que justement sinon nous on devient trop [...] on*

refait le même travail que les directions fonctionnelles aussi qui elles ont leurs objectifs de 12 mois ».

La dimension temporelle explique aussi en partie l'écart entre univers des risques et univers d'audit puisque les sous-systèmes n'ont pas les mêmes horizons de temps pour appréhender les risques.

5 - 2 LE PROCESSUS D'AUDITABILITE : LA TRANSFORMATION DES RISQUES EN RISQUES AUDITABLES

Selon Power (1999), contrairement à l'image officielle de l'audit souvent présenté comme une activité neutre, il s'agit d'un processus actif qui vise à « rendre les choses auditables ». Toutefois, Power ne décrit pas comment l'audit procède pour rendre les objets de risque auditables. La deuxième contribution de cette thèse est de décrire le processus d'auditabilité qui permet de comprendre comment les auditeurs internes rendent les objets de risque auditables.

Il est nécessaire de préciser quelles sont les caractéristiques d'un risque non auditable. Il sera ensuite possible d'analyser le processus mis en œuvre par les auditeurs pour transformer les objets de risque en objets auditables.

5 - 2 1 LA DISTINCTION ENTRE RISQUE AUDITABLE ET NON AUDITABLE

Les auditeurs considèrent que tous les risques ne sont pas auditables ou bien qu'ils le sont mais de façon partielle. Le critère d'auditabilité se traduit de différentes façons avec néanmoins un certain nombre de points communs.

5 - 2 1 1 L'AUDITABILITE EN LIEN AVEC LE NIVEAU DE DESCRIPTION DU RISQUE

Les directeurs de l'audit illustrent leurs difficultés pour passer des risques de la cartographie aux missions du plan d'audit tout d'abord par le faible niveau de description des risques dans la cartographie.

VESTIMOD : « *En gros, il y a, c'est un fichier Excel, il y a quinze lignes. C'est vraiment très, très macro en termes de risque, c'est « risque fournisseur ». C'est vraiment des, le plus macro qu'on puisse être, est-ce qu'on a quelques contrôles au-dessus, on est à risque on l'accepte ou pas, voilà [...]. C'est une vue d'avion et on ne s'en sert pas aujourd'hui. Elle n'est pas à la base du plan d'audit. Ça fait partie des missions de cette année de la mettre à jour et d'avoir un truc un peu plus robuste ».*

De surcroît, les risques de la cartographie ne font pas toujours référence à des processus. Or, l'audit appréhende les risques par une approche processuelle. Le fait de désigner une entité ou bien un pays comme étant un risque n'est pas suffisant pour déterminer quels sont les processus qui sont potentiellement susceptibles d'impacter négativement l'atteinte des objectifs de ces organisations. De la même manière, le fait de désigner un projet comme étant un risque ne

permet pas d'identifier de façon précise quels sont les processus ou les activités spécifiques qui sont de nature à pouvoir impacter l'atteinte des objectifs du projet concerné.

RESTAULIB : « *On ne peut pas dire j'arrive en France et je fais un audit en deux semaines. Je ne couvre pas la France, il faut que j'attaque par processus. Donc en fait la France, on va découper la France en processus. On va faire un audit des achats, on va faire un audit des RH. Et à l'intérieur des RH, on va peut-être même découper en sous-processus tellement c'est gros en disant qu'il y a le processus de recrutement, le processus d'évaluation des performances, de gestion de carrières, de formation, jusqu'au processus de termination* ».

CHIMICOR : « *Il m'a fallu du temps pour arriver à ça parce qu'en fait, parce que jusqu'à présent avant d'avoir mon organisation intégrée je voyais la carto et je me disais je ne sais pas convertir ça. C'est le premier truc qu'on a discuté en mission d'audit, je ne sais pas comment traduire ça en mission. Et à force de tourner autour du truc comme un requin, j'ai fini par me dire la seule façon, c'est qu'il faut que je change de maille, que je descende un cran en dessous, que je sorte du risque stratosphérique* ».

5 - 2 1 2 L'ORIGINE DES EVENEMENTS COMME SOURCE DE NON AUDITABILITE

La deuxième caractéristique associée à un risque qualifié de non auditable concerne l'origine des événements qui sont qualifiés comme étant des risques. Lors de l'élaboration des cartographies des risques, certains éléments sont qualifiés à tort comme étant des risques alors qu'il s'agit de danger au sens de Luhmann (1993). De surcroît, il s'agit de facteurs externes pour lesquels il n'existe pas toujours de processus identifiables. Et lorsque des processus existent pour minimiser les impacts liés à la survenance d'un danger, la couverture ne peut être que partielle.

BATICOSTO : « *Quand c'est totalement exogène c'est difficilement auditable, quand c'est plutôt endogène on a forcément plus de prise* ».

PETROLIUM : « *Moi, j'ai des thématiques qui sont validées au niveau du Comex, je n'ai aucune idée de la façon dont je vais le traiter. Et donc je commence à discuter avec les uns les autres, à réfléchir. Bon je vais prendre un exemple concret parce qu'il est d'actualité : contrôle des fournisseurs et des chaînes de sous-traitance par rapport à la conformité sociétale (rire). Bon, sujet intéressant, sujet qui comporte des risques*

majeurs. Comment on traite ça ? On ne peut pas faire des audits chez les fournisseurs, enfin voilà on ne peut pas avoir une méthodologie d'audit standard. Donc là moi, mon réflexe c'est déjà de documenter ce qui existe en termes de pilotage et de dispositif de maîtrise au niveau des branches, des activités. Et je vais essayer de documenter ça. Ça va être le but de cet audit. Documenter et montrer les problèmes qui se posent, si effectivement il y a des approches qui sont très, enfin peu cohérentes on va dire, si dans certains secteurs on n'a pas d'approche parce qu'on n'a pas perçu les enjeux ».

Tout comme les dangers, les risques identifiés dans la cartographie qui ne sont pas couverts par des dispositifs de maîtrise destinés à en minimiser les effets sont jugés comme étant difficile à auditer.

GAZEO : *« Parce que là on revient aux scénarios dont on a parlé tout à l'heure, les black Swan, où aujourd'hui en termes d'audit, on ne se positionne pas là-dessus. Parce que les risques, ils ne sont même pas identifiés comme tels dans nos organisations. On est en train de les imaginer en prospective et donc il n'y a pas de dispositif de maîtrise puisqu'ils ne sont pas formalisés aujourd'hui ».*

5 - 2 1 3 LA COMPETENCE DES AUDITEURS COMME SOURCE DE NON AUDITABILITE

Certains risques de la cartographie sont considérés comme difficiles à auditer du fait de l'absence de compétence au sein de l'équipe d'audit. Au sens de Luhmann (1993), les auditeurs jugent que certains risques ne sont pas auditables dès lors qu'ils ne rentrent pas dans leurs codes de communication.

VESTIMOD : *« Pas de compétence informatique particulière, enfin on n'est pas des auditeurs informatiques, donc, le volet informatique, on l'a pas ».*

LUXESTORE : *« Oui mais je pense que c'est les deux. Vous avez raison parce que aussi bien ça pouvait s'auditer mais j'ai une limite dans l'exercice de cet audit parce qu'on est censé être la maison qui vend les produits de qualité avec la qualité la plus élevée au monde dans son domaine. Et donc je n'ai pas un auditeur qui serait capable d'auditer le dispositif de qualité de cette nature. Mon critère c'était, oui ça peut être la compétence. Mais même en s'obstinant, à supposer qu'on en ait de la compétence, par exemple le processus artistique, non, je n'irais pas, je n'irais pas. Je n'irais pas auditer ça parce que, comment dire, je trouve que pour l'emploi de nos ressources dans un exercice*

coût/valeur ajoutée, je ne trouve pas que ça serait le meilleur placement que je puisse faire, avec un gros risque de se faire arakiri au passage, d'accord ?! ».

Malgré ces difficultés, l'audit parvient à traiter des risques de la cartographie en mettant en œuvre un processus spécifique de transformation des risques pour les rendre auditables.

5 - 2 2 LE PROCESSUS DE TRANSFORMATION DU RISQUE EN RISQUE AUDITABLE

Power (1999) décrit dans sa théorie sur la société de l'audit comment l'audit contribue pour donner à une organisation l'illusion de la transparence de ses activités. Le paradoxe décrit par l'auteur est que ce qui est considéré comme pouvant être le défaut de l'audit, à savoir le fait qu'il ne détecte pas un dysfonctionnement ou une faiblesse renforce sa position et sa prise sur le fonctionnement même de l'organisation. Selon l'auteur, en tant que telle, une entreprise ne peut être soumise à un audit : seuls les systèmes laissant une trace publique de ses activités le peuvent. Dès lors, pour que l'audit soit en mesure d'évaluer et de vérifier, il faut rendre les choses auditables. L'audit, qui déclare réaliser une observation neutre et objective des activités influe en réalité sur celle-ci. Ce qui devient officiellement visible aux yeux du public est considéré et reconnu comme étant important. À l'inverse, les activités et les pratiques rivées de cette visibilité ont un problème de légitimité, ce qui occasionne un transfert des ressources et des énergies vers les activités "auditables".

L'auditabilité n'est pas une propriété naturelle des opérations ni fonction non plus de la qualité des preuves qui existent dans l'environnement dans lequel l'audit opère. Au contraire, l'audit construit activement la légitimité de sa propre base de connaissances et cherche à créer un environnement favorable pour rendre celle-ci efficace. Les techniques de l'audit font partie de cette base de connaissance qui doit répondre à un impératif : rendre les objets auditables. Toutefois, l'auteur ne décrit pas comment l'audit procède pour y parvenir.

La deuxième contribution de cette thèse est de préciser comment les auditeurs internes parviennent à transformer les risques en risques auditables et de décrire le processus d'auditabilité.

5 - 2 2 1 L'ÉVALUATION DU RISQUE SUR LA BASE DES PLANS D'ACTION

Le risque une fois identifié dans le cadre du processus de gestion des risques est en principe adressé par le management qui peut décider soit de l'accepter en l'état ou bien de le réduire par la mise en place de dispositif de contrôle interne. L'audit considère qu'il doit pouvoir s'appuyer

sur des éléments vérifiables pour établir son opinion d'audit. C'est la raison pour laquelle il considère qu'un risque identifié en tant que tel mais qui ne fait pas l'objet d'un plan d'actions ou d'un dispositif de contrôle interne est difficile à auditer. L'auditabilité est ainsi liée à la notion de vérifiabilité. Aussi, un risque qui est considéré comme non auditable au moment le devient dès lors que l'audit dispose pour ce même risque d'un plan d'actions formel établi par le management pour le traiter. L'audit n'évalue pas dans cette situation le risque en soi mais le plan d'actions destiné à le traiter. Le processus de transformation mis en œuvre par l'audit consiste à considérer qu'auditer le plan d'actions permet indirectement d'auditer le risque auquel il est associé. Le plan d'actions constitue dans ce cas-là l'objet auditable auquel se raccroche l'audit.

CHIMICOR : *« Oui il y a pas mal de risques sur lesquels on approche comme ça parce que la maille est beaucoup trop large pour qu'on sache l'auditer. Donc on recommence à serrer la maille et le jour où on aura des actions concrètes décrites dont on nous dira qu'elles sont mises en œuvre, on vérifiera leur mise en œuvre ».*

5 - 2 2 2 L'ÉVALUATION DU RISQUE SUR LA BASE DU DISPOSITIF DE CONTRÔLE INTERNE

Parmi les options de traitement possibles face à un risque, le management peut décider de le partager (assurance, partenariat, ...) ou bien de le réduire en mettant de place des dispositifs de contrôle interne. Les dispositifs de contrôle interne représentent l'ensemble des dispositifs de maîtrise d'un risque qui sont déployés au sein d'une organisation. Le plan d'actions est l'étape préalable à la mise en place de ces dispositifs de maîtrise. Une fois ces dispositifs définis, l'audit peut aller au-delà de la simple évaluation du plan d'actions qui avait été initialement établi et s'appuyer sur de nouveaux objets auditables. Dans ce cas, les objets auditables ne sont plus les plans d'actions mais les dispositifs de contrôle interne qui ont été déployés à l'issue du plan d'actions.

Considérons par exemple le cas du risque de fraude qui peut figurer en tant que tel dans une cartographie des risques afin de mieux comprendre comment l'auditeur procède pour le traiter. Le risque de fraude se rapporte aux dispositifs de contrôle interne relatifs à la protection des actifs. Ce risque tel que stipulé en l'état pose une première difficulté car il peut se rapporter à de nombreux processus au sein de l'organisation. Il peut concerner le processus de paye, le processus achat, le processus de gestion des stocks, le processus de vente ou encore le processus financier. L'auditeur qui doit traiter le risque de fraude ne peut pas couvrir l'ensemble de tous

les risques de fraude possible et doit donc procéder à des choix. L'auditeur doit donc dans un premier temps déterminer les processus qu'il souhaite couvrir, sans quoi il lui sera difficile de traiter du risque de fraude en l'état.

Le risque de fraude qui figure dans une cartographie des risques peut se rapporter à un grand nombre de processus et de risques spécifiques. Le fait de rattacher un risque à des processus permet à l'audit de déterminer des risques plus spécifiques en lien direct avec les processus concernés. Le fait de déterminer un processus pour traiter du risque de fraude identifié dans la cartographie permet à l'audit de le couvrir en partie. Pour le couvrir intégralement, il faudrait traiter du risque de fraude au niveau de tous les processus concernés et cela au niveau de toutes les entités. Dès lors, la couverture d'un risque de la cartographie n'est que partielle. Néanmoins, en procédant ainsi, l'audit réussit à passer du risque de la cartographie à un risque auditable comme l'illustre le tableau ci-dessous.

Tableau 48. Illustration de l'approche d'audit sur un risque de fraude

Processus	Risques inhérents
Processus paye	Paiement de salaires à des salariés fictifs, paiement de bonus non justifiés, paiement de salaires non conformes aux contrats de travail, ...
Processus achat	Collusion entre un acheteur et un fournisseur, paiement de factures pour des biens ou services fictifs, ...
Processus de gestion des stocks	Vol de marchandise, déclaration de faux rebuts pour détourner les produits finis destinés à la revente.
Processus financiers	Etablissement de faux états financiers, utilisation frauduleuse des moyens de paiement, ...
Processus vente	Corruption de fonctionnaires pour l'obtention de marchés, ...

Afin de l'illustrer considérons par exemple que l'audit décide de traiter du risque de fraude dans le processus achat et plus spécifiquement du risque de fraude sur les paiements des fournisseurs. Le risque principal pour ce processus est de payer une facture non justifiée, c'est-à-dire de

verser de façon délibérée des sommes d'argent en contrepartie de services inexistantes ou bien pour un prix supérieur à celui prévu au contrat. Dans le cas du processus de paiement des factures fournisseur, la fraude peut se réaliser s'il n'existe pas de contrôles prévus au moment du paiement des factures pour s'en prémunir ou bien que les contrôles prévus soient mal définis et donc inefficaces.

Il est par exemple possible d'imaginer le risque d'avoir un fournisseur qui facture des quantités non commandées et qui est payés faute d'avoir des contrôles de prévention. Le dispositif de contrôle peut consister à avoir un blocage automatique de toutes les factures reçues pour lesquelles il n'existe pas de bon de commande dans le système d'information. Un deuxième contrôle peut consister à réconcilier systématiquement le montant facturé du bon de commande et du bon de réception pour vérifier la cohérence des quantités et des prix livrés et facturés. Un troisième contrôle peut consister à prévoir qu'il n'est pas possible pour une même personne de réaliser à la fois la commande et la réception des biens. L'ensemble de ces contrôles qui sont complémentaires peut contribuer à limiter le risque de fraude sur le paiement des fournisseurs.

Tableau 49. Illustration de l'approche d'audit sur un risque de fraude sur les paiements

Processus achat	Risques inhérents	Dispositifs de contrôle
Processus de règlement des fournisseurs	Paiements de factures non justifiés (surfacturation du fournisseur non détecté lors du paiement, paiement de quantités non réceptionnées physiquement...).	Séparation des tâches entre celui qui commande, celui qui reçoit et celui qui comptabilise Rapprochement entre bon de commande, bon de réception et facture Blocage des factures sans commande Contrôle des droits informatiques

Auditer un risque en l'appréhendant par les processus revient alors à auditer non pas le risque en soi mais les dispositifs de contrôle interne destinés à s'en prémunir. Le principal avantage de cette approche est de fournir à l'audit des objets auditables.

RESTAULIB : « *Je m'assure qu'il y a un département sécurité alimentaire qui fait des audits tous les mois. En fait je viens m'assurer que le contrôle existe. Je ne viens pas faire un contrôle moi-même sur un domaine que je ne connais pas* ».

PETROLIUM : « *Et le regard d'un naïf est souvent très percutant. Quand vous demandez à un manager bon je ne connais pas votre métier, expliquez-moi à quoi ça sert, quels sont vos objectifs, qu'est-ce qui peut se produire qui fasse qu'un objectif ne soit pas atteint. En général, ils n'ont jamais abordé leur métier comme ça donc ils y vont et ils sortent tous les risques possibles. Bon maintenant qu'est ce qui a comme dispositifs pour que ça, ça tienne la route et que ces risques ne se produisent pas* ».

Le processus de transformation mis en œuvre par l'audit consiste à considérer qu'auditer les dispositifs de contrôle interne liés à des processus sous-jacents à un risque permet indirectement d'auditer le risque auquel ils sont associés implicitement par l'audit. Les dispositifs de contrôle interne constituent les objets auditables auxquels se raccroche l'audit.

5 - 2 2 3 L'ÉVALUATION DU RISQUE SUR LA BASE DU RÉFÉRENTIEL DE CONTRÔLE INTERNE

Il est possible que l'audit soit confronté à des risques pour lesquels des dispositifs de maîtrise ont été définis mais que ces derniers soient plus ou moins formalisés ou bien déclinés de façon partielle ou hétérogène au sein de l'organisation. L'audit peut alors avoir des difficultés pour apprécier la qualité des dispositifs de contrôle interne en place et émettre une opinion sur leur robustesse. Pour pallier ces difficultés, les auditeurs internes peuvent alors recourir à une procédure spécifique qui vise à construire ce qu'ils nomment un référentiel de contrôle interne.

BATI-F : « *C'est ce que j'appelle une base 100 qui est sept processus. Et c'est ça que j'audite quand je fais un audit d'entité opérationnelle, je vais auditer les sept processus qui sont les même qu'ici vous voyez, vous retrouvez les codes couleurs. Organisation, prise d'affaire, RH, prévention, etc. On est censé avoir toutes ces bonnes pratiques-là. Donc on va vérifier qu'en termes de coordination commerciale, on a bien identifié telle et telle chose, qu'il y a bien des préparations commerciales en amont, ensuite il va y avoir [...]. C'est ce qu'on appelle notre guide de référence, c'est notre référentiel de contrôle interne. [...] On l'a appelé comme ça parce qu'avant on l'appelait guide des bonnes pratiques, on l'a appelé maîtrise de nos risques et puis on l'a diffusé aux entités opérationnelles* ».

DISTRIMART : « On établit un cahier de bonnes pratiques, on fait valider, par exemple, si c'est les achats, on envoie à tous les patrons d'achats ou au minimum à la moitié, et on dit on va vous auditer sur ça, ça, ça. On parle surtout des bonnes pratiques. Évidemment, il y a des bonnes pratiques pour être plus performants et des bonnes pratiques pour maîtriser le risque. Après, on doit balancer tout ça mais on crée un référentiel des bonnes pratiques ».

La norme 2130.A1 (IIA, 2014) précise que l'évaluation du dispositif de contrôle interne doit porter sur les aspects suivants :

- l'atteinte des objectifs stratégiques de l'organisation ;
- La fiabilité et l'intégrité des informations financières et opérationnelles ;
- l'efficacité et l'efficience des opérations et des programmes ;
- la protection des actifs ;
- le respect des lois, règlements, règles, procédures et contrats.

Pour établir ce référentiel, le travail de l'audit procède en deux temps. Un premier temps qui consiste à décliner le risque à auditer de façon méthodique pour l'appréhender en fonction de chacun des cinq axes définis dans la norme 2130. A1 (ci-dessous). Considérons pour illustrer la démarche le cas d'un risque de la cartographie : la gestion des stocks. Afin que l'audit puisse comme dans le cas précédent faire le lien avec des processus, il va traduire le risque pour chacun des axes. A titre d'exemple, dans le cas de l'objectif de protection des actifs, le risque spécifique lié à la gestion des stocks peut être traduit en deux sous-risques.

Tableau 50. Exemple de déclinaison du risque de la cartographie en risque spécifique

Objectif de contrôle interne	Risques de contrôle interne
Protection des actifs	Sous-risque n°1 : vol des stocks Sous-risque n°2 : détérioration involontaire des stocks en lien avec les mauvaises conditions d'entreposage

Ce travail devra être effectué de façon méthodique pour chacun des cinq axes (stratégie, performance, protection, qualité de l'information, respect des lois et règlements).

Une fois après avoir décliné le risque en sous-risques spécifiques sur la base des catégories d'objectif de contrôle interne, l'auditeur va chercher à inventorier l'ensemble des événements possibles qui sont susceptibles de remettre en cause l'atteinte des objectifs de contrôle interne.

Tableau 51. Exemple de déclinaison du risque spécifique en événements risqués

Objectifs de contrôle interne	Risques inhérents	Risques inhérents spécifiques
Protection des actifs	Sous-risque n°1 : vol des stocks	Magasin d'entreposage non sécurisé
		Absence de contrôle à la sortie du site
	Sous-risque n°2 : détérioration des stocks	Incendie
		Inondation

Par exemple pour le risque d'incendie, il pourra être possible d'équiper les zones d'entreposage d'équipements de prévention comme les détecteurs d'incendie, des extincteurs automatiques.

Ce référentiel peut être établi par l'auditeur en interrogeant les managers. L'objectif pour l'auditeur est de se faire décrire les processus dont les managers sont en charge, les risques associés aux processus et les contrôles type nécessaires pour y faire face. L'audit pourra une fois ce référentiel établi sur l'aide des experts du sujet au sein de son organisation pour le compléter et le valider.

ELECTROSTORE : « *J'ai identifié dans le business quels étaient les experts de différents domaines et je les ai rencontrés, je leur ai dit expliquez-moi quels sont vos risques et expliquez-moi comment vous les gérez. Et après si vous voulez toute la beauté de l'exercice enfin la complexité aussi c'est de sortir par ce que ces gens-là m'ont expliqué qu'ils faisaient dans leur propre organisation, c'est d'en faire des principes généraux pour qu'ils soient universellement applicables* ».

ENGINICO : « *Alors on a testé notre analyse des risques sur une entité test justement qui était réputée comme fonctionnant bien. Et c'était ça qui nous intéressait justement, c'était de voir en termes de top comment les gens se comportaient, ce qu'ils faisaient. Donc on a enrichi notre base de contrôle, on en a retiré certains, on en a remis d'autres etc. en introduisant dès le début puisque donc le référentiel de contrôle interne était quelque chose qui était paradoxalement relativement bien connu grâce au questionnaire annuel d'auto-évaluation de contrôle interne dont on reparlera* ».

Une fois le référentiel de contrôle interne établi, l'audit est en mesure d'apprécier l'écart entre les pratiques effectives constatées dans le cadre de ses missions et les principes de bonne gestion du risque issus du référentiel.

SANTEFORM : « *On a proposé une approche par process en faisant un benchmark de différentes entreprises et discuté avec des consultants, parce qu'on a des anciens consultants dans le département. On a fait une première proposition et au bout d'un moment quand on a eu un souci de re-renforcer le contrôle interne, on a mis le fameux département Internal Control and Process qui est passé de SOX à quelque chose de plus globale. Et donc il est reparti de nos process, il a refait la value chain et a demandé à chacun des business de valider l'ensemble de ses processus. Dans les deux premières colonnes process/sous process sont validés par les métiers. Le contrôle interne a défini les mandatory controls qu'il y a en face, il y en a 300 au total. Et nous, notre programme d'audit, il fait 300 lignes multipliées par 4-5 tests à chaque fois, donc ça fait 1500 lignes* ».

L'avantage que présente cette démarche est qu'elle permet à l'auditeur d'appréhender de façon méthodique un risque sous plusieurs dimensions qui sont toutes interdépendantes. Elle limite pour l'auditeur le risque d'omettre une de ces dimensions lors de son évaluation des risques. Pour illustrer cette idée, considérons de nouveau le risque de gestion des stocks. Le fait que les auditées aient mené les actions d'optimisation satisfaisantes n'exclut pas le vol ou bien les erreurs de comptabilisation.

Il est important de noter que les objectifs de contrôle interne sont intimement liés aux objectifs du modèle de l'*Entreprise Risk Management (ERM)*.

On retrouve dans le modèle de l'ERM les objectifs stratégiques, de performance (sous l'intitulé opération), de qualité de l'information (sous l'intitulé reporting) et de respect des lois et règlements (sous l'intitulé compliance). Le seul qui n'y figure pas est la protection des actifs.

Le fait que les catégories d'objectif et donc de risque du modèle de l'ERM soient les mêmes (à l'exception de la protection des actifs) que ceux du contrôle interne permettent à l'auditeur de faire le lien entre les risques de la cartographie et les risques de contrôle interne auditables. L'auditeur parvient à établir le lien en le risque de la cartographie et le contrôle interne en raccrochant le risque et des processus dotés de dispositifs de contrôle interne. Auditer les risques de la cartographie revient à auditer les processus sous-jacents au risque et donc à auditer les dispositifs de contrôle interne auditables.

Ce modèle implique que les menaces externes difficiles à couvrir par des processus ne sont pas considérées comme des risques auditables alors qu'ils peuvent impacter l'organisation. Les risques appréhendés par l'audit correspondent aux risques de contrôle interne auditables, c'est-à-dire les risques couverts par des dispositifs de maîtrise en lien avec des processus.

5 - 2 2 4 L'EVALUATION DU RISQUE EN PASSANT PAR LE SYSTEME D'AUTO-EVALUATION DU CONTROLE INTERNE

Le référentiel de contrôle interne établi par l'audit ne constitue pas en tant que tel un dispositif de contrôle interne qui a une nature prescriptive pour l'ensemble des entités de l'organisation. Un moyen pour l'audit de les faire appliquer par le plus grand nombre au sein de l'organisation est de s'appuyer sur la mise en place d'un système d'auto-évaluation du contrôle interne. Dès lors que l'audit interne construit le processus d'auto-évaluation du contrôle interne en lien avec son référentiel de contrôle interne, il lui donne un caractère prescriptif qui oblige les entités de son organisation à s'y conformer.

BATICOSTO : « *Le contrôle interne définit l'ensemble des principes applicables. C'est par rapport à ça que les auditeurs pourront auditer. La règle, c'est les règles de contrôle interne. Donc les auditeurs vont vérifier que les principes sont bien appliqués opérationnellement. Donc ça ça sert* ».

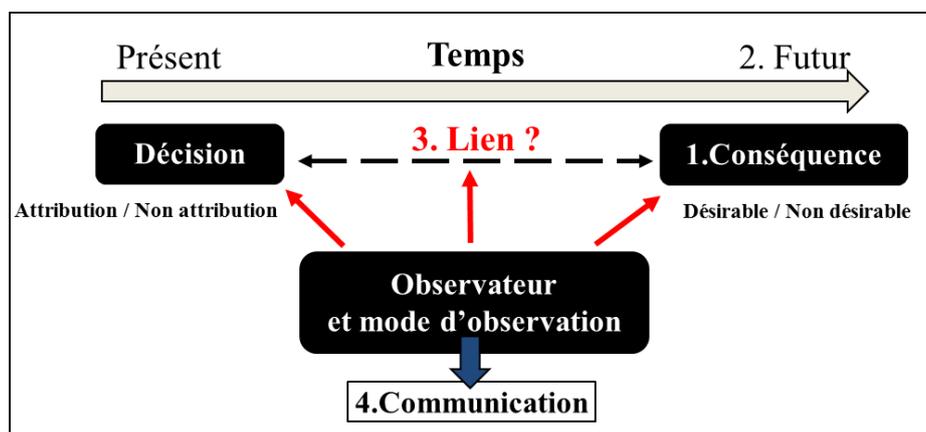
Le système d'auto-évaluation permet à l'audit de transformer les risques de son organisation en traitant des risques de contrôle interne au travers des questionnaires d'auto-évaluation du contrôle interne.

5 - 2 2 5 L'AUDIBILITE COMME RESULTAT DES HEURISTIQUES ORGANISATIONNELLES

Pour Luhmann (1993), le risque n'est pas indépendant des modes d'observation. Pour Luhmann, il est nécessaire de remplir quatre conditions pour désigner et distinguer un risque d'un danger. La première est d'apprécier la conséquence d'un événement et de déterminer s'il s'agit d'une fortune ou d'une infortune. La seconde est d'appréhender cette conséquence en lien avec l'horizon de temps. La troisième est de réussir à établir un lien qui n'est pas naturel entre d'une part la conséquence et d'autre part une éventuelle décision. Sans ce lien, il ne s'agira pas d'un risque mais d'un danger au sens de Luhmann, qui sera alors attribué à des facteurs externes. Et la dernière condition est que le risque soit communiqué, sans quoi il n'existe pas et n'a pas de valeur sociale. Chacune de ces opérations sera dépendante du mode d'observation mis en œuvre et des distinctions associés. Selon Luhmann (1993), chaque sous-système observe avec ses propres modes opératoires et l'audit en tant que sous-système social observera d'une façon spécifique les risques au sein de son organisation. Un risque identifié dans la cartographie pour lequel l'audit n'est pas en mesure d'établir un lien avec une décision ne constitue pas un risque auditable. Il est en effet nécessaire pour l'audit d'établir le lien entre les risques de l'organisation et des décisions qui se matérialisent par la mise en place de dispositifs de contrôle interne. Cela nécessite aussi de communiquer sur ces risques auditables au travers du plan d'audit.

Le schéma ci-dessous représente les quatre dimensions complémentaires et interdépendantes du risque qui sont reprises dans la définition du risque établie par Luhmann (1993). L'heuristique consiste à apprécier une conséquence en lien avec le temps qu'il faut réussir à relier à une décision. Une fois le risque identifié, il est nécessaire de communiquer à son sujet.

Figure 24. Heuristiques organisationnelles pour transformer les risques en risques auditables



Les résultats de cette recherche décrivent les différentes dimensions techniques que peut revêtir le processus d'auditabilité. Néanmoins, il est essentiel de comprendre qu'il présente des enjeux qui vont au-delà d'un simple problème technique et qui sont d'ordre sociétal. Le processus d'auditabilité n'est pas une activité neutre.

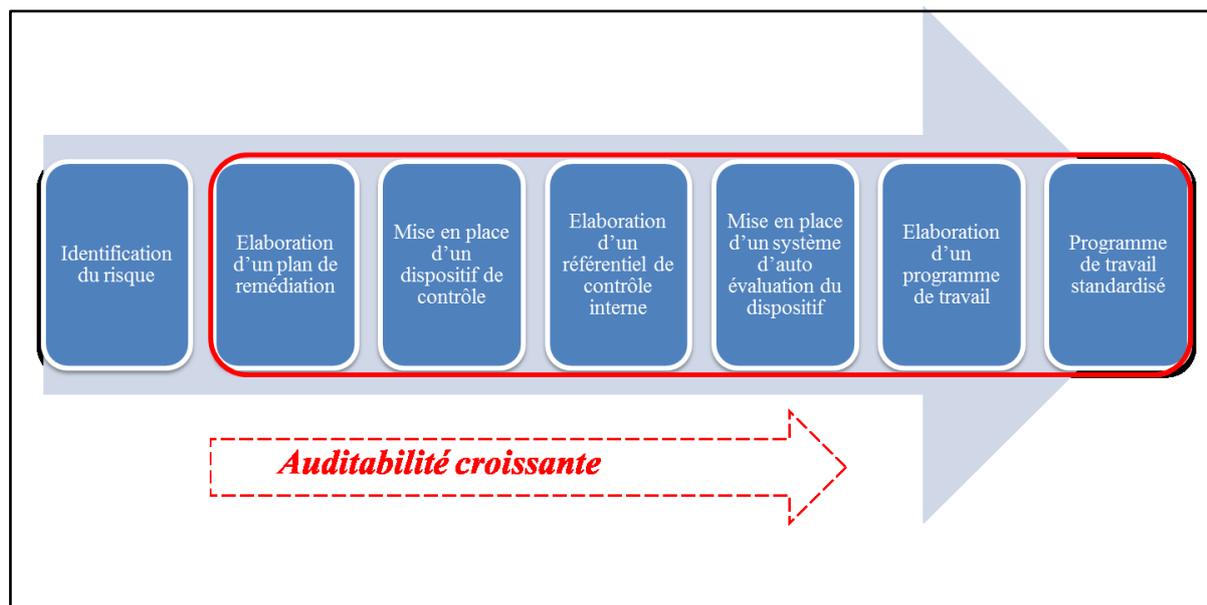
Une auditabilité croissante dans le temps

Les résultats de cette recherche montrent que l'auditabilité du risque est croissante dans le temps en fonction de la nature et du niveau de déploiement des actions mis en œuvre par le management en réponse face aux risques qu'il a identifiés. Le processus d'auditabilité amène l'organisation à formaliser de façon progressive ses dispositifs de contrôle interne et à les généraliser. Du fait de la généralisation et la standardisation progressive des dispositifs de contrôle interne, les auditeurs disposent d'un plus grand nombre d'objets de risque auditables.

MULTIMEDSTORE : « *Alors comme moi je suis parti de zéro il y a cinq ans et vous voyez et vous voyez la première version c'était avril 2012, il a fallu construire les règles, après il a fallu les faire auto évaluer, puis après j'ai commencé à les auditer. Donc il a fallu que je construisse des programmes de travail. Les premiers datent de début 2013, donc maintenant on a des programmes de travail. Mais la logique est la même, on part de ces règles qui ont des risques sous-jacents et puis à l'intérieur on a des tests, et où on a, oui des tests, des demandes de documents qui justifient que les contrôles sont bien en place ».*

Le schéma qui figure à la page suivante représente le processus d'auditabilité. et montre que l'auditabilité est croissante.

Figure 25. Représentation du processus d'auditabilité



Le risque au moment où il est identifié est considéré par l'audit comme difficile à auditer en l'état en l'absence de plan de traitement. Les directeurs de l'audit considèrent qu'ils peuvent être audités dès lors que des plans d'action auditables sont établis par le management pour y faire face. Cette première exigence a pour effet de pousser l'organisation à formaliser ses plans de traitement des risques. L'audit peut évaluer non pas le risque en soi mais les plans d'actions qui visent à les traiter. L'objet de risque auditable devient le plan d'action et le risque associé correspond à sa non mise en œuvre.

Une fois cette exigence satisfaite et les plans d'action mis en œuvre, l'audit dispose de dispositifs de contrôle interne qui peuvent être plus ou moins formels et développés. Ces dispositifs sont réputés pouvoir contribuer selon l'audit à réduire l'exposition aux risques au sein de l'organisation. Le fait de rendre ces contrôles formels permet à l'audit de disposer de nouveaux objets auditables.

Les auditeurs peuvent une fois ces dispositifs établis exiger d'avoir une homogénéisation plus importante de ces dispositifs en prenant comme référence les pratiques habituellement efficaces et qui se traduisent par des référentiels de contrôle interne introduits par l'audit.

L'homogénéisation et la standardisation des pratiques passent néanmoins par une étape de prescription auprès des entités des dispositifs de contrôle interne attendus. Pour s'assurer de la correcte application des standards, l'audit déploie introduit alors des systèmes d'auto-évaluation du contrôle interne. Les entités de l'organisation doivent déclarer si elles ont

effectivement mis en place les contrôles exigés et reconnus comme des standards. Le cas échéant, elles doivent définir un plan d'actions destiné à permettre la mise en place des dits dispositifs qui pourront à leur tour être audités et constituer de nouveaux objets auditables.

Une fois que certains dispositifs de contrôle interne ont été définis comme étant les standards à appliquer au sein de l'organisation, l'audit peut alors développer des programmes de travail de plus en plus standardisés. Ces programmes de travail viseront alors à apprécier la conformité des pratiques avec les dispositifs qui ont été définis comme les standards de l'organisation. Les cas de non-conformité donneront lieu à la définition de plan d'actions qui seront audités.

Les implications sociétales du processus d'auditabilité

La nécessité qu'a l'audit de traduire les risques de la cartographie en risques auditables renforce l'idée que l'audit représente un sous-système social. Les risques de la cartographie constituent des bruits issus de l'environnement que l'audit doit interpréter en fonction de ses propres codes de communication afin de les rendre auditables.

Le fait que les auditeurs observent les risques avec leurs propres codes de communication peut constituer un risque pour l'organisation ; plus précisément de porter son attention sur les risques sélectionnés par l'audit au détriment des autres risques. L'hétérogénéité des codes de communication qui sont utilisés pour appréhender les risques au sein des organisations constitue à ce titre-là une source de risque pour l'organisation.

Le déploiement du modèle de l'*Enterprise Risk Management* combiné au besoin de le rendre auditable amène l'organisation tout entière comme le décrit Power (1999, 2009) à porter ses efforts sur la formalisation croissante de dispositifs de contrôle pour justifier et démontrer la bonne gestion de ses risques.

Le processus d'auditabilité illustre bien comment l'organisation tout entière est amenée de façon progressive et continue à définir des dispositifs de contrôle, à les formaliser pour assurer la production des preuves nécessaires pour les rendre auditables.

L'activité d'audit n'est pas neutre sur la construction des objets de risque au sein des organisations. L'audit façonne au sein de son organisation la manière de voir les risques des autres membres et va au-delà en désignant les risques qui sont importants et cela peut-être même au détriment d'autres risques ou menaces qui pourraient être plus graves.

5 - 3 LES CONSEQUENCES SUR LA QUALITE DE L'AUDIT ET LE LIEN ENTRE AUDIT INTERNE ET GOUVERNANCE.

Les résultats de cette thèse montrent que les risques pris en compte par les auditeurs internes dans le cadre de la planification de leurs travaux ne sont pas les mêmes que ceux des opérationnels et notre cadre d'analyse permet de l'expliquer.

Cet écart constaté entre l'univers d'audit et l'univers des risques ainsi que le processus d'auditabilité mis en œuvre par les auditeurs nous amène à nous interroger sur ses conséquences, sur le rôle et sur l'efficacité de l'audit interne dans le dispositif de gouvernance ainsi que sur les critères pour apprécier la qualité de l'audit.

5 - 3 1 LE LIEN ENTRE AUDIT INTERNE ET GOUVERNANCE

La littérature sur l'audit interne s'est particulièrement développée ces dernières années, notamment à la suite des évolutions réglementaires en matière de sécurité financières comme avec la loi Sarbanes Oxley aux Etats-Unis et d'autres lois au niveau international (Sarens, 2014). Les travaux qui ont été réalisés mettent notamment en évidence que l'audit interne représente une des composantes clés du dispositif de gouvernance (Archambeault *et al.*, 2008 ; Bédard and Gendron, 2010 ; Gramling *et al.*, 2004 ; Holt and DeZoort, 2009 ; Mat Zain and Subramaniam, 2007 ; Prawitt *et al.*, 2009 ; Rezaee, 2005 ; Stewart and Subramaniam, 2010).

Nous pouvons néanmoins au vu des résultats de cette recherche nous interroger sur la capacité réelle de l'audit à être efficace dans le rôle qui lui est assigné.

5 - 3 1 1 LA PLACE ET LE ROLE DE L'AUDIT DANS LE DISPOSITIF DE GOUVERNANCE

Les normes d'audit interne (IIA, 2014) recommandent un double rattachement de l'audit interne dans lequel l'audit reporte fonctionnellement au comité d'audit et hiérarchiquement au management de l'organisation. Cette règle est considérée comme une pratique qui permet d'assurer le niveau d'indépendance nécessaire pour que l'audit puisse remplir son rôle de façon efficace. Le cadre conceptuel de gouvernance des trois lignes de maîtrise établi par l'*Institute of Internal Auditors* (IIA, 2013) reprend cette exigence normative pour montrer la position unique de l'audit dans le dispositif général de gouvernance.

Ce cadre décrit un dispositif destiné à mieux gérer et maîtriser les risques au sein d'une organisation. L'audit interne apparaît comme une composante clé de ce dispositif et représente

une des trois lignes de défense à part entière. Les deux premières sont en charge de définir et déployer des dispositifs de gestion de gestion des risques et de contrôle alors que l'audit interne est en charge de les évaluer pour le compte des instances de gouvernance. Contrairement aux deux premières lignes de défense, l'audit interne dispose d'une indépendance qui lui permet de remplir ce rôle au sein de l'organisation.

L'indépendance est selon les directeurs de l'audit assurée par le fait de ne pas être impliqué dans les opérations et d'être rattaché au plus haut niveau de l'organisation.

SANTEFORM : « *Nous on considère qu'on n'a pas demandeur dans notre souci d'être indépendant. On peut avoir des demandes. En fait, nous on la retranscrit sur est ce que ça fait du sens par rapport à la gestion des risques du groupe* ».

BATIMODERN : « *Dans la méthode pourquoi ils apprécient mieux que les opérationnels, bah ils ne sont pas plongés dans le quotidien, dans des habitudes, qu'ils ont vu dériver* ».

GAZEO : « *Et aussi nous sommes indépendants. Donc le fait d'être indépendant nous permet d'avoir cette ouverture d'esprit. Alors que si on devrait dépendre uniquement de la finance, elle va nous orienter la finance vers, avec un certain angle de vue. Si je dépends que de la RH (rire)* »

Lenz et Sarens (2012) avancent l'idée que le positionnement de l'audit tel que préconisé dans les normes établies par l'*Institute of Internal Auditors* explique en partie sa marginalisation de son rôle dans le dispositif de gouvernance depuis la crise de 2008. Le double rattachement de l'audit préconisé par les normes d'audit ainsi que leur volonté de réaliser à la fois des services d'assurance et de conseil pour évaluer les processus de gestion des risques, de gouvernance et de contrôle présente des difficultés.

Le fait que l'audit cherche à remplir plusieurs rôles à la fois et ce pour beaucoup de personnes en même temps génère un certain flou sur le niveau auquel il s'adresse et sur ce qu'il doit fournir comme service. Les auditeurs proposent d'un côté un service d'assurance au comité d'audit et de l'autre ils se positionnent comme étant un « *business partner* » en offrant au management un service de conseil. Les auteurs suggèrent que pour améliorer le positionnement de l'audit interne dans le dispositif de gouvernance, il est nécessaire de clarifier envers qui l'audit doit véritablement rendre compte et se concentrer en priorité sur les services d'assurance.

5 - 3 1 2 L'APPORT DE NOTRE CADRE D'ANALYSE POUR MIEUX COMPRENDRE LES DIFFICULTES
AUXQUELS EST CONFRONTE L'AUDIT INTERNE.

La distinction risque/danger établie par Luhmann (1993) a une implication forte sur les pratiques d'audit interne dès lors que nous cherchons à répondre à la question suivante : « *l'audit interne évalue les risques pour qui ?* ».

Pour Luhmann les risques des uns ne sont pas les risques des autres. Dans cette perspective, les risques des actionnaires ne sont pas les mêmes que ceux de la direction générale et du management.

Ce problème est aussi soulevé par Power (2009) qui juge que le concept d'appétence au risque tel que développé dans le modèle de l'*Entreprise Risk Management* est contestable. L'appétence au risque y est décrite comme une notion unique et homogène pour l'ensemble de l'organisation et qu'il est possible de la déterminer sans ambiguïté. Cette conception de l'appétence au risque exclut l'existence de conflits d'intérêts entre les différents types et niveaux d'appétence.

Les travaux de Lenz et Sarrens (2012) confirment la nécessité de clarifier le rôle et le positionnement de l'audit interne et combien il est nécessaire de préciser envers qui l'audit doit véritablement rendre compte.

BATI-F : « *Alors de vous à moi, j'ai absolument aucune envie que le comité d'audit me dise « je veux que vous fassiez ça et ça ». Ça serait infernal donc faut faire gaffe. Déjà, il va me demander des trucs. Évidemment, quand il me demande, je suis obligé de le faire mais je considère que mon patron, ce n'est pas le comité d'audit. J'ai bien deux patrons hein mais je ne me trompe pas de cible parce que si vous rentrez là-dedans, c'est [...] enfin vous faites des rapports dans tous les sens* ».

Une autre question mérite d'être soulevée. Elle concerne le rôle que devrait jouer le comité d'audit en matière de supervision des activités d'audit et les moyens dont il devrait disposer pour pouvoir remplir de façon plus efficace sa mission. Les directeurs de l'audit déclarent que les membres des comités d'audit expriment rarement des demandes auprès de l'audit et certains vont au-delà en s'interrogeant sur la capacité de ces membres à poser les « bonnes » questions.

ENGINICO : « *Moi, ce qui me choque surtout, c'est la superficialité et des conseils d'administration et des comités spécialisés du conseil d'administration. Concrètement,*

leur dire qu'ils ont la supervision des dispositifs de gestion des risques et des dispositifs de contrôle interne dans la boîte, c'est n'importe quoi. Jamais ils n'auront, enfin je veux dire et nous ils sont encore chez nous plutôt présents et il n'y a pas trop d'absence. Mais c'est parce que les jetons de présence, ils sont bons aussi. Mais en tout cas, le niveau de connaissances est [...]. Moi, je me demande si la véritable question ce n'est pas surtout à eux de renforcer les messages et de se former et d'être capable de poser les bonnes questions. Parce qu'aujourd'hui, ce n'est pas le cas ».

CHIMICA : *« Un comité d'audit n'est pas réellement un contre-pouvoir. Ils n'ont pas le temps, ils ont pas les compétences alors ils font, entre guillemet ils font semblant, et c'est sympathique. Alors, la réunion du comité d'audit, c'est vachement important. Je la prépare vachement bien, j'essaye d'être bien sérieux, d'avoir leur confiance, de ne pas raconter de « bêtises », enfin bon, etc. ».*

L'indépendance de l'audit qui repose selon les normes d'audit sur le double rattachement de l'audit au management puis au comité d'audit apparaît comme une condition nécessaire mais non suffisante. Certes, il faut clarifier le positionnement et le rôle de l'audit comme le préconise Lenz et Sarrens (2012). Toutefois, il est nécessaire d'aller au-delà en précisant le rôle et les moyens dont doit disposer le comité d'audit et les instances de gouvernance.

5 - 3 2 LA QUALITE DE L'AUDIT

Il n'existe pas aujourd'hui de consensus selon DeFond et Zhang (2014) sur ce qui pourrait constituer le bon critère de mesure de la qualité de l'audit. Pour Peecher et al. (2013) la perception de la qualité de l'audit varie en fonction des parties prenantes. Lenz et Sarens (2012) considèrent que l'audit interne dans sa configuration actuelle peut difficilement satisfaire tout le monde et qu'il est nécessaire de clarifier son rôle et son positionnement. Le principe de double rattachement de l'audit ainsi que son offre cumulée de services d'assurance et de conseil ne sont pas tenables.

Selon Roussy et Brivot (2016), la revue de la littérature montre que la qualité de l'audit interne a été essentiellement traitée sous l'angle des auditeurs externes et de leurs appréciations fondées principalement sur les attributs des auditeurs (indépendance et compétence).

Les travaux existants abordent la qualité de l'audit principalement du point de vue des attributs de l'audit, à savoir son indépendance et sa compétence. Ils ne traitent pas de la pratique de l'audit interne au regard de la question du risque qui en constitue pourtant le fondement.

Le processus d'auditabilité décrit précédemment montre que le processus mis en œuvre par les auditeurs pour rendre les risques auditables pose une question fondamentale quant à ses conséquences sur la qualité des observations réalisées par l'audit.

Pour que leurs observations soient de qualité, elles doivent être objectives selon les normes d'audit (IIA, 2014) qui rappelle qu'il s'agit d'un des principaux critères d'efficacité de l'audit.

La définition qui en est donnée est la suivante :

« L'objectivité un état d'esprit non biaisé qui permet aux auditeurs internes d'accomplir leurs missions de telle sorte qu'ils soient confiants en la qualité de leurs travaux menés sans compromis. L'objectivité nécessite que les auditeurs internes ne subordonnent pas leur jugement professionnel à celui d'autres personnes. L'objectivité découle en partie de l'approche systématique et méthodique prévue dans la définition de l'audit interne».

La distinction introduite par Luhmann (1993) entre observation de premier ordre et observation de second ordre nous amène à nous interroger sur la pratique de l'audit du point de vue notamment de la méthodologie qu'il met en œuvre pour lui assurer cette objectivité nécessaire.

Dès lors, la question qui se pose est de savoir dans quelle mesure la méthodologie d'audit permet à l'auditeur interne d'être un observateur de second ordre pertinent dont le jugement n'est pas altéré par celui d'un observateur de premier ordre ?

L'auditeur interne peut être un observateur de second ordre pertinent au sens de Luhmann (1993) grâce à la méthodologie qu'il met en œuvre sous certaines conditions. L'une des principales conditions est que les auditeurs n'observent pas directement les risques mais évaluent comment les managers identifient eux-mêmes les risques. A ce titre, il doit les interroger pour être en mesure d'apprécier comment ces derniers observent les risques et ceux qu'ils ne voient pas.

Toutefois, le processus d'auditabilité décrit précédemment nous montre qu'il est de nature à altérer cette position d'observation de second ordre. Dès lors que l'audit fonde ses contrôles sur des risques et des dispositifs décrits par les managers sans les remettre en cause, l'auditeur perd le bénéfice de sa position d'observateur de second ordre. Pour faire le lien avec les normes, l'audit subalterne son jugement professionnel à celui des managers en procédant ainsi.

CHIMICOR : « *Les premières missions par exemple qu'on a fait sur les achats ou les R&I, on les a travaillées avec les experts. C'est-à-dire on a dit, à l'époque il n'y avait pas de programme de travail sur ces sujets-là, on ne savait pas comment les aborder [...]. On a construit en fait un programme de travail avec les experts, en disant c'est quoi les points pour auditer ce type de sujet, et on a commencé* ».

MUTLIMEDSTORE : « *Pas pendant l'audit, par contre sur certaines missions, notamment comme Internet ou le SAV, pour la préparation du programme de travail, on a des échanges avec des experts internes, on a des filières métiers, des référents. Vous préparez les programmes de travail avec eux* ».

Le fait d'établir des référentiels de contrôle interne sur la base des risques tels qu'ils sont appréhendés par les managers sans chercher à avoir un regard critique maintient aussi l'audit dans un simple position d'observation de premier ordre. L'audit n'observe pas la manière dont les managers observent et ce qu'ils ne voient pas. En procédant de cette manière, l'audit duplique le mode d'observation des managers et est soumis aux mêmes points aveugles.

GAZEO : « *Alors je vous donne un exemple, il y a quelques années, on a traité le sujet des assurances. Personne ne savait traiter les assurances dans les équipes d'audit interne. Donc on s'est dit comment on va faire ? Donc du coup on a travaillé avec les courtiers d'assurance. On s'est dit, faut qu'on arrive à comprendre comment ça fonctionne, donc on a travaillé, bon avec notre responsable assurance au niveau du groupe* ».

La standardisation des programmes de travail de l'audit est de nature à altérer la position d'observation de second ordre des auditeurs.

5 - 3 2 2 L'IMPACT DE LA NATURE DES MISSIONS ET DU POSITIONNEMENT DE L'AUDIT SUR LA QUALITE DE L'AUDIT INTERNE.

Les processus de cartographie des risques ainsi que d'élaboration du plan d'audit peuvent être menés selon différentes approches (top down, bottom up ou mixte) et suivant l'approche qui sera retenue, les personnes interrogées ne sont pas les mêmes. Une approche bottom-up qui consisterait à interroger essentiellement les managers des entités sans prendre en compte la vision de la direction générale ou bien des membres du comité d'audit peut dès lors amener l'audit à exclure certains risques. Nous pouvons dès lors sur le rôle effectif de l'audit interne

dans le dispositif de gouvernance si celui-ci ne prend pas en compte les risques des instances de gouvernance lors de l'élaboration de son plan d'audit et de ses missions.

Le choix de missions d'audit qui se rapportent à de risques peu significatifs pour la direction générale et le comité d'audit pose la question du positionnement de l'audit et la nature des risques qu'il traite au sein de l'organisation.

GAZEO : « *Tous les sujets de contrôle interne sont des sujets locaux, ce ne sont pas des sujets de siège. Donc pourquoi j'irais mettre la totalité de mes auditeurs internes dans le siège pour aller faire des audits avec des problématiques locales, qui n'intéressent pas la direction générale. Quand je dis ça, je force le trait mais volontairement. Savoir que le cycle achat n'est pas très bien maîtrisé en Thaïlande, ça ne va pas mettre la maison par terre et donc mon client qui est la direction générale, les comités d'audit et le comité exécutif, n'est pas très intéressé par ces problématiques-là* ».

MUTLIMEDSTORE : « *Une mission d'audit ne donnera jamais une indication de criticité pour le groupe, jamais et ça ne sera pas une mission d'audit qui directement va nous faire alimenter une cartographie des risques groupe. C'est une notion de criticité à plusieurs détails mais en gros c'est l'entité, au maximum le pays [...]. On peut dire les missions d'audit, c'est plutôt des risques de contrôle interne ou des risques entité, process qui font partie de notre référentiel de contrôle interne, pratiquement très opérationnel, donc des risques liés aux entités, aux responsables des entités qu'on audite ou des responsables de process et des porteurs de process. Mais pas forcément j'allais dire ceux de la direction générale ou ceux d'actionnaires qui pourraient demander des comptes* ».

La distinction risque/danger introduite par Luhmann (1993) pour définir le concept de risque est éclairante pour comprendre qu'il n'est pas possible d'évaluer le risque sans préciser au préalable en fonction de qui et ce malgré que les conditions d'indépendance soient remplies. La littérature la perception de la qualité de l'audit varie en fonction des parties prenantes (Peecher et al., 2013). Cette question qui a été abordée dans la partie relative à la gouvernance montre que l'audit souffre d'un manque de clarté sur son rôle ainsi que son positionnement (Lenz et Sarrens, 2012).

Conclusion générale :

Cette thèse apporte trois contributions principales.

La première est de démontrer les différentes dimensions de l'écart décrit par Power (1999) entre le système abstrait de l'audit et sa pratique et d'explorer les causes potentielles qui permettent de l'expliquer.

L'écart entre univers des risques et univers d'audit revêt plusieurs dimensions qui se traduisent dans les différents modes d'observation mis en œuvre pour identifier les risques : l'horizon de temps considéré, le niveau organisationnel interrogé, les outils de collecte, les modalités d'évaluation et l'origine des événements considérés comme risqués.

Notre cadre d'analyse apporte des explications sur l'écart entre l'univers d'audit et l'univers des risques. Cet écart résulte notamment de :

- l'absence de la distinction risque/danger dans le cadre de l'élaboration des cartographies des risques. Les dangers qui figurent dans la cartographie des risques sont exclus du plan d'audit ;
- l'absence de code de communication commun aux différents sous-systèmes sociaux. Les auditeurs observent les risques avec leurs propres codes et ne disposent pas des codes utilisés par les autres sous-systèmes ;
- la nature des modes d'observation qui sont de premier ordre pour les managers et de second ordre pour les auditeurs. Les managers observent les risques avec des points aveugles et les auditeurs observent ce que les managers voient et ce qu'ils n'observent pas ;
- la multiplicité des horizons de temps considérés par les différents sous-systèmes au sein de l'organisation.

La seconde contribution est de décrire le processus d'auditabilité.

Le processus d'auditabilité est un processus complexe mis en œuvre par l'audit pour traduire les risques en risque auditable. Le code de communication de l'audit est fondé sur les risques auditables que l'audit interne assimile à des objets matériels et vérifiables. Seuls les systèmes qui laissent une trace « matérielle » qui prend la forme de plan d'actions, de dispositifs formels de contrôles peuvent être audités. Le fait que les auditeurs observent les risques avec leurs propres codes de communication peut dès lors constituer un risque pour l'organisation puisque les risques qui « comptent » deviennent en priorité les risques auditables.

Le processus d'auditabilité illustre bien comment l'organisation tout entière est amenée de façon progressive et continue à définir des dispositifs de contrôle, à les formaliser pour assurer la production des preuves nécessaires pour les rendre auditables, peut-être même au détriment d'autres menaces.

La troisième contribution est un regard renouvelé par rapport à la littérature existante sur le lien entre audit interne et gouvernance, ainsi que sur l'appréciation de la qualité de l'audit pour améliorer les pratiques managériales. L'audit interne souffre d'un manque de clarté de son rôle et de son positionnement. Son double rattachement à la direction générale et au comité d'audit associé au fait d'offrir à la fois des missions de conseil et d'assurance est une position difficile à tenir pour réussir à satisfaire tout le monde.

CONCLUSION

La question de recherche principale de cette recherche est la suivante : « *Comment les organisations construisent-elles leurs objets de risques et par quelles heuristiques ?* » en lien avec les activités de l'audit interne au sein des organisations. C'est-à-dire comprendre *comment les directions d'audit construisent leurs objets de risque ... pour les rendre auditables.*

Notre objectif était d'étudier le processus de construction sociale des analyses de risque formelles réalisées au sein des organisations en mettant en relation les procédures mises en œuvre par les acteurs avec les résultats produits. Il s'agissait plus précisément d'analyser les heuristiques mises en œuvre au sein des organisations ainsi que les modes d'interaction des acteurs pour construire les objets de risque.

Les questions posées pour y répondre étaient les suivantes :

- comment les risques identifiés dans l'organisation (cartographie des risques) orientent-ils les travaux des auditeurs internes ?
- comment sont évalués les risques de l'organisation lors de la construction du plan d'audit ?
- comment sont définies les missions sur la base de l'évaluation préliminaire des risques ?
- dans quelle mesure l'auditeur interne peut être un observateur pertinent des risques de l'organisation ?

À l'issue de ce travail de recherche, nous avons réussi à mieux comprendre le rôle que joue la fonction d'audit interne dans le processus de construction des objets des risques au sein de son organisation et quelle était la nature de ses interactions avec les autres acteurs. Nous avons dépassé cet objectif en mettant aussi en perspective les enjeux et les impacts sociétaux qui en découlent à travers le processus d'auditabilité qui constitue une de nos trois principales contributions.

La méthodologie de recherche fondée principalement sur des entretiens semi-directifs (individuels et collectifs) qui ont été réalisés avec des directeurs de l'audit des grands groupes français nous a permis de répondre à notre objectif de recherche initial. Les données collectées auprès des directeurs de l'audit (quarante-sept heures d'entretien et mille cent pages de

transcription) ont fourni des données extrêmement riches pour permettre une analyse approfondie.

Le résultat de l'analyse des données a montré que l'identification des risques est conditionnée par les modes d'observation mise en œuvre ainsi que des modes d'interaction entre les acteurs dans le cadre des processus de cartographie des risques et d'élaboration du plan d'audit. Cette même analyse nous a permis de constater un écart entre l'univers des risques établi par les opérationnels et l'univers d'audit établi par les auditeurs. Les risques des opérationnels ne sont pas les mêmes que ceux pris en compte par les auditeurs pour élaborer leur plan d'audit réputé être pourtant fondé sur les risques de l'organisation selon les normes d'audit.

Dans sa théorie de la société de l'audit, Power (1999) développe l'idée qu'il existe un écart entre le système abstrait de l'audit représenté par les normes et la pratique effective des auditeurs mais sans décrire les dimensions qu'elle revêt. L'existence de cet écart peut sembler problématique dès lors que l'audit déclare jouer un rôle clé dans l'évaluation des dispositifs de gestion des risques au sein des organisations pour répondre aux attentes sociétales nées de la crise de confiance.

La première contribution de cette thèse est de démontrer les différentes dimensions de l'écart décrit par Power (1999) entre le système abstrait de l'audit et sa pratique et d'explorer les causes potentielles qui permettent de l'expliquer avec notre cadre d'analyse.

La première explication est l'absence de distinction entre les risques et les dangers lors de l'élaboration des cartographies des risques contrairement au processus d'élaboration du plan.

La seconde explication réside dans le fait que l'audit interne représente un sous-système social au sens de Luhmann (1993) qui dispose de sa propre sémantique et de ses propres modes opératoires. L'audit interne en tant que sous-système social couvre partiellement les risques de la cartographie qu'il perçoit comme des « bruits » externes et qu'il observe avec ses propres codes afin de pouvoir les traduire en mission d'audit.

La troisième explication est que la méthodologie d'audit repose sur plusieurs actions qui confèrent à l'audit interne une position d'observateur de second ordre qui lui permet d'identifier les points aveugles des autres sous-systèmes. La quatrième explication résulte de l'existence de temporalités multiples.

La seconde contribution de cette thèse est de mieux comprendre le processus d'auditabilité, c'est-à-dire le processus mis en œuvre par l'audit interne pour transformer les risques en risques

auditables. Selon Power (1999), contrairement à l'image officielle de l'audit souvent présenté comme une activité neutre, il s'agit d'un processus actif qui vise à « *rendre les choses auditables* » que l'auteur ne décrit pas. Les résultats de cette recherche vont au-delà pour recenser et décrire les différentes dimensions techniques que peut revêtir le processus d'auditabilité. Néanmoins, il est essentiel de comprendre qu'il présente des enjeux qui vont au-delà d'un simple problème technique et qui sont d'ordre sociétal. L'activité d'audit n'est pas neutre sur la construction des objets de risque au sein des organisations puisque les risques qui « comptent » deviennent les risques auditables. L'audit façonne au sein de son organisation la manière d'appréhender les risques des autres membres et va au-delà en désignant les risques qui sont importants ; peut-être même au détriment d'autres risques ou menaces qui pourraient être plus graves.

Enfin, ces travaux permettent de porter un regard renouvelé par rapport à la littérature existante sur le lien entre audit interne et gouvernance ainsi que sur l'appréciation de la qualité de l'audit dans le but d'améliorer les pratiques managériales.

Sur le thème de la gouvernance, l'indépendance de l'audit qui repose selon les normes d'audit sur son double rattachement au management puis au comité d'audit apparaît comme une condition nécessaire mais non suffisante.

Notre recherche a confirmé non seulement la nécessité de clarifier le positionnement et le rôle de l'audit comme le préconise Lenz et Sarrens (2012) mais également d'aller au-delà en précisant le rôle et les moyens dont doivent disposer le comité d'audit et les instances de gouvernance.

Sur le thème de la qualité de l'audit, l'écart constaté entre l'univers d'audit et l'univers des risques génère de fortes implications.

Les processus de cartographie des risques ainsi que d'élaboration du plan d'audit peuvent être menés selon différentes approches. Suivant l'approche qui sera retenue, les personnes interrogées ne sont pas les mêmes. La distinction risque/danger introduite par Luhmann (1993) pour définir le concept de risque est éclairante pour comprendre qu'il n'est pas possible d'évaluer un risque sans préciser au préalable l'identité du tiers concerné, malgré le fait que les conditions d'indépendance soient remplies. Il est dès lors essentiel de reconsidérer sur cette base le rôle et le positionnement de l'audit interne.

Les limites et les pistes de recherche futures

Cette recherche qui apporte plusieurs contributions majeures présente néanmoins certaines limites qui pourraient donner lieu à de nombreuses pistes de recherche futures. La méthodologie retenue a consisté à interroger principalement les directeurs de l'audit. Il serait intéressant d'élargir les entretiens aux managers et aux membres des instances de gouvernance dans le but d'enrichir les données déjà collectées ou pour améliorer la connaissance sur de nombreux sujets. D'autres travaux pourraient être réalisés sur la base des connaissances acquises afin de procéder à des études plus ciblées à partir d'autres méthodes de recherche. L'analyse qualitative-quantitative comparée pourrait ainsi être retenue pour des recherches futures. Cette thèse développe enfin l'idée que l'audit constitue un sous-système clos. Une nouvelle piste de recherche pourrait permettre d'analyser quels sont les facteurs externes ou bien organisationnels qui peuvent conduire l'audit à une forme d' « isolement ».

BIBLIOGRAPHIE

- Allegrini M. et D'Onza G. (2003), Internal Auditing and Risk Assessment in Large Italian Companies: An Empirical Survey, *International Journal of Auditing*, Vol. 7, No. 3, pp. 191-208
- Abdolmohammadi M.J. (2009), Factors Associated with the Use of and Compliance with the IIA Standards: A Study of Anglo-culture CAEs, *International Journal of Auditing*, Vol. 13, No. 1, pp. 27–42
- Abdolmohammadi M.J. (2012), Chief Audit Executives' Assessment of Internal Auditors' Performance Attributes by Professional Rank and Cultural Cluster, *Behavioral Research in Accounting*, Vol. 24, No. 1, pp. 1-23
- Abbott A. (1998), *The system of professions: An essay of the division of expert labor*, published by University of Chicago Press
- Abbott L.J, Parker S. et Peters G.F. (2010), Serving Two Masters: The Association between Audit Committee Internal Audit Oversight and Internal Audit Activities. *Accounting Horizons*, Vol. 24, No. 1, pp. 1-24
- Abbott L.J, Parker S. et Peters G.F. (2012), Audit Fee Reductions from Internal Audit-Provided Assistance: The Incremental Impact of Internal Audit Characteristics. *Contemporary Accounting Research*, Vol. 29, No. 1, pp. 94–118
- Autorité des Marchés Financiers (2010), Cadre de référence sur les dispositifs de gestion des risques et de contrôle interne, accessible sur www.amf-france.org
- Archambeault D.S, DeZoort F.T. et Holt T.P. (2008), The Need for an Internal Auditor Report to Stakeholders to Improve Governance Transparency. *Accounting Horizons*, Vol. 22, No. 4, pp. 375-388
- Arel B. (2010), The influence of litigation risk and internal audit source on reliance decisions. *Advances in Accounting*, Vol. 26, No. 2, pp. 170–176
- Arena, M, Arnaboldi M. et Azzone G. (2011). Is enterprise risk management real ?. *Journal of Risk Research*. Vol. 14, No.7, pp. 779–797
- Basel III (2010), A global regulatory framework for more resilient banks and banking systems (accessible à l'adresse: <http://www.bis.org/publ/bcbs189.htm>)
- Barua A, Rama D.V. et Sharma V. (2010), Audit committee characteristics and investment in internal auditing. *Journal of Accounting and Public Policy*, Vol. 29, No. 5, pp. 503–513
- Beasley M. S, Clune R. et Hermanson D.R. (2008), The impact of enterprise risk management on the internal audit function. *Journal of Forensic Accounting*, Vol. 9, No. 1, pp. 1-20
- Bédard J. et Gendron Y. (2010), Strengthening the financial reporting system: Can audit committees deliver? *International Journal of Auditing*, Vol. 14, No. 2, pp. 174-210
- Bertin E. (2007), *Audit interne : enjeux et pratiques à l'international*, Eyrolles

- Bertin E. et Godowski C. (2012), The global audit process: source of development of a cognitive governance ?, *Comptabilité, Contrôle, Audit*, Vol. 18, No. 3, pp. 143-184
- Brandon D. (2010), External Auditor Evaluations of Outsourced Internal Auditors. *Auditing, a Journal of Practices & Theory*, Vol. 29, No. 2, pp. 159-173
- Beck U. (1986), La société du risque : sur la voie d'une autre modernité, Flammarion (version française 2001)
- Bertalanffy L.V. (1968), Théorie générale des systèmes, Dunod (version française 2012)
- Burnaby P. et Hass S. (2009), A summary of the global Common of Knowledge 2006 (CBOK) study in internal auditing. *Managerial Auditing Journal*, Vol. 24, No. 9, pp. 813–834
- Burton G. F, Emett S. A, Simon C. A. et Wood D.A. (2012), Corporate Managers' Reliance on Internal Auditor Recommendations. *Auditing: A Journal of Practice & Theory*, Vol. 31, No. 2, pp. 151-166
- Carcello J.V, Hermanson D.R. et Raghunandan K. (2005), Factors Associated with U.S. Public Companies' Investment in Internal Auditing. *Accounting Horizons*, Vol. 19, No. 2, pp. 69-84
- Casta J.F. et Mikol A. (1999), Vingt ans d'audit : de la révision des comptes aux activités multiservices. *Comptabilité, Contrôle, Audit*, Mai, pp. 107- 121
- Champy F. (2009), La sociologie des professions, PUF, coll. « Quadrige Manuels »
- Chemangui M. (2009), Proposition d'une métrique de la qualité de l'audit : expérimentation dans le cadre des relations d'agences internes. *Comptabilité-Contrôle-Audit*, Vol. 1, pp 225-248
- Christopher J, Sarens G. et Leung P. (2009), A critical analysis of the independence of the internal audit function: evidence from Australia. *Accounting Auditing and Accountability Journal*. Vol. 22, No. 2, pp. 200-220
- Castanheira N, Rodrigues L. et Craig R. (2010), Factors associated with the adoption of risk-based internal auditing. *Managerial Auditing Journal*, Vol. 25, No. 1, pp. 79-98
- Coetzee P. et Lubbe D. (2014), Improving the Efficiency and Effectiveness of Risk-Based Internal Audit Engagements, *International Journal of Auditing*, Vol. 18, No. 2, pp. 115-125
- Cohen J, Krishnamoorthy G. et Wright A. (2004), The Corporate Governance Mosaic and Financial Reporting Quality. *Journal of Accounting Literature*, Vol. 23, No. 8, pp. 87-152

- Cohen J, Krishnamoorthy G. et Wright A. (2010), Corporate Governance in the Post-Sarbanes-Oxley Era: Auditors' Experiences. *Contemporary Accounting Research*, Vol. 27, No. 3, pp. 751-786
- Committee of Sponsoring Organisations of the Treadway Commission (COSO), Enterprise Risk Management - Integrated Framework (2004) and Internal Control -Integrated Framework (2013). Available at: <http://www.coso.org> (accès en Septembre 2014)
- Covaleski M.A, Dirsmith M.V. et Rittenberg L. (2003), Jurisdictional disputes over professional work: the institutionalization of the global knowledge expert. *Accounting, Organization and Society*, Vol. 28, No. 4, pp. 323-355
- Curtis E. et Turley S. (2007), The business risk audit – A longitudinal case study of an audit engagement. *Accounting, Organizations and Society*, Vol. 32, No. 4-5, pp. 439-461
- DeAngelo L.E. (1981a), Auditor Independence, 'Low Balling', and Disclosure Regulation. *Journal of Accounting & Economics*, Vol. 3, No 2, pp. 113-127
- DeAngelo L.E. (1981b), Auditor Size and Audit Quality, *Journal of Accounting & Economics*, Vol. 3, No. 3, pp. 183-199
- De Dreu C.K.W. et Weingart L. R. (2003), Task Versus Relationship Conflict, Team Performance, and Team Member Satisfaction: A Meta-Analysis. *Journal of Applied Psychology*, Vol. 88, No. 4, pp. 741-749
- DeFond M.L. et Zhang J. (2014), A Review of Archival Auditing Research. *Journal of Accounting & Economics*, Vol. 58, No. 2, pp. 275-326
- Desai N, Gerard G. et Tripathy A. (2011), Internal Audit Sourcing Arrangements and Reliance by External Auditors. *Auditing*, Vol. 30, No. 1, pp. 149-171
- Desai V, Roberts R.W. et Srivastava R. (2010), An analytical model for external auditor evaluation of the internal audit function using belief functions. *Contemporary Accounting Research*, Vol. 27, No. 2, pp. 346
- Dezoort F.T, Houston R.W. et Peters M.F. (2001), The Impact of Internal Auditor Compensation and Role on External Auditors' Planning Judgments and Decisions. *Contemporary Accounting Research*, Vol. 18, No. 2, pp. 257-281
- Dirks K. T. (1999), The Effects of Interpersonal Trust on Work Group Performance. *Journal of Applied Psychology*, Vol. 84, No. 3, pp. 445-455

- Dodd-Frank Wall Street Reform and Consumer Protection Act (2010). (disponible à l'adresse suivante:http://banking/senate.gov/public/_files/070110_Dodd_Franck_Wall_Street_Reform_comprehensive_summary_Final.pdf)
- Douglas M. et Wildavsky A. (1982), Risk and Culture: An Essay on the Selection of Technological and Environmental Dangers, University of California Press
- Eisenhardt K.M. (1989), Building Theories From Case Study Research. *The Academy of Management Review*, Vol. 14, No. 4, pp. 532-550
- Everett J. et Tremblay M.S. (2014), Ethics and internal audit: Moral will and moral skill in a heteronomous field. *Critical Perspectives on Accounting*, Vol. 25, No. 3, pp. 181-196
- Foreign Corrupt Practices Act (1977). (disponible en anglais à l'adresse: <http://www.usdoj.gov/criminal/fraud/fcpa>)
- Felix W, Gramling A. et Maletta M. 2005. The influence of non-audit service revenues and client pressure on external auditors' decisions to rely on internal audit. *Contemporary Accounting Research*, Vol. 22, No. 1, pp. 31–53
- Flesher D.L. (1991), The Institute of Internal Auditors: 50 years of progress through sharing. Altamonte Springs, FL: The Institute of Internal Auditors.
- Flint C, Fraser I.A.M et Hatherly D.J (2008), Business risk auditing: A regressive evolution? A research note. *Accounting Forum*, Vol. 32, No. 2, pp. 143–147
- Francis J. R. (2011), A Framework for Understanding and Researching Audit Quality. *Auditing: A Journal of Practice & Theory*, Vol. 30, No. 2, pp. 125-152
- Giddens A. (1991), The Consequences of Modernity, Stanford University Press
- Glover S.M, Prawitt D.F. et Wood D.A. (2008), Internal audit sourcing arrangement and the external auditor's reliance decision. *Contemporary Accounting Research*, Vol. 25, No. 1, pp. 193–213
- Goodwin-Stewart J. et Kent P. (2006a), Relation between external audit fees, audit committee characteristics and internal audit. *Accounting and Finance*, Vol. 46, No. 3, pp. 387-404
- Goodwin-Stewart J. et Kent P. (2006b), The use of internal audit by Australian companies. *Managerial Auditing Journal*, Vol. 21, No. 1/2, pp. 81-101

- Gramling A.A, Maletta M.J, Schneider A. et Church B.K. (2004), The role of the internal audit function in corporate governance: a synthesis of the extant internal auditing literature and directions for future research. *Journal of Accounting Literature*, Vol. 23, pp.194-244
- Gray J. et Hunton J.E (2011), External Auditors' Reliance on the Internal Audit Function: The Role of Second-Order Belief Attribution. Working paper, Bentley University
- Griffin A. et Hauser J.R (1993), The Voice of the Customer. *Marketing Science*, Vol. 12, No.1, pp. 1-27.
- Hackman J. R. (1987), The Design of Work Teams. In Handbook of Organizational Behavior, edited by J. W. Lorsch. Englewood Cliffs, NJ: Prentice-Hall
- Holt T.P et DeZoort T. (2009), The Effects of Internal Audit Report Disclosure on Investor Confidence and Investment Decisions. *International Journal of Auditing*, Vol. 13, No 1, pp. 61-77
- Ilgen D. R, Hollenbeck J. R, Johnson M. et Jundt D. (2005), Teams in Organizations: From Input-Process-Output Models to IMOI Models. *Annual Review of Psychology*, Vol. 56, No. 1, pp. 517-543
- ISO 31000 (2009), Management du risque : principe et ligne directrice, disponible sur www.iso.org/iso/fr/home/standards/iso31000.htm (accès en Septembre 2014)
- Institute of Internal Auditors (IIA), International Professional Practices Framework. Disponible sur: <https://na.theiia.org/standards-guidance> (accès en Juillet 2014)
- Institute of Internal Auditors (IIA), The three lines of defense in effective risk management and control. Disponible sur: <https://na.theiia.org/standards-guidance> (accès en Juillet 2015).
- Institute of Internal Auditors (IIA), The IIA's global Internal audit Survey : a component of the CBOK Study; disponible sur: [https://na.theiia.org/iiaarf/Public Documents/2010-CBOK-Core](https://na.theiia.org/iiaarf/Public_Documents/2010-CBOK-Core) (accès en Juillet 2014)
- Jensen M. C. et Meckling W.H. (1976), Theory of the Firm: Managerial Behavior, Agency Costs, and Ownership Structure. *Journal of Financial Economics*, Vol. 4, No. 4, pp.305-360
- Knechel W.R. (2002), The Role of the Independent Accountant in Effective Risk Management. *Review of Business and Economics*, Vol. 47, No. 1, pp. 65-86
- Knechel W.R. (2007), The business risk audit: origins, obstacles and opportunities. *Accounting, Organizations and Society*, Vol. 32, No. 4-5, pp. 383-408

- Knight F. (1921), *Risk, Uncertainty and Profit*. Edition Martino Fine Books (*2014)
- Koutoupis A.G. & Tsamis A. (2009), Risk-based internal auditing within Greek banks: a case study approach. *Journal of Management and Governance*, Vol. 13, No. 1-2, pp. 101-130
- Krishnamoorthy G. et Maletta M. (2012), The Role of Internal Audit in the Financial Statement Audit: The Contingent Effects of Board Independence and Audit Committee Effectiveness. Working paper, Northeastern University
- Krishnan G.V. (2005), Did Houston Clients of Arthur Andersen Recognize Publicly Available Bad News in a Timely Fashion? *Contemporary Accounting Research*, Vol. 22, No. 1, pp. 165-193
- Krueger R.A. et Casey M.A. (2002), *Focus Group: a practical guide for applied research* (3rd edition), Thousand Oaks, CA: Sage Publications
- Lenz R. et Sarens G. (2012), Reflections on the internal auditing profession: what might have gone wrong? *Managerial Auditing Journal*, Vol. 27, No. 6, pp. 532-549
- Leung P. et Cooper B.J. (2009), Internal audit—Asia-Pacific profile and the level of compliance with internal auditing standards. *Managerial Auditing Journal*, Vol. 24, No. 9, pp. 861-882
- Luhmann N. (1993), *Risk: A sociological Theory*, Berlin, Walter de Gruyter
- Luhmann N. (1986), *Social Systems*, Stanford, Stanford University Press
- Marais M, Burnaby P.A, Hass S, Sadler E. et Fourie H. (2009), Usage of internal auditing standards and internal auditing activities in South Africa and all respondents. *Managerial Auditing Journal*, Vol. 24, No. 9, pp. 883–898
- Margheim L.L. (1986), Further evidence of external auditors' reliance on internal auditors. *Journal of Accounting Research*, Vol. 24, No. 1, pp. 194-205
- Mat Zain M. et Subramaniam N. (2007), Internal Auditor Perceptions on Audit Committee Interactions: A Qualitative Study in Malaysian Public Corporations. *Corporate Governance: An International Review*, Vol. 15, No. 5, pp. 894-908
- Messier W.F. et Schneider A. (1988), A hierarchical approach to the external auditor's evaluation of the internal auditing function. *Contemporary Accounting Research*, Vol. 4, No 2, pp. 337-353

- Mikes A. (2009), Risk management and calculative cultures. *Management Accounting Research*. Vol. 20, No. 1, pp. 18-40
- Mikes A. (2011), From counting risk to making risk count: Boundary-work in risk management. *Accounting, Organizations and Society*. Vol. 36, No. 4-5, pp. 226-245
- Miles et Huberman (2003), Analyse des données qualitatives, De Boeck
- Munro L. et Stewart J. (2011), External auditors' reliance on internal auditing: Further evidence. *Managerial Auditing Journal*, Vol. 26, No. 6, pp. 464–481
- Neely M.P. et J.S. Cook. (2011), Fifteen Years of Data and Information Quality Literature: Developing a Research Agenda for Accounting. *Journal of Information Systems*, Vol. 25, No. 1, pp.79-108
- Norman C, Rose A. et Rose J. (2010), Internal audit reporting lines, fraud risk decomposition, and assessments of fraud risk. *Accounting, Organizations and Society*, Vol. 35, No. 5, pp. 546-557
- NYSE (2004), Corporate Governance Rules section 303A final rules sur www.nyse.com.
- Paape L, Scheffe J. et Snoep P. (2003), The Relationship Between the Internal Audit Function and Corporate Governance in the EU – A Survey. *International Journal of Auditing*, Vol. 7, No. 3, pp. 247-262
- Patton M.Q. (2002), Qualitative research & evaluation methods, 3^{ème} édition. Thousand Oaks, Calif, Sage Publications.
- Peecher M.E, Solomon I, et Trotman K.T. (2013), An Accountability Framework for Financial Statement Auditors and Related Research Questions. *Accounting, Organizations & Society*, Vol. 38, No. 8, pp. 596-620
- Pelletier J. (2008), Adding risk back into the audit process. *Internal Auditor*, Vol. 65, No. 4, pp. 73-76
- Pires A.P. (1997), « Echantillonnage et recherche qualitative : essai théorique et méthodologique », dans Poupart D., Groulx L., Mayer P., « La recherche qualitative : enjeux épistémologiques et méthodologiques », édition Gaëtan Morin, pp. 113-169
- Public Company Accounting Oversight Board (2007), An Audit of Internal Control over Financial Reporting that is Integrated with an Audit of Financial Statements. *PCAOB*

- Release*, No. 2007-005. Washington, DC: PCAOB (disponible à l'adresse: <http://www.pcaobus.org>)
- Public Company Accounting Oversight Board (2011), PCAOB Standards and Interim Standards. Washington, DC: PCAOB (disponible à l'adresse: <http://www.pcaobus.org>)
- Power M. (1999), *La société de l'audit : l'obsession du contrôle*, édition La Découverte
- Power M. (2004), *The Risk Management of Everything. Rethinking the Politics of Uncertainty*. Demos, London.
- Power M. (2009). The risk management of nothing. *Accounting, Organizations and Society*, Vol. 34, No. 6-7, pp. 849-855
- Prawitt D.F, Smith J.L. et Wood D.A. (2009), Internal Audit Quality and Earnings Management. *The Accounting Review*, Vol. 84, No. 4, pp. 1255–1280
- Rainer L. et Sarens G. (2012), Reflections on the internal auditing profession: what might have gone wrong ? *Managerial Auditing Journal*, Vol. 27, No. 6, pp. 532-549
- Ramamoorti S. (2003), *Internal Auditing: History, Evolution, and Prospects*. Research opportunities in Internal Auditing (Altamonte Springs, FL: The Institute of Internal Auditors, 2003).
- Redding K.F et Sobel P. (2013), A solid understanding of risk. *Internal auditor*, June 2013, pp. 21-23
- Rezaee Z. (2005), Causes, Consequences, and Deterrence of Financial Statement Fraud. *Critical Perspectives on Accounting*, Vol. 16, No. 3, pp. 277-298
- Rittenberg L. et Miller P.K. (2005), *Sarbanes-Oxley Section 404 Work Looking at the Benefits*. Altamonte Springs, FL: The Institute of Internal Auditors
- Robson K, Humphrey C, Khalifa R. et Jones J. (2007), Transforming audit technologies: Business risk audit methodologies and the audit field. *Accounting, Organizations and Society*, Vol. 32, No. 4-5, pp. 409–438
- Roussy M. (2013), Internal auditors' roles: From watchdogs to helpers and protectors of the top manager. *Critical Perspectives on Accounting*, Vol. 24, No. 7-8, pp. 550- 571
- Roussy M. et Brivot M. (2016), Internal audit quality: a polysemous notion?. *Accounting, Auditing & Accountability Journal* Vol. 29 No. 5, pp. 1-25

- Sarbanes-Oxley Act (2002), Public Law No. 107-204. Washington, D.C.: Government Printing Office
- Sarens G. et Abdolmohammadi M. (2011). Monitoring Effects of the Internal Audit Function: Agency Theory versus other Explanatory Variables. *International Journal of Auditing*, Vol. 15, No. 1, pp.1-20
- Sarens G, De Beelde I. (2006b). The Relationship between Internal Audit and Senior Management: A Qualitative Analysis of Expectations and Perceptions. *International Journal of Auditing*, Vol. 10, No. 3, pp. 219-241
- Sarens G, De Beelde I. et Everaert P. (2009), Internal audit: A comfort provider to the audit committee. *The British Accounting Review*, Vol. 41, No. 2, pp. 90-106
- Sarens G. (2014), Editorial: Internal Audit Research at the Crossroads: Time to Turn a Page? *International Journal of Auditing*, Vol. 18, No. 2, pp. 103-104
- Schneider A. (1984), Modeling external auditors' evaluations of internal auditing. *Journal of Accounting Research*, Vol. 22, No. 1, pp. 657–678
- Schneider A. (1985), The reliance of external auditors on the internal audit function. *Journal of Accounting Research*, Vol. 23, No. 2, pp. 911–919
- Schneider A. (2009), The nature, impact, and facilitation of external auditor reliance on internal auditing. *Academy of Accounting and Financial Studies Journal*, Vol. 13, No. 4, pp. 41–54
- Spira L.F. et Page M. (2003), Risk management: The reinvention of internal control and the changing role of internal audit. *Accounting, Auditing & Accountability Journal*, Vol. 16, No. 4, pp. 640-661
- Stefaniak C. M, Houston R.W. et Cornell R.M. (2012), The Effects of Employer and Client Identification on Internal and External Auditors' Evaluations of Internal Control Deficiencies. *Auditing: A Journal of Practice & Theory*, Vol. 31, No. 1, pp. 39-56
- Stewart J. et Subramaniam N. (2010), Internal audit independence and objectivity: emerging research opportunities. *Managerial Auditing Journal*, Vol. 25, No. 4, pp. 328-360
- Stvilia B, Gasser L, Twidale M.B. et Smith L.C. (2007), A Framework for Information Quality Assessment. *Journal of the American Society for Information Science & Technology*, Vol. 58, No. 12, pp. 1720-1733

Taggar S. (2002), Individual Creativity and Group Ability to Utilize Individual Creative Resources: A Multilevel Model. *Academy of Management Journal*, Vol. 45, No. 2, pp. 315-330

Thiétart R-A (2003), *Méthodes de Recherche en Management*, Edition Dunod