Comment rendre les risques “ auditables ”? Une analyse des approches des directeurs d’audit des grandes entreprises françaises.

Coskun Cakar, Frédéric Gautier

Comment rendre les risques « auditables » ?

Une analyse des approches des directeurs d'audit des grandes entreprises françaises

Coskun CAKAR
Frédéric GAUTIER

Résumé : L'Institut des Auditeurs Interne (IIA) a établi un cadre normatif qui fonde la pratique de l'audit interne sur les risques. Cette recherche fournit une analyse qualitative pour mieux comprendre comment les départements d'audit planifient leurs travaux en lien avec les risques au sein des organisations. Le cadre d'analyse est la théorie de la société de l'audit de Power qui développe l'idée que l'audit est *un processus actif pour rendre les choses auditables*. La méthodologie est fondée sur des entretiens individuels et collectifs avec 32 directeurs d'audit de sociétés cotées. Nos travaux démontrent l'existence d'un écart entre l'univers des risques et l'univers d'audit et fournissent une description détaillée des processus mis en œuvre par les auditeurs pour rendre les risques auditables.

Mots clés : audit interne, risque, auditabilité, contrôle interne, gouvernance

Abstract: International Institute of Auditor's (IIA) professional standards provide authoritative and normative guidance to internal auditors who must apply a risk based approach. This research provides a qualitative analysis of how audit departments plan their activities in consistency with organizations' risks. Our conceptual framework is the society of audit of Power who developed the idea that *audit is an active process of making things auditable.* Our methodology relies upon individual interviews performed with 32 Chief Audit Executives of listed companies and a focus group session. Our results are twofold. First, we demonstrate a gap between the universe of risks and the universe of audit. Second, we provide a detailed description of how auditors are then addressing and making risks auditable.

Keywords: internal audit, risk, auditability, internal control, governance

1 Introduction

Dans le contexte actuel de crise de confiance, « l'audit interne doit jouer un nouveau rôle concernant le processus de gestion des risques, de contrôle et de la gouvernance au sein des organisations (IIA, 1999) ». Leurs activités sont encadrées par un code de déontologie et des normes d'audit décrites dans le Cadre de Référence International des Pratiques Professionnelles de l'Audit Interne (CRIPP). L'audit interne s'appuie sur une approche par les risques et l'évaluation des risques constitue le cœur d'activité de l'auditeur interne.

Par conséquent, nous pouvons nous interroger sur l'efficacité du processus d'évaluation des risques mis en œuvre par les auditeurs internes et dans quelle mesure les normes d'audit contribuent à limiter le risque d'audit et à mieux évaluer les risques au sein des organisations. C'est-à-dire comment les normes peuvent-elles contribuer à améliorer la qualité de l'audit et limiter la sélection arbitraire ou inadéquate des zones à risques par les auditeurs ? La revue de

la littérature existante nous a montré que la revue des pratiques des auditeurs internes en matière d'évaluation des risques reste peu développée alors que la notion de risque apparait comme problématique. La notion de risque n'est pas définie de façon suffisamment précise dans les normes alors qu'elle représente le cœur d'activité de l'audit interne. En effet, le risque est défini dans les normes comme étant un événement qui s'il se réalise pourrait compromettre la réalisation des objectifs de l'organisation considérée. C'est-à-dire que l'univers des risques possibles apparait comme pouvant être illimité du fait de l'incertitude qui pèse sur les événements futurs. Dès lors, nous devons comprendre comment les risques sont en pratique identifiés et sélectionnés par les auditeurs internes au sein de leur organisation, avec l'idée qu'il ne dispose pas de statistiques pour tout. Par ailleurs, le risque en tant que mesure ne permet pas de savoir comment apprécier le risque au niveau organisationnel dès lors que l'appétence au risque n'est pas homogène au sein de l'organisation.

La théorie de la société de l'audit (Power, 1999) nous fournit un cadre d'analyse particulièrement riche pour mieux comprendre comment les objets de risques sont socialement construits et comment l'audit participe à cette construction. Nous développons dans notre cadre d'analyse l'idée que le processus d'audit impacte le dispositif de gestion des risques en cherchant à obtenir des risques « auditables » et des objets de risques « formels ».

Cette recherche, menée principalement sur la base d'entretiens (individuels et focus group) réalisés auprès de 32 Directeurs de l'audit de sociétés cotées (CAC 40 et SBF 120), vise à répondre aux questions suivantes : Comment les départements d'audit établissent leur plan d'audit en lien avec les cartographies des risques des organisations au sein desquelles ils opèrent ? Comment peut-on expliquer l'écart entre les risques identifiés de la cartographie des risques et ceux retenus dans le plan d'audit ?

Dans cette étude, nous avons privilégié la compréhension du phénomène étudié compte tenu du niveau relativement limité des travaux sur les pratiques de l'audit interne en lien avec les risques.

Il apparaît que l'écart entre les risques recensés dans la cartographie des risques et ceux couverts par le plan d'audit peut notamment s'expliquer par l'absence de plans d'action formels pour les risques qui sont exclus par les auditeurs. Cette recherche fournit par ailleurs une description détaillée de la manière dont les risques peuvent être progressivement couverts par l'audit interne au travers de la mise en œuvre du processus d'auditabilité. Le processus d'auditabilité est à mettre en relation avec la mise en place de procédures de contrôles formels qui peuvent être progressivement standardisés.

L'article est structuré en trois parties. La première correspond à la revue de la littérature, au cadre d'analyse et aux questions de la recherche. La seconde partie présente la méthodologie utilisée pour analyser les données collectées. La troisième partie correspond aux principaux résultats obtenus.

2 Revue de la littérature, cadre d'analyse et questions de recherche

Cette partie fournit les principaux éléments d'information qui sont nécessaires pour mieux comprendre la relation qui existe entre l'audit interne et le concept de risque ainsi qu'une synthèse des principaux travaux réalisés sur ce thème. Nous aborderons dans un premier temps le thème de la cartographie des risques qui constitue une des composantes clés des processus de management des risques au sein des organisations. Nous traiterons dans un second temps du contenu des normes professionnelles de l'audit interne en lien avec le concept de risque et de la relation entre la planification des travaux d'audit et de la cartographie. Nous présenterons quelques questions et problématiques mis en avant par les travaux existants sur le thème de l'auditabilité des risques. Nous conclurons cette section par nos questions de recherche.

2.1 Revue de la littérature

La définition de l'audit interne a été récemment révisée afin de refléter son nouveau rôle, centrée sur les risques. *« 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 »* (IIA, 1999). Les nouvelles normes professionnelles ont été émises quelques années après. La littérature existante qui traite de la relation entre le risque et l'audit interne est relativement récente au regard du nouveau rôle assigné à l'audit.

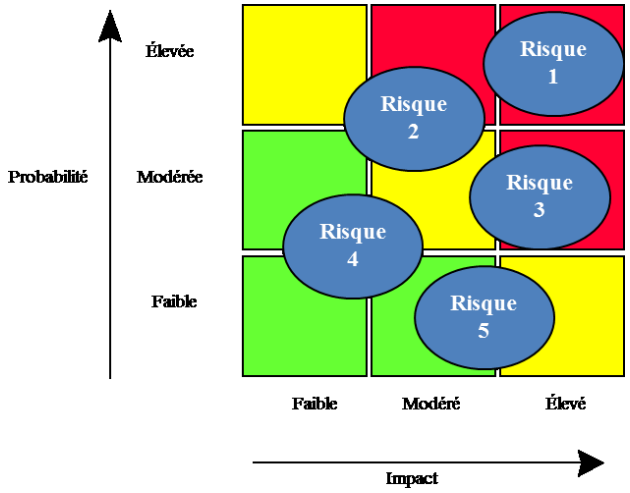
2.1.1 La cartographie des risques : une composante clé du modèle Entreprise Risk Management (ERM)

La crise financière du début des années 2000 a conduit à un fort développement des dispositifs destinés à prévenir ou à limiter l'impact des risques au sein des organisations. En particulier l'*Enterprise Risks Management* (ERM) incarne l'espoir d'une meilleure maîtrise des aléas de la vie économique et d'évitement des dérapages qui ont conduit à cette crise. C'est dans ce contexte de crise de confiance que différents référentiels se sont développés en proposant un cadre conceptuel et méthodologique destiné à maîtriser les risques, dont celui du COSO 2 élaboré par le *Committee Of Sponsoring Organizations of the Treadway Commission.* « L'adoption par les entreprises de ce type de dispositif est devenue quasiment incontournable. L'une des raisons de leur large adoption est liée au vote de lois de sécurité financière (Sarbannes Oxley Act en 2002 pour les Etats Unis, …) qui exigent aux sociétés cotées d'évaluer l'efficacité de leurs dispositifs de gestion des risques et de contrôle interne. La pression institutionnelle a elle-aussi contribué à les adopter, soit pour leur intérêt intrinsèque, soit par souci de conformité. Les agences de notation ont également adopté l'ERM dans les processus de notation des risques crédit et le considèrent comme le signe d'une bonne gouvernance (Miller and al., 2008 ; Standard & Poor's, 2008) ».

La cartographie des risques apparait comme étant un outil fondamental pour la mise en œuvre de l'ERM et des autres dispositifs de gestion des risques, dès lors qu'il n'est pas possible de gérer les risques s'ils ne sont pas connus et clairement identifiés.

Une cartographie des risques est une représentation schématique qui récapitule les événements susceptibles d'affecter négativement l'atteinte des objectives pour une organisation donnée. Une fois ces risques identifiés, ils sont évalués et hiérarchisés en fonction de la probabilité de survenance des événements redoutés et de leur impact potentiel. Un risque qui présente une forte probabilité de survenance combiné à un fort impact sera considéré comme critique. Les risques sont représentés de façon visuelle sur une "carte" qui décrit les risques majeurs identifiés avec leur degré de criticité (tel qu'illustré dans le schéma ci-dessous).

Schéma 1 : exemple de représentation d'une cartographie des risques



« La cartographie des risques représente l'un des dispositifs les plus fréquemment utilisé pour identifier et évaluer les risques (Collier et al., 2007, Woods 2009) ». « Une étude réalisée par KPMG (2013) a par ailleurs mis en évidence que parmi les principales activités des comités d'audit, la revue des cartographies des risques apparaît comme étant un élément relativement important ».

« Selon Power (2007), le besoin d'identifier les risques et le besoin exprimé par les instances de gouvernance de pouvoir disposer de représentations graphiques suffisamment synthétiques priment sur les techniques et les outils d'évaluation qui sont nécessaires pour les établir ».

« Les recherches qui portent sur l'outil de cartographie des risques restent relativement limitées malgré son fort développement au sein des organisations et l'intérêt qu'il peut susciter tant du point de vue conceptuel que pratique (Jordan et al., 2013) ».

2.1.2 Cadre de Référence International des Pratiques Professionnelles de l'Audit Interne (CRIPP)

L'Institute of Internal Auditors (IIA) est une association professionnelle qui a été créé en 1941 aux Etats-Unis en réponse à la croissance des activités d'audit interne au sein des organisations. L'IIA a tout d'abord établi une « déclaration de responsabilités » en 1947, puis un « Code de déontologie » en 1968. C'est une dizaine d'années plus tard, en 1978, que les premières "normes pour la pratique professionnelle de l'audit interne" ont été publiées par l'IIA. En 1998, le Conseil d'administration de l'IIA a décidé de constituer un groupe de travail en charge d'évaluer la pertinence et l'applicabilité des normes existantes. Le groupe de travail recommanda à la fin de ses travaux d'établir une nouvelle définition de l'audit interne (rôle d'assurance et de conseil), un cadre de référence pour la pratique professionnelle et une

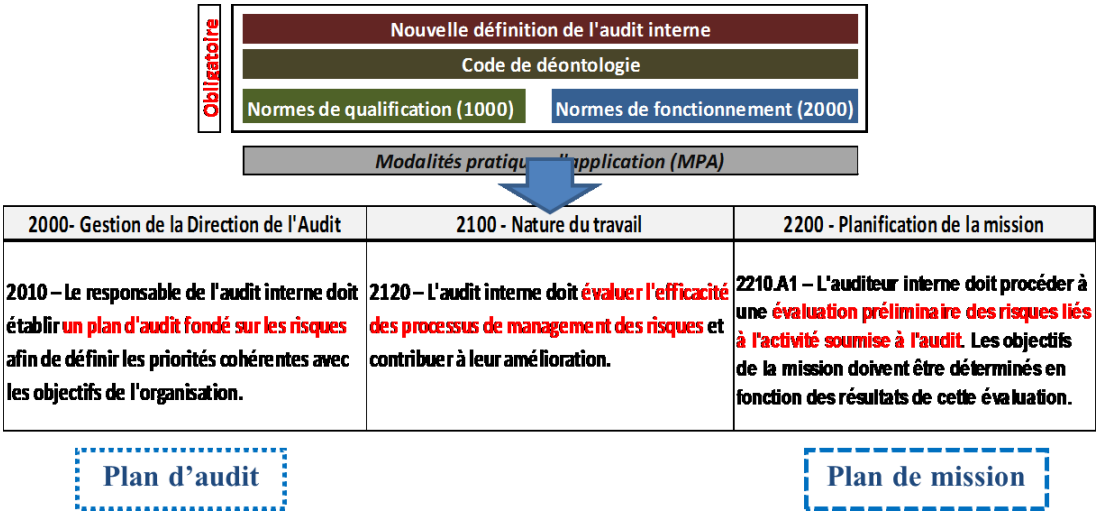
refonte des normes pour qu'elles soient mises en cohérence avec la nouvelle définition de l'audit interne.

« En 1999, un nouveau Code de déontologie et une nouvelle définition de l'audit interne ont été établis. En 2009, le Cadre de Référence pour la Pratique Professionnelle de l'audit interne (CRIPP) est entré en vigueur. Ce cadre normatif contient des dispositions obligatoires (définition de l'audit interne, Code de déontologie et normes internationales pour la pratique de l'audit interne) qui sont complétées par des dispositions fortement recommandées (modalités pratiques d'application, guides pratiques) ».

« L'Audit Interne est à défini par l'IIA comme étant "*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 approuvée par l'IIA en 1999 (qui est reprise comme telle dans le CRIPP) montre que le cœur d'activité de l'audit interne est centré sur les risques. L'objet même de l'audit interne est d'évaluer les processus de gestion des risques et de contrôle en ayant lui-même recours à une approche centrée sur les risques. Les normes professionnelles de l'audit interne exigent par ailleurs que la pratique de l'audit interne soit fondée sur une approche par les risques (tel qu'illustré dans l'extrait des normes présenté ci-dessous).

Schéma 2 : extrait du cadre normatif de l'audit interne



La norme 2010 relative à la planification annuelle des activités de l'audit précise que le directeur de l'audit doit établir un plan d'audit fondé sur une analyse documentée des risques.

La norme précise par ailleurs que les priorités de l'audit doivent être cohérentes avec les objectives de l'organisation au sein de laquelle il opère. Les cartographies des risques établies dans le cadre des processus de gestion des risques (présentés dans la section précédentes) peuvent dès lors constituer une base pour permettre à l'audit d'établir son plan d'audit annuel.

En complément de cette exigence, la norme 2210 rappelle que l'audit interne doit réaliser pour chacune des missions d'audit inscrite au plan d'audit une analyse préliminaire des risques spécifiques relatifs à l'activité ou l'entité auditée. Le choix du périmètre de revue de l'audit devra découler principalement de cette analyse de risque spécifique.

Une revue plus détaillée des normes d'audit interne met en évidence un paradoxe : la notion de risque n'est pas définie de façon suffisamment précise alors qu'elle représente le cœur d'activité de l'audit interne. Pour pallier à cette lacune, les normes font référence à certains cadres de référence en matière de gestion des risques comme par exemple celui du *« COSO 2 - Entreprise Risk Management » (ERM).* Le modèle du COSO 2 – ERM (2004) fournit un cadre de référence qui précise en quoi consiste la gestion des risques et quelles sont les principales étapes à suivre pour mettre en œuvre un tel processus au sein de son organisation. Le processus de gestion des risques qui est décrit par ce référentiel consiste tout d'abord à définir clairement les objectifs de l'organisation pour ensuite identifier tous les événements qui pourraient compromettre la réalisation de ces mêmes objectifs. Une fois ces événements identifiés, il faut évaluer les risques, c'est-à-dire la probabilité de survenance des événements ainsi que leur impact pour y apporter une réponse (éviter le risque, l'accepter ou bien le réduire). Le risque est défini dans ce cadre de référence comme étant un événement qui peut influer et compromettre l'atteinte des objectifs de l'organisation. Cette définition ne permet toutefois pas de répondre à la question de savoir comment les risques peuvent être identifiés parmi un univers illimité d'événements possibles qui sont soumis à de l'incertitude. Beaucoup de choses peuvent ne pas se dérouler comme nous l'envisageons. L'approche probabiliste n'est pas non plus d'une grande aide dès lors que nous ne disposons pas de données historiques pour « tout ». A ce stade, nous savons que l'audit interne doit mettre en œuvre une approche par les risques mais nous ne savons pas comment il procède en pratique. Il est essentiel de voir dans quelle mesure et comment les travaux existants traitent de cette question.

2.1.3 L'audit interne et les risques

« Le rôle et les responsabilités de l'audit interne répondent aujourd'hui à un besoin qui n'est pas indépendant de l'évolution des principes de gouvernance d'entreprise (Gramling et al., 2004; Sarens et De Beelde, 2006 ; Gendron et al., 2007) ». « En réponse aux nouveaux besoins, l'audit interne doit jouer un nouveau rôle en ce qui concerne les risques et les processus de gestion des risques (McNamee et Selim, 1999 ; Allegrini et D'Onza, 2003 ; Paape et al., 2003 ; Spira et Page, 2003) ». Comme nous l'avons vu dans la partie précédente, les normes d'audit interne reflètent bien l'idée que le processus de gestion des risques constitue le cœur d'activité de l'audit interne en réponse à ce nouveau besoin.

Les normes internationales d'audit interne requièrent que les travaux d'audit soient planifiés sur la base d'une analyse préliminaire des risques. Cela concerne aussi bien l'élaboration du plan annuel d'audit que la planification des travaux d'audit pour une mission donnée. « Certaines recherches ont analysé dans quelle mesure ces exigences étaient appliquées par les fonctions d'audit interne (Pelletier, 2008 ; Koutoupis et Tsamis, 2009 ; Castanheira et al., 2010) ». « Les travaux montrent que même si certaines fonctions d'audit interne font référence à une approche par les risques lorsqu'elles décrivent leur méthodologie, leurs pratiques révèlent que cette approche n'est que partiellement appliquée. L'approche par les risques de l'audit est principalement mise en œuvre pour établir le plan annuel d'audit et elle n'est pas toujours utilisée pour le plan de mission (Castanheira, Rodrigues et Craig, 2010) ». « Alors que certaines fonctions d'audit interne déclarent appliquer une approche fondée sur les risques, la documentation associée à leurs travaux d'audit n'est pas suffisante pour le démontrer (Koutoupis et Tsamis, 2009) ». « Enfin, d'autres recherches ont montré combien était difficile en pratique de mettre en œuvre un processus d'audit fondé sur les risques (Knechel, 2007) ». « Ce qui est selon Power (2003, 2004) aussi généralement reconnu à présent est que l'audit n'est pas simplement une technologie neutre mais un processus socialement construit visant à assoir une certaine légitimité ».

« La littérature qui existe sur le thème de l'audit interne et son approche par les risques est limitée (Coetzee et Lubbe, 2014) ». Nous savons que les auditeurs internes doivent suivre une approche fondée sur les risques, mais nous ne savons pas comment ils procèdent en pratique.

2.1.4 La question de l'auditabilité en lien avec les différents styles de management des risques

« Selon Power (2004), il peut être aujourd'hui largement admis qu'en matière de gestion des risques, une bonne organisation dispose nécessairement d'un processus formalisé, structuré et intégré de gestion des risques ». Toutefois, certains auteurs restent sceptiques quant aux impacts réels d'un tel dispositif sur la performance de l'organisation. « Certains travaux mettent plus particulièrement en avant l'idée selon laquelle la mise en œuvre de tels dispositifs suit avant tout une logique de conformité et de recherche de légitimité (Arena and al, 2011) ».

Toujours « selon Power (2009), la conception "comptable" et la logique d'auditabilité qui dominent dans le modèle du COSO 2 – *Entreprise Risk Management* ont certainement limité la portée et les impacts attendus par la mise en place des dispositifs de management des risques. La logique d'auditabilité a été privilégié à celle d'efficacité des processus de gestion des risques. Il en découle en pratique des contrôles formels des activités qui visent à assurer à une plus grande traçabilité et auditabilité. Power définit la notion d'auditabilité dans la théorie de la société de l'audit (1999) lorsqu'il décrit la pratique de l'audit ». « Selon Power (1999), contrairement à l'image officielle de l'audit souvent présenté comme une activité qui observe les objets de façon neutre, l'audit met en œuvre un processus actif qui vise à rendre les choses auditables. Pour y parvenir, l'audit il est nécessaire pour l'audit de négocier une base de connaissance légitimé et institutionnalisé et de créer un environnement qui soit réceptif à cette base de connaissance ».

« Mikes (2009, 2011) a étudié plus spécifiquement le développement des dispositifs de gestion des risques au sein des banques. Ses travaux mettent en évidence l'existence de deux différents styles de management des risques. Le premier style se caractérise par un "enthousiasme quantitative" orienté sur la mesure et l'évaluation du risque. Le second style se caractérise par un "scepticisme quantitatif" et qui est fondé sur des méthodologies moins quantitatives, moins formelles et plus orientés sur les incertitudes stratégiques qui ne sont pas mesurables ». « Pour Mikes (2011), il y a d'une part une approche holistique des risques qui traite en priorité des risques majeurs et des décisions stratégiques et d'autre part une approche quantitative qui traite plus des risques techniques et opérationnels. Dans le cas de l'approche holistique, les modèles sont moins formels et donc plus difficile à auditer ».

2.2 Questions de recherche

La revue de la littérature montre combien le concept de risque s'avère être problématique et nous amène à nous interroger sur la nature des risques pris en compte par l'audit interne au regard du critère d'auditabilité mis en avant par Power (1999, 2009) et Mikes (2009, 2011). Notre recherche vise à apporter des réponses aux questions de recherches suivantes et accroître la connaissance sur l'approche par les risques de l'audit interne.

Question de recherche n°1 : Comment les départements d'audit établissent leur plan d'audit en lien avec les cartographies des risques des organisations au sein desquelles ils opèrent ?
Question de recherche n°2 : Comment peut-on expliquer l'écart entre les risques identifiés de la cartographie des risques et ceux retenus dans le plan d'audit ?

Nous allons développer dans la partie suivante la méthodologie que nous avons utilisée pour répondre à ces questions.

3 Méthodologie de recherche

Dans cette étude, nous nous concentrons sur la compréhension du phénomène étudié, étant donné la quantité limitée de connaissances approfondies sur la pratique des auditeurs internes en matière d'évaluation des risques.

3.1 Collecte des données

La méthodologie de collecte des données est principalement fondée sur des entretiens individuels et collectifs sous forme de focus group réalisés avec 32 directeurs de l'audit au sein de grand groupes cotées du CAC 40 et du SBF 120.
Les répondants font partie de sociétés du secteur industriel, commercial et des services. Ce choix est justifié par le fait que les entreprises sélectionnées ne disposent pas (contrairement à d'autres secteurs (comme celui des assurances) de données statistiques suffisantes pour leur permettre d'appliquer une approche fréquentiste des risques. Cette difficulté présente un intérêt particulier : comprendre comment ces organisations procèdent pour identifier et évaluer les risques. Nous avons décidé d'exclure les banques et les assurances qui sont soumises à un cadre réglementaire spécifique ainsi que les petites et moyennes entreprises dès lors qu'elles ne disposent pas de département d'audit dédiée. Le nom des sociétés qui ont participé à l'étude a été rendu anonyme pour des raisons de confidentialité.

Tableau 1 : liste des répondants par secteur d'activité

15 entreprises		*9 entreprises*	*8 entreprises*
Industries		**Commerces**	**Services**
Fromago	Santeform	Vestimod	Restaulib
Equipauto	Batimodern	DistriMart	Naturelia
Vehicar	Cimento	Vino	Bati-F
RaceCar	Voltage	Mediacorp	Baticosto
Micropix	Elec	Sportflex	Enginico
LuxStore	Petrolium	WallDistrib	Autocar
Chimica		BeauMag	Aéro
Gazeo		ElectroStore	Voyago
Chimicor		MultimedStore	

L'unité d'analyse retenue est le département d'audit qui opère dans un contexte organisationnel spécifique. Il est essential de comprendre comment les objets de risque sont socialement construits au sein des organisations en considérant les interactions entre les acteurs, notamment entre les auditeurs internes et les autres membres au sein de l'organisation.

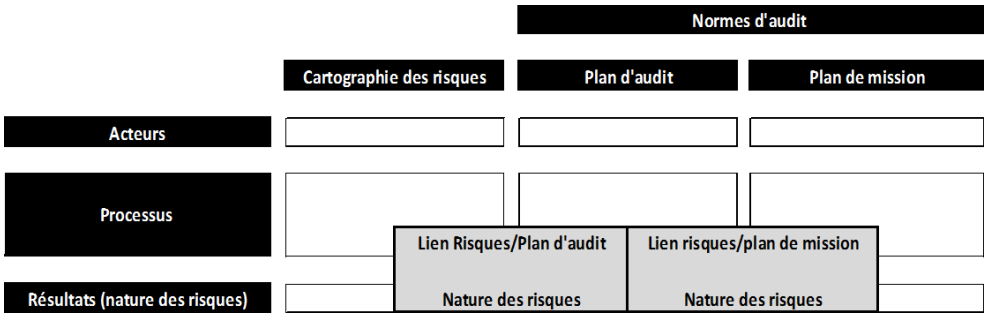
Les données collectées représentent plus de 1.000 pages d'entretiens ainsi que des documents internes tels que les cartographies des risques, les plans d'audit et les rapports d'audit.

3.2 Analyse des données

Les entretiens (47 heures au total) ont tous été enregistré puis retranscrits de façon intégrale. Les données ont été codées avec l'outil NVivo 10 et ont fait l'objet d'un double codage. La méthodologie utilisée pour analyser les données est fondée sur celle de l'étude de cas (Yin, 2003). La grille de codage appliquée pour l'analyse des données combine des codes issues à la fois des normes d'audit interne et les principaux concepts identifies dans la revue de la littérature.

Le schéma ci-dessous présente la structure générale qui nous a permis d'identifier les acteurs, les principaux processus mis en œuvre dans le cadre des processus de cartographie des risques et de planification des travaux de l'audit réputés être basés sur les risques selon les normes.

Schéma 3 : structure générale de la grille de codage



Le tableau ci-dessous précise les principaux aspects couverts pour chacun de ces processus (cartographie des risques, plan d'audit et plan de mission).

Tableau 2 : thèmes couverts par processus

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

Plan d'audit
Construction de l'univers d'audit
identification des sujets en lien avec les risques
Hiérarchisation 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
Elaboration du programme de travail

Après avoir identifié pour chacun des catégories issues de notre matériau, nous avons appliqué une seconde grille d'analyse afin d'identifier pour chacune des catégories issues du premier codage les points de ressemblance et de dissemblance, en lien avec le type d'organisation. La section suivante présente les principaux résultats de cette analyse.

4 Principaux résultats

En préambule de nos résultats, il est important de rappeler certaines exigences normatives qui encadrent l'activité de l'audit interne. Les normes d'audit 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 ces mêmes organisations sont exposées. Nos résultats mettent en évidence un écart entre les risques identifiés par les managers et les opérationnels dans la cartographie des risques et les risques pris en compte dans les plans d'audit.

Les entretiens nous ont permis de montrer que certains risques sont considérés par les auditeurs comme étant des risques non auditables ou bien que certains risques ne sont auditables que de façon partielle.

Selon Power (1999), contrairement à l'image officielle que nous pouvons avoir de l'audit en tant qu'activité neutre qui observe les objets d'audit au sein des organisations, l'audit est un processus actif qui vise à rendre les objets "auditables". Toutefois, Power ne décrit pas de façon précise comment l'audit procède pour y parvenir. La principale contribution de cet article est de décrire de processus d'auditabilité pour nous permettre de mieux comprendre comment les auditeurs transforment les risques identifiés dans les cartographies des risques en risques auditables.

Cette section présente les différentes dimensions que revêt l'écart qui existe entre l'univers des risques et l'univers d'audit et le processus d'auditabilité qui consiste à convertir les risques en risques auditables qui peuvent être couverts dans le cadre des missions d'audit.

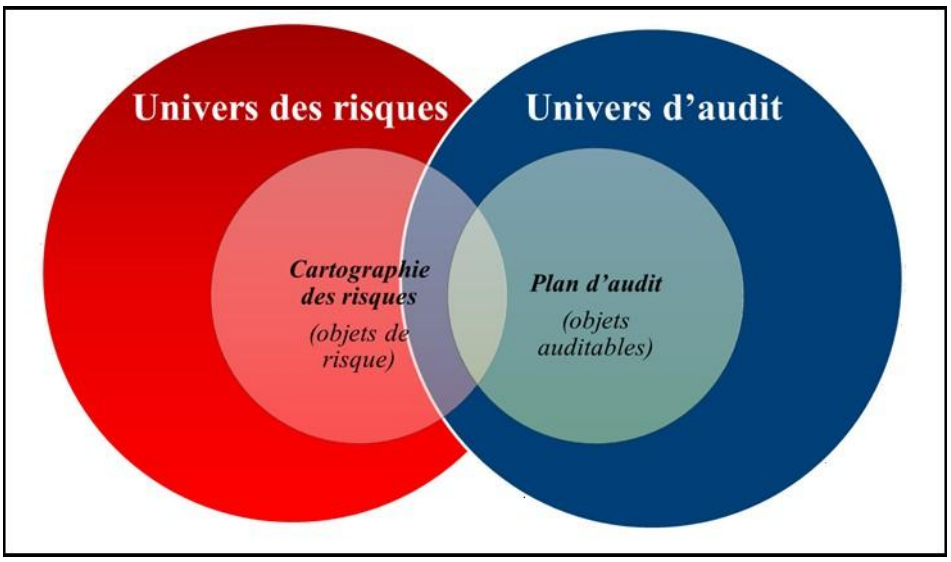
4.1 L'écart entre univers des risques et univers d'audit

Nos résultats montrent que la couverture par l'audit des risques identifiés dans les cartographies des risques peut être plus ou moins importante en fonction de l'organisation concernée. Les plans d'audit intègrent un certain nombre de missions qui sont difficiles à rattacher au contenu des cartographies des risques.

Le processus d'élaboration du plan d'audit tel que décrit par les directeurs de l'audit met ainsi 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 découle dès lors un écart entre l'univers des risques représenté par la cartographie des risques et l'univers d'audit représenté par le plan d'audit comme l'illustre le schéma ci-dessous.

Schéma 2 : écart entre univers des risques et univers d'audit



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.

Nos données mettent en évidence que cet écart résulte des modes d'observation appliqués pour appréhender les risques ainsi que de la nature des risques. Ces deux éléments ne sont pas les mêmes pour d'une part le processus de cartographie des risque et d'autre part le processus d'élaboration du plan d'audit.

4.1.1 La distinction entre les risques « auditables » et « non auditables ».

Les données collectées au travers des entretiens nous ont permis d'identifier que les auditeurs considéraient certains risques comme étant non auditables ou bien auditable de façon partielle. La notion d'auditabilité repose sur un certain nombre de points communs décrits par les répondants tout en conservant certaines spécificités en lien avec les organisations interrogées.

Les directeurs de l'audit illustrent tout d'abord leurs difficultés pour passer des risques de la cartographie aux missions du plan d'audit 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 ».*

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 surcroit, 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 ».*

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 ».*

Certains risques de la cartographie sont aussi considérés comme difficiles à auditer du fait de

l'absence de compétence au sein de l'équipe d'audit.

> ***VESTIMOD :*** *« Pas de compétence informatique particulière, enfin on n'est pas des auditeurs informatiques, donc, le volet informatique, on l'a pas ».*
>
> ***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 ».*

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.

4.1.2 L'absence de code de communication commun pour traiter du risque au sein des organisations

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 méthodo, 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 ».*

L'audit interne a une approche qui est en lien avec les processus d'entreprise alors que les cartographies des risques n'établissent pas toujours un tel lien entre un risque identifié et les processus qui y sont associés.

4.2 Le processus d'auditabilté

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 principale contribution de cet article est de préciser comment les auditeurs internes parviennent à transformer les risques en risques auditables et de décrire le processus d'auditabilité.

4.2.1 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.

> ***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 ».*

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.

4.2.2 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.

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 4 : 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 inexistants 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 5 : 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.

4.2.3 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 mêmes 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 et puis on l'a diffusé aux entités ».*

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 6 : 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.

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.

Tableau 7 : 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

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 audités 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.

4.2.4 L'évaluation du risque au moyen du système d'autoévaluation du contrôle interne (questionnaire d'autoévaluation)

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.

4.2.5 Le processus d'auditabilité et ses conséquences au niveau sociétale

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.

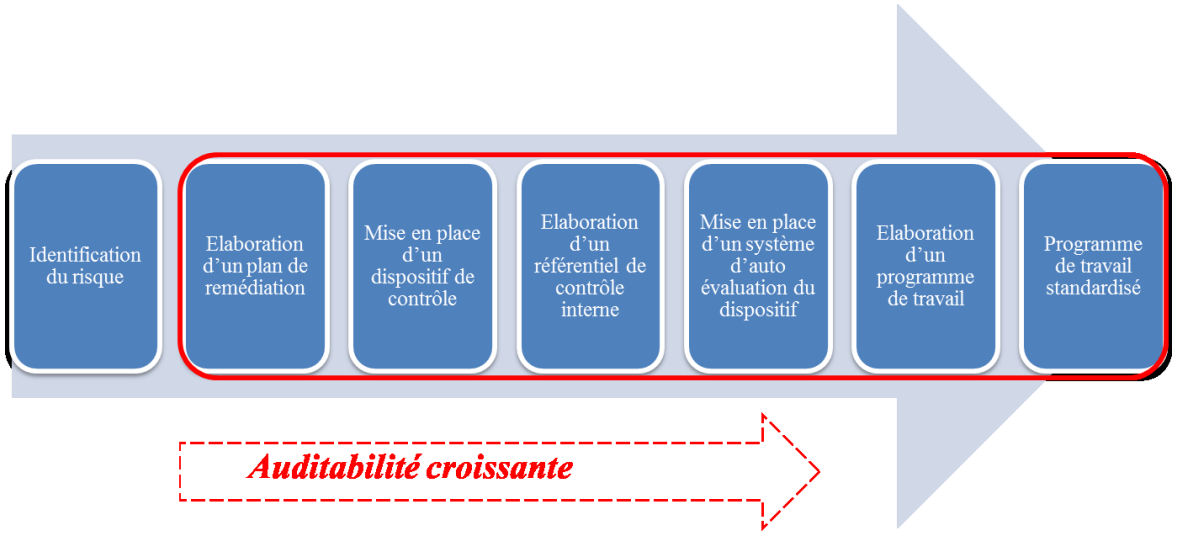
Le processus d'auditabilité amène l'organisation à formaliser de façon progressive ses dispositifs de contrôle interne et à les généraliser. Du fait de la généralisation et la standardisation progressive des dispositifs de contrôle interne, les auditeurs disposent d'un plus grand nombre d'objets de risque 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 construise 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 ci-dessous représente le processus d'auditabilité.et montre que l'auditabilité des risques est croissante dans le temps avec la mise en place progressive des dispositifs de contrôle interne.

Schéma 3 : 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'autoévaluation 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'*Entreprise 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 Conclusion

La question de recherche principale de cette recherche était la suivante : *« 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.

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 la principale contribution de cette recherche.

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. Nos conclusions rejoignent celles de Power (1999) en démontrant l'existence d'un écart entre l'univers des risques et l'univers d'audit. Certains risques ne sont pas couverts par l'audit interne qui les considère comme non auditable.

Pour les risques de la cartographie qui sont pris en compte dans le plan d'audit, nous rejoignons aussi l'idée avancée par Power (1999) selon laquelle l'activité d'audit n'est pas neutre et a un impact sur la construction des objets de risque au sein de l'organisation. La principale contribution de cette recherche est de décrire le processus mis en œuvre par l'audit interne pour transformer les risques de la cartographie en risques auditables, c'est-à-dire de

décrire le processus d'auditabilité et ses différentes dimensions. Il est néanmoins essentiel de comprendre que le processus d'auditabilité ne se limite pas à une dimension technique et qu'il a un impact au niveau sociétal. Le besoin qu'a l'audit de rendre les risques auditables amène l'organisation à développer dans le cadre du processus de gestion des risques des systèmes de contrôle formels tel que décrit par Power (1999, 2009). Nos résultats mettent ainsi en évidence que l'activité d'audit interne n'est pas neutre car elle façonne la manière d'observer les risques et amène à traiter en priorité des risques auditables au risque de faire oublier les dangers qui n'ont pas pour autant disparu.

Cette recherche 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.

Mikes (2019, 2011) décrit deux types de gestion des risques : le premier de type "quantitatif" (*quantitative optimistic*) qui privilégie la mesure des risques techniques, le second "non quantitatif" (*quantitive pessimistic*) qui privilégie la planification stratégique et qui est moins formalisé. Comme l'a montré notre recherche, les risques auditables correspondent à des risques qui sont couverts par des dispositifs et des contrôles formels en lien avec des processus. Notre recherche a permis de mettre en évidence que les risques gérés avec un style "quantitatif" tel que décrit par Mikes sont certainement plus faciles à auditer que les risques identifiés dans le style "non quantitatif "dès lors que les risques stratégiques relèvent d'objets d'audit moins formels. Une piste de recherche pourrait être envisagée pour étudier l'activité de l'audit interne en lien avec cette dimension développée par Mikes.

Par ailleurs, compte tenu de l'hétérogénéité et de la diversité des pratiques d'audit selon les organisations, il serait opportun d'étudier l'intérêt d'avoir fondé la pratique de l'audit interne sur la notion de risque à travers les normes professionnelles.

6 Bibliographie

6.1 Articles

Allegrini M. & D'Onza G. (2003), Internal Auditing and Risk Assessment in Large Italian Companies: An Empirical Survey, *International Journal of Auditing* 7 (3): 191-208

Arena, M, Arnaboldi M. & Azzone G. (2011). Is enterprise risk management real ?, *Journal of Risk Research* 14 (7): 779–797

Coetzee P. & Lubbe D. (2014), Improving the Efficiency and Effectiveness of Risk-Based Internal Audit Engagements, *International Journal of Auditing* 18 (2): 115-125

Gendron Y, Cooper D. J. & Townley B. (2007), The construction of auditing expertise in measuring government performance, *Accounting, Organisations and Society* 32 (1-2): 105-133

Gramling A.A, Maletta M.J, Schneider A. & 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* 23:194-244

Jordan S, Jørgensen L. & Mitterhofer H. (2013), Performing risk and the project: Risk maps as mediating instruments, *Management Accounting Research* 24: 156–174

Knechel W.R. (2007), The business risk audit: origins, obstacles and opportunities, *Accounting, Organizations and Society* 32 (4–5): 383-408

Koutoupis A. G. & Tsamis A. (2009), Risk-based internal auditing within Greek banks: a case study approach, *Journal of Management and Governance* 13 (1-2): 101-130

KPMG (2013), Benchmark of practices for french group listed in CAC 40 (index https://www.kpmg.com/FR/fr/IssuesAndInsights/ArticlesPublications/Documents/Benchmark-pratiques-groupes-CAC-40-122013.pdf)

Mikes A. (2009), Risk management and calculative cultures, *Management Accounting Research* 20 (1): 18-40

Mikes A. (2011), From counting risk to making risk count: Boundary-work in risk management, *Accounting, Organizations and Society* 36 (4-5): 226-245

Miller P, Kurunmaki L & O'Leary T. (2008), Accounting, hybrids and the management of risk, *Accounting, Organizations and Society* 33 (7–8): 942-967

Paape L, Scheffe J. & Snoep P. (2003), The Relationship Between the Internal Audit Function and Corporate Governance in the EU - a Survey, *International Journal of Auditing* 7 (3): 247-262

Pelletier J. (2008), Adding risk back into the audit process, *Internal Auditor* 65 (4): 73–76

Power M. (2003), Auditing and the production of legitimacy, *Accounting, Organizations and Society* 28 (4): 379-394

Power M. (2009), The risk management of nothing, *Accounting, Organizations and Society* 34 (6-7): 849-855

Selim G. & McNamee D. (1999a) "Risk Management and Internal Auditing: What are the Essential Building Blocks for a Successful Paradigm Change", *International Journal of Auditing* 3 (2): 147-155.

Sarens G. & De Beelde I. (2006), Internal Auditors' Perception about their Role in Risk Management. A Comparison between US and Belgian Companies, *Managerial Auditing Journal*, Emerald Group Publishing Limited 21 (1): 63-80.

Spira L. F. & Page M. (2003), 'Risk management: the reinvention of internal control and the changing role of internal audit', *Accounting, Auditing & Accountability Journal* 16 (4): 640-661

6.2 Ouvrages

Committee of Sponsoring Organisations of the Treadway Commission (COSO), *Enterprise Risk Management - Integrated Framework (2004) and Internal Control - Integrated Framework (2013).* Disponible à l'adresse suivante : http://www.coso.org.

Creswell, J.W. (2007). *Qualitative inquiry and research design: Choosing Among Five Approaches,* 2 nd edition. Thousand Oaks, Sage Publication.

Institute of Internal Auditors (IIA), *International Professional Practices Framework*. Disponible à l'adresse suivante : https://na.theiia.org/standards-guidance.

Krueger R.A. & Casey M.A. (2002), *Focus Group: a practical guide for applied research* (3rd edition), Thousand Oaks, CA: Sage Publications

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. (2007), *Organized Uncertainty - Designing a World of Risk Management*, Oxford University Press, Oxford

Saldaña, J. (2009). *The Coding Manual for Qualitative Researchers.* Sage Publication.

Standard & Poor's (2008), *Enterprise risk management for ratings of nonfinancial corporations*. Ratings Direct, June 5 (www.standardandpoors.com/ratingsdirect)

Yin, R. K. (2003). *Case Study Research: Design and Methods,* 3rd edition. London: Sage Publication.