Contribution à l'analyse critique de la norme de contrôle. : Le cas des risques opérationnels dans le secteur financier : de la normativité à l'effectivité

Nicolas Dufour

le cnam

ÉCOLE DOCTORALE Management & Société

Laboratoire Interdisciplinaire de Recherche en Sciences de l'Action (LIRSA)

Thèse

présentée par :

Nicolas DUFOUR

soutenue le : **4 mars 2015**

pour obtenir le grade de : **Docteur du Conservatoire National des Arts et Métiers**

Discipline/ Spécialité : Gestion (Comptabilité Contrôle Audit)

Contribution à l'analyse critique de la norme de contrôle. Le cas des risques opérationnels dans le secteur financier : de la normativité à l'effectivité.

THÈSE dirigée par :

M. CAPPELLETTI Laurent	Professeur, Cnam

RAPPORTEURS :

Mme ZARDET Véronique	Professeur des Universités, IAE de Lyon
M. DE LA VILLARMOIS Olivier	Professeur des Universités, IAE de Paris

---

JURY :

M.PESQUEUX Yvon	Professeur, Cnam
M.BENCHEIKH Abdel	Directeur risques et conformité, Natixis Asset Management

Remerciements

Remerciements

Je tiens tout d'abord à remercier mon directeur de thèse Laurent Cappelletti pour sa disponibilité à toute épreuve durant mon parcours doctoral au sein du Cnam. Sans ses remarques, conseils et alertes, mon travail de thèse n'aurait pas la même consistance. Je le remercie également pour m'avoir transmis sa vision de la recherche, empreinte de pragmatisme et de rigueur autant que d'autonomie et de recul. J'estime que c'est une réelle chance que d'avoir eu un encadrement de ce niveau ainsi que d'avoir été associé à divers projets connexes à mon domaine de recherche. Ces années de thèse auront été très formatrices à de nombreux égards.

Je souhaite également remercier mes proches collègues, chercheurs et praticiens, Gilles Teneau, Béatrice Bon-Michel et Jean-David Darsa avec qui j'ai pu partager mon intérêt de la recherche sur ce domaine encore émergent qu'est le risque opérationnel. Pendant toute cette période de thèse, nos échanges fréquents ont permis de faire évoluer ma réflexion et de revoir certains points à la lumière d'informations auxquelles je n'aurais pas pensé spontanément.

Je me dois également de remercier l'ensemble des professionnels du secteur financier qui m'ont ouvert leurs portes et accordé du temps afin d'échanger sur ce sujet de recherche. Grâce à eux, ma recherche a gagné en qualité et la richesse des échanges réalisés lors des nombreux entretiens notamment, m'a permis d'avancer dans les différentes étapes de la thèse.

Au titre des remerciements je dois citer mon père, Jacques, et l'ami de toujours, Matthieu Padilla, qui m'ont fourni une aide et un soutien important tout au long de cette recherche sur un sujet assez éloigné de leurs préoccupations.

Mes remerciements concernent également mes amis, notamment Florian Fizaine et Charaf David Chalaoui, qui ont partagé de près ou de loin mes préoccupations et m'ont aidé, parfois sans le savoir, à faire aboutir ce projet de recherche.

Il me faut également remercier le professeur Yvon Pesqueux pour m'avoir transmis cette envie de réaliser des recherches en gestion, d'interroger des concepts mais aussi de découvrir les différentes théories d'une discipline encore riche et jeune.

Je remercie également Carole Simonnet pour son soutien sans faille au cours de cette recherche et son éternel optimisme, mais aussi Marion Houlet et Hélène Adam dont l'aide fut plus que précieuse dans la phase finale de cette thèse.

Il y a forcément d'autres personnes que je n'ai pu citer ici et j'espère qu'elles ne m'en tiendront pas rigueur, mais mes remerciements les concernent également.

Résumé

Résumé de la thèse

L'objet du présent projet de thèse porte sur l'analyse critique des normes de contrôle du risque opérationnel. Il s'agit de mettre en lumière la manière dont le Risk Management mobilise les parties prenantes des organisations pour créer et animer une culture du risque opérationnel. L'approche retenue est la triangulation méthodologique combinant deux recherche-action réalisées au sein d'un établissement bancaire et d'une compagnie d'assurance ainsi que des entretiens semi-directifs et une analyse de contenu sur un ensemble de documents internes à chacun des cas étudiés. Les résultats de la recherche font état de la nécessité de traduire les normes de contrôle prudentiel dans l'organisation et de structurer les nombreux contrôles pour mettre en œuvre une politique de risque effective.

Les récentes évolutions règlementaires dans le domaine bancaire et en assurance (Bâle 2 et Bâle 2.5, Bâle 3, Solvabilité 2) tendent à renforcer les dispositifs de contrôle interne et de Risk Management ainsi que la communication d'informations sur ces dispositifs pour une meilleure maîtrise des risques. Ainsi, le règlement CRBF 97-02 parle de filière risque opérationnel, la directive à venir Solvabilité II évoque dans son pilier 2 la nécessité de développer un contrôle interne et un Risk Management tournés vers la prise en compte du risque dans l'organisation et non seulement comme un sujet de provisionnement de fonds propres.

Cependant ces efforts n'empêchent pas la survenance et la médiatisation de scandales financiers dont l'ampleur est à la hauteur des montants financiers traités. Ainsi, de nombreux établissements financiers sont touchés par le risque opérationnel. Ce risque est avant tout un risque organisationnel, contingent du facteur humain et prenant de multiples formes (les catégories baloises du risque opérationnel en sont une illustration). Les exemples de survenance de risque opérationnel sont nombreux : les cas de JP Morgan, d'UBS, de Société Générale, de Barclays, de HSBC, de Goldman Sachs en attestent. Toutefois, le risque opérationnel n'est pas seulement le fait de banques de financement et d'investissement et n'est pas uniquement un risque extrême par ses conséquences. Il concerne également les banques de détails et les sociétés d'assurance et est le plus souvent un risque de fréquence et de faible impact (fraudes aux moyens de paiement et fraude à l'assurance par exemple). La réglementation prudentielle comprend un ensemble de normes tendant à inciter les établissements financiers à mieux prendre en compte cette catégorie encore émergente et mal connue de risque (les risques de marchés ou de crédits faisant l'objet de davantage d'études).

Nous décrivons et analysons l'influence de ces évolutions normatives sur les dispositifs internes de maîtrise du risque opérationnel (Risk Management opérationnel, contrôle interne) et nous interrogeons la manière dont les établissements financiers structurent leur contrôle des risques, plus particulièrement en ce qui concerne l'effectivité de ces dispositifs. Afin d'éviter de développer des contrôles manquant d'effectivité, il devient essentiel de situer cette

régulation prudentielle dans une perspective de structuration des contrôles et de traduction/compréhension de la norme de contrôle.

Mots-clés: Risk Management, risque opérationnel, politiques de risque, Banque, Assurance, normes prudentielles, traduction des normes, structuration des contrôles, structure, comportements.

Résumé en anglais

The aim of this thesis is to bring to light the way the Risk management mobilizes the stakeholders of organizations to create and lead a culture of the operational risk.

Our research approach is the methodological triangulation, combining two action-research case studies, arising within a banking institution and within an insurance company, as well as semi-directive interviews and an analysis of contents on a set of internal documents in each of the studied cases. The research results state the necessity of translating the standards of prudential control in the organization and of structuring the numerous controls to implement an effective risk mastering policy.

The recent statutory evolutions in the banking and insurance sectors (Basel 2 and Basel 2.5, Basel 3, Solvency II) tend to strengthen systems of internal control and Risk Management as well as the communication of information over these devices for a better control of the risks. So, the regulation CRBF 97-02 speaks about operational risk systems, the directive to come Solvency II evokes in its pillar 2 the necessity of developing an internal control and a Risk Management turned to the consideration of the organizational risks.

However these efforts do not prevent the emergence and the mediatization of financial scandals the scale of which is as high as the financial handled amounts. So, numerous financial institutions are affected by the operational risk. This risk is before any an organizational risk, a contingent of the human factor and taking multiple forms (the Basel categories of the operational risk).

There are numerous examples of extremes operational risks: the cases of JP Morgan, UBS, Société Générale, Barclays, Goldman Sachs give evidence of it. However, the operational risk is not only the fact of corporate and investment banking and is not only an extreme risk by its consequences and in low probability. It also concerns retail banks and insurance companies and is most of the time a risk of frequency and low impact (frauds in payment activities, and fraud in life and non-life the insurance for instance). The prudential regulation include a set of standards tending to incite financial institutions to take into account better this category still emergent and badly known by risk (markets risks or credits risks have being the object of more studies).

We describe the influence of these normative evolutions on the internal devices of the operational risk (Operational Risk Management, Internal Control) and we question the sense given by establishments to the information onto the control of the risks, more particularly as regards the effectiveness of these devices. To avoid an informative overload regarding control, it becomes essential to place this prudent regulation in perspective of structuring of the controls and the translation / understanding of the risk control standards.

Keywords: Risk Management, operational risk, risk policy, banking, insurance, prudential standards, standards translation, controls structuration, structure, behaviors.

Table des matières

Liste des tableaux

Liste des figures

Liste des annexes

Introduction

Chapitre introductif - L'intérêt d'une recherche sur le contrôle des risques opérationnels

« L'aversion pour le risque est une préoccupation qui mène à une gestion centralisée et organisée du danger à venir. Gestion dans laquelle le pouvoir mobilise massivement ses ressources face aux maux possibles de la société »
Douglas M., Wildavsky A., 1983

1. Un essor du risque opérationnel dans la perception collective.

Notre objet d'étude concerne le contrôle du risque au sein des entreprises du secteur financier (banque et assurance). Plus précisément nous étudions la manière dont les politiques de maîtrise des risques sont mises en œuvre par les sociétés du secteur financier en vue de réduire les risques opérationnels que ces dernières pourraient subir.

Cette recherche se caractérise donc par l'étude des enjeux de contrôle en sciences de gestion associés à la notion de risque. Comme l'évoquent certaines recherches françaises en épistémologie (Larkèche, 2011 ; Pesqueux, 2011), nous sommes aujourd'hui dans une ère ayant mis le risque au centre des préoccupations à la fois sociétale, individuelle mais aussi organisationnelle et managériale. Une telle approche est notamment le fait de l'essor des grandes organisations mais de manière plus spécifique une nécessité de contrôle de l'environnement interne et externe de celle-ci. La majorité des recherches en sciences de gestion portant sur la thématique du contrôle des risques se situe en finance mais aussi, et c'est dans ce champ de recherche que nous nous inscrivons, en comptabilité-contrôle-audit.

Objet d'étude :

L'objet de notre thèse est d'étudier les politiques de maîtrise des risques opérationnels mises en place par les établissements financiers (banque et assurance en vue de répondre aux exigences normatives). Nous étudions le risque opérationnel subi par ces établissements et non le risque que l'établissement fait potentiellement subir à d'autres agents économiques (risque pour les autres établissements, risque porté par le client). Cette recherche se situe dans le champ des sciences de gestion (comptabilité-contrôle-audit) et implique d'étudier les dispositifs de Risk Management et de contrôle associés au risque opérationnel (dont contrôle interne).

Contexte de la recherche :

La période contemporaine s'inscrit dans la dialectique d'une aspiration au contrôle pour les organisations (Power, 1999). Elle correspond à ce que certains appellent une « perspective gestionnaire de risque », mettant en lumière l'importance de la notion de risque dans le secteur financier (Shiller, 2003). Gérer le risque, se couvrir face aux incertitudes de l'avenir, s'inscrit dans une perspective de confiance et de sécurité face à l'avenir. Dans un contexte où la financiarisation tend à devenir un vecteur d'avènement d'une société du risque (Beck, 1986) la thématique du contrôle et de la gestion des risques dans les organisations du secteur financier trouve tout son sens.

Face à cela, des auteurs se sont demandées si les entreprises du secteur financier, notamment les banques, savent encore gérer le risque (Hanlon, 2010). Ces métiers (banque, assurance) sont fondés sur la gestion des risques, notamment opérationnels, un moyen de maîtriser son activité tout en atteignant des objectifs de performance de manière durable (Girotra, Netessine, 2011).

Toutefois, l'actualité de ces dernières années met sur le devant de la scène une catégorie encore récente que sont les risques opérationnels.

Les risques opérationnels et les contrôles qui leur sont associés au sein du secteur financier font l'objet d'un processus de normalisation (Cappelletti, 2006). Si les réglementations Bâle II (arrêté du 20 février 2007) puis Solvabilité II (à venir) abordent le risque opérationnel comme un enjeu d'organisation, force est de constater que les nombreux efforts déployés par les organismes financiers pour mettre en place des contrôles et une gestion des risques n'ont pas permis d'éviter certains risques opérationnels majeurs à la base de nombreux autres risques (de marché ou de crédit) ; comme l'illustrent les affaires d'AIG, de Société Général, de Bernard Madoff Investment, de Dexia ou encore JP Morgan Chase plus récemment. A fortiori ces efforts en matière de contrôle du risque opérationnel se heurtent fréquemment à de nombreuses problématiques : la qualité des données remontées, l'intérêt des parties prenantes pour ce sujet, l'investissement dans des outils et méthodes dédiées, l'application des politiques, processus et procédures mis en place sur ces sujets etc..
Dans un monde où le risque est omniprésent, la finance moderne a fait de la gestion des risques un enjeu désormais incontournable (Shiller, 2003 ; Miller, 2009). La gestion des risques, bien que largement présente aujourd'hui dans les organisations, existe à différents

stades de maturité (Power, 2009). Elle est depuis longtemps présentée comme l'un des piliers d'un dispositif de contrôle efficace (COSO, 1992).

L'actualité récente montre néanmoins que les enjeux de contrôle dans le secteur financier sont loin d'être résolus. Force est de constater que les contrôles, bien qu'en augmentation, ne parviennent pas à réduire de manière significative les risques majeurs, principalement opérationnels : rogue trading (affaire Kerviel de la Société Générale en 2008), manipulation d'indices de référence découverte en 2012 (Libor et Euribor), soupçons de blanchiment d'argent pour HSBC, vente forcée d'assurance vie lors de l'octroi de crédit n'en sont que quelques illustrations. En matière de risque opérationnel, les nombreuses affaires récentes montrent la nécessité de questionner l'opportunité de telles normes car elles n'apportent pas nécessairement un cadre de compréhension et d'intervention satisfaisant (Jiang et al., 2010). Bien souvent, l'objectif qui prime est celui de la conformité, on parle alors de contrôle de conformité pour s'assurer de cette concordance des enjeux et des pratiques aux exigences normatives[1]. Toutefois, une telle approche nous apparait aujourd'hui comme limitée face aux déficiences récurrentes du contrôle comme le montrent les cas de JP Morgan ou encore de Commerzbank, de Goldman Sachs, de Barclays, d'HSBC en banque, d'AIG ou encore d'Assor en assurance plus récemment.

En France, l'Autorité de Contrôle Prudentiel et de Résolution (ACPR) a insisté sur le renforcement des exigences règlementaires en matière de contrôle interne des établissements de crédit, notamment en termes organisationnel et de transparence informationnelle dès 2005. Les banques ont alors fortement investi pour répondre à l'obligation de moyens. La technique de contrôle ainsi déployée se définit à partir des pratiques auxquels elle répond et réduit la dimension culturelle de cet objet (Steiner, 2010). Face aux risques et dans un contexte d'incertitude croissante, les banques sont incitées d'une part à améliorer la transparence quant à la qualité de leur dispositif de contrôle notamment vis à vis des instances délibérantes et d'autre part à structurer leur dispositif face aux différents risques identifiés.

Dans un contexte de renforcement à la fois des contrôles et des informations sur ces contrôles, notre étude vise à mieux comprendre d'une part la manière dont les récentes évolutions règlementaires ont influencé l'organisation des contrôles et la manière de prendre en compte le risque opérationnel

[1] Certains dirigeants parlent davantage de contraintes normatives. Ces dispositifs normatifs insistent peu sur l'analyse critique des risques et sur le regard critique à avoir pour les dirigeants dans leur système de gestion des risques.

Après chaque crise majeure, il est coutume de rechercher de nouvelles règles, de nouveaux paradigmes et cadres de pensée pour structurer et orienter l'action des agents économiques dans un but précis.
Dans le secteur financier, les oppositions sont fréquentes entre partisans d'une régulation renforcée (en vue d'éviter des pratiques abusives et de nombreuses dérives) et opposant à celle-ci (arguant du fait que la régulation est source de rigidités et qu'elle a toujours un certain retard sur les problèmes de notre temps).

Notre étude concerne plus spécifiquement les normes de contrôle traitant du risque opérationnel dans le secteur financier. Ces normes, aussi nombreuses qu'elles soient (Sarbannes-Oxley, Bâle II, règlement CBF 97-02 et Bâle III à venir dans le domaine bancaire, Solvabilité II à venir en assurance) sont toujours en phase de structuration dans leur application. L'attention porta pendant longtemps sur les normes de solvabilité des établissements, puis l'on compri l'importance du risque de liquidité. Les crises récentes ont mis encore l'accent sur le risque opérationnel et l'importance de prendre en compte des pratiques loin d'être récentes tels que la créativité d'expert en matière de produits financiers (Merton, 1995 ; Méric, Sfez, 2011), les pratiques de rogue trading ou plus généralement l'importance des fraudes aux moyens de paiement, de la cybercriminalité affectant les banques, de l'enjeu que représente la lutte anti-blanchiment, des abus en matière de vente de produits financiers etc.. Ces nombreux cas traduisent donc un essor du risque opérationnel dans la perception collective.

2. Risque opérationnel, Risk Management, politique de risque, des notions complémentaires.

Nous cherchons ici à préciser certains des concepts clés (risque, politique de risque, risque opérationnel) quant à notre sujet de recherche et ayant amené cette réflexion puis cette perspective de recherche.

Les principaux termes de notre sujet de recherche (Etude du contrôle des risques opérationnels, de la normativité à l'effectivité) sont définis comme suit :

-la notion de risque : Plusieurs définitions peuvent être données de la notion de risque, celles-ci sont parfois juridique, économique et financière, sociologique ou encore

managériale. Nous retiendrons, avant de développer ce sujet dans le paragraphe suivant, une définition envisageant le risque comme la mesure du niveau de développement et de préparation à l'action d'une organisation face à des évènements externes ou internes à celle-ci et potentiellement dommageables dans le futur (ou étant déjà survenus mais ayant un potentiel de récurrence). Le risque est donc la mesure de l'action, l'élément à prendre en compte lorsque l'on se fixe un objectif donné et ce compte tenu de son appétence au risque (le risque que l'on souhaite prendre) et son niveau de tolérance au risque (jusqu'où on ne souhaite cependant pas aller en cas de perte) ; ces composantes déterminant le profil de risque d'une organisation, d'un agent économique etc..

-le contrôle (dans l'organisation) : la notion de contrôle est envisagé dans notre recherche en cohérence avec les théories issues des travaux de R.Simons (1991) et d'auteurs comme A.Mikes (2007, 2009, 2011) ou M.Power (2005, 2009) comme l'ensemble des fonctions, dispositifs et actions visant à réduire l'incertitude entourant l'organisation dans la conduite de la stratégie d'affaire ou l'atteinte de ses objectifs. Nous situons donc nécessairement le contrôle par rapport à l'approche organisationnelle. La notion d'organisation étant elle-même définie comme une structure de coordination dotée de frontières identifiables et intégrant un système normatif supérieur aux choix et valeurs individuelles (Martinet, Pesqueux, 2013).

-le contrôle des risques : partant de la précédente définition de la notion, cela comprend l'ensemble des fonctions et actions mises en place afin de maîtriser les risques pouvant affecter l'organisation ou être créés du fait de l'activité de cette dernière, dans l'espace (risques internes et externes) et dans le temps (risques avérés ou potentiels).

-la normativité : elle consiste dans le fait de se référer de manière explicite pour une organisation, des acteurs ou groupe d'acteurs, à des cadres de références normatifs (corpus réglementaires de hard ou de soft law : normes de fonctionnement sectorielles, réglementation prudentielle, droit commun ou droit dérivé etc.). On parle de normativité dès lors que la conformité à la règle prend l'ascendant sur son adaptation et son interprétation pragmatique (prise en compte le contexte spécifique d'une organisation ou d'un secteur d'activité). En lien avec la notion de normes (corpus de règles s'imposant ou étant choisi par un acteur ou groupe d'acteurs donné dans un cadre préconstruit).

-l'effectivité : L'effectivité des contrôles dans le monde organisationnel est un concept à

plusieurs facettes. Elle dépend de chaque groupe et de ses critères de préférences permettant son évaluation. Elle se distingue de l'efficience dans l'analyse des comportements organisationnels mais ces deux notions constituent des normes indépendantes pour évaluer une organisation (Price, 1968 ; Pfeffer, Salancik, 1978, p.33).

Partant de ces définitions, il nous faut contextualiser la notion de risque dans notre étude et aborder les questionnements y étant sous-jacents (la notion de risque opérationnel étant définie ci-après).

2.1. Contextualiser le risque : comme mesure du niveau de développement

2.1.1. La notion de risque

- **Approches théoriques de la notion de risque**

Le risque est fréquemment défini comme un évènement imprévu ou un ensemble de conditions réduisant de manière importante l'habileté des gestionnaires dans la conduite de la stratégie d'affaires envisagée. Cette approche rassurante pour certains (les managers) ne l'est pas forcément pour tous. Certains auteurs (Knight, 1921) distinguent clairement risque et incertitude : la notion de risque renvoyant à la prise en compte d'un évènement dommageable sur la base de probabilité objectives (un historique d'évènements similaires étant survenus) ; la notion d'incertitude renvoyant quant à elle à une étude de phénomènes dommageables dont il n'est pas possible d'établir d'historique. Ils sont alors appréhendés sur la base de probabilités conditionnelles (ou subjectives car leur analyse est fondée sur des avis d'experts), on parle également d'incertitude radicale. Les risques sont des évènements définis par une distribution de probabilités objectives (c'est-à-dire des probabilités établies à partir d'informations statistiques). Le risque est donc une incertitude objectivement probabilisable. Il est alors question de risque avéré. L'incertitude, quant à elle, ne peut être cernée par une distribution de probabilités objectives, il s'agit du hasard avec des probabilités inconnues. On parle alors de risque potentiel.

D'autres auteurs appréhendent le risque dans une logique sociologique. Le risque est alors une forme particulière du sentiment de danger : la formalisation dans un cadre sociétale d'une vérité ontologique pour chaque individu : la peur du danger et la nécessité de s'en prémunir (Giddens, 1994 ; Solé, 2009). Certains complètent cette approche dans une perspective socio-

économique comme la mesure de l'action pour les individus. Le risque est alors un facteur d'incitation à l'action (ou de désincitation) permettant d'envisager le niveau de développement d'une Société (Beck, 1986). Pour d'autres penseurs, le rapport de l'Homme dans la Société, mais aussi de l'Homme à la Nature, doit être étudié pour démontrer cette volonté de contrôler ce qui peut avoir un caractère intangible mais devient réel une fois survenu. C'est à ce stade que l'on retrouve cette forme particulière du sentiment de peur : un évènement dommageable qui une fois survenu remet en cause l'existence de l'individu ou son existence dans les conditions connues jusque-là. Cette peur de l'inconnu, de l'incertain, et de ses conséquences potentiellement dommageables, pousse l'individu à se placer dans une posture de compréhension et à sortir de son ignorance pour peu à peu établir une connaissance des différentes formes de danger. D'où la volonté de vouloir se prémunir contre cet évènement dommageable. Le risque est donc un construit social lié à la nature auto-protectrice de l'Homme face à des éléments externes (évènements naturels) mais aussi internes à la vie en Société et aux conséquences de l'activité humaine. Ces conséquences sont notamment les risques industriels tel que le risque technologique majeur (Charbonneau, 1992 ; Leibenstein, 1996), dans les exemples les plus souvent cités.

Dans le contexte organisationnel, la notion de risque est ambigüe et bien souvent, plusieurs collaborateurs d'une entreprise traitant du sujet croient parler de risque alors qu'ils abordent en fait des notions distinctes au titre desquelles on peut citer les évènements redoutés, les menaces, les vulnérabilités, les faiblesses et les pertes etc. (Méric et al., 2009 ; Pesqueux, 2011).

Les nombreuses activités de la vie courante font l'objet d'une « mise en risque » : soit des constats chiffrés sur les probabilités de survenance de pathologies liées à la consommation alimentaire, aux activités sportives, aux pratiques courantes des individus. Ils sont à rattacher à la notion de modes de vie et de perception mais aussi de discours (un sujet est-il dangereux au regard de pratiques instituées dans un cadre socio-organisationnel ?), de valeurs, de culture (d'entreprise, sociétale). Parler de risque c'est intégrer à la fois le rapport à la science (que connait-on d'un sujet en termes de risques avérés ou potentiels ?) et à l'individu (Peretti-Watel, 2000).

Parallèlement à cela, et c'est là différence entre risque et incertitude, l'essor de certaines activités humaines engendre un accroissement de l'incertitude (soit des évènements à survenance non probabilisable et aux conséquences difficilement mesurables). Ces pratiques et activités à risque se développant, on constate peu à peu un passage d'une approche

moderne fondée sur la rationalité où il est question d'un danger à éliminer par une action normative (interdire, restreindre, contraindre) ou par l'analyse scientifique (analyser et comprendre un phénomène et ses causes racines) ; à une vision post-moderne où l'individu, l'entreprise, l'organisation ont également pour rôle de gérer l'aléa consubstantiel à leur activité (Lascoumes, 1991).

Face à cette diversité d'approches, le risque peut cependant se résumer de manière assez simple comme un événement dont la survenance, aléatoire, est susceptible de causer un dommage aux personnes ou aux biens voire aux deux à la fois. Cette approche est souvent complétée par une vision duale séparant les risques avérés et probabilisables des risques potentiels (latents) et non probabilisables. Une autre manière de résumer le risque dans l'organisation consiste à l'appréhender comme la convergence d'une menace, le plus souvent externe à l'organisation, laquelle exploite une vulnérabilité interne à celle-ci, en vue de causer un dommage aux actifs ou aux personnels de ladite organisation.
La question des risques est souvent sujette à difficulté, elle suppose l'expertise en même temps que la rationalité instrumentale mais est source d'ambigüité, de controverse (Beck, Kropp, 2011). Le risque se situe clairement entre ce sentiment public qui veut que l'organisation adopte une perspective gestionnaire et ce vice privé qui implique que l'individu soit par nature averse à adhérer à une telle approche. Cette controverse rend difficile une réponse organisée face aux nombreux risques entourant une organisation au quotidien.

- **Approches normatives du risque**

La déclinaison d'une réponse au risque n'étant pas naturelle dans les organisations, il existe de nombreuses normes traitant du risque et concernant directement les entreprises (qu'il s'agisse de hard ou de soft law).
Dans le secteur financier les normes sont principalement issues de la réglementation prudentielle. On citera les accords de Bâle (I, II et III à venir) concernant les activités de banque, les directives Solvabilité I et II (à venir) en assurance, la loi de sécurité financière étant plus englobante. L'objectif de ces normes est d'inciter les établissements financiers à mettre en œuvre les diligences nécessaires pour apporter une réponse organisée face à leurs différents risques.
Dans le secteur industriel, des normes telles que Seveso ou encore la directive Reach ont encadré les conséquences liées aux activités industrielles.

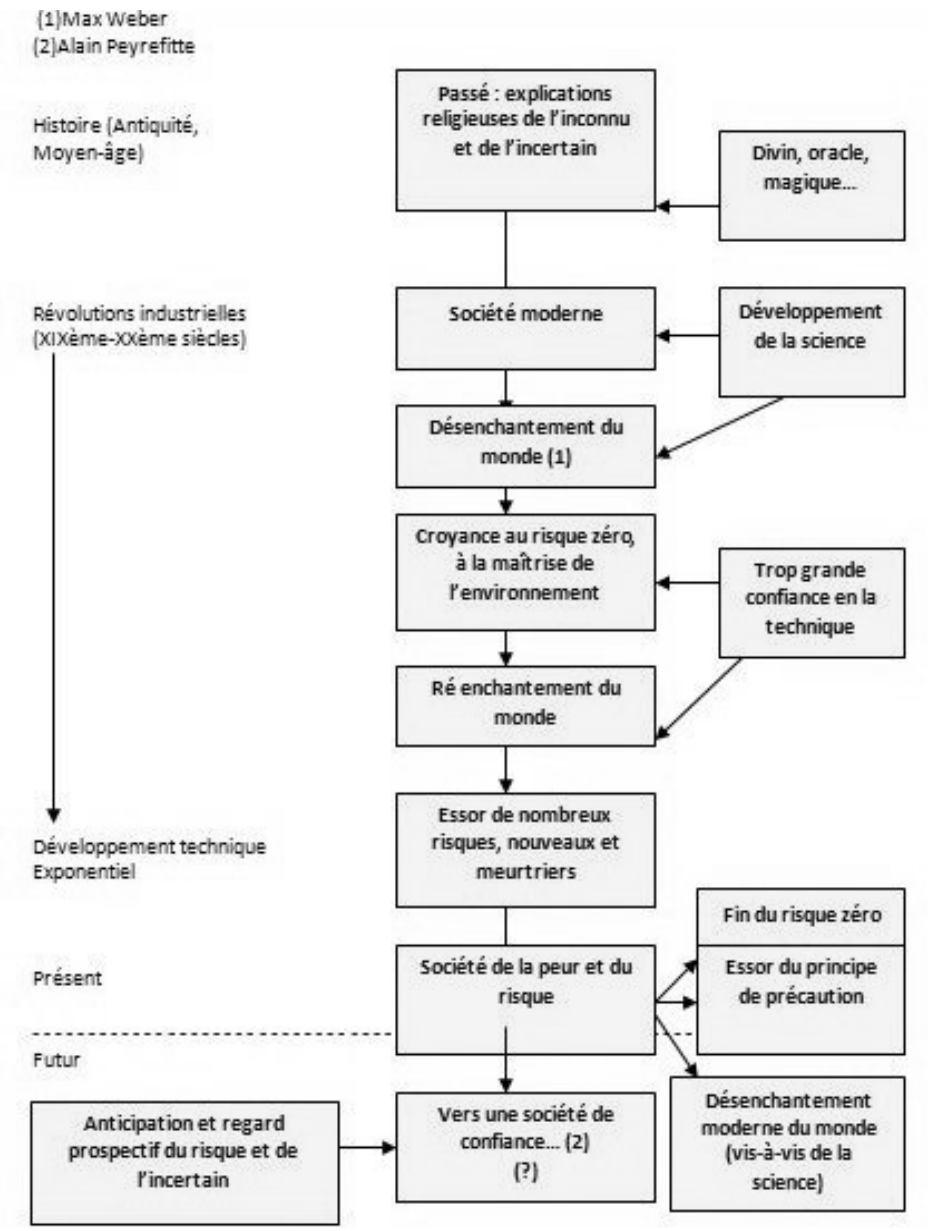
A titre d'exemple, nous revenons sur le cas d'une norme centrée sur les enjeux de risque :
La norme ISO 31000 (Management du risque, Principes et lignes directrices) fixe les principes et lignes directrices du management des risques. Elle définit le risque comme l'effet de l'incertitude sur l'atteinte des objectifs. Cette définition, bien que non exhaustive, a le mérite d'être suffisamment générale pour tenir compte de la diversité des risques que doivent traiter les entreprises. Elle est ainsi proche dans la prise en compte des conséquences des approches de risques financiers, de risques opérationnels ou encore de risques à caractère technique. Cette approche présente encore le mérite de corréler la question des risques à celle de la décision et des objectifs. Il y est clairement question de procéder à des arbitrages (coûts-bénéfices d'une décision donnée dans un contexte précis). Une telle vision située et relative du risque apparaît comme fondamentale car en pratique, pour une organisation soumise à des contraintes de temps, un risque n'est pas à rejeter en soi. Un risque est à prendre ou non si ce dernier peut être absorbé, transféré ou encore compensé par la création de valeur occasionnée dans le même temps.

- **Risque et cadre sociétal**

Pour Ulrich Beck, le risque et son corollaire le coût du risque sont à intégrer comme faisant partie des « effets induits latents » (1986, p.62) associés à toute activité économique. Ce coût du risque est à mettre en lien avec la notion de pari sur l'avenir. Le risque est à rapprocher de l'action. La prise de risque est en soi la conséquence de la prise de décision dans un but précis : *« l'évènement non encore survenu qui motive l'action »* (Beck, 1986, p.60). Ce but précis, c'est dans le contexte de l'entreprise la recherche de relais de croissance, de rentabilité supérieure, de développement de l'organisation. Elle implique de se poser la question du coût d'opportunité : le bénéfice attendu est-il supérieur au coût du risque en cas de survenance ?
Ce questionnement est pour certains auteurs aux origines de notre société où rationalité économique et éthique du profit se conjuguent (Méric et al., 2009). Le contrôle et la gestion du risque se positionnent entre ces enjeux économiques de pérennisation d'une activité et des enjeux éthiques de responsabilité de la gouvernance d'entreprise :
Pour M.Power (1999), il n'y a pas de risques fictifs ni inventés en soi : les risques de pertes financières, de pollution, de produits défectueux sont bien réels. Il y a un véritable enjeu de perception par rapport au risque qui détermine l'importance qu'on lui accorde et l'attitude alors adoptée : ne rien faire face au risque, transférer le coût du risque via des mécanismes assurantiels, développer une approche complète de gestion des risques visant à diffuser une

culture de prise en compte du risque dans une organisation (dont le but est d'anticiper le risque et ses conséquences, de transférer son coût ou de définir des moyens de protection et de prévention). Le schéma ci-après dresse un rapide historique des phases de prise en considération du risque tel que résumés par Weber, Jonas, Beck mais aussi Peyrefitte. Pour ces différents auteurs, le lien entre risque et degré de connaissance (croyance dans ce degré de connaissance et de maîtrise de notre environnement, savoir socio-technique[2]) caractérise la posture de l'individu face au risque.

Figure 1. Perception du risque et croyance dans la technè



[2] La technè au sens d'Hans Jonas (1998).

- **Coût du risque et acceptabilité sociale**

Pour Grandazzi (2007), poser la question du risque c'est envisager avant tout son acceptabilité sociale. Le développement de toute logique industrielle comportant des risques pour l'environnement ou tout simplement économique suppose d'introduire l'enjeu de coût du risque : calcul de coût / avantage, calcul de probabilité). Comme le rappelle F.Ewald (1991), si l'on donne souvent une dimension objective au risque (un calcul « froid » de probabilité), ce dernier comprend en tout état de cause une dimension subjective au-delà des vocabulaires d'expertise. Le risque en soi n'évolue pas nécessairement (sauf en cas de présence de facteurs d'aggravation) mais l'importance qui lui est accordée et sa politisation sont fonctions du nombre d'individus et d'organisations touchés, de la distance entre ces derniers et l'évènement à risque et des conséquences alors supportées (Borraz, 2008).

2.1.2. Risque et cadre entrepreneurial : la politique de risque

- **Définition et composantes des politiques de maîtrise des risques**

La notion de politique de risque est un concept largement étudié en sciences politiques et en sociologie mais elle reste récente en sciences de gestion et dans le champ de la théorie des organisations. Une politique de risque peut être définie de manière large comme la manière dont un groupe d'individu entend traiter des conséquences d'une activité ou d'un ensemble d'activités. Par des réglementations et des normes, des chartes ou encore par délégation à des individus (experts ou mandataires), la politique de risque entend préciser les risques que le corps social accepte et ceux qu'il désigne comme n'étant pas acceptables (Boraz, 2008). La politique de risque concerne donc l'acceptation des risques et la fixation des limites. Dans le champ des organisations, cette définition est généralement complétée par la désignation des acteurs en charge de coordonner et de suivre ces risques ainsi que des responsabilités associés à ces acteurs. Ce, dans une logique d'intégration de la complexité et d'une nécessité de penser le risque en termes d'allocation de ressources dédiées à sa gestion ainsi que de suivi dans le temps de la capacité d'un système et des acteurs qui le composent à anticiper ses risques ou à les réduire quand ils ne peuvent l'être totalement (Amalberti, 1996).

- **Les politiques de maîtrise des risques en entreprise : le Risk Management moderne**

Fondamentalement, les politiques de maîtrise des risques doivent être définies à l'appui d'une double exigence : l'existence d'une vision partagée du risque entre les décideurs principaux de l'entreprise d'une part, et l'impérieuse nécessité pour l'équipe dirigeante d'assurer la plus grande cohérence entre la stratégie globale de l'entreprise et la politique de risque à définir et à déployer d'autre part. De cette affirmation de vision partagée, d'appétence -ou non- aux risques et de cohérence stratégique, découlera une politique de risques adaptée au contexte spécifique de l'entreprise (Darsa, 2011).

La définition de la politique de risque doit s'inscrire comme l'une des composantes à part entière de la vision de l'entreprise. Elle se situe entre stratégie, architecture organisationnelle et définition des procédures de fonctionnement mais aussi recherche de performance globale (Jemison, 1987). Son existence formalisée constitue un acte fondateur essentiel à la mise en œuvre d'une véritable culture du risque cohérente dans l'organisation. Mais cette culture n'existera qu'en présence d'une véritable volonté de mise en œuvre de la part de l'encadrement. Il est clairement question en matière de politique de risque de mettre en place un management, au sens de gestion coordonnée par laquelle certains acteurs définissent les actes d'autres, orientée autour de l'enjeu dédié « risque ». Définir la politique de risque ne suffit pas, trop d'entreprise se limitant à une culture du diagnostic et un « désir » de politique risque. Dans de telles occurrences, il n'est pas question que d'une politique de transfert de risque ou de décision des investissements à réaliser sous contrainte d'indicateurs quantitatifs de risque (quels contrats d'assurance ou mécanismes financiers mettre en place pour couvrir les risques, pour les transférer à des sociétés d'assurance par exemple). Le déploiement effectif de la politique de risque ne se décrète pas, même si la politique de risque existe. Elle doit être animée par des acteurs dédiés, affirmée par des actes récurrents et à la fois symboliques et pratiques et affinée constamment au regard des échanges qu'elle suppose de mettre en place (Braithwaite, 1989 ; Li, Wu, 2009). Définir une politique de risque doit donc s'avérer être un subtil mélange entre constance des actions mises en place et adaptabilité permanente des acteurs aux situations, mais aussi par des actes de sensibilisation, de formation ou encore des actions préventives et curatives concernant les différents risques de l'entreprise. La politique de risque consiste encore à établir une cartographie statique mais aussi un déploiement dynamique d'outils de gestion du risque en couvrant un domaine des

possibles presque infini avec des ressources cependant limitées (Richardson, 2010). Définir une politique de risque n'est pas une fin en soi, mais plutôt le début d'une prise de conscience dans une organisation, au-delà d'une réponse à une norme donnée. Il s'agit de l'affirmation d'une volonté stratégique de la direction de l'entreprise de réduction du coût du risque, mais également et surtout de sauvegarde de la valeur de cette dernière, de fédération des équipes et de différenciation pour l'organisation (Simister 2000 ; Galloway, Funston, 2000 ; Burnaby, Hass, 2009).

- **L'ERM : conduire la politique de risque en lien avec la stratégie d'entreprise**

La Federation of European Risk Management Associations (FERMA)[3] identifie la gestion des risques comme *« un processus continu d'amélioration qui commence avec la définition de la stratégie et se poursuit avec l'exécution de celle-ci. Elle devrait traiter systématiquement de tous les risques qui entourent les activités de l'organisation, que celles-ci soient passées, présentes et surtout futures. »*

La gestion des risques, ou Enterprise Risk Management, peut encore être définie comme *« l'ensemble des politiques, des stratégies, des dispositifs de maîtrise, de contrôle et de suivi ainsi que des moyens humains, financiers et matériels mis en œuvre par une organisation afin d'identifier, de détecter, limiter et maîtriser les risques liés directement ou indirectement à ses activités* » (Darsa, 2010, p.15 et s.)[4].

L'Institut Français de l'Audit et du Contrôle Interne (IFACI) et PriceWaterhouseCoopers (PWC), reprenant le référentiel COSO II, définissent le management des risques comme un processus mis en œuvre par le Conseil d'Administration, la Direction Générale, le management et les opérationnels. Ce processus est pris en compte dans l'élaboration de la stratégie et dans toute l'organisation et vise à éviter les évènements potentiels dommageables à l'organisation et à fournir une assurance raisonnable quant à l'atteinte des objectifs. Dans un contexte de flou des frontières de l'entreprise et de ses sous-traitants, notre période fait évoluer l'entreprise dans un monde de plus en plus incertain, un environnement de plus en plus agressif, de moins en moins prévisible. Face à cela, la gestion des risques vise l'atteinte des objectifs en répondant aux risques organisationnels et non seulement au risque pris de manière isolée.

[3] FERMA. Fédération regroupant les associations traitant des problématiques de gestion des risques, à l'instar de l'AMRAE, de l'Institute of Risk Management. Elle identifie les différentes pratiques en termes de risk management et organise des séminaires et conférences sur les actualités de ce domaine. Site officiel.
[4] Darsa, J-D. (2010). *La gestion de crise en entreprise*. Gereso, Le Mans.

La gestion des risques suppose une compréhension globale des risques de l'entreprise (Guillon, 2009). Laquelle se veut d'appréhender une pluralité de risques faisant interagir des domaines divers (droit, économie, gestion, ingénierie…) et mobilisant une multitude de compétences dans le cadre de ce qui peut être appelé le *« total Risk Management ».* En matière de risque, l'interdisciplinarité est nécessaire. Le Risk Management suppose l'intervention dans des domaines stratégiques, organisationnels et techniques, par le Risk Manager, homme de terrain, *« touche-à-tout »* (Véret, Mékouar, 2005, p.52) participant à la transformation de son entreprise (sécurité des personnes et des installations, problèmes environnementaux, contrats avec les sous-traitants, dimension informatique, gestion de crise…).

Le Risk Management peut être défini comme un processus transversal de création de valeur (Morlaye, 2006, p.60) au centre du processus organisationnel et impliquant toutes les fonctions de la chaine de valeur au sens de Michael Porter (1986). Cette approche globale aussi qualifiée d'ERM (Enterprise wide Risk Management) suppose de déterminer en accord avec l'objet social de l'entreprise, ses valeurs et sa stratégie, le profil de risque que cette dernière souhaite adopter et mettre en œuvre dans la conduite de son activité courante (voir schéma ci-après). Cette approche suppose dans un second temps le transfert ou la prévention et la protection contre les risques se situant hors de ce cadre et que l'entreprise n'entend pas assumer en tant que tels. Cette notion d'acceptation du risque apparaît comme fondamentale. Elle découle de l'appétit au risque des décideurs d'une organisation (ou a contrario de leur aversion). Sitkin et Weingart (1995) analysaient les comportements de prise de décision en univers risqué pour démontrer que la variable risque devient un paramètre dont la prise en compte va nécessairement croissante à notre époque, ce pour des raisons liées au poids d'autres parties prenantes que le seul *« Top Management »* ne peut gérer uniquement (poids des actionnaires, dimension responsabilité environnementale, opinion publique, rôle des médias, etc.).

- **Les limites contemporaines de la gestion des risques**

De nombreuses recherches mettent en avant à la fois l'intérêt d'un cadre formalisé en matière de risque en entreprise mais aussi les limites empiriques, méthodologiques et conceptuelles des politiques de gestion des risques. Hammond dès 2002 mettait en avant le fait que trop souvent les dispositifs de maîtrise des risque sont axés sur les processus et l'organisation de l'entreprise avant même d'être des logiques de raisonnement favorisant l'action des individus

en vue de réduire les risques dans leurs pratiques courantes (la meilleure manière de gérer le risque serait donc de modifier les attitudes et comportements selon l'auteur). A cette vision issue de la psychologie du risque, il faut également ajouter celle de Pelzer (2009) pour qui les défaillances fréquentes des systèmes de gestion des risques (notamment dans le secteur financier) sont dues à l'absence de sanction et de système contraignant. Ces politiques sont trop largement incitatives et sont sujettes à l'influence des acteurs les mettant en place ou de leur dirigeant, ce qui les rend peu comparable d'une organisation à une autre mais rend difficile la formalisation de bonnes pratiques en la matière, tant les facteurs de contingences sont importants sur cette thématique. Définir une politique de maîtrise des risques efficace serait donc une gageure sauf à y intégrer un système de sanction. Pour d'autres auteurs, la limite de la gestion des risques réside notamment dans le mauvais positionnement des acteurs en charge de ces politiques (les fonctions « risque ») souvent trop éloigné des lignes hiérarchiques des dirigeants (Chong, 2004). Le positionnement de la fonction est un facteur de crédibilité mais aussi de légitimité sans lequel la gestion des risques n'est que théorique. La bonne gouvernance de la fonction risque est un des facteurs déterminant de réussite de la mise en œuvre des politiques de risque (Demidenko, McNutt, 2010).

Il existe un ensemble d'erreurs en gestion des risques formalisé notamment par en Stulz, 2009:

- La première consiste à penser que l'on peut gérer les risques en prévoyant les évènements extrêmes. Il n'y a pas d'emprise sur la survenance de ces évènements, raison pour laquelle se concentrer sur les conséquences potentielles est important.

- Nous sommes souvent convaincus qu'étudier les évènements passés nous permettra de mieux gérer les risques futurs. Les aléas socio-économiques rendent peu pertinente cette approche, pour ce qui est des évolutions non typiques. Se baser sur des historiques de données apparaît comme limité. L'extrapolation du passé ne permet pas de prendre véritablement en compte les évènements futurs peu vraisemblables. Ce type de vision centrée sur les évènements passées est tel qu'un Risk Manager en 2006 aurait manqué de crédibilité s'il avait mis en avant le plongeon du marché immobilier en 2007. Le *« Top Management »* lui aurait demandé des éléments sur la période de survenance et le montant des pertes potentielles, impossible à prévoir en se basant sur des données passées.

- Ne pas se baser sur des mesures restrictives du risque. Une part essentielle d'un risque ne peut pas être mesurée.

- Se concentrer de manière excessive sur les risques connus et identifiés est aussi un écueil à éviter car il survient toujours des risques non prévus et non recensés dans les bases de données de perte et les cartographies faisant l'état des lieux des risques d'une entreprise.

- Ce qui est mathématiquement équivalent ne l'est pas en terme psychologique. Cette loi psychologique est essentielle en gestion des risques. La manière dont le risque est perçu influence la compréhension des individus.

- Ne pas rechercher les risques dissimulés : dans de nombreux cas, les risques posant réellement problème dans une organisation ne sont pas remontés alors qu'identifiés. Cela vaut en interne, de nombreux dirigeants ayant découverts la situation de leur établissement en période de crise financière ; mais aussi dans les relations avec les autorités de contrôle, la crise de 2007-2008 révélant un défaut de ces dernières. La Security and Exchange Commission révéla avoir sous-estimé l'exposition au risque de nombreuses banques. Tout comme les coûts cachés, il existe bien souvent des risques cachés pour les entreprises.

- Un défaut de communication sur les risques caractérise le plus souvent les dispositifs de gestion manquants d'effectivité. Trop rarement, les managers écoutent les recommandations empreintes de précaution. Il n'est pas satisfaisant pour un Risk Manager de proposer que l'entreprise se désengagent d'un domaine d'activité, raison pour laquelle des investissements parfois hasardeux sont réalisés.

-Ne pas considérer que l'efficience et l'optimisation soient toujours possibles. L'optimisation rend parfois l'entreprise vulnérable aux changements de l'environnement économique et financier. Elle suppose une configuration donnée et la maximisation de la valeur ne correspond pas toujours à la maximisation de la valeur d'option (soit les possibilités de revenir en arrière sur des choix stratégiques et d'investissement donnés).

- Ne pas gérer les risques suffisamment à temps constitue l'une des erreurs. Parfois, les expositions aux risques vont au-delà des limites fixées par le management et l'on s'en aperçoit trop tard, cela pose la question de la pertinence et l'adaptation des dispositifs d'alerte.

2.1.3. Le risque opérationnel, une notion frontière, un enjeu organisationnel

La notion de risque est extrêmement large, elle doit cependant être resituée dans son cadre entrepreneurial (Méric et al., 2009). A cet effet, notre étude se concentre sur une des catégories de risque, en soi extensive et survenant par nature dans l'entreprise ou en lien avec celle-ci. On trouve en effet différentes catégories de risque formalisées à la fois par la littérature académique mais aussi par les études sectorielles et professionnelles dans le

domaine de la gestion des risques. On peut ainsi citer les risques industriels, les risques informatiques et les cyber-risques, les risques politiques, les risques naturels, les risques financiers, les risques opérationnels etc,. Notre recherche concerne plus spécifiquement le risque opérationnel. Cette catégorie concerne tous les risques pouvant engendrer un dommage, une perte, un coût, créés ou subis lors de la réalisation de l'activité courante de l'entreprise, c'est-à-dire dans ses cycles d'exploitation quotidiens : infrastructures, énergies, télécommunications, cycles de production, de distribution, d'approvisionnement, processus logistique, gestion documentaire, activités quotidiennes d'exploitation et de réalisation de l'objet social, directement ou indirectement etc. En résumé, les risques opérationnels matérialiseront tous les impacts directs ou indirects engendrés par l'entreprise dans son activité quotidienne, dans son cycle d'exploitation.

Au sein de la pyramide des risques, ils figurent immédiatement après les risques financiers, résultant du « cœur opérationnel » de l'entreprise. Leur analyse sera réalisée par grandes familles de processus.
Trois types de risques opérationnels spécifiques, particulièrement importants, seront considérés de manière dédiée et à traiter de façon particulière : les risques juridiques, les risques informatiques, et les risques sociaux et psychosociaux (plus simplement dénommés les risques « ressources humaines »).

Le risque opérationnel, cas du secteur financier : Notre recherche traite plus spécifiquement du risque opérationnel dans le secteur financier (secteurs banque et assurance).
Les secteurs de la banque et de l'assurance, dans leurs dispositifs de gestion des risques issus de la réglementation prudentielle Bâle II (arrêté du 20 février 2007) et de la réglementation à venir Solvabilité II, les définissent comme *« les risques de pertes résultant d'une inadaptation ou d'une défaillance imputable à des procédures, personnels et systèmes internes, ou à des événements extérieurs, y compris les événements de faible probabilité d'occurrence, mais à risque de pertes élevées ».*
Une telle définition, bien qu'exhaustive et présentant l'étendue des impacts liés aux risques opérationnels est difficile à appréhender pour des entreprises souhaitant y apporter une réponse efficace. Cette définition suppose encore une certaine culture du risque et une expertise car il est aisé de confondre la notion de risque avec d'autres notions proches telles que les menaces, les incidents ou encore les évènements redoutés. De telles approches rendent

difficiles la collecte des pertes et le renseignement d'une cartographie des risques (Bon-Michel, Dufour, 2013).

De manière plus intelligible, les risques opérationnels incluent l'ensemble des risques pouvant affecter l'organisation de par leur potentiel de désorganisation. Ces risques peuvent ainsi inclure les risques juridiques (procès suite au non-respect de certaines obligations), les risques sociaux (grève, émeute) et psychosociaux (suicide d'un collaborateur) ou encore les risques informatiques (panne d'un serveur ou de l'installation informatique paralysant l'activité). A titre d'exemple, pour M.Ferrary, *« le risque humain est une des composantes du risque opérationnel qu'il convient d'identifier et de gérer. Les outils et les pratiques de GRH constituent des moyens d'analyse et des modalités de couverture de ce risque »* (2009, p.101[5]).

Dans les faits, si de nombreux évènements dommageables ont comme cause première un risque opérationnel, ces derniers sont bien souvent en pratique sous-estimés y compris dans les secteurs banque et assurance où ils font l'objet d'une obligation réglementaire de provisionnement. A titre d'exemple, la survenance d'un risque de marché après le dépassement de certains engagements alors que des procédures spécifiaient l'interdiction de ces dépassements constitue une source première de risque opérationnel. Dans les faits, l'attention est bien souvent davantage portée sur d'autres risques tels que les risques de crédit, de taux d'intérêt, de contrepartie, de marché etc,. On qualifie alors ces risques de *« risques frontières »* (Chelly, 2012, p.22)[6] car ces risques opérationnels sont parfois associés à d'autres risques : le risque de marché, le risque de contrepartie (ou de crédit), le risque de souscription et le risque stratégique notamment.

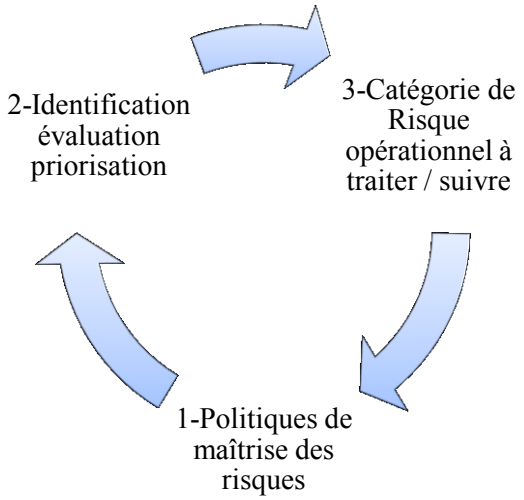
Suite à la médiatisation de certaines affaires (scandales Société Générale, AIG, UBS, JP Morgan Chase…), la prise en compte du risque opérationnel y compris en salle de marché devient un élément essentiel pour préserver l'image des banques et des compagnies d'assurance notamment. Comme l'évoque Eric Lamarque (2009, p.198) : « *Si les autorités de régulation internationale se sont saisies du problème, c'est que leur coût financier est apparu de plus en plus important et de nature à affecter significativement la rentabilité et les fonds propres des établissements* ». Au regard des sommes engagées et des risques que peuvent subir les établissements financiers, ces derniers par leur complexité et la nature de leur activité sont des systèmes à risque au sens d'Amalberti (1996).

[5] Ferrary, M. (2009). Les ressources humaines à risque dans le secteur bancaire. Une application de la gestion des risques opérationnels. *Gestion 2000*, p. 85-102.

[6] Chelly, D. (2012). Risques frontières : une bonne raison de ne pas sous-estimer les risques opérationnels. *Revue Risques,* 89, p. 19-28.

Comme l'expose simplement le schéma ci-après, la recherche d'une « mise en gestion » du risque opérationnel par le biais de politiques de maîtrises des risques induit la découverte d'autres risques nécessairement corrélés à ces premiers (causes ou conséquences d'un risque opérationnel) ; ce en un processus d'apprentissage interne dans l'organisation. Ce processus vise à mettre en place des politiques de maîtrise des risques centrée sur l'identification, l'évaluation et la priorisation du risque opérationnel en vue de définir les moyens de traitement et de suivi les plus adaptés.

Figure 2. Processus clés de l'objet de recherche « risque opérationnel »



Ces différents éléments relatifs aux notions clés de notre recherche nous amènent à la problématique de recherche que nous envisageons de traiter.

3. Problématique et questions de recherche

Notre recherche s'inscrit donc dans ce contexte d'objectivation accrue du risque opérationnel dans le but d'interroger les systèmes de contrôle et de gestion des risques développés ces dernières années dans le secteur financier. Notre étude vise à réintégrer le Risk Management dans sa perspective organisationnelle (Arena et al., 2010), ce qui semble essentiel et d'actualité en ce qui concerne le risque opérationnel comme le démontre A .Mikes (2007) ou encore M.Power (2005 ; 2007) dans des études dédiées à cette thématique.

L'objet de la thèse est d'envisager de manière détaillée les facteurs déterminants des politiques de maîtrise des risques opérationnels dans les organisations.

Nous souhaitons spécifiquement étudier la manière dont les risques opérationnels sont gérés et contrôlés dans le secteur financier, en nous centrant sur les risques opérationnels « courants » dans le cadre d'une activité de banque ou d'assurance (les risques à forte probabilité, ou de fréquence, plus spécifiquement par opposition aux risques opérationnels extrêmes et peu probables).

Notre recherche s'inscrit dans le prolongement de certaines recherches doctorales traitant de thématiques proches dans le secteur financier, notamment :
-la thèse de Béatrice Bon-Michel (2010) traitant de l'identification du risque opérationnel et des moyens de faire de ce sujet un enjeu d'apprentissage en structurant l'information sur le risque et en lui donnant du sens,
-la thèse d'Olivier de Lagarde (2010) traitant de l'invention du contrôle des risques dans les organismes d'assurance,
-la thèse d'Emmanuel Laffort (2013) traitant des problématiques d'appropriation croisée relativement à une catégorie spécifique de risque opérationnel, le risque de fraude, envisagée dans le contexte des salles de marché.

Ces deux recherches doctorales montrent le caractère exploratoire de la thématique du contrôle des risques opérationnels. Elle l'est dans le secteur bancaire où la réglementation est prudentielle fait état depuis de nombreuses années de cette nécessité et a fortiori en assurance où les dispositifs sont encore naissants.

Nous nous concentrons cependant sur un axe proche mais néanmoins complémentaire dans cette logique d'étude exploratoire : la nécessité de structurer les dispositifs de contrôle dans le cadre de politiques de maîtrise du risque se développant. Un tel sujet est une préoccupation croissante dans un environnement post-crise comme le démontrent les recherches récentes attestant de la nécessité de mettre en place des dispositifs effectifs et efficaces de Risk Management (Mikes, 2008a ; Kaplan, Mikes, 2012 ; Huber, Scheytt, 2013). Notre thématique de recherche sur le contrôle des risques soulève des problématiques plus larges à la fois techniques, humaines et comportementales à l'instar des autres champs du contrôle tel que le contrôle de gestion (Simons, 1995, 2000 ; Cappelletti, 2010).

Face à ce contexte de recherche, notre question de recherche centrale est alors la suivante :

Question centrale : Notre question de recherche consiste à déterminer comment convertir les normes de contrôle du risque opérationnel en un dispositif effectif de contrôle orientée vers la maîtrise pérenne et durable de l'activité.

Comment la structuration du contrôle permet-elle de passer d'une simple recherche de conformité aux normes à une gestion effective du risque opérationnel ?

C'est-à-dire à une gestion réelle dans laquelle le facteur risque constitue une préoccupation des acteurs en charge du contrôle mais aussi des collaborateurs contrôlés dans la recherche d'amélioration de la gestion du risque opérationnel.
Nous parlons alors de la normativité comme le fait de répondre aux normes de manière conformiste et d'effectivité au sens de contrôles permettant d'éclairer la prise de décision dans l'organisation sans prétendre être infaillibles en soi (Power, 2005, 2007 ; Mikes, 2012).

Sous-questionnements : Les questions sous-jacentes à cette recherche sont alors les suivantes :

-Le contrôle des risques opérationnels est aujourd'hui le fait d'une fonction dédiée, la direction des risques opérationnels. Toutefois d'autres acteurs traitent du contrôle de ces risques. Nous cherchons donc à répondre à la question suivante. Existe-t-il une unicité ou une pluralité de contrôle des risques opérationnels :
Peut-on parler du contrôle des risques opérationnels ou des contrôles du risque opérationnel ?
(Risk Management, contrôle interne, audit interne, contrôle qualité, contrôle de conformité, contrôle de gestion etc.)

- Quelle structuration du contrôle des risques opérationnels faut-il concevoir pour tendre à l'effectivité de la politique de risque opérationnel, ce qui induit la question suivante : Dans quelle mesure la structuration de la confiance dans l'organisation améliore-t-elle la gestion du risque opérationnel ?

- Le Risk Management opérationnel vise la contribution à l'atteinte des objectifs et la pérennisation de l'activité : peut-on orienter le contrôle et la gestion du risque opérationnel vers un modèle organisationnel de recherche d'effectivité orientée performance durable?

- Le contrôle et la gestion des risques opérationnels peuvent-ils s'envisager selon un modèle de contrôle de gestion de l'immatériel (Cappelletti, 2012), par l'étude des dysfonctionnements organisationnels qu'il suppose ?

-Les risques opérationnels étant des risques liés à l'organisation et aux comportements des acteurs au sein de celle-ci : Peut-on envisager les risques opérationnels en tant que coûts et performances cachés dans l'organisation ?

4. Corps d'hypothèses

Face à cette question centrale et aux questions sous-jacentes qu'elle implique, nos hypothèses de recherches sont les suivantes :

Le sujet de thèse est basé sur l'hypothèse centrale suivante que les organisations développant des politiques de maîtrise des risques opérationnels doivent dépasser la simple recherche de conformité aux normes si elles veulent avoir une gestion efficace de leurs risques opérationnels. Cette recherche de conformité n'étant à elle seule pas suffisante pour garantir une vraie réduction du risque, s'agissant d'une approche a minima.

La thèse se base alors sur les sous-hypothèses suivantes (voir le tableau ci-après).
Ces hypothèses sont à la fois descriptives, explicatives et prescriptives. Comme l'évoquent certains auteurs, les connaissances produites en sciences de gestion se structurent nécessairement autour de plusieurs séries d'apports, lesquels sont des descriptions (de pratiques et de techniques mobilisés par les acteurs des organisations), des explications (de la diversité des modèles mobilisés par ces derniers ainsi que des cadres de référence théoriques auxquels se réfèrent ou s'inspirent les individus dans leur pratique) et des prescriptions (les sciences de gestion étant des sciences de l'action) en vue d'améliorer ou de repenser les pratiques émergentes ou situés desdits acteurs (Martinet, Pesqueux, 2013)

Tableau 1. Corps d'hypothèses

Code hypothèse	Hypothèses descriptives	Hypothèses explicatives	Hypothèses prescriptives
H1	Les processus d'institutionnalisation et de normalisation permettent une marge de manœuvre réglementaire	Même dans les secteurs réglementés tels que les secteurs bancaire ou assurantiel, l'inflation normative contribue à créer des confusions voire des conflits de normes de telle sorte qu'il existe une marge non négligeable d'interprétation de la réglementation prudentielle.	Il existe certains acteurs clés (Risk Manager notamment) dans l'organisation dont le rôle est de permettre une lecture et une traduction commune de la réglementation prudentielle 'risque opérationnel'. Ce rôle doit être un rôle d'influence et non de coercition.
H2	Les risques opérationnels sont des risques subis, diffus et mal compris. Ils sont sources de défiance dans l'organisation.	Leurs normes de contrôle et de gestion sont sources de confusions, ils se gèrent par la négative, par la recherche des dysfonctionnements et des sources de défiance.	Le passage du négatif au positif dans la gestion des risques opérationnel suppose un management actif par des acteurs clés dédiés. Ces derniers permettent de renforcer la confiance dans l'organisation.
H3	La création de valeur associée à la gestion du risque opérationnel se situe dans la réponse à ces dysfonctionnements.	La création de valeur dans le cas du risque opérationnel est davantage une « sauvegarde de la valeur » qu'une création nette de valeur.	L'analyse de la valeur concernant les démarches de gestion du risque opérationnel doit à la fois reposer sur des approches qualitatives (valeur organisationnelle) et quantitatives (économie de fonds propres et maîtrise des coûts)
H4	Les risques opérationnels sont principalement des coûts et performances cachés pour les institutions financières	Les coûts-performances cachés 'risques opérationnels' sont une catégorie issues de difficultés de dénombrement (quantitatif) mais aussi de discernement dans l'organisation (qualitatif).	La gestion du risque opérationnel doit s'inscrire dans le passage d'une démarche conformiste à une logique d'intelligence du risque (démarche cohérente et apprenante).
H5	Les politiques de maîtrise des risques opérationnels se structurent autour de plusieurs fonctions et dispositifs dédiés en totalité ou partiellement	L'effectivité d'une politique de maîtrise des risques opérationnels est liée à la capacité des acteurs à comprendre et à se mobiliser	Les politiques de maîtrise des risques opérationnels nécessitent une approche intégrée et un

	dont les attributions divergent mais pour lesquels il existe un objectif commun 'risque opérationnel'.	autour de l'enjeu 'risque opérationnel' tout en tenant compte de leur lecture spécifique de cet enjeu.	management actif des différentes fonctions de contrôle (Audit, Contrôle Interne, Conformité, Risk Management…) pour être effectives.

Justification des hypothèses :

Nos hypothèses émanent de notre pratique lors des missions réalisées en entreprise en tant que contrôleur interne et Risk Manager (en charge des risques opérationnels). Elles ont pu être formalisées et modifiées pour certaines à plusieurs reprises au cours de cette recherche, ce en lien avec la littérature académique qui nous a permis de conforter notre démarche dans l'idée que les hypothèses décrites représentent de réelles questions de recherche intéressant la communauté scientifique car elles sont porteuses de questionnements plus larges que l'objet auquel elles s'appliquent (Thiétart, 2003). L'émergence de notre corps d'hypothèse en lien étroit avec la pratique professionnelle atteste de la démarche inductive-exploratoire qui caractérise notre recherche.

Cette confrontation de nos hypothèses, issue de la pratique professionnelle, à la littérature académique sur le Risk Management, s'inscrit dans l'approche défendue par Van de Ven et Johnson (2006) en ce qui concerne le concept d'*engaged scholarship* : analyser l'écart entre théorie et pratique en posant des problématiques de recherche enracinées dans la réalité, concevoir un projet de recherche par l'approche collaborative de longue durée et avec des méthodes variées (dans notre recherche le recours à la triangulation méthodologique) tout en révisant régulièrement les hypothèses de recherche.

Nous avons cherché à valider nos hypothèses au regard des trois processus de rigueur scientifique que sont les processus interne (processus de recherche adapté pour tester les hypothèses), externe (des résultats généralisables) et écologique (intégration et description du milieu étudié). Il s'agit de conditions de rigueur au même titre que la définition de la problématique de recherche (Lee, 1999 ; Cappelletti, 2010). Nous renvoyons à l'annexe 1 concernant la validation des hypothèses (Annexe 1-Validation des hypothèses au travers des résultats de recherche).

Partie I- Contexte professionnel des politiques de maîtrise des risques opérationnels : vers une institutionnalisation du contrôle des risques

Introduction de la première partie - Le secteur financier, un monde de risques

L'objet de cette première partie est d'appréhender l'enjeu spécifique que constitue le risque opérationnel pour les établissements financiers (banques et assurance), ce au travers de la littérature professionnelle.

Nous abordons successivement dans les deux chapitres qui constituent cette première partie les périmètres d'activité et de risques couverts par les établissements bancaires et les sociétés d'assurance puis les enjeux normatifs associés à la prise en compte des risques sur ces différentes activités.

Il ressort du premier chapitre que la diversification de l'activité réalisée, tant par les banquiers que les assureurs, implique de mieux prendre en compte les périmètres élargis de ces entités et l'apparition de nouveaux risques pour ces dernières. Cumulativement, le périmètre des risques opérationnels s'en trouve élargi et cela impose une adaptation des contrôles portant sur ces activités. Nous abordons en conséquence la nécessité pour les établissements financiers de se doter de politiques dédiées à la problématique du risque opérationnel.

Ces politiques, et c'est l'objet de notre second chapitre, s'inscrivent dans un cadre normatif et réglementaire (Bâle II, Solvabilité II) souvent présenté comme contraignant. Nous abordons, dans une logique critique, le rôle de ces normes, leur manière d'inciter les établissements financiers à gérer les risques opérationnels. Ce chapitre aborde également les limites des dispositifs normatifs (s'inscrivant davantage dans une perspective d'auto-contrôle) face aux différents cas médiatiques de survenance de risque opérationnel. Cette présentation critique des normes face à la persistance des risques opérationnels en banque et assurance constitue le socle de base de notre réflexion théorique et empirique développée dans les deux parties suivantes.

Chapitre 1 - Les établissements bancaires et les sociétés d'assurance: une diversité d'activités et de risques

« Toute société qui ne reconnaitrait pas la légitimité de la prise de risque et ne la favoriserait pas jusqu'à un certain point serait vouée au déclin »
Claude Henry

Introduction : la finance moderne, une évolution sans précédent affectant banques et compagnies d'assurance

Il convient de mettre en avant ces dernières années les évolutions majeures de la finance ayant affectées les banques et les compagnies d'assurance, sujets de notre étude. Ces évolutions sont notamment l'essor des innovations financières, la dérèglementation de la finance, la dématérialisation et l'internationalisation des flux financiers. Ces acteurs de l'économie sont présentés comme centraux dans le processus de globalisation financière (Plihon et al., 2006). A cela s'ajoutent d'autres évolutions spécifiques concernant les banques, plus particulièrement : la mobiliérisation de l'actif bancaire (soit l'accroissement de la part des titres), le déclin de l'intermédiation bancaire traditionnelle et l'essor du rôle des marchés financiers comme vecteur de croissance pour les établissements bancaires. Face au déclin de l'intermédiation traditionnelle, les banques se sont orientées peu à peu vers des prêts plus risqués ainsi que vers la détention de titres. Cette restructuration sur une vingtaine d'années des bilans bancaires s'est amorcée en premier aux Etats-Unis et a suivi, notamment en France.

Cette tendance se poursuit dans la période récente et la banque évolue vers de nouvelles stratégies et de nouveaux métiers, le plus souvent mondialisés (Plihon et al., 2006). Ainsi, la banque est aujourd'hui sur une distribution « multicanale », elle accorde au marketing stratégique une place prépondérante et son activité est diversifiée et plus sophistiquée que par le passé (entre banque en ligne, centres de services et plateformes multimédias, gestion d'actifs etc.).
La mutation financière a ainsi renforcé le lien entre banques et marchés tout en allant dans le sens d'un développement parallèle et complémentaire de l'intermédiation financière. Les banques ont en effet tiré parti de la mutation financière et ne l'ont pas subi passivement. Il en va de même pour la plupart des assureurs. L'activité traditionnelle de banques de détail

demeure une base fondamentale sur laquelle s'adossent les activités plus récentes de gestion d'actifs et de titres (Plihon et al., 2006).

La finance moderne et la financiarisation de l'économie, une ère de risques :

Face au pouvoir croissant de la finance moderne, de nombreux facteurs d'instabilité sont mis en avant (spéculations boursières, OPA bancaires, inflation des actifs, globalisation des marchés etc.). Les nombreuses crises que traverse la finance tendent à mettre en avant cette ère du risque transposée au système financier (Orléan, 1999).

-L'importance de la confiance dans le secteur financier: Pour Hubert Bonin le nom et le renom des banques constituent un enjeu fondamental car « l'enseigne joue beaucoup dans la mise en confiance du client » (1992, p.195).
C'est cette vision qui explique que pendant longtemps, les établissements bancaires furent appelés par le qualificatif d'établissement de crédit (Crédit lyonnais, Crédit du Nord, Crédit Agricole, Crédit Foncier, Crédit Industriel et Commercial etc.) en vue de ne pas être confondu avec les activités spéculatives (Bonin, 1992). L'image de marque des banques, bien que constituant un sujet d'actualité face aux nombreuses fraudes récentes (Société Générale, caisse d'Epargne, UBS, plus récemment JP Morgan etc.) n'est pas une préoccupation nouvelle. Comme le remarque Hubert Bonin (1992, p.269), les banques sont soumises en permanence à de vives critiques et à une *« image de marque incertaine »* car l'opinion publique doute fréquemment face à des structures empreintes d'opacité (notamment quant à la fixation des prix de leurs prestations, à l'insuffisance du sens relationnel des banques, aux pratiques d'investissement et aux décisions prises etc.).

Tableau 2. Risque et secteurs banque et assurance

Banquiers	Assureurs
Activité de preneur de risque	Activité de couverture de risque
Le risque est la contrepartie de l'activité financière	Le risque est une « matière première », la source de création de valeur
Une activité procyclique d'accompagnement des activités économiques	Un système contra-cyclique de couverture des risques, reposant sur l'inversion du cycle de production

La banque est par nature un métier de gestion des risques. Tout comme l'assurance, cette variable constitue l'une des matières premières des multiples activités financières que

regroupent banques et assurance (Hakenes, 2004). L'objet de ce chapitre est d'expliciter le rôle de l'activité bancaire et de l'activité d'une société d'assurance dans une perspective gestionnaire (au sens de davantage située dans une logique managériale que technique pour les acteurs de l'organisation). Après avoir décrit le cadre global de ces deux types d'activités, nous aborderons la dimension risque et la manière dont se caractérise le risque opérationnel au sein de ces entités.

Le secteur bancaire, de par ses spécificités, fait interagir de nombreuses activités se traduisant par des risques variés, en lien avec la question de la conformité. Le métier de banquier est fondamentalement un métier de preneur de risque. Il s'agit notamment de prendre en compte le risque de marché, le risque de crédit, le risque de taux d'intérêt, le risque de liquidité, le risque d'atteinte à l'image, le risque systémique (instabilité générale concernant l'ensemble du système financier), le risque de défaut de conseil, le risque de fraude…

Le secteur de l'assurance, quant à lui se caractérise par un certain nombre de risques spécifiques impliquant que le rôle du régulateur et le poids de la réglementation se soient peu à peu renforcés. Outre son business model particulier, reposant sur un cycle de production inversé qui s'exprime par la prise en compte comptable des primes d'assurance comme des dettes à l'égard des assurés, il importe de ne pas négliger le poids des risques tels que le manquement au devoir d'information et de conseil, les risques liées aux activités de souscriptions de contrats d'assurance (en assurance vie comme en assurance non-vie), les risques spécifiques à la structure des actifs des entreprises d'assurance (majoritairement des obligations) ou encore le caractère particulier des fraudes à l'assurance.

1. L'activité de banque

Pour Bonin (1992), l'évolution du secteur bancaire s'est tendanciellement faite vers une spécialisation et une diversification accrue des activités en France et à l'international. A l'activité historique de collecte des dépôts et d'octroi de crédits s'est peu à peu ajouté une palette diversifiée d'activités. Cette tendance lourde explique la multiplicité des activités que recouvrent un établissement bancaire (banque de détail, banque de financement et d'investissement, activité de marché, de crédit, vente d'assurance etc.).

1.1. Les activités des établissements bancaires aujourd'hui

Qu'est ce que la banque ?

La banque se définit comme un intermédiaire financier venant compenser les différences entre recettes et dépenses dans les comptes des différents agents économiques. La banque rapproche les agents à capacité de financement de ceux à besoin de financement. Cette activité d'intermédiaire financier vise encore à transformer les actifs financiers en vue d'assurer la transformation des échéances, des risques et des rendements. Les banques ont à ce titre un rôle dans le renforcement de la liquidité des marchés financiers, elles sont à ce titre *« market maker »* (Scialom, 2004, p.8).

L'existence des intermédiaires financiers se justifie par l'aversion pour le risque des agents non financiers (Pyle, 1971). L'activité de services financiers est sujette aux économies d'échelle, le coût du service financier diminue à mesure que la quantité de services fournis augmente. Le volume des opérations permet encore une diversification des risques. La banque d'aujourd'hui est largement industrialisée et suit une logique de rationalisation accrue. Les restructurations bancaires opérées depuis le début des années 1990 vise à intégrer de nouveaux canaux de communication et de distribution, mais avant tout à renforcer la compétitivité des banques en rationalisant la structure de coûts internes, en diversifiant les sources de bénéfices et en augmentant leur efficience (Plihon et al., 2006). La recherche de meilleure prise en compte du risque s'inscrit dans cette tendance.

L'activité classique d'intermédiation financière a donc fortement évolué pour faire face à cette logique de recherche d'efficacité. Ces activités de la banque d'aujourd'hui peuvent être résumées ainsi:

-La **banque de détail** : qui, par le biais de réseaux d'agences propriétaires mais aussi de cabinets de gestion de patrimoine partenaires, distribue un ensemble de produits à destination des clientèles de particuliers mais aussi de petites et moyennes entreprises. Il s'agira notamment de l'octroi de moyens de paiement (cartes bancaires, chèques bancaires, virements, mandats exprès et internationaux), des crédits aux particuliers (crédits relais, crédits primo-accédant, crédit automobile, crédit à la consommation) et aux entreprises (crédits divers avec des spécificités par secteur et en fonction des contraintes d'investissement et de paiement-livraison des clients et fournisseurs), des produits d'épargne et de placements

(de type livrets d'épargne réglementé, plan d'épargne en action, contrats d'assurance-vie en fonds euros et unités de compte), des solutions assurantielles proposées par les banques depuis les années 1970-1980 et s'étant fortement développées depuis le milieu des années 2000 (garanties des accidents de la vie, protection juridique, assurance automobile et multirisques habitation, contrat prévoyance-santé individuelle).

-**Le crédit aux entreprises et aux collectivités publiques ainsi que les services financiers spécialisés** (qui peuvent être distingués du crédit aux TPE/PME de par la nature et le montant des crédits alloués ainsi que des mécanismes d'octroi de crédit : complexité plus grande via des mécanismes de répartition en plusieurs tranches de crédit). Cette activité concerne davantage les grandes entreprises et les PME à taille critique. Elle engage davantage de fonds propres de la banque et se caractérise par des octrois de crédit d'ampleur plus importante.

-La **banque de financement et d'investissement :** cette activité est fortement rémunératrice pour les banques françaises l'ayant développé (le plus souvent des banques ayant des clients de type firmes multinationales, fonds d'investissement, investisseurs institutionnels, Etats). Il s'agit notamment de BNP Paribas, de Société Générale ou de Crédit Agricole CIB (Corporate and Investment Banking). D'autres établissements dans ce domaine sont fréquemment cités à l'instar de CitiGroup, de Goldman Sachs, de Morgan Stanley, des banques Lazard et Rothschild. L'activité comprend notamment : la collecte des ressources sur les marchés financiers (émission d'actions sur le marché primaire et achat-vente sur le marché secondaire), le conseil en fusions et acquisitions (notamment dans la partie due diligence[7]), l'activité de courtage (intermédiaire entre des investisseurs et des agents à besoins de financement) en matière d'actions, d'obligations, de dérivés de crédit, de produits de taux et de change, le financement des matières premières et des énergies diverses, le financement des activités d'import-export, le financement de projet (infrastructures, ouvrages d'art, constructions d'usines etc.), les activités de financements structurés (crédits syndiqués, *private-equity*/LBO[8], la promotion immobilière, le financement maritime, aéronautique ou

[7] Revue des éléments de fonds d'un projet d'investissement : aspects comptables, financiers, juridiques, risques. L'objectif est d'évaluer de manière quantitative et qualitative la valeur d'un bien ou d'une société, d'un projet d'investissement en étudiant en détail son contenu sous différents angles. Cette démarche est ainsi très proche de l'audit.

[8] LBO : Leverage Buy Out. Il s'agit de l'achat et revente d'entreprise avec fort effet de levier par des fonds de *private equity*, après une période de restructuration de l'entreprise acquise.

encore le financement des activités économiques par secteur ou par région (dans les pays émergents notamment).

-La gestion d'actifs et la banque privée : Cette activité consiste en un métier de prestation de services. Il s'agit de gérer des portefeuilles de titres de divers nature : par types d'entreprise, secteur d'activité, par type de titre (actions, portefeuilles d'obligations, portefeuilles de dérivés, portefeuilles de titrisation etc.) ce pour le compte de plusieurs types de clients. Ces clients peuvent être des investisseurs institutionnels tels que les sociétés d'assurance et de réassurance, les caisses de retraites (notamment les caisses de retraites du privé et les différents fonds de pension tels que le fond de pension des fermiers, des fonctionnaires aux Etats-Unis), mais aussi les clients particuliers disposant de fortunes importantes ou encore les organismes de placements collectifs en valeurs mobilières et les fonds communs de placements. Il faut, à ce titre, distinguer l'activité de gestion d'actif pour compte propre (la banque a une activité de gestion et de spéculation pour son compte propre sur la base de ses actifs) et celle dite pour compte de tiers (pour les différentes catégories de clients évoquées précédemment). L'activité de banque privée, souvent rattachée à ce type de structure, comprend également différentes catégories en fonction des fortunes détenues par les clients. De nombreuses banques privées acceptent une clientèle sur des montants de fonds à placer entre 1 et 3 millions d'euros et ont ainsi des conseillers spécialisés par type de fortunes. Les plus grandes fortunes ayant des conseillers dédiés (parfois plusieurs par client) et spécialisés en fonction de stratégies d'investissement voulues par le client.

A ces lignes métiers, il faut également ajouter une organisation des activités dans une logique de filialisation. Les établissements bancaires généralistes s'organisent ainsi autour de différentes filiales et entités:

-les sièges des établissements,
-le réseau français,
-les réseaux internationaux,
-les banques en ligne (filiales d'établissements bancaires à l'instar de Fortunéo, Boursorama, BforBank etc.),
-les filiales de bancassurance en assurance vie et en assurance non-vie (exemple pour Crédit Agricole Assurances, filiale de Crédit Agricole SA on citera Prédica et Pacifica respectivement en assurance non-vie et en assurance-vie),

-les filiales et/ou caisses d'ampleur régionale (Crédit du Nord et ses différentes filiales pour Société Générale, les différentes caisses régionales pour Crédit Agricole, les assurances du Crédit Mutuel etc.),
-des filiales spécialisées sur des activités et services additionnels (la gestion de trésorerie des entreprises, l'activité de financement en matière de commerce international, les activités dites de *correspondent banking*, les activités d'affacturage, services de change etc.).

1.2. La chaine de valeur d'un établissement bancaire

Michael Porter, en 1986[9], proposa une représentation synthétique d'une organisation intégrant les différentes fonctions de l'entreprise, la chaine de valeur (ou supply chain). Le schéma ci-après représente l'organisation classique d'un établissement bancaire, distinguant ses activités supports de ses activités opérationnelles.

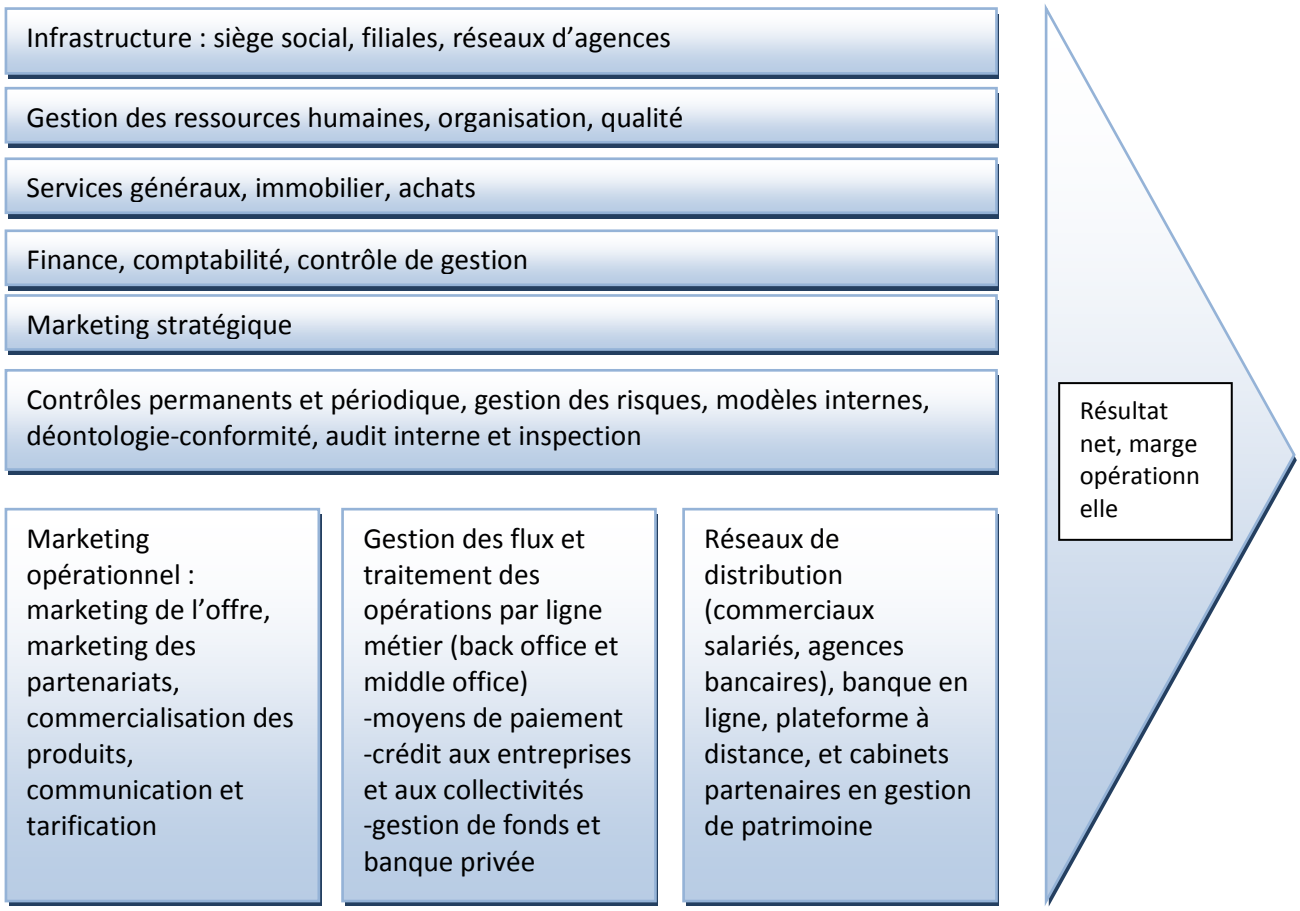
L'architecture organisationnelle classique d'un établissement bancaire comprend pour les fonctions supports les composantes classiques d'une organisation (fonctions finance, comptabilité, contrôle de gestion et départements 'pilotage', marketing stratégiques, fonctions d'achats et de gestion des enseignes immobilières et du parc d'agence, fonction qualité et gestion de la relation client, gestion et surveillance du portefeuille). A cela s'ajoute un ensemble de fonctions supports liées aux exigences réglementaires (sur lesquelles nous reviendrons dans le chapitre suivant). Il s'agit du contrôle périodique et du contrôle permanent, de l'audit interne et des corps d'inspection, de la gestion des risques (de marché le cas échéant, de crédit et des risques opérationnels), des départements en charge de la gestion des modèles traitant du calcul de provisionnement et d'allocation de fonds propres de l'établissement.

Les fonctions opérationnelles sont généralement réparties entre front, middle et back office (respectivement les réseaux en relation directe avec le client, les départements en lien avec les réseaux commerciaux et les centres de gestions des flux et opérations qui constitue quant à eux le back office : enregistrement des ordres de virements, des chèques, gestion du renouvellement des cartes bancaires, traitement des flux financiers liés aux crédits et aux remboursements etc.). A cela s'ajoute généralement le marketing opérationnel et les fonctions

[9] Michael porter, 1986, *L'avantage concurrentiel (the Competitive Advantage).*

de communication et de gestion des partenariats étant à la fois des supports mais souvent très liées en pratiques aux opérationnels de par la nature de leur activité.

Figure 3. Chaine de valeur, exemple d'une banque de détail



1.3. Des stratégies bancaires orientées vers la maîtrise des risques

La gestion des risques (et son objectif la maîtrise des différentes catégories de risque) est un élément essentiel dans la bonne gestion des établissements bancaires. Accepter un client et lui fournir différents services financiers (moyens de paiement, crédits, assurances) c'est accepter de prendre un risque en contrepartie des commissions, intérêts et primes payés par ce dernier. Les différents établissements bancaires mettent en avant le rôle stratégique de la gestion des risques dans leur mode de fonctionnement[10].

[10] Voir notamment les documents de référence 2013 des groupes Société Générale, BPCE, BNP-Paribas, La Banque Postale, Crédit Agricole, Crédit Mutuel-CIC, HSBC, Barclays etc. faisant tous référence au rôle essentiel de la prise en compte du risque dans la mise en œuvre de leur modèle d'affaires.

- **Des stratégies bancaires intégrant le facteur 'risque' :**

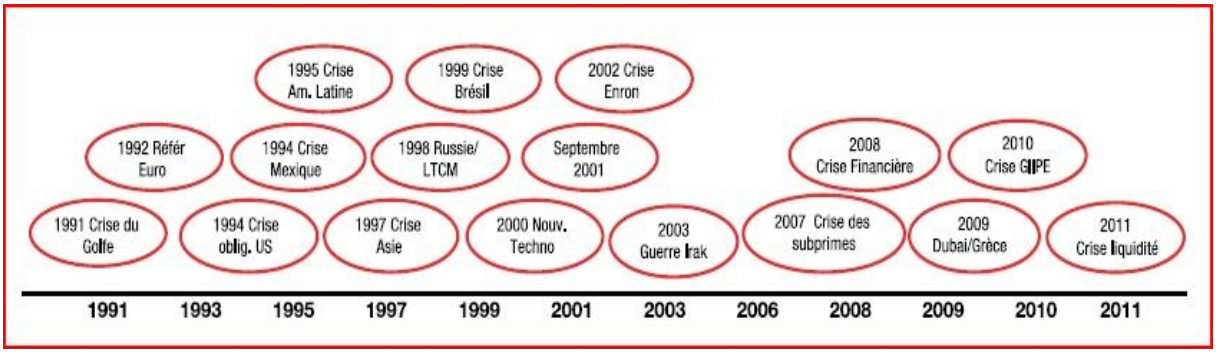
Plusieurs établissements bancaires ciblent la notion de risque au cœur de leur stratégie. On peut citer notamment Société Générale qui dans son document de référence 2013 (ainsi que dans les versions précédentes) évoque *« une stratégie de croissance à moindre risque »* pour faire référence aux nombreux évènements dommageables auxquels elle peut avoir à faire face (risques souverains, les risques liés à la diversification des activités dans un modèle de banque universelle, les risques liés à la détention mais aussi lors de programmes de cession d'actifs). Pour cet établissement, la question des risques fait partie intégrante du programme de maîtrise des coûts dans la durée. D'autres établissements précisent encore que la déclinaison de l'approche stratégique se fait par l'intégration des conséquences de l'activité sur le long terme. La recherche de croissance sur les marchés émergents intègre la logique de risque notamment dans la recherche d'une bonne gouvernance, de stabilité dans le top management mais aussi d'une politique de rémunération encadrée pour limiter les prises de risques excessives (c'est notamment le cas de BNP-Paribas). A l'instar du groupe Crédit Agricole ou du groupe BPCE (Banque Populaire Caisse d'Epargne), la recherche d'homogénéité du dispositif global de gestion des risques est également avancée comme un facteur d'amélioration de l'efficacité opérationnelle face à une diversité de risques (liés au contexte macroéconomique et financier, au secteur bancaire lui-même et au positionnement spécifique de chaque groupe). D'autres établissements insistent sur la nécessité d'intégrer le risque dans la prise de décisions stratégiques notamment du fait d'une logique de filialisation croissante du secteur bancaire (notamment le cas D'HSBC, de La Banque Postale, de Crédit Mutuel-CIC etc.).

Ces établissements, dans leurs communications institutionnelles mais aussi dans les différents échanges de leurs dirigeants avec la presse, font état de l'importance de développer les efforts en matière de gestion des risques dans un contexte post-crise de 2007-2008 (dite des subprimes) et de 2010-2012 (dite de la dette souveraine).

Le schéma ci-après (extrait du rapport annuel 2013 du groupe Société Générale) fournit un exemple significatif de la diversité des crises auxquels doivent faire face les établissements bancaires dans la conduite de leur stratégie d'affaires.

Figure 4. Les crises récentes vues par le groupe Société Générale

(Extrait du document de référence 2013)



- **Une multitude de risques pour les établissements bancaires**

Pour le banquier d'aujourd'hui, de nombreuses raisons impliquent de maîtriser plus que jamais le risque lié à ses diverses activités, plus particulièrement en ce qui concerne le risque opérationnel (Ogien, 2008):

-une contrainte d'allocation de fonds propres au titre de la couverture du risque opérationnel,

-le risque de sanction en cas de non-conformité des pratiques et des dispositifs à la réglementation prudentielle, l'avènement de Bâle II dans le secteur bancaire a été l'occasion d'affirmer la prise en compte le risque opérationnel mais a posé d'emblée la difficulté du champ élargi d'une telle catégorie de risque (Nouy, 2006),

-une nécessité de démontrer au client la bonne gestion de la banque et le caractère responsable de son management (Gadioux, 2010).

-la recherche de rentabilité sur tous les segments de marché dans un environnement bancaire de plus en plus concentré et concurrentiel (De Coussergues, Bourdeaux, 2010).

Les principaux risques des établissements bancaires sont les suivants :

-**Le risque de crédit et de contrepartie.** Il est souvent présenté comme le principal risque des établissements bancaires car il renvoi au cœur de leur activité historique (prêter à un particulier ou à une entreprise en anticipant un revenu futur qui peut ne pas survenir, le client se retrouvant alors en situation de défaut de paiement). Ce risque, lié à l'activité de crédit, est couramment appelé risque de contrepartie. Il comprend l'incapacité du client à verser les revenus liés au crédit (versement des intérêts) ou à rembourser le capital emprunté. La politique de crédit de la banque est donc un axe majeur en ce sens qu'elle doit permettre de cibler les clients ayant une capacité de remboursement suffisante pour honorer leurs

engagements, et ne présentant donc pas le risque d'être en situation d'insolvabilité (Brender, Pisani, 2007 ; Orléan, 2010).

-**Le risque de liquidité**. Cette catégorie de risque est loin d'être récente mais la récente crise de 2007-2008 a montré toute l'importance de cette dernière dans le secteur financier (notamment concernant les difficultés connues par Lehman Brothers, Merrill Lynch, Bear Stearns, Fortis Banque, Dexia etc). Il s'agit du fait pour un établissement bancaire de faire l'objet de retraits importants de la part des clients, lesquels ne sont pas compensés par des dépôts à court termes réalisés par ces derniers. Il provient généralement d'une impossibilité pour la banque de se refinancer auprès d'autres établissements bancaires. Ce type de risque peut survenir alors même qu'un établissement est réputé solvable. Certains économistes l'analysent comme la conséquence d'une crise de défiance entre établissement bancaire à l'instar de celle survenue suite à la crise des subprimes de 2007-2008 (Aglietta, 2008 ; Betbèze, 2010).

-**Le risque de marché** (et le risque lié aux différents portefeuilles) : le risque de marché est généralement divisé en différentes composantes que sont le risque de taux d'intérêt (l'évolution des taux d'intérêt fait courir un risque au porteur d'une créance ou d'une dette), le risque de change (qui concerne les créances et dettes valorisées en devises et provenant de la variation de prix des devises par rapport à une monnaie nationale donnée), le risque de variation de cours des actifs (variation du prix sur les différentes positions détenues par un établissement sur des actifs financiers). De nombreux articles, ouvrages et rapports ont étudié cette catégorie de risque en vue de savoir si ce type de risque, particulièrement difficile à identifier et à évaluer, pouvait être réellement gérer. Certains auteurs ont ainsi souligné l'impossibilité de prévoir rationnellement les fluctuations des marchés quant à ces risques, critiquant ainsi une pensée longtemps dominante selon laquelle la science mathématique et les couvertures de risque avaient permis de stabiliser lesdits marchés (Aglietta, Berrebi, 2007 ; Armatte, 2009 ; Orléan, 2009). D'autres insistent sur le caractère fondamentalement irrationnel et instable des marchés financiers comme l'ont montré les crises des marchés obligataires, des crises sur certains pays émergents, l'éclatement de bulles spéculatives, sur des secteurs ou des industries en particulier (Shiller, 2000 ; Minsky, 2008).

-**Le risque opérationnel** (qui intègre également les risques portant sur les infrastructures). Cette catégorie est également extensive car elle comprend plusieurs sous-ensembles tels que

le risque de fraude externe (provenant de clients ou de personnes extérieurs aux fichiers clients), de fraude interne (pouvant émaner de collaborateurs), les risques liés aux systèmes d'informations, à la continuité d'activité, à la sécurité des biens et personnes, aux pratiques commerciales etc. Cette catégorie est souvent appréhendée par la négative dans les établissements bancaires : ce qui n'est pas du risque de marché ou de crédit peut-être rattaché au risque opérationnel.

-**Le risque juridique.** Cette catégorie de risque renvoi aux différentes contraintes liées à la réglementation. Il s'agit notamment du respect de la réglementation prudentielle (Bâle II et III, Solvabilité II, Dodd-Franck-Act), de la réglementation européenne en matière de politique monétaire, du droit Etatique et européen en matière bancaire et financière, des règles en matière de droit de la concurrence (contrôle des concentrations, des politiques tarifaires, des pratiques de dumping), de droit de la consommation, de droit social, de fiscalité, de reporting financier, la jurisprudence aux niveaux local, national et européen etc. On retrouve parfois dans la catégorie du risque juridique le risque de conformité (qui peut-être rattaché au risque opérationnel cependant). Le risque de non-conformité est quant à lui définit par le règlement CRBF 97-02[i] comme « *le risque de sanction judiciaire, administrative ou disciplinaire, de perte financière significative ou d'atteinte à la réputation, qui naît du non-respect de dispositions propres aux activités bancaires et financières, qu'elles soient de nature législatives ou réglementaires, ou qu'il s'agisse de normes professionnelles et déontologiques, ou d'instructions de l'organe exécutif prises notamment en application des orientations de l'organe délibérant* ». Une telle définition, bien que visant l'exhaustivité, est par principe extensive et présente comme caractéristique d'énumérer d'autres risques parfois imbriqués. Certains des risques évoqués sont ainsi les conséquences de la survenance d'autres risques. On citera ainsi le risque de sanction judiciaire pouvant engendrer des pertes financières ou le risque de sanctions disciplinaires pouvant être à l'origine d'une atteinte à l'image de l'entreprise concernée (Fox, 1999 ; Morton, 2005 ; Mainelli, Yeandle, 2006).

-**Les autres risques**. D'autres types de risques peuvent concerner les établissements bancaires (et sont parfois inclus dans la catégorie des risques opérationnels). Il s'agit notamment du risque de bilan, du risque lié à la production d'informations comptables et financières, des conséquences financières ou d'impact image issues des obligations en matière de lutte anti-blanchiment et de lutte anti-financement du terrorisme. Ces risques sont souvent la conséquence d'un risque opérationnel.

Ces contraintes variées conduisent a priori l'établissement bancaire à mieux maîtriser son activité et à développer des fonctions de contrôle et gestion des risques dédiées aux différents risques et notamment au risque opérationnel.

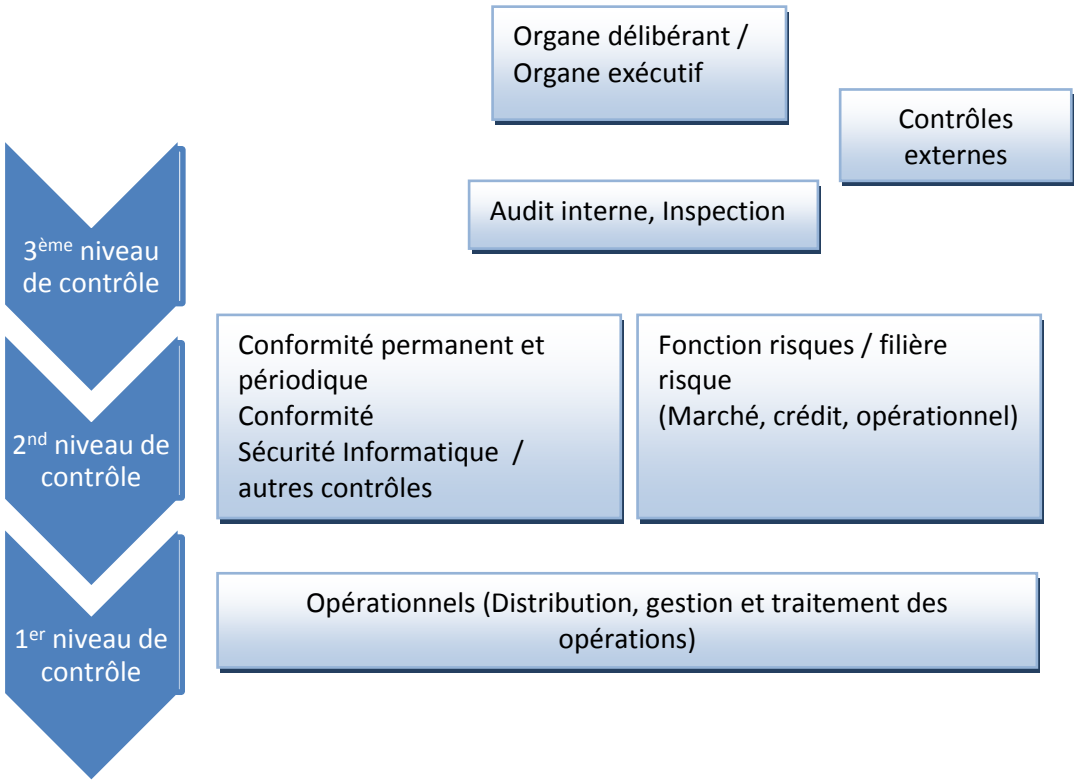
1.4. Les politiques générales de gestion des risques des établissements bancaires

C.Véret et R.Mékouar (2005)[ii] appréhendent la politique générale de gestion des risques comme incontournable pour permettre un arbitrage dans l'organisation sur l'importance relative de chaque risque. Cette politique permet la définition de contrôles systématiques et occasionnels, elle contribue à préparer les parties prenantes de l'entité à une éventuelle crise, elle vise une allocation appropriée des fonds propres et contribue à une hiérarchisation des objectifs en termes de risques en instaurant des actions curatrices de manière ordonnée. Une telle politique devient nécessaire dans des environnements économiques et juridiques complexes, changeants, protéiformes. Une telle politique doit être claire, c'est-à-dire définir des objectifs formels s'illustrant par des actions planifiées et quantifiées.

Dans le secteur bancaire l'architecture organisationnelle du contrôle des risques se décline généralement selon le schéma ci-après[11] :

[11] Adaptation, d'après : Ok Chandara, 2013, Organisation du contrôle interne, Vers un rapprochement entre risques et contrôles pour répondre aux nouveaux enjeux, *Revue Banque*, n°755-756.

Figure 5. Architecture du contrôle des risques bancaires



L'organisation du contrôle des risques en banque évolue aujourd'hui vers une structuration en trois niveaux : le contrôle de premier niveau, réalisé par les managers d'équipe et certains opérationnels (à la fois dans les fonctions supports et les fonctions opérationnelles). Un second niveau vient en appui sur la réalisation de contrôles dédiés (sur pièces et documents ou sur place en agence et dans les filiales et directions diverses) : on y retrouve alors le contrôle de conformité, le contrôle interne périodique et permanent, mais aussi la sécurité informatique et la sécurité des services d'investissement. Il faut également y ajouter les métiers dits de la filière risque (directions des risques de crédit, de marché et risques opérationnels). Un troisième niveau de contrôle est réalisé par l'audit interne et l'inspection qui reportent généralement directement aux organes exécutif et délibérant.

Le contrôle des risques en banque comprend donc généralement les fonctions suivantes, encadrant la notion de risque, de manière directe ou indirecte, leur importance est variable selon les secteurs d'activités (réglementés ou non, sources de danger pour la sécurité des biens et personnes, selon la taille de la structure etc.). Nous décrivons ci-après certaines des principales fonctions ayant à traiter du facteur risque dans une organisation bancaire.

- **La fonction risque :** Il s'agit de la fonction en charge de la gestion des risques au sein d'une organisation bancaire (répartie entre les risques de crédit, de marché et les risques opérationnels). Elle est dépositaire des outils et méthodes mis en œuvre en vue d'identifier les risques entourant l'organisation, d'évaluer, de quantifier et de modéliser ces derniers une fois recensés. La fonction risque met également en place des moyens visant à réduire le risque, à le contrôler sans chercher à l'éliminer complètement (ce qui en pratique relève de l'impossible).

- **La fonction d'audit interne :** L'IFACI (Institut Français de l'Audit et du Contrôle Interne) définit sur son site officiel l'audit interne comme « *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 ».* En banque, on parle également d'inspection pour désigner les corps d'audit interne réalisant des missions au sein des réseaux et filiales de l'établissement bancaire.

- **La fonction conformité (secteur financier principalement) :** La fonction de conformité comprend l'ensemble des collaborateurs de l'organisation ayant pour mission de s'assurer du respect des dispositions encadrant les activités bancaires et financières. Principalement présente (pour des raisons réglementaires) dans le secteur financier, cette fonction a pour rôle, de manière indépendante, d'identifier, évaluer, contrôler et établir un reporting sur le risque de non-conformité, lequel est un risque qui consiste à subir potentiellement des sanctions légales ou réglementaires, des pertes financières, ou des pertes associées à la détérioration de la réputation de l'organisation (suite à une non-conformité à des lois, règlements ou des normes).

- **Le dispositif de contrôle interne (contrôle périodique, contrôle permanent) :** En pratique les dispositifs de contrôle sont liés aux enjeux de conformité. Egalement très présent dans le secteur financier, le contrôle interne est à la fois réalisé par des opérationnels comme par des départements en charge de l'activité de contrôle à plein

temps (on parle alors de contrôles de premier et deuxième niveau). Il existe des référentiels (type COSO, Sarbannes-Oxley, Section 404) spécifiant la mise en œuvre du contrôle interne dans les organisations (faisant suite à de nombreux scandales financiers). L'Ordre des Experts Comptables définissait dès 1977 dans ses rapports annuels et documents de référence ce rôle de contrôle interne : *« le contrôle interne est l'ensemble des sécurités contribuant à la maîtrise de l'entreprise. Il a pour but d'un côté d'assurer la protection, la sauvegarde du patrimoine et la qualité de l'information, de l'autre l'application des instructions de la Direction et de favoriser l'amélioration des performances. Il se manifeste par l'organisation, les méthodes et les procédures de chacune des activités de l'entreprise, pour maintenir la pérennité de celle-ci ».*

- **La fonction de sécurité (parfois sûreté) :** La fonction de sécurité est une fonction obligatoire dans toutes les entreprises. Les articles L.4121-1 et suivants du Code du Travail imposent aux chefs d'établissements de gérer la prévention des risques professionnels en vue d'assurer la sécurité et de protéger la santé des collaborateurs (dont la présence est permanente comme temporaire dans l'entreprise). Cette fonction identifie et évalue les risques professionnels, met en place des moyens de protection et de prévention et développe des actions de sensibilisation et d'information ainsi que des formations visant à développer une atmosphère propre à créer une culture de sécurité dans l'organisation.

- **La fonction qualité :** Cette fonction est en charge de mettre en œuvre la démarche de management par la qualité dans l'entreprise. Son rôle est de s'assurer que les standards en vigueur soient respectés et de contribuer de manière continue à l'amélioration de la qualité des biens et services fournis par l'entreprise, de la conformité des procédures de qualité et de leur bonne mise en œuvre par une maîtrise des processus, une réduction des malfaçons, gaspillages, surcoûts, surqualités. Elle contribue à réduire les risques entourant la fourniture de biens et services pouvant présenter des défauts (éviter par exemple un rappel de produit). Cette fonction contribue à développer la confiance des clients de l'entreprise et à améliorer son image par le respect d'engagement pris par l'entreprise en matière de qualité.

- **La fonction financière :** Cette fonction a pour objectif principal de permettre le financement de l'activité de l'entreprise (obtention des fonds nécessaires au moment voulu). Son objectif est encore de s'assurer que l'activité de l'entreprise soit rentable et pérenne. La fonction financière a aussi pour objectif de procurer à l'entreprise les capitaux nécessaires à son fonctionnement, ce au moindre coût. La mise en œuvre de cette fonction implique d'inclure des tâches telles que la gestion des risques financiers (solvabilité, liquidité, risques des apporteurs de capitaux…). Elle vise à aider les dirigeants de l'entreprise à prendre des décisions sur la base des informations financières (établies notamment par la comptabilité et le contrôle de gestion). Elle rend compte de la rentabilité de chaque activité mais aussi des risques pris et de leurs impacts financiers pour l'organisation (utilisation pertinente, efficiente et efficace des ressources de l'entreprise).

Il existe d'autres fonctions pouvant traiter des risques : contrôle de gestion socio-économique, comptabilité (risques comptables et financiers), fonction « organisation » (risques opérationnels), fonction en charge des systèmes d'information (risques liés aux technologies de l'information), fonction ressources humaines (pour les risques psychosociaux), fonction recherche et développement (pour les risques liés à la conception), fonction d'intelligence économique, de communication (pour les risques stratégiques, la gestion de crise) etc.

2. L'activité d'assurance

Le cœur du métier d'assurance se définit comme suit : *« un mécanisme social ou commercial qui verse une indemnité financière lors d'un évènement malheureux, dont le paiement est effectué à partir des contributions cumulées de l'ensemble des membres participant au régime »* (Liedtke, 2005). Ces contributions étant fonctions des différents profils de risque des individus ou entités assurés, elles déterminent leurs cotisations respectives.

Il existe plusieurs définitions de l'activité d'assurance. Niall Ferguson (2009, p.187), reprenant les travaux de l'expert allemand Alfred Manes la définie comme *« Une institution économique fondée sur le principe de la mutualisation et établie dans le but de créer un fonds, dont le besoin apparait d'une manifestation du hasard dont la probabilité est estimée ».* L'activité d'assurance repose donc sur la mutualisation des aléas : un grand nombre

d'agents économiques verse une prime qui permettra d'indemniser le nombre plus restreint d'entre eux subissant un dommage. Pour un risque donné, les cas de dommages doivent être indépendants et le nombre d'individus pouvant être soumis à ce même risque doit être élevé.

2.1. L'assureur a plusieurs casquettes

Les sociétés d'assurance, quel que soit leur mode de fonctionnement, répondent généralement aux types d'activité suivant :

-L'assureur est gérant d'un fond dont il est le dépositaire. Il doit alors veiller à la performance du fond, notamment en vue de compenser les résultats techniques par ses résultats financiers, un des objectifs de la gestion actifs-passifs (ou Asset Liability Management, ALM).

-Il est également propriétaire des risques. L'assureur aura obligation d'indemniser les sinistres respectant les critères préétablis. A noter que l'assureur doit prendre en compte l'intérêt de l'ensemble des cotisants dans sa politique d'indemnisation et dans l'usage des fonds disponibles. La qualité de dépositaire d'un groupe de risques, soit du fond appartenant à une communauté, est donc caractéristique des objectifs de « trésorier » d'un assureur.

-En parallèle, l'assureur remplit des fonctions d'expert et de gestionnaire de risque (il analyse et évalue les risques qui lui sont soumis et acceptent ou refusent alors de les assurer). Il se pose la question de l'assurabilité d'un nouveau risque et prend la décision de couvrir ou non ce dernier (Couilbaut., Eliashberg, 2009).

Les activités des entreprises d'assurance sont plurales. Les sociétés d'assurance sont soumises au principe de spécialisation distinguant les activités d'assurance-vie des activités d'assurance non-vie (qu'il s'agisse d'assureurs généralistes soumis aux codes des assurances, d'institution de prévoyance ou de mutuelles, de filiales d'assurance d'établissements bancaires).

Certains assureurs sont spécialisés en assurance-vie (les mutuelles spécialisées sur le secteur de la santé ou encore les institutions de prévoyance) et d'autres davantage en assurance non-vie (certains assureurs de faible taille de portefeuille-clients davantage présents au niveau régional que national). On distingue généralement les lignes d'activité suivantes au sein des entreprises d'assurance :

-L'assurance de biens et de responsabilités (assurance non-vie): Cette branche comprend l'assurance automobile, l'assurance des immeubles et des risques d'habitation, l'assurance des risques d'entreprises (des flottes automobiles, des risques industriels, des risques de pertes d'exploitation, de vol de marchandise, de dommages causés lors d'opérations de livraisons à des clients), les couvertures de risques juridiques et de responsabilités (responsabilité civiles des particuliers et des professionnels), les risques liés aux accidents de la vie, les risques de réputation etc.. Il s'agit des marchés historiques des assureurs qui se sont peu à peu développés pour intégrer des garanties de plus en plus complexes et couvrir de nouveaux produits en parallèle du développement de l'économie (à la base couvrir les risques liés au commerce international, les risques des industries naissantes, les risques liés à la construction des gratte-ciels, les risques liés aux ouvrages d'art, aux centrales, les risques spécifiques à chaque industrie, la couverture des risques financiers des entreprises, l'assurance-emprunteur). Le champ couvert par l'assurance est extensif et en accroissement constant en fonction des problématiques de nouveaux risques à couvrir[12].

-L'assurance de personnes (assurance-vie): Cette branche de l'assurance comprend différents segments que sont la couverture des risques liés à la prévoyance-santé des individus et des collaborateurs d'entreprises (on distingue à cet effet la santé-individuelle et la santé-collectives), les activités d'épargne-retraite et celles qualifiées d'assurance-vie (contrats d'épargne avec régime fiscal de faveur et ayant comme base de placement les fonds euros ou les fonds en unités de compte). Cette branche comprend également la couverture des risques liés aux situations de dépendance des individus. Elle s'est fortement développée dans le courant de la seconde moitié du XXème siècle et a tendance à supplanter la branche non-vie par des chiffres d'affaires et une rentabilité plus élevée.

-L'assistance : l'activité d'assistance se distingue de celle d'assurance de manière simple. L'assurance consiste à fournir des prestations financières (le paiement d'une somme). L'assistance se distingue en cela qu'elle concerne le versement de prestation en nature (un service accompli généralement par un prestataire mandaté par la société d'assistance). Les sociétés d'assistance sont généralement des filiales des assureurs généralistes (Axa, Allianz,

[12] A noter que comme l'évoque Robert Leblanc, Coprésident de la Chambre syndicale des courtiers d'assurance, le taux de progression de l'assurance est supérieur à celui de l'économie en général. *Risques,* n°65, Mars 2006, *Vers le tout assurance* ?

Generali et leurs filiales d'assistance Axa Assistance, Mondial Assistance, Europe Assistance). L'activité d'assistance a concerné historiquement le rapatriement à l'international (de voyageurs, de touristes, de professionnels) ou le dépannage en automobile notamment. Cette activité se développe cependant et concerne de plus en plus les services à la personne, la télésurveillance etc..

-Le conseil en gestion des risques : Les sociétés d'assurance développent également, par le biais de filiales spécialisées ou de filiales dites « grands risques » (Axa Corporate Solutions, Allianz Global Corporate and Specialty) et par l'aide de cabinets de courtage en assurance (Aon Risk Consulting, Marsh Risk Consulting), des services de conseil en matière d'ingénierie du risque auprès des moyennes et grandes entreprises. Ces services concernent l'analyse de risque et la définition de solutions en termes de protection et de prévention des patrimoines couverts par l'assureur auprès de son client entreprise. Cette activité conduit également les assureurs à développer une expertise sur des risques encore difficilement assurables mais pouvant constituer, à termes, des relais de croissance futurs : risques liés aux biotechnologies, risques informatiques et cyber-risques, risques de fraude, risques financiers complexes, dérivés et titrisation de risque etc. (Raimbault, Barr, 2010).

-La gestion d'actifs et l'activité de financement et d'investissement : Outre certains assureurs qui ont mis en place des filiales bancaires (Axa Banque, Groupama Banque, Allianz Banque), l'activité des sociétés d'assurance est en grande partie une activité de financement de l'économie et d'investisseur institutionnel. Il s'agit en grande partie du placement des primes et cotisations d'assurance perçues et des collectes d'épargne dans l'économie réelle et sur différents supports financiers. Cette activité, bien que risquée, s'explique par la spécificité de l'activité d'assurance : l'inversion du cycle de production. Il s'agit du fait que les assureurs perçoivent les primes d'assurance avant même d'avoir délivré les services financiers (l'indemnisation de l'assuré) qui est hypothétique et soumise à la survenance d'un sinistre. Ces primes constituent des sommes importantes (plus de 1700 milliards d'euros en 2013 en France) orientées, par la réglementation, sur des placements suffisamment sûrs (immobiliers, obligations d'Etats, obligations d'entreprises etc.). En plus de ce levier des primes d'assurance, les assureurs bénéficient de l'épargne importante collectée auprès des ménages. Il s'agit de ce fait d'un levier de mutualisation des fonds.

A noter que d'autres classifications des activités peuvent être faites selon le type de risque : risques extrêmes, réassurance, risques spécifiques ; et selon le types de solutions proposés aux

assurés : produits joints (garanties complémentaires incluses dans des contrats d'assurance), produits classiques et hétérogènes (Gourieroux, 1999).

- **Le risque comme matière première de l'assureur**

Ewald et Thourot (2013) résument le métier d'assureur comme celui de « preneur de risque » pour le compte des clients particuliers et des entreprises. Un assureur identifie les risques et définie dans quelles mesures ceux-ci sont assurables et à quels prix. L'assureur mutualise les risques, donne un prix à un évènement dommageable futur et potentiel (lui attribuant ainsi une valeur monétaire).
Toutefois, l'activité d'assurance n'est pas sans risque pour l'assureur: il accepte de couvrir les risques de ses clients assurés. Il doit donc avoir une parfaite connaissance des risques acceptés (risques souscrits) en assurance non-vie et pouvoir anticiper des vagues massives de décollectes d'épargne en assurance-vie (vagues de rachats en ce qui concerne les contrats d'assurance-vie). Si le risque est la matière première pour l'assureur, la prime perçue par ce dernier constitue une dette à l'égard de l'assuré pour lequel il lui faut honorer ses engagements (être solvable pour pouvoir indemniser l'assuré en cas de survenance de sinistre).

- **Un métier en évolution, des stratégies de diversification**

L'assurance est un métier en évolution pour plusieurs raisons : ce secteur est considéré comme étant fortement réglementé et les stratégies des assureurs doivent tenir compte à la fois de fortes contraintes économiques et financières dans leur activité de placement mais aussi d'une multitude d'autres menaces telles que les catastrophes naturelles pouvant être fortement coûteuses en assurance non-vie ou encore les évolutions réglementaires et fiscales (potentiellement défavorables). A cela s'ajoute un contexte juridique à prendre en compte : les régimes d'assurance obligatoire incitent les assureurs à avoir une parfaite maîtrise de certaines catégories de risques (assurance automobile, responsabilité civile des professions réglementées ou à risques, assurance des locataires, des chasseurs ; obligations de fait telles que les assurances-emprunteurs reportant ainsi le risque de défaut de l'emprunteur sur l'assureur etc.). Il faut également citer un contexte de droit de la consommation et de jurisprudence plus protecteur à l'égard des assurés (Morlaye, 2006).

Ces dernières décennies, les contraintes réglementaires et jurisprudentielles se sont accrues, sollicitant un effort supplémentaire des assureurs vers une gestion des risques se voulant plus globale (et pas seulement limitée aux risques souscrits par les assurés auprès de ces derniers). Les logiques managériales des assureurs telles qu'Axa, Allianz, Aviva, Generali, sont donc clairement orientées vers le pilotage stratégique de nombreux risques : financiers et économiques mais aussi juridiques et organisationnels.

2.2. La chaine de valeur et l'organisation d'une société d'assurance

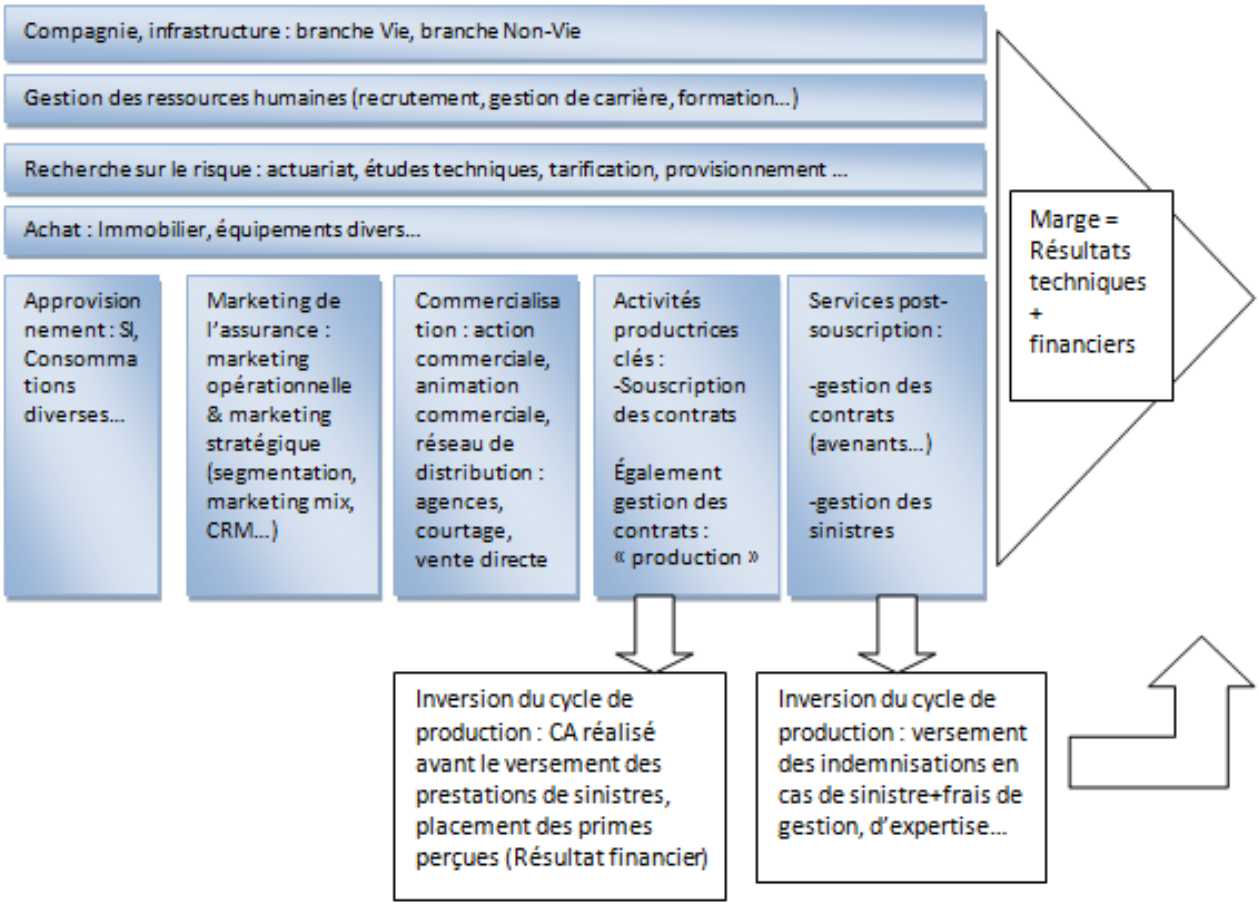
La chaine de valeur de l'assurance permet d'aller de la mise en place des systèmes d'information, des études techniques de tarification du risque et de provisionnement des fonds pour l'indemnisation des assurés jusqu'à la construction des contrats et leur commercialisation. Viennent ensuite leur souscription, leur gestion et, le cas échéant, l'indemnisation des sinistres.

Du fait de l'inversion du cycle de production cité précédemment, la marge bénéficiaire de l'assureur est constituée de deux éléments, les résultats techniques (issus de l'activité d'assurance elle-même, l'encaissement des primes ou cotisations moins les frais de gestion divers et le coût des indemnisations) ainsi que les résultats financiers (issus du placement des primes sur divers supports financiers, ces primes ne servant pas immédiatement au paiement des sinistres lors de leur encaissement).

Cette spécificité du secteur de l'assurance est un atout permettant d'équilibrer certaines branches d'activité, techniquement peu voire non rentables, mais compensées par les résultats financiers liés au placement des primes perçues. On citera alors le cas de l'assurance construction (Responsabilité Civile décennale notamment), où les primes perçues sont placées sur une longue période qui permet, par ses résultats financiers, de compenser des résultats techniques souvent négatifs pour un type de risques coûteux car fréquents dans sa survenance (de nombreuses malfaçons et fissures sur des constructions nouvelles avec un coût de l'expertise, nécessaire, souvent plus élevé que le coût du sinistre lui-même).

Appliquée à une société d'assurance, la chaine de valeur comprend les éléments ci-après.

Figure 6. Exemple de chaine de valeur d'un assureur



2.3. La diversité des risques des sociétés d'assurance

-**Les risques de souscription, des risques liés à l'offre produit**. Il s'agit de l'une des particularités du métier de preneur de risque qu'est celui des assureurs. Les risques de souscription peuvent être définis comme les risques qu'encoure un assureur suite à l'acceptation d'un client en tant qu'assuré. Le fait d'accepter de couvrir un assuré implique le fait d'accepter de subir le risque en lieu et place de ce dernier. De nombreux travaux académiques et professionnels mettent en avant deux difficultés à la base du risque de souscription : les asymétries d'information d'une part (un assureur accepte de couvrir les risques de l'assuré sur la base de certaines informations le concernant en termes de risques passés, d'accidentologie, de comportement de conduite par exemple en automobile, soit l'antériorité de ses sinistres, le détail des biens à assurer et la valeur réelle de ces derniers, la présence de facteurs aggravants ou de moyens de protections-préventions etc.). D'autre part l'assureur doit faire face à des comportements qualifiés d'aléa moral (un assuré sachant qu'il

est couvert par l'assureur sera moins prudent et aura tendance à avoir de plus grande chance de subir un risque).

Les risques de souscription sont spécifiques en fonction de la nature même du risque souscrit :

-le risque de souscription en automobile est souvent envisagé comme un risque de fréquence et dépend de la qualité des assurés couverts (de nombreux cas de survenance chaque jour, mais des impacts financiers importants[13]) : assurés jeunes conducteurs, conducteurs confirmés, véhicule utilisé et zone d'utilisation du véhicule etc.,

-le risque de souscription des entreprises dépend des industries assurées (un risque incendie est plus ou moins fort selon si nous sommes dans une industrie chimique, de haute technologie, dans le secteur des énergies, ou dans le domaine tertiaire etc.),

-le risque lié aux garanties-emprunteurs dépend de la qualité de sélection des assurés et de leur profil patrimonial (revenus et capacité de remboursement, situation professionnelle stable, biens en gages, sûretés, épargne préconstituée etc.),

-le risque de souscription en santé dépend du profil de clients couverts et de la diversification des portefeuilles (assurés jeunes, personnes âgées, jeunes actifs ayant tous des comportements différents en matière de consommation de services de santé) etc.

-Le risque de marché. Le risque de marché des assureurs se définit comme le risque de pertes de valeur liées à des fluctuations non maîtrisées ou non anticipées sur les marchés financiers. Il résulte généralement du fait qu'en assurance-vie, il existe des taux de rendement minimum garantis que s'engagent à verser les assureurs à leurs clients. En cas de faibles rendements ou de pertes sur les marchés financiers, ces derniers doivent compenser la différence entre le résultat réalisé et le montant à verser aux assurés. Les assureurs sont également soumis au risque de liquidité (suite à une décote des actifs par rapport aux prix de vente, à l'impossibilité de vendre des actifs).

-Le risque de crédit. Les assureurs sont encore soumis au risque de crédit en cas de dégradation de la capacité de remboursement des créanciers de l'assureur. Il peut s'agir à la fois des établissements financiers pour lesquels les assureurs consentent des prêts mais aussi d'autres catégories de clients (obligations souveraines notamment).

[13] Hors cas spécifiques de types carambolages ou accidents dits corporels graves (blessures d'un conducteur, d'un piéton, d'un passager etc.)

-Le risque opérationnel. On retrouve, tout comme en banque, différentes catégories de risque opérationnel dans l'activité d'assurance. L'une des catégories les plus importantes concerne la fraude externe (aussi appelée fraude à l'assurance). Les assureurs sont cependant soumis à d'autres risques tels que le manquement au devoir d'information et de conseil (pouvant engendrer des risques juridiques de type recours d'assurés et actions en justice). On citera également le risque de fraude interne, le risque lié aux systèmes d'information et les risques liés à la sécurité des biens et personnes etc.

-Le risque juridique. Le risque juridique des assureurs est tout comme en banque un sujet de préoccupation croissant, notamment en matière de droit de la consommation et de droit social. De multiples contraintes européennes et nationales concernent les assureurs (notamment l'essor progressif des actions de groupe, pour lesquels les assureurs sont concernés de par l'importance du marché de la protection juridique).

-Les autres risques. Parmi ces risques, nous pouvons citer le risque stratégique (lié au positionnement produits-marchés d'un assureur, au dimensionnement et à l'adaptation de l'offre produit et du réseau de distribution etc.), le risque d'image et de réputation, le risque statistique (déviation d'une loi des grands nombres du fait d'activités ou de situations nouvelles de risques cependant couvertes aux termes des contrats d'assurance, comportements modifiés des assurés du fait de la souscription du contrat, un produit mal conçu et donc mal tarifé etc.).

2.4. Le contrôle des risques des sociétés d'assurance

Dans le secteur assurantiel, l'architecture organisationnelle du contrôle des risques est plus récente que dans le domaine bancaire (voir le chapitre suivant relatif à la réglementation prudentielle). On distingue cependant certaines fonctions spécifiques à l'assurance ayant un rôle clé dans la connaissance et la maîtrise du risque. Il s'agit notamment de la fonction actuarielle et de sa déclinaison concernant l'actuariat-produit. Ces fonctions participent activement à la construction de l'économie des contrats d'assurance : calcul des probabilités de survenance de risque, évaluation des impacts en cas de survenance, évaluation du montant de provisionnement par type de risque et de produit d'assurance, tarification du risque (fixation de la prime d'assurance, de la franchise, du plafond d'indemnisation en cas de sinistre).

Le contrôle des risques d'une société d'assurance porte à la fois sur les fonctions supports et sur les fonctions opérationnelles. Son objectif est de vérifier la bonne application des procédures en interne (procédures de souscription des contrats, procédures d'indemnisation des sinistres, procédures de gestion des contrats, procédures de tarification et provisionnement des risques etc.). L'objectif de ces contrôles, outre la conformité des pratiques aux procédures, est d'éviter les risques dits « opérationnels » (voir la partie suivante) et les coûts qu'ils peuvent engendrer pour l'assureur.

On distingue ainsi plusieurs types de contrôle en interne :

Une distinction entre **contrôle périodique** et **contrôle permanent**. Le contrôle périodique est réalisé par des fonctions dédiées à l'activité de contrôle. Il peut s'agir d'un contrôle réalisé sur dossier ou sur place.

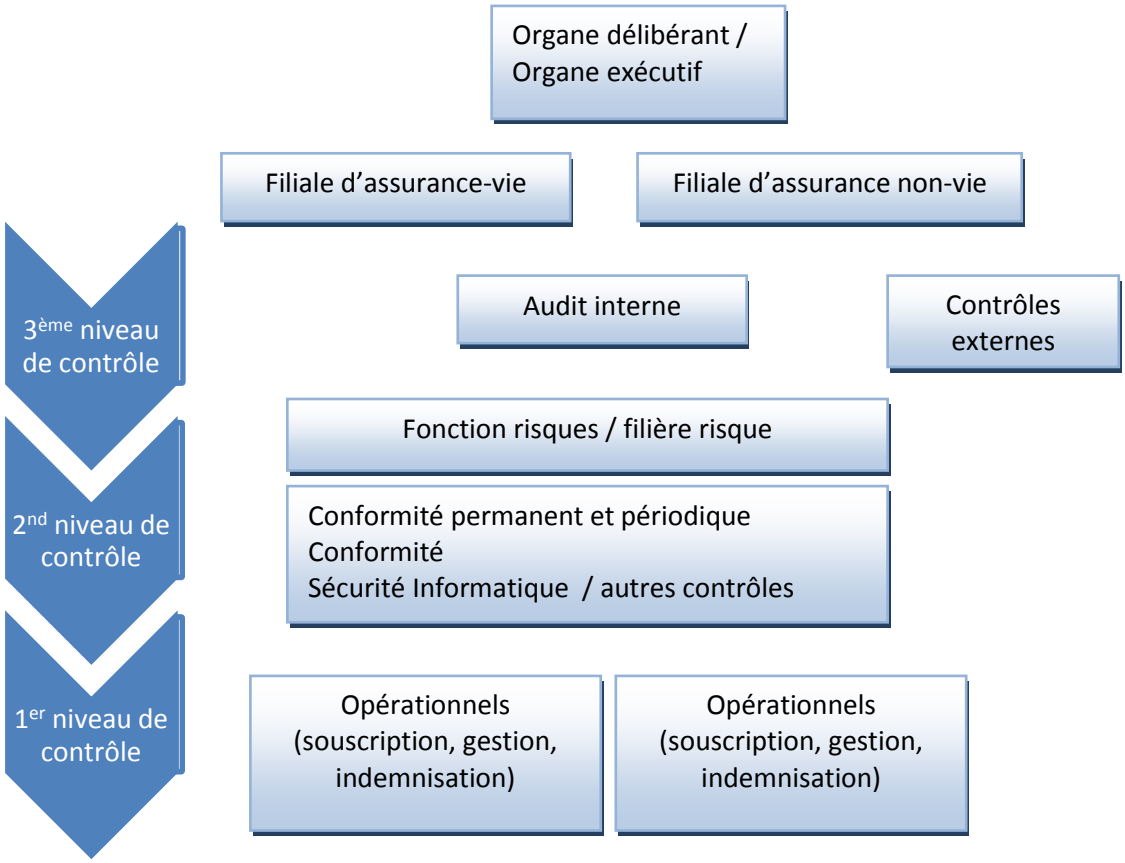
Exemple : une équipe de contrôleur d'une société d'assurance souhaite contrôler le processus de souscription des contrats d'assurance vie des différentes agences de l'assureur. Elle peut, soit demander aux différents agents de lui envoyer les dossiers des contrats qu'elle aura identifié préalablement, ou se rendre sur place pour réaliser des contrôles dans les agences (étudier la manière de travailler des agents et de leurs collaborateurs, le contenu des dossiers, fournir des conseils en vue de l'amélioration des pratiques).
Le contrôle permanent, quant à lui, est réalisé par les opérationnels en premier lieu ainsi que par des équipes de contrôleurs dédiées à cette mission. On parle alors de **contrôles de premier** et **de second niveau**. Le contrôle de premier niveau concerne les contrôles réalisés par les opérationnels et/ou les managers, en parallèle de leur activité « métier » principale.

Par exemple, le responsable d'un plateau de gestion de sinistres réalise chaque semaine un contrôle sur l'ensemble des procédures d'indemnisation réalisées afin de prévenir d'éventuelles fraudes ou des erreurs de traitement des dossiers.
Le contrôle de second niveau (aussi intégré dans le contrôle périodique avec l'audit interne) concernera par exemple un contrôleur du portefeuille auto ou MRH ayant pour but de voir si les procédures de souscription, d'indemnisation ou encore de gestion des contrats sont respectées et si l'on constate une amélioration d'année en année.

L’organisation du contrôle des risques en assurance évolue aujourd’hui vers une structuration en trois niveaux : le contrôle de premier niveau, réalisé par les managers d’équipe et certains opérationnels (à la fois dans les fonctions supports et les fonctions opérationnelles). Un second niveau vient en appui sur la réalisation de contrôle dédié (sur pièces et documents ou sur place en agence et dans les filiales et directions diverses). On y retrouve alors le contrôle de conformité, le contrôle interne périodique et permanent, mais aussi la sécurité informatique et la sécurité des services d’investissement. Il faut également y ajouter les métiers dits de la filière risque (directions des risques de crédit, de marché et opérationnels). Un troisième niveau de contrôle est réalisé par l’audit interne et l’inspection qui reportent généralement directement aux organes exécutifs et délibérants.

Comme le présente le schéma ci-après, l’organisation du contrôle des sociétés d’assurance tend à se rapprocher de l’organisation existante en banque, en y ajoutant cependant le principe de spécialisation distinguant les filiales d’assurance-vie et d’assurance non-vie. Tout comme dans le secteur banque, il faut également distinguer des fonctions et dispositifs de contrôle la filière risque qui concerne les risques de marché, les risques de souscription mais aussi les risques opérationnels, juridiques et de conformité.

Figure 7. Architecture du contrôle des risques bancaires



3. L'importance de gérer le risque opérationnel dans les établissements financiers

Dès 2005, M. Power insista sur la prise en compte par les entreprises du secteur financier d'une catégorie de risque à part entière : le risque opérationnel. Il ajouta notamment que cette thématique, bien que loin d'être récente en pratique, devait être prise en compte en tant qu'enjeu à part entière de gestion des risques. Les établissements bancaires et les sociétés d'assurance ont développé, en appui de la réglementation, des dispositifs dédiés d'identification, d'évaluation et de suivi du risque opérationnel. Avant d'aborder cet enjeu sous l'aspect réglementaire, il nous faut insister sur ce que recouvre le champ du risque opérationnel en pratique. Le tableau ci-après fait référence aux catégories de risque opérationnels telles que définies par la réglementation prudentielle (Bâle II en cours d'application et Solvabilité II à venir). Cela illustre la diversité des situations auxquelles les établissements peuvent être exposés ainsi que la nécessité d'une politique globale dédiée à la maîtrise de risques opérationnels.

Tableau 3. Catégories et exemples de risques opérationnels

Catégories de risque opérationnel de niveau 1	Catégories de risque opérationnel de niveau 2	Exemples banque	Exemples assurance
Clients, produits et pratiques commerciales	-Conformité (lois, règlements, normes) -Défaut de production -Service conseil -Pratiques commerciales incorrectes	Non-conformité d'un produit au droit de la consommation (en matière de crédit, en matière d'information clientèle) Vente de crédit et manque de clarté sur les caractéristiques du taux (taux variable, taux fixe)	Défaut d'information sur le rendement d'un contrat d'assurance-vie, sur le risque de perte en capital. Clauses abusives, peu claires ou illicites dans un contrat. Exclusion de garantie ruinant l'économie du contrat.
Dommages aux actifs corporels	-Catastrophes et autres sinistres	Catastrophes naturelles (inondation, tempête endommageant les locaux), incendie, vol, dégradation	
Dysfonctionnement de l'activité des systèmes	-Sécurité des systèmes	Indisponibilité du SI empêchant la banque de passer des ordres, d'octroyer des crédits, comptes clients indisponibles, non actualisés (retraits, dépôts)	Indisponibilité du SI rendant difficile l'indemnisation des sinistres, erreur dans le calcul des fonds à provisionner pour indemniser les sinistres des assurés
Exécution, livraison et gestion des processus	-Admission et documentation clientèle -Contreparties commerciales -Fournisseurs -Saisi, exécution et livraison des transactions -Surveillance et notification financière	Dossier de crédit incomplet, contrat d'assurance-vie comprenant des informations parcellaires. Mauvaises exécutions des processus pour chaque activité (front, middle, back office)	Contrat d'assurance comprenant des informations parcellaires (antécédents de risque, facteurs de risque, éléments de prévention etc.). Mauvaise exécution des processus (gestion, souscription, indemnisation).
Fraude externe	-Vol et fraude	Retrait, virement frauduleux ; détournement de fonds, vol de chèque	Fausse déclaration de sinistre, déclaration excessive de sinistre
Fraude interne	-Activité non autorisée	Retrait, virement frauduleux ; détournement de fonds, vol de chèque avec complicité interne de collaborateurs	Fausse déclaration de sinistre, déclaration excessive de sinistre avec complicité interne de collaborateurs
Pratiques en matière d'emploi et sécurité sur le lieu de travail	-Egalité et discrimination -Relations de travail -Sécurité du lieu de travail	Pratiques discriminatoires à l'encontre d'un collaborateur, non respect du droit social/droit du travail. Prise en compte des risques psychosociaux (stress, fatigue, harcèlement etc.)	

3.1. Exemples relatifs au risque opérationnel bancaire

Il existe de multiples exemples relatifs au risque opérationnel au sein des banques.
-Donner à un client qui demande des précisions sur le calcul de rentabilité de ses contrats uniquement la formule mathématique complexe. Le client contact alors la presse (manquement au devoir d'information et de conseil).
-Investir dans un progiciel de calcul des tarifs inadapté sans étude de besoin préalable, ledit logiciel sera in fine inutilisable par les opérationnels.
-Un collaborateur a recours à des pratiques commerciales trompeuses auprès des clients en vue d'atteindre ses objectifs commerciaux.
-Les clients s'étant aperçu d'une défaillance d'un distributeur automatique de billets en profitent pour retirer des sommes indues (le distributeur ne débitant pas des comptes clients les sommes d'argent retirées par les clients).
-Des fraudeurs exploitent le manque de sécurisation d'une banque en ligne pour effectuer des virements à l'insu des clients de la banque.

De nombreux documents et rapports internes aux établissements bancaires ainsi que les guidelines publiées en 2010 par le CEBS (Committee of European Banking Supervision) ont mis en avant les risques opérationnels liés à la complexité des nouveaux produits financiers, pouvant engendrer des pertes aux conséquences systémiques. Un autre exemple concerne la fraude interne comme l'illustrent les cas du rogue trading au sein des établissements bancaires, de la corruption ou encore du vol d'identité. Ces risques opérationnels se situent alors à la frontière juridique, économique, éthique et des sphères de la conformité (Laffort, 2013).
Cette diversité d'occurrence des risques opérationnels est également illustrée. Certaines bases de données communes telles que la base ORX (Huebner, 2010). Cette base de données est commune à plus de 65 banques dans 18 pays telles qu'ABN AMRO, Barclays, BNP Paribas, Commerzbank, Crédit Suisse, Crédit Agricole, JP Morgan, Morgan Stanley, Société Générale, Wells Fargo & Co etc. Ainsi sur la période 2006-2010, il ressort notamment de cette base de données que sur l'ensemble des pertes opérationnelles par lignes d'activité des banques, les pertes liées au risque opérationnel de l'activité de trading arrivent en tête si l'on prend comme critère le montant de perte opérationnelle pour 100 euros de revenu généré par ligne d'activité (Voir l'annexe 2-Evènements de risque opérationnel, extraits de la base de données ORX).

Nous pouvons également citer d'autres exemples comme l'illustre le tableau ci-après :

Tableau 4. Exemple simplifié de tableau de bord risque opérationnel d'une banque de détail

Clients concernés	Lieux	Types d'incidents	Nombre d'incidents déclarés	Coût du risque potentiel	Coût du risque après mesure de récupération	Processus et activités concernées
14	Région Ile de France, Centre de services A	Retraits frauduleux carte bancaire	9	5600 €	5600 €	Retrait d'espèces
		Virement frauduleux	5	1150 €	0 €	Réalisation de virement
6	Région PACA, centre de services T	Fraude sur une opération de crédit	4	10 000 €	10 000€	Octroi de crédit
		Chèques falsifiés	2	900 €	300 €	Encaissement de chèque
9	Région Centre, centre de Services B	Chèques bancaires falsifiés	3	2670 €	560 €	Encaissement de chèque
		Retraits frauduleux carte bancaire	6	5500 €	4900 €	Retrait d'espèces
7	Région Normandie, centre de services F	Fraudes banque en ligne	4	23 000 €	12 000 €	Gérer ses comptes en ligne
		Chèques bancaires falsifiés	3	2100 €	1100 €	Encaissement de chèque
5	Région Bretagne, centre de services I	Faux chèques bancaire étranger	2	4000 €	4000 €	Encaissement de chèque
		Virement frauduleux	1	800 €	0 €	Réalisation de virement

Total risque opérationnel avant récupération : 55 720 €
Total risque opérationnel après récupération : 38 460 €

Face à cette diversité, les établissements bancaires ont mis en place des dispositifs dédiés au risque opérationnel s'appuyant notamment sur des outils de quantification et de suivi (voir les exemples en annexe 3-Exemples de dispositifs de contrôles relatifs aux risques opérationnels).

3.2. Exemples relatifs au risque opérationnel des sociétés d'assurance

En assurance nous pouvons également citer plusieurs exemples de cette diversité de risques opérationnels :

-L'acceptation par l'assureur de la souscription d'un barrage. Ce risque majeur a été accepté par l'assureur seul (sans coassurance avec une autre société et sans réassurance). Un tel risque peut être envisagé comme un risque financier car il peut remettre en cause la solvabilité de l'assureur mais sa cause première est bien un risque opérationnel : un risque accepté sans analyse préalable et sans contrôle des contrats signés par les commerciaux de l'assureur.

-Un mauvais document est annexé à un contrat de réassurance, impliquant de couvrir une entreprise cliente à hauteur de 50 millions d'euros de plus ce qui a été prévu lors de la signature du traité de réassurance. Le réassureur se retrouve engagé sur des montants non provisionnés du fait de cette erreur du personnel.

-Le document confidentiel relatif à la couverture santé d'un assuré est envoyé au mauvais client, le client réellement concerné ne recevant pas son document. Ce type de cas récurrents peut avoir un impact sur l'image de l'entreprise et se traduire par des pertes de clientèles. On peut ainsi établir un parallèle fort avec le risque de non-conformité, s'agissant des exigences en matière de conservation et de respect de la confidentialité des données clients.

-Exemple d'une erreur de traitement et de saisie d'information au sein d'une société d'assurance : Le service comptable d'une société d'assurance se rend compte que suite à une vague de sinistres, les sinistres indemnisés dépassent le montant habituel versé aux assurés par le service d'indemnisation.

L'indemnisation moyenne habituelle est de 1200 €, ce qui répond à une logique forfaitaire d'indemnisation prévue dans les contrats d'assurance. Les sommes sont provisionnées en conséquence par la mutuelle. Le coût total suite à une tempête ayant touché 136 assurés aurait du être de 136 x 1200 € = 163 200 €. Le coût réel est de 197 200 €. Soit un surcoût moyen pour la mutuelle de 250 € par contrat (34 000 € au total).

En cause, une erreur de saisie de l'information: le gestionnaire des contrats n'a pas coché dans le logiciel d'indemnisation la case indiquant « plafonnement de l'indemnisation » permettant d'appliquer le barème forfaitaire de 1200 € et induisant un dépassement de la garantie accordée.

3.3. Analyse comparative et spécificités sectorielles du risque opérationnel

Le tableau ci-après fait état des similarités entre lignes métiers et des spécificités associées à chacune en termes de risque opérationnel. Si certaines problématiques sont similaires (notamment en termes de risque d'atteinte aux actifs corporels, en matière de gestion des processus et de sécurité sur le lieu de travail), les catégories relatives aux fraudes internes et externes, aux pratiques commerciales ainsi qu'aux systèmes d'information ont un impact différent selon les secteurs (Banque / Assurance) et les lignes métiers dans chaque secteur. Certaines catégories de risques opérationnels sont également similaires entre les secteurs banque et assurance (en matière de gestion d'actifs pour ce qui concerne la fraude ainsi que les pratiques commerciales et les risques pouvant affecter les clients).

Tableau 5. Spécificités du risque opérationnel Lignes Métiers / Catégories de risques opérationnels

Catégories de risque opérationnel	**Lignes métiers Banque**				**Lignes métiers Assurance**				
	Gestion d'actifs et banque privée	Banque de financement et d'investissement	Crédit aux entreprises / services financiers spécialisés	Banque de détail	Gestion d'actifs, financement et investissement	Assurances de personnes (vie)	Assurances de biens et de responsabilités (non-vie)	Assistance	Conseil en gestion des risques
Clients, produits et pratiques commerciales	Défaut de conformité aux lois et règlements, respect des engagements à l'égard des clients, risque de réputation important pour les clients 'grand compte'	Mauvaise maîtrise des engagements financiers, défaut de contrôle pouvant engendrer des pertes financières importantes	Mauvaise connaissance des portefeuilles clients, politique non restrictive pouvant engendrer des risques financiers	Respect des pratiques commerciales exacerbé : droit de la consommation protecteur et caractère médiatique en cas de récurrence des défaillances	Défaut de conformité aux lois et règlements, manquement aux règles de prudence en matière de gestion des fonds	Devoir d'information et de conseil important ; réglementation restrictive (risque d'amendes et de recours contentieux des clients)	Risques de souscription : mauvaise politique d'acceptation des risques, mauvaise connaissance des clients couverts	Obligation de résultats à l'égard du client	Devoir d'information et de conseil important (risque d'image et de réputation en cas de conseils inadaptés)
Dommages aux actifs corporels	Problématique similaire quels que soient les lignes métiers : catastrophes, vols de matériels, incendies et autres sinistres pouvant affecter les actifs de l'entreprise								
Dysfonctionnement de l'activité des systèmes	Sécurité des données clients grands compte exacerbée (perte, vol de données	Indisponibilité du SI pouvant occasionner des pertes sur les positions financières prises (exemple : défaut de réactivité)	Incapacité temporaire à répondre aux clients	Pertes ou vol de données relatives aux clients, occasionnant un risque d'image et de réputation	Indisponibilité du SI pouvant occasionner des pertes sur les positions financières prises (exemple : défaut de réactivité)	Pertes ou vol de données relatives aux clients, occasionnant un risque d'image et de réputation	Pertes de données occasionnant un manque de maîtrise des engagements futurs ou un défaut de réactivité dans l'indemnisation des assurés	Incapacité à prendre en charge les assurés (occasionnant un risque juridique et d'image)	Incapacité temporaire à répondre aux clients

Exécution, livraison et gestion des processus	Problématique similaire aux différentes activités : -Admission et documentation clientèle -Contreparties commerciales -Fournisseurs -Saisi, exécution et livraison des transactions -Surveillance et notification financière								
Fraude externe	Vol et fraude des placements des clients	Détournement de fonds par des hackers, manipulation des données financières et des prises de position de l'établissement	Fraude au crédit (données clients erronées en vue d'obtenir un crédit de manière indue)	Vol et fraude aux moyens de paiement, risque d'image pour l'établissement si récurrents et non traités rapidement	Détournement de fonds par des hackers, manipulation des données financières et des prises de position de l'établissement	Usurpation d'identité : vol de fonds des clients, changement de bénéficiaire indu	Déclaration assuré erronée et recours abusif au service d'indemnisation	Déclaration assuré erronée et recours abusif aux services d'assistance	-
Fraude interne	Activité non autorisée réalisée par un collaborateur de l'établissement engendrant des pertes financières	Rogue trading : risque de pertes financières importantes pouvant remettre en cause la solvabilité de l'établissement, dissimulations de pertes	Fraude au crédit avec complicité d'un collaborateur conseiller client ou personnel administratif	Vol et fraude aux moyens de paiement, risque d'image pour l'établissement si récurrents et non traités rapidement	Activité non autorisée réalisée par un collaborateur de l'établissement engendrant des pertes financières	Usurpation d'identité : vol de fonds des clients, changement de bénéficiaire indu par un collaborateur	Participation d'un collaborateur à une indemnisation indue, détournement des règles en matière d'indemnisation	Complicité de collaborateurs en interne dans le cadre d'un recours abusif aux services d'assistance	-
Pratiques en matière d'emploi et sécurité sur le lieu de travail	Problématique commune aux différentes activités : -Egalité et discrimination -Relations de travail -Sécurité du lieu de travail								

Conclusion du chapitre premier – le risque opérationnel, problématique centrale

En conclusion de ce premier chapitre, le contexte des activités bancaires et d'assurance est celui d'une diversification croissante et d'une logique de banque dite « universelle » et d'assureur dit « généraliste ». D'autres acteurs (certaines banques mutualistes, certaines mutuelles d'assurance) sont parfois spécialisés sur des lignes métiers en particuliers. Ces assureurs et banquiers multimétiers (auxquels nos études de cas empiriques feront référence) sont donc soumis à différentes catégories de risques ainsi qu'à une multitude de risques opérationnels que nous avons illustrés par plusieurs exemples.

Ces risques opérationnels sont répartis en plusieurs catégories par la réglementation prudentielle en banque et en assurance. Pour faire face à ces risques, des dispositifs de contrôle existe à plusieurs niveaux (opérationnels, contrôleurs dédiés, corps d'audit et d'inspection). Cette même réglementation impose également la mise en place d'une gestion des risques globale au sein des établissements financiers ainsi qu'une filière risque opérationnel dédiée. Ce caractère institutionnalisé de la gestion des risques opérationnels fait l'objet du chapitre suivant.

Chapitre 2 - Cadre normatif et réglementaire des politiques de risques opérationnels dans les secteurs banque et assurance

« Les risques comme les richesses sont l'objet de répartitions…et leur répartition donne lieu à des conflits radicalement différents »
Ulrich Beck

Introduction

Le dispositif de contrôle interne et de gestion des risques vise à réduire les risques opérationnels de l'entreprise en lui permettant de répondre à ses objectifs de fiabilité des états financiers et extra financiers et de conformité aux lois et règlements (Spira, Page, 2003 ; Dumontier et al., 2008).

Selon l'AMF[14], *« en continuant à prévenir et à gérer les risques, les dispositifs de gestion de risques et de contrôle interne jouent un rôle clé dans la conduite et le pilotage des différentes activités »*. Le dispositif de contrôle interne est une des réponses possible face au risque. Il fourni à une organisation un niveau d'assurance raisonnable quant à la réalisation de ses différents objectifs (Coso, 1992). Son évolution s'est faite en intégrant progressivement la notion de gestion globale des risques (ERM) en vue notamment de faire face aux exigences croissantes (notamment réglementaires) de rapprochement entre fonctions risques et contrôles (Coso, 2004, 2013). Cette évolution vise à rendre compte des nouvelles attentes en matière de prise en compte des risques internes et externes à l'entreprise (risques émergents) mais aussi des problématiques de responsabilisation des acteurs et de la gouvernance d'entreprise. Cette logique est qualifiée d'environnement de contrôle et intègre différentes composantes : surveillance des risques, évaluation des risques, information et communication notamment (voir l'annexe 4-« Coso 2013 »).

Dans des organisations de type « légalistes », où le rapport à la norme est important (notamment les organisations de type bureaucratique), l'enjeu du cadre normatif est une préoccupation centrale des managers, poussant ces derniers à adapter les procédures, les modes de décision et même le langage utilisé (Sitkin, Bies, 1993). Les organisations du secteur financier s'inscrivent dans cette perspective en y ajoutant une problématique

[14] Cadre de référence de l'Autorité des Marchés Financiers (AMF).

spécifique : le poids de la régulation et le couple règle/risque, sorte de balancier entre une prise d'initiative et de risque trop forte des établissements financiers et une régulation contraignante encadrant strictement toute activité. Il s'agit là d'un point centrale dans le secteur financier où la gestion des risques est « institutionnalisée » (Alemanno et al., 2013).

La régulation en matière financière est souvent envisagée comme le moyen d'intégrer le rapport au risque et à ses conséquences sur la Société. Comme le rappelle M. Ojo (2006), parmi les nombreuses raisons expliquant la demande de régulation, il y a nécessairement le caractère politique de la question du risque dès lors que l'environnement financier est lié à l'économique et au social. Cette « financiarisation » (soit l'intégration croissante du lien entre financier et cadre économique et social) croissante de l'économie est envisagée comme un facteur d'avènement d'une société du risque au sens d'U.Beck (1986). Le risque devient également politique dès lors que l'opinion publique prend conscience que certains établissements financiers, en cas de faillite, peuvent remettre en cause leur manière de vivre et leur situation financière (Hutter, 2000). Les nombreux cas médiatiques de ces dernières années attestent de cette nécessité d'une régulation des pratiques et du cadre de fonctionnement des établissements financiers. Parmi ces cas, on peut ainsi citer de nombreux exemples où le risque, plus spécifiquement le risque opérationnel est à prendre en compte dans les difficultés des établissements financiers: le cas de Barings, plus récemment les cas de Calyon et Société Générale en 2007-2008, les cas d'AIG et de la Caisse d'Epargne en 2008, d'UBS de 2008 à 2011, de Goldman Sachs en 2010, de JP Morgan en 2011et 2013.

Ces nombreux cas médiatiques représentent des coûts importants ayant poussé les instances de régulation internationales à se saisir du sujet que représente la gestion des risques au sens large et des risques opérationnels en particulier (Lamarque, 2009). Au-delà du cas de la Société Générale ou des autres établissements ayant connus des dysfonctionnements médiatisés, il est essentiel d'insister sur un point clé, auquel fait également référence la réglementation prudentielle : le risque opérationnel n'est pas limité aux cas extrêmes. Il existe en effet un ensemble d'autres risques opérationnels exigeant une sécurisation optimale du fonctionnement des banques mais aussi des sociétés d'assurance. L'enjeu de cette sécurisation visée par la réglementation est bien de renforcer la résilience opérationnelle d'un établissement en donnant à ses décideurs une vision claire de leur exposition aux risques (Lamarque, Maurer, 2009 ; Torre-Enciso, Barros, 2013).

En effet, une régulation efficace insiste nécessairement sur des systèmes de planification et de contrôle permettant la responsabilisation des acteurs mais aussi une bonne connaissance des risques pris et encourus par les organisations (Bessire, 1995). Son objectif est à la fois de renforcer la solidité de l'organisation, la capacité de ses décideurs à anticiper des risques et des crises potentiels mais aussi à faire-savoir aux parties prenantes l'étendue des dispositions prises à cet effet (Hutter, 2000).

L'objet de ce chapitre est donc de détailler les exigences réglementaires en matière de gestion des risques opérationnels dans le secteur financier. Nous abordons en premier lieu le contexte général de la réglementation prudentielle avant de détailler les principales dispositions en matières bancaires puis assurantielles relatives au cadre de la gestion des risques et à la thématique du risque opérationnel. Nous nous livrons enfin à une analyse critique des normes relatives au risque et à sa gestion dans le secteur financier.

1.Le cadre normatif et prudentiel au sein des établissements financiers, contexte général

La thématique de la régulation en matière prudentielle a fait l'objet de débats anciens. Cela reste cependant un sujet d'actualité au regard des nombreuses crises récentes du secteur financier dans lesquelles la gestion des risques a fait l'objet de critiques.

1.1.La réglementation des activités de banque et d'assurance, un débat ancien

Pour André Orléan (1999, p.259), la théorie autoréférentielle des marchés conclue à l'incapacité de la finance à s'autoréguler. Le poids des comportements individuels, la volatilité des cours et la fragilité des conventions sont autant de facteurs d'instabilité impliquant une nécessaire intervention face à l'improbable autorégulation de la finance moderne.

Les ressorts des mouvements de dérèglementation : La crise des années 1930 a conduit à une forte réglementation des activités bancaires. La stabilité du système bancaire a été mise en avant comme cause d'une nécessaire réglementation (agrément pour exercer l'activité, séparation entre banque et autre activité etc.). Les années 1980 ont toutefois vu évoluer ce système. Sous l'effet d'un choc technologique, d'une hausse de la demande de services financiers et de produits bancaires, il s'est opéré un changement majeur de la réglementation

pour permettre un développement de ce secteur ainsi qu'une meilleure concurrence (Scialom, 2004, p.22). Grâce à la dérèglementation, le marché bancaire s'est en effet peu à peu concentré emportant la fin des banques les plus fragiles. Ce marché a vu aussi apparaitre une diversification de l'offre de produits des banques pour concurrencer leurs rivales. Enfin, les banques se sont encore rapidement internationalisées.
Face à cela, l'une des tendances de fond de la banque moderne a été le mouvement de développement de la banque universelle. La banque universelle s'oppose à la banque spécialisée qui consiste à séparer les banques commerciales de dépôts des banques d'investissement (le *Glass Steagle Act* de 1933 aux Etats-Unis). Il s'agit d'offrir l'ensemble des services financiers disponibles (collecte de dépôts, octroi de crédits, opérations sur titres, prise de participation dans des entreprises, activité d'assurance, opérations hors bilan).

Dans une société où les nombreuses crises mettent la question des risques au centre des attentions, la régulation comprend un volet de mise en place de dispositifs dédiés à la gestion des risques.

Toutefois, malgré les nombreuses crises et scandales financiers du XXème siècle et du début du XXIème siècle, le débat sur la pertinence de la régulation des établissements financiers reste d'actualité. De nombreux travaux ont mis en avant le coût de l'intervention Etatique ex post à ces évènements, mais ils insistent également sur l'évolution de la réglementation bancaire et assurantielle, progressive et parfois plus réactive que préventive (Alemanno et al., 2013).

1.2.La réglementation des activités de banque et d'assurance, un sujet d'actualité

Depuis quelques années, le management subit de plus en plus de pressions pour améliorer l'efficacité de son périmètre de contrôle (Sutton, 2006). De nombreuses études montrent la vulnérabilité des entités du secteur financier. Qu'ils s'agissent d'organismes d'assurance ou d'établissements bancaires, ces entités sont confrontées à des risques sur chaque type d'activité (risques de solvabilité, de liquidité, de souscription, risque-produit, risque de non-conformité etc.) dont l'anticipation constitue une gageure, mettant de fait en avant la fragilité du système financier (Bernoth, Pick, 2011). L'un des objectifs principaux des dispositifs de contrôle est alors à la fois éthique et esthétique face à ces risques (Méric et al.2009). Le contrôle d'inspiration réglementaire des établissements financiers se caractérise à la fois par

les dispositifs de contrôle interne orientés risque, conformité mais aussi de politiques de risque dédiées orientées stratégie et acteurs (Hakenes, 2004 ; Fiordisely et al., 2011). Toutefois, comme le montre la crise de 2007-2008, qui est avant tout une crise du contrôle et du Risk Management pour de nombreux auteurs, une telle approche se caractérise principalement par sa dimension auto-contrôle. Il en découle des stratégies de résistance à ces dispositifs : contournement, évitement, hypocrisie organisationnelle (Shapiro, Matson, 2008 ; Cappelletti, 2009b). La crise financière, justement car elle est particulière, montre la faille de cet auto-contrôle et constitue une opportunité de repenser le Risk Management de l'après-crise (Huber, Scheytt, 2013).

Cela est d'autant plus exact dans le domaine bancaire où les différentes parties prenantes ont besoin de restaurer une confiance mise à mal par les récents scandales. Une réponse organisée face aux risques apparait aujourd'hui comme indispensable (Power, 2007). Les systèmes de contrôle se déploient afin d'assister le management dans son objectif de maîtrise des risques de son périmètre (Chenhall, 2003), système qui doit laisser une certaine flexibilité au management.

De nombreux éléments, à l'origine de quelques crises récentes, étaient prévisibles voire même en partie pris en compte. Toutefois, nous continuons à être surpris par la survenance de ces risques ainsi que par leur ampleur. L'enthousiasme du quantitatif et des modèles a fait émerger l'idée que la science financière était un moyen confortable d'analyser les risques, avec une *« illusion du contrôle »* derrière les modèles (Kaplan et al., 2009). Cette *« illusion du contrôle »* repose sur le fait que trop souvent le management a tendance à surestimer la capacité de son organisation à tirer partie des risques entourant l'entreprise. Il y a une large part d'illusion du contrôle dans ces dispositifs dès lors qu'il est impossible de voire émerger des responsabilités. Nous assistons aujourd'hui à une volonté de tout rationaliser et organiser au sein d'une entreprise (Power, 2009) ainsi qu'à une approche davantage axée sur le reporting et la conformité que sur la résolution des causes racines de risque et de la réduction de l'incertitude (Kim, Park, 2009 ; Altamura, Beatty, 2010).

Ces constats issus de la littérature académique sur la régulation des risques nous invitent à étudier plus largement l'évolution de la réglementation prudentielle dans les secteurs banque et assurance.

Une évolution du contexte règlementaire des banques et des sociétés d'assurance

Il existe de nombreux dispositifs réglementaires et prudentiels visant le développement du contrôle dans les établissements financiers : Bâle I, II et III, Solvabilité I et II, Sarbannes-Oxley, Cadbury Code etc. Ces dispositifs ont contribué au renforcement des fonctions dédiées au risque.

A cela s'ajoutent les enjeux de **supervision macro-prudentielle**, via, depuis la loi du 22 octobre 2010 ayant créé en France le Conseil de régulière financière et du risque systémique, dans la continuité du Comité Européen du risque systémique.

La supervision dite **micro-prudentielle** comprend différentes autorités de surveillance par lesquelles sont concernés les assureurs mais aussi les établissements bancaires : Autorité bancaire européenne, Autorité européenne des marchés financiers, Autorité européenne des assurances et des pensions professionnelles puis au niveau national l'Autorité de Contrôle Prudentiel et de Résolution (ACPR) ainsi que l'Autorité des Marchés Financiers (AMF).

1.3. Une approche incrémentale de la régulation sur le contrôle des risques

Dans le domaine bancaire, les dispositifs réglementaires relatifs aux fonctions de contrôle, de surveillance et de gestion des risques sont nombreux. Ils se caractérisent par la diversité des risques abordés mais aussi par une recherche progressive d'exhaustivité dans la réponse apportée à ces derniers.

- Le règlement CRB 90-08 du 25 juillet 1990 instaurant le responsable du contrôle interne,

- La loi du 12 juillet 1990 concernant la participation des établissements financiers à la lutte contre le blanchiment des capitaux,

- La loi du 13 février 1991 instaurant un correspondant TRACFIN[15],

[15] TRACFIN : Traitement du Renseignement et Action contre les Circuits Financiers clandestins.

- La loi de modernisation des activités financières du 2 juillet 1996 relative à la surveillance des risques et à l'efficacité des contrôles au sein des établissements de crédit,
- L'arrêté CRBF 97-02 du 1er octobre 1997 renforçant ces dispositifs par l'instauration d'un dispositif complet de contrôle des risques (responsable des risques et responsables de la sécurité des systèmes d'information),

- Le règlement du 14 octobre 1997 imposant la nomination d'un responsable du contrôle des services d'investissement et d'un déontologue,

- L'arrêté du 31 mars 2005 instaure quant à lui un dispositif complet d'identification et de contrôle du risque de non-conformité, créant la fonction de responsable de la conformité,

- En mars 2005, le CRBF 97-02 a évolué pour préciser aux établissements financiers le rôle des différents niveaux de contrôle et en structurant la notion de « contrôle permanent » en complémentarité avec le « contrôle périodique ». On peut lire ainsi : « les entreprises assujetties doivent, selon des modalités adaptées à leur taille et à la nature de leurs activités, disposer d'agents réalisant les contrôles, permanent ou périodique » (art. 6 du CRBF 97-02). Les contrôleurs permanents sont « certains agents, au niveau des services centraux et locaux, exclusivement dédiés à cette fonction et d'autres agents exerçant des activités opérationnelles ». Le contrôle périodique, c'est-à-dire l'audit interne, est assuré aux moyens d'enquêtes « par des agents au niveau central ».

- En 2006, les fonctions de déontologue, de responsable de la conformité et de responsable de la conformité des services d'investissement sont rassemblées tout en maintenant une distinction entre ces fonctions, selon qu'il s'agisse d'établissement de crédit et d'entreprises d'investissement (responsable de la conformité pour les services d'investissement) ou de société de gestion de portefeuille (responsable de la conformité et du contrôle interne).

- En vue de l'application des accords de Bâle II, le règlement 97-02 a été complété notamment par l'arrêté du 20 février 2007 relatif aux exigences de fonds propres

applicables aux établissements de crédit et aux entreprises d'investissement (d'autres arrêtés ayant précédé et succédé à ce dernier concernant des dispositions réglementaires plus spécifiques).

- Ainsi, en 2009, l'arrêté du 19 janvier, suite à l'affaire Kerviel, précise que les systèmes d'analyse et de mesure des risques « doivent prévoir les critères et seuils permettant d'identifier comme significatifs les incidents révélés par les procédures de contrôle interne (…) » (art. 17 ter). Le régulateur insiste sur l'importance d'un dispositif réactif entre les anomalies identifiées et leurs résolutions. Ainsi des procédures doivent être mises en œuvre pour « vérifier l'exécution dans des délais raisonnables des mesures correctrices qui ont été décidées par les personnes compétentes dans le cadre du dispositif de contrôle interne ». Les instances de gouvernance doivent disposer « des informations pertinentes sur l'évolution des risques encourus par l'entreprise assujettie » (art. 38), les incidents significatifs devant notamment lui être portés sans délai, ce qui suppose un dispositif qui facilite rapidement leur identification. Ces éléments ont contribué à institutionnaliser la fonction de contrôle interne et à développer des dispositifs de management actifs du risque (Cappelletti, 2006). Cette perspective s'inscrit dans une tendance à la normalisation du contrôle interne (Cappelletti, 2009b), qui se traduit alors dans les manuels de procédures (Pigé, 2001).

- En 2011, en France, l'arrêté du 23 novembre 2011 a transposé des exigences complémentaires relatives au contrôle des risques (Bâle 2.5) et à des exigences renforcées concernant certaines catégories de risque soulevées lors de la crise financière débutée en 2007.

Les principales évolutions règlementaires dans le domaine du contrôle interne portent ainsi, à la fois sur la structure des dispositifs de contrôle, et les procédures permettant d'agencer l'information essentielle au regard des risques majeurs. L'information et la communication font partie des cinq éléments du dispositif de contrôle selon le Coso (1992). Cependant il ne s'agit pas d'une fin en soi mais d'une logique informationnelle qui s'insère dans tous les éléments du dispositif, de l'organisation au pilotage en passant par la gestion des risques.

Le comité de Bâle en banque et l'EIOPA (ex-Ceiops) en assurance ont défini le cadre dans lequel se situent les politiques de risques et de contrôle, traitant notamment du risque opérationnel. Il s'agit des piliers II de ces dispositifs prudentiels (résumés ci-après).

Plus récemment, il importe de considérer le poids de la réglementation émergente Solvabilité II qui se traduit par un essor de la fonction de contrôle interne dans le secteur des assurances, de l'audit interne, de l'évaluation et de la gestion des risques.

Dans le secteur financier, ces fonctions s'inscrivent dans le cadre du Pilier II des réglementations prudentielles, et obligent les organismes du secteur financier à créer, mettre en place et fournir les moyens adéquats auxdites fonctions pour accomplir leurs missions. Qu'il s'agisse de la réglementation Bâle II, du règlement CRBF 97-02 concernant les établissements de crédit et de la directive Solvabilité II applicable au 1er janvier 2016 en ce qui concerne les organismes d'assurance ; dans les deux cas, il est question de développer les éléments suivants permettant une meilleure prise en compte du risque :

-un système de quantification permettant d'évaluer les risques et de réaliser des avances de fonds en vue de se couvrir de manière proportionnée face à ces derniers.

-un ensemble de fonctions et de dispositifs propres à assurer la bonne maîtrise des risques dans l'organisation et à responsabiliser les fonctions opérationnelles comme les fonctions supports en central ou dans les filiales (Risk Management, contrôle interne périodique et permanent, audit interne, contrôle de conformité etc.).

-un reporting prudentiel et une communication institutionnelle sur l'exposition aux risques de l'établissement et sur les mesures prises pour encadrer et réduire cette exposition (reporting destiné aux autorités de régulation, aux investisseurs, aux agences de notation ainsi qu'aux clients des établissements financiers).

Tableau 6. La réglementation prudentielle et l'obligation de rendre des comptes, cadre général

Pilier 1 **Exigences de fonds propres requis**	**Pilier 2** **Processus de surveillance réglementaire des risques**	**Pilier 3** **Discipline de marché / communication financière**
Modalité de calcul des risques à couvrir Recherche d'un calcul adapté par rapport au profil de risque Risques de crédit, de marché, Risque opérationnel Risque de souscription (assurance vie et non vie) Rendre des comptes sur : -la répartition des actifs en classes homogènes -La pondération des fonds alloués au risque selon les sûretés, la probabilité de défaut ou l'exposition en cas de défaut	Cohérence entre la stratégie de la banque et la politique de risque (informations financières et non financières) **Organisation de la gestion des risques, validation des méthodologies, interactions avec les acteurs de la filière risque et le régulateur** Détermination d'actions préventives Les instances de gouvernance (organe exécutif et délibérant) sont directement responsables des processus de gestion des risques mis en œuvre.	Informations à publier en matière de : -dotation des fonds propres, -risque de crédit, -risque de marché, -risque opérationnel -opérations de titrisation -méthodes d'évaluation et de gestion des risques Enjeux de transparence

Ces trois éléments (quantitatif-pilier 1, qualitatif-pilier 2 et communicationnel-pilier 3) du dispositif de Risk Management apparaissent comme complémentaires et dès lors que ces derniers sont développés et diffusés de manière parallèle, ils permettent de contribuer à rendre des comptes face au risque actuel et futur (Vyas, Singh, 2010). Toutefois, et comme le montrent les scandales financiers récents, de tels dispositifs ont pu faire l'objet de contournements. L'une des critiques récurrente face à ce Risk Management est encore celle de sa capacité à cerner l'objet complexe « risque » dans un monde où le risque se diversifie, est à la fois partout et devient un « lieu de nulle part » et où les outils de réduction du risque deviennent des véhicules de risque (Shiller, 2003 ; Kaplan et al., 2009). Qu'ils s'agissent des cas de rogue trading ou encore des politiques de prise de risque agressives et conflits d'intérêts caractérisant certains établissements, l'obligation de rendre des comptes fut, à de nombreux égards, malmenée.

2.Le cadre prudentiel en banque : de Bâle à Bâle III

Ce paragraphe aborde l'évolution d'un cadre prudentiel depuis les accords de Bâle jusqu'aux récents enjeux de Bâle III en situant l'attention accordé au risque opérationnel face à ce contexte normatif et prudentiel.

2.1. De Bale I à Bâle II puis, Bâle III

Dans le secteur bancaire, les accords de Bâle de 1988 ont entendu poser les jalons de base de la réglementation prudentielle bancaire européenne. Cette réglementation avait vocation à être mise en œuvre dès 1993 pour les banques ayant une activité internationale. Ces dernières devaient disposer d'un montant de fonds propres de base respectant un ratio minimale de solvabilité (appelé alors le ratio Cooke). Des compléments ont été ajoutés à cet accord en 1996 en vue de davantage prendre en compte la couverture du risque de marché.

Le 26 juin 2004, l'accord dit de Bâle II a été conclu et traduit dans l'Union Européenne par le biais de la directive CRD de 2006.

Les objectifs des accords de Bâle II sont notamment de :

-prendre en compte de nouvelles catégories de risque peu abordées auparavant tels que les risques opérationnels, le risque de taux d'intérêt ou encore le risque de liquidité,

-contribuer à renforcer la prise de conscience qu'un capital minimum n'est pas suffisant pour garantir la solvabilité d'un établissement bancaire, d'où l'intégration d'exigences qualitatives telle que la maîtrise des risques,

-optimiser le calcul des risques et l'allocation des fonds propres en couverture des risques pris par les banques.

Le dispositif Bâle II est fondé sur trois piliers décrits dans la figure ci-après :

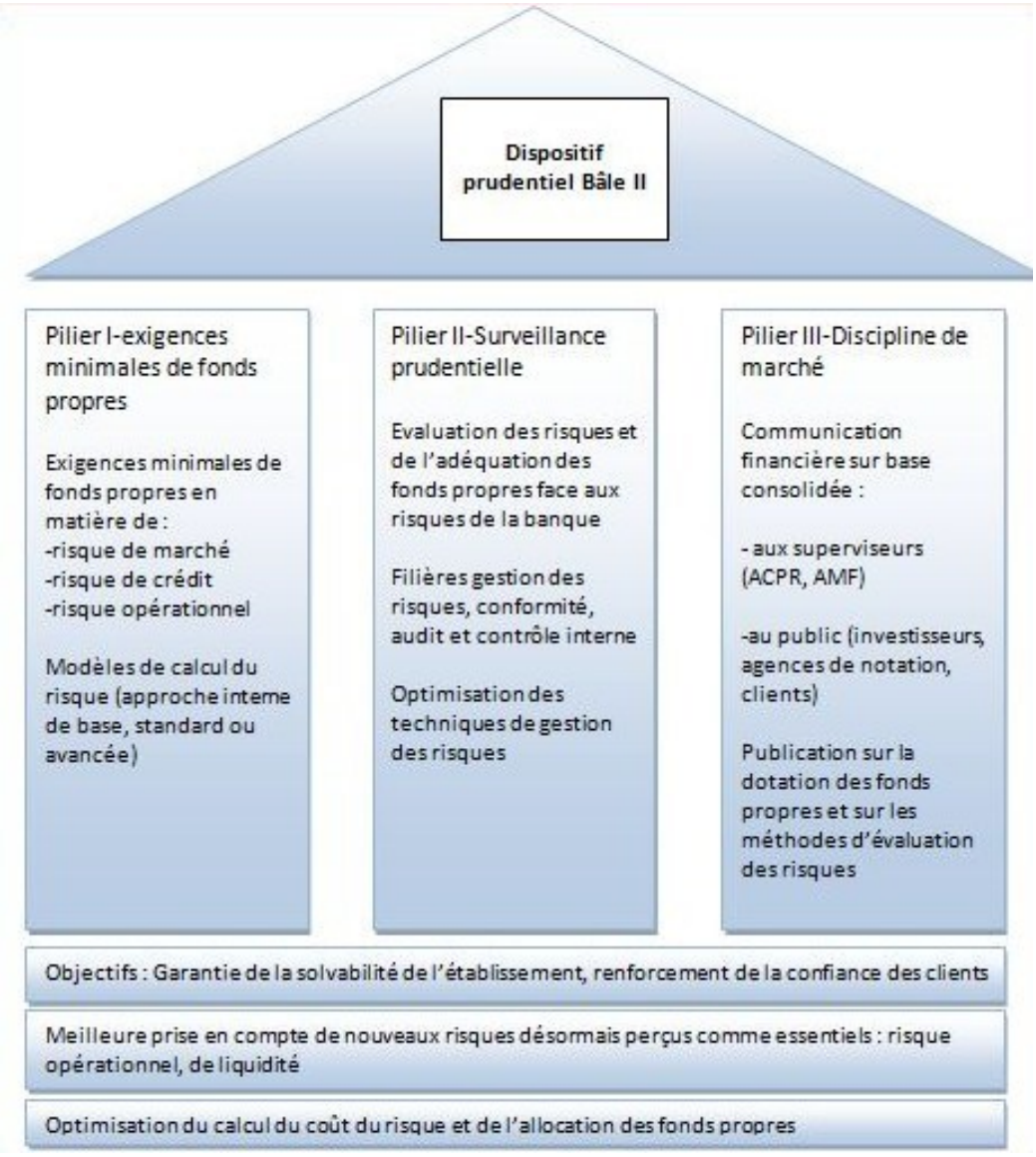
-un premier pilier relatif aux exigences minimales de fonds propres,

-un second pilier abordant la surveillance prudentielle des établissements,

-un troisième pilier concernant la « discipline de marché ».

Le fondement de cet accord est que : mieux la banque est gérée, par l'investissement dans un système de calcul et de gestion du risque efficace, moins le coût en fonds propres est élevé, sorte de « prime » donnée aux établissements soucieux d'optimiser la prise en compte de leur différents risques (Sardi, 2012).

Figure 8. Piliers du dispositif prudentiel Bâle II



- **Les exigences en matière de fonds propres (pilier I)**

Le pilier quantitatif du dispositif prudentiel Bâle II est relatif aux exigences de capitaux minimum que doivent détenir les banques en tenant compte de leur exposition à la fois aux risques de crédit, de marché mais aussi aux risques opérationnels (Comité de Bâle, 2003a).

Sur ce premier pilier, plusieurs éléments sont à prendre en compte :
-le ratio de solvabilité global (hérité du ratio Cooke de Bâle I abandonné et remplacé par le ratio dit Mac Donough évoqué ci-après). Il s'agit du calcul du rapport entre les fonds propres de la banque et ses risques pondérés cumulés (risque de marché, opérationnel et de crédit). Ce ratio devant être supérieur à 8%. Le calcul des risques pondérés suppose de définir les exigences en fonds propres pour risques (pondérée x 12,5) pour le risque de marché et le risque opérationnel.
Ce ratio Mac Donough vise donc une sensibilité aux risques affectant réellement la banque là où le précédant ratio (Cooke) définissait un montant de fonds propres minimum en contrepartie des engagements de la banque au sens large (fonds propres + quasi-fonds propres) / Ensemble des engagements > 8 %.

A cela s'ajoutent les éléments relatifs au bilan bancaire ayant un rôle direct dans le calcul de la solvabilité de l'établissement :

-les fonds propres de base : (ou noyau dur, aussi appelé *Tiers One*) fonds propres bruts en retirant certains actifs (hybrides notamment),
-les fonds propres complémentaires (*Tiers Two,* dont le montant atteint 50% des fonds propres de base comme limite),
-les fonds propres surcomplémentaires (il s'agit des fonds propres restant disponibles une fois couverts les exigences relatives aux risques de crédit et aux risques opérationnels ainsi que des fonds propres résiduels tels que ceux concernant les emprunts subordonnés).

Les établissements bancaires peuvent avoir recours à différentes méthodes pour évaluer leur exposition aux risques et les exigences en fonds propres idoines.

Tableau 7. Méthodes d'estimation du risque en banque

Risque de crédit	Risque de marché	Risque opérationnel
Approche standard Notations internes Notations internes avancées	Approche standard Modèles internes	Approche indicateur de base Approche standard Mesures avancées

Pour chaque grande catégorie de risque, comme le décrit le tableau ci-dessus, il existe plusieurs méthodes d'estimation du risque. Les établissements bancaires doivent ainsi choisir entre plusieurs approches :

- Une approche de base, forfaitaire, pour l'ensemble des activités de la banque, calculant le risque de manière agrégée par catégorie,
- Une approche standard, forfaitaire par type de métier de la banque,
- Une approche dite par modèle interne, fondée sur des méthodes de calcul sophistiquées du risque. Dans cette approche, les modèles mis en place par l'établissement sont fondés sur un jeu d'hypothèses complexes et visent une optimisation du calcul des besoins en fonds propres. Dans cette approche, l'établissement définit ses propres techniques et hypothèses en prenant en compte un nombre de paramètres importants (niveau de granularité élevé du risque et dissociation de chaque type d'activité et de sous-activité avec les catégories de risques associées ; recours aux simulations de Monte Carlo, à l'analyse historique ou encore au calcul des valeurs en risques etc.) là où les approches de base et standard sont fondées sur une approche plus simple, reposant sur des paramètres, en partie fournis par le régulateur quant à la manière de calculer le risque.

- **Les exigences en matière de surveillance prudentielle (pilier II)**

L'objectif de ce pilier est de s'assurer que les fonds propres de la banque permettent de supporter l'ensemble des risques de son activité. Ce pilier vise également à encourager le développement et l'amélioration des techniques de gestion des risques. Pour ce faire, il s'agit de développer des filières organisationnelles dédiées à la gestion des risques ainsi que de se doter de politiques de maîtrise des risques. Un autre objectif concerne l'évaluation du respect des standards et exigences quantitatives relatives au premier pilier.

Les exigences relatives à la surveillance prudentielle des établissements bancaires comprennent la mise en place d'un processus interne d'évaluation des fonds propres de la

banque (Internal Capital Adequacy Assessment Process), une revue de ce processus par l'Autorité de Contrôle Prudentiel et de Résolution (ACPR), ainsi que la réalisation de stress test permettant d'évaluer la résistance de la banque à des chocs jugés crédibles ou à des situations extrêmes potentiellement coûteuses.

Ces exigences, davantage qualitatives du pilier II, comprennent la mise en place de fonctions dédiées à l'enjeu que constitue le risque en banque :

- la filière conformité (article 5 du CRBF 97-02): qui a pour mission de réaliser des contrôles et une activité de veille afin de s'assurer que le risque de non-conformité soit sous surveillance,

- le dispositif de contrôle interne de la banque : qui a pour but de mettre sous surveillance les opérations en vue de s'assurer du respect des procédures internes, de vérifier la bonne organisation comptable et du traitement de l'information en interne (dont la vérification de la documentation des activités et procédures : évaluation, enregistrement, conservation des informations), de contribuer à la surveillance des risques. L'objectif du contrôle interne, tel que décrit à l'article 5 du CRBF 97-02, est de contribuer à la sécurité, la fiabilité et l'exhaustivité de la conformité des opérations au règles et procédures.

- D'autres dispositifs sont venus s'ajouter à cela : telle que la lutte contre le blanchiment des capitaux et le financement du terrorisme.

- Mettre en place un système de mesure des risques et de collecte des pertes tel que définis aux articles 17 et 17ter du CRBF 97-02 (prévoyant notamment les critères et seuils de prise en compte des incidents significatifs susceptibles d'affecter la banque).

Le Titre V du règlement CRBF 97-02 portant sur le système de surveillance et de maîtrise des risques est l'une des composantes essentielles du second pilier de Bâle II.
Les dispositions précisent notamment que l'activité de surveillance du risque doit : sur les risques de marché, de crédit et les risques opérationnels, procéder à un examen régulier des risques au regard de l'activité de la banque et de son évolution, réaliser une analyse spécifique

des risques dans une logique prospective (analyse préalable à chaque activité nouvelle ou avant un projet d'évolution), vérifier l'adéquation des procédures de mesure, de contrôle ainsi que des limites de risques et prévoir le cas échéant les adaptations nécessaires.

- **Les exigences en matière de communication et de discipline de marché (pilier III)**

L'arrêté du 20 février 2007 en France précise les dispositions des accords de Bâle II concernant les exigences en matière de discipline de marché.
Il est notamment précisé la liste des informations à publier par les établissements bancaires. Celle-ci comprend des informations en matière de gestion des risques (orientation, objectifs et périmètres de la stratégie de gestion des risques de l'établissement), le champ d'application des actions menées en matière de réduction/prévention des risques, la composition des fonds propres de la banque, l'évaluation ainsi que l'adéquation du capital interne et des fonds propres de la banque au regard de ses activités et de son exposition aux risques, l'exposition de l'établissement au risque de crédit, au risque de marché (titrisation, dérivés, actions, risque de taux sur le portefeuille bancaire etc.), au risque opérationnel, aux risques liés au contexte global de marché. Ces informations comprennent aussi des éléments relatifs aux techniques de réduction du risque de crédit, de marché ainsi que des éléments concernant la méthode de calcul des fonds propres choisie par l'établissement.

- **L'apport complémentaire de Bâle III**

Face à l'insuffisance constatée dans l'application des règles existantes au sortir de la crise de 2007-2008, le comité de Bâle s'est tenu en 2010 pour aménager progressivement ce cadre prudentiel. Cela concerne notamment le cadre macroprudentiel et la couverture des risques systémiques. Bâle III vise à mieux prendre en compte les opérations complexes des établissements bancaires (titrisation complexe, véhicules hors bilan) en limitant le risque de sous-capitalisation.
Pour cela, les accords dits de Bâle III ont imposé un renforcement du capital exigé (actions ordinaires et résultats mis en réserves), des mesures de prise en compte des risques significatifs (notamment ceux liés aux activités de négociation de titres, du risque de contrepartie pour les activités sur dérivés). Le ratio de capitalisation a été relevé sous Bâle III (le niveau minimal de fonds propres des banques en actions ordinaires passant de 2 à 7%, des fonds propres dits de conservation ont été ajoutés au dispositif, un capital dit contra cyclique

s'ajoute également au capital dit réglementaire. L'objectif est en partie de renforcer la résilience des banques face au risque de liquidité, en prévoyant un liquidity coverage ratio, lequel doit permettre à chaque établissement de mieux résister à une crise de liquidité à un horizon court terme (un mois). Un second ratio (net stable funding ratio) ayant pour vocation de renforcer leur résilience à un horizon un an en les incitants à se refinancer sur des ressources plus stables (moins procycliques).

Focus sur la gestion des risques opérationnels bancaires

Comme l'exprime Bon-Michel (2010), le risque opérationnel bancaire (défini précédemment en banque) est un risque par nature multiforme mais étant cependant devenu explicite au travers de la réglementation prudentielle. Pour M.Power (2005), le risque opérationnel est un sujet diffus, voire ambigu au-delà de son caractère multiforme. Cette catégorie de risque est au cœur de la banque mais ne concerne pas uniquement des activités bancaires (voir le tableau des catégories baloises du chapitre précédent). La réglementation prudentielle, suite aux accords de Bâle II, a donné une réelle importance à cette catégorie au sein du dispositif global de gestion des risques de la banque. Cependant, si cette reconnaissance a été une avancée majeure, les accords de Bâle III n'y font pas référence et les nombreuses critiques de Bâle II sur la nécessité d'aller plus loin sur ce sujet n'ont ainsi pas été entendues (Haouat-Asli, 2011).

Les principales dispositions à propos du risque opérationnel tel que défini par le règlement CRBF97-02 prévoient :

- la mise en place d'une filière dédiée à la gestion des risques opérationnels : partant de la direction des risques et devant assurer la gestion centralisée de cette catégorie de risque. cette filière a comme relai des correspondants dédiés dans chaque départements et unités de la banque, assurant la remontée des informations et pouvant s'appuyer sur les managers et opérationnels de la banque (par exemple : le responsable de la sécurité des moyens de paiement, les responsables sécurité, les responsables du suivi des risques RH etc.).

- l'obligation de se doter d'une politique de maîtrise du risque opérationnel dédiée, formalisée (écrite),

- la mise en œuvre des démarches d'identification, d'évaluation et de réduction des risques opérationnels (via la cartographie des risques opérationnels et la collecte historique des pertes).

A ces éléments de contexte général, le Comité de Bâle a progressivement ajouté des bonnes pratiques et recommandations visant une meilleure gestion du risque opérationnel. Ces principales recommandations sont les suivantes :

Des recommandations dédiées au risque opérationnel :

- la définition du risque opérationnel et les principes de base de la gestion de cette catégorie de risque (1998), dès l'origine le Comité évoquait que les principales catégories de risques opérationnels étaient liés à des carences en matière de contrôle interne et de gouvernance d'entreprise. Ce dernier insistait également sur la nécessité d'accroitre la conscience du risque opérationnel ainsi que le fait de mettre en place un cadre de mesure et de surveillance appropriée. Ce rapport évoquait en outre l'importance d'attribuer des responsabilités claires pour gérer le risque opérationnel dans une logique participative comprenant le contrôle interne, l'audit interne, le contrôle financier ou encore le responsable de l'information, en complément des équipes dirigeantes sensées initier cette démarche. Si à l'époque la définition du risque opérationnel précitée n'était pas formalisée, le Comité insistait sur le rôle des erreurs techniques et humaines ainsi que sur la distinction avec d'autres catégories de risques tels que les risques de crédit et de marché.

- 2001-2002-2003 : Au titre des bonnes pratiques alors émergentes concernant la gestion du risque opérationnel. On peut citer notamment le rapport de février 2003 (p.2 et s.) *« saines pratiques pour la gestion et la surveillance du risque opérationnel* » qui indique : *« Le Comité reconnait que le concept de risque opérationnel prend des significations très diverses dans la profession bancaire et, par conséquent, aux fins du contrôle interne, les banques peuvent donc décider d'adopter leur propre définition de ce risque. Quelle que soit la définition retenue, il est crucial pour une gestion et un*

contrôle efficace du risque opérationnel que les acteurs en aient une compréhension parfaite ». Cela atteste du caractère interprétatif et adaptatif de la norme de contrôle du risque opérationnel. Le comité, qui fournit également des exemples de cas de survenance de risque opérationnel (voir l'annexe 5 - Exemples de risques opérationnels-Comité de Bâle, 2003), reconnait que le risque opérationnel est antérieur à la réglementation prudentielle, les banques ayant toujours cherché à réduire les risques de fraudes ou les erreurs de traitement des transactions. Cependant le Comité insiste sur le fait que, par le passé, les banques se basaient principalement, voire presque exclusivement, sur les dispositifs de contrôle interne par activité ainsi que sur la fonction d'audit interne pour réduire ces risques. Une telle approche est à dépasser. Le Comité préconise l'apparition de fonctions dédiées travaillant en lien avec le contrôle interne et l'audit interne « en créant un environnement adéquat pour la gestion du risque opérationnel » reposant sur l'identification, l'évaluation, le suivi des risques opérationnels et la mise en place de mesures d'atténuation-traitement de ces risques. Le Comité insiste encore sur le rôle crucial de vigilance des régulateurs et autorités de tutelle ainsi que sur la nécessité d'intégrer cette catégorie de risque dans le processus global de communication financière. Dans son rapport de 2003, le Comité détail les principes et saines pratiques à mettre en œuvre. Ces principes (Annexe 6 - Principes de gestion du risque opérationnel) sont également déclinés dans la suite du rapport au travers de conseils pratiques pour la création d'un environnement adéquat de gestion du risque opérationnel. Ces éléments visent à la fois à guider les établissements dans un contexte récent d'objectivation du risque opérationnel, et en vue de préparer ces derniers à l'intégration, dans le cadre prudentiel des enjeux de gestion du risque opérationnel.

- En 2003, le transfert des risques opérationnels par des mécanismes financiers et notamment assurantiels est évoqué par le Comité comme une pratique déjà existante mais à développer par les établissements bancaires,

- En 2004 : dans l'optique des accords de Bâle II, des éléments relatifs aux méthodes avancées de gestion du risque opérationnel (AMA) sont détaillés par le Comité qui évoque une opportunité pour les banques de renforcer la connaissance du risque opérationnel, (concernant son coût en fonds propres principalement),

- En 2005, le Comité précise les éléments de détails sur la manière d'assurer la continuité d'activité, ce qui constitue en soi, un axe de gestion des risques opérationnels,

- En 2010, le Comité fournit, tout comme en 2003, des éléments de détails sur l'assurance des risques opérationnels et les bonnes pratiques en matière de couverture et de transfert de ces risques,

- En 2011 : le Comité produit une étude synthétique sur les effets des méthodes avancées de gestion du risque opérationnel ainsi qu'une étude reprenant les avancées des principes et bonnes pratiques en matière de gestion du risque opérationnel. Ces derniers étant davantage axés sur le rôle de la gouvernance d'entreprise et du management dans la création d'un environnement de gestion du risque opérationnel. Ils insistent davantage sur le rôle des contrôles mais aussi sur la connaissance que doivent avoir les différentes parties prenantes des efforts réalisés ou restants à faire au sein d'une banque face au risque opérationnel.

Des recommandations relatives à la gestion des risques mais concernant indirectement les risques opérationnels sont également formulées :

- des éléments relatifs aux risques liés à l'externalisation des services financiers (2005) pouvant engendrer d'autres risques, notamment opérationnels,

- Le fait de définir une meilleure gouvernance des organisations bancaires comme moyen de maîtrise des risques constitue un axe global de progrès tel que l'évoque le Comité en 2006,

- en 2009 le Comité a émis un ensemble de recommandations sur la mise en place du second pilier, relatif à la surveillance prudentielle des établissements bancaires (objectifs du pilier, transposition concrète des exigences de Bâle II sur ce domaine, partage des rôles et responsabilités entre gouvernance des établissements et implications des fonctions dédiées et non dédiées à la gestion des risques),

- ces recommandations concernent notamment la collecte et l'agrégation des données relatives aux risques (2013) : le renforcement de la capacité des établissements bancaires à agréger leur données participe à la connaissance interne des risques et contribue à un meilleur calcul de ces derniers, in fine l'objectif est de renforcer la solvabilité desdits établissements. Ces recommandations interviennent dans un contexte où les établissements bancaires ont, depuis Bâle II, fait de nombreux efforts pour collecter des données relatives aux pertes associées aux risques. Ces mêmes données, importantes en nombre, doivent pourvoir être utilisées plus efficacement mais aussi être mieux collectées pour rendre le dispositif d'information sur le risque effectif, c'est-à-dire permettant d'aider et d'inciter à la prise de décision au sein des banques. A cet effet, sont mises en place des normes de collectes et d'agrégation des données permettant de faciliter la collecte et la comparaison en interne au sein d'une banque mais aussi entre établissements pour les instances de régulation (notamment mieux savoir quels sont les établissements les plus significativement impactés par un évènement de risque ou une crise). Ce type de principes permettra encore de mieux connaitre les expositions aux risques par région, par pays, par activités et par type d'instruments financiers.

3.Le cadre prudentiel en assurance

Ce paragraphe, dans la continuité des éléments relatifs au secteur bancaire, détaille le cadre prudentiel et normatif relatif au contrôle des entreprises d'assurance.

3.1. De Solvabilité I à Solvabilité II

3.1.1.Le cadre de la gestion des risques des organismes d'assurance

Depuis les années 1970, le secteur de l'assurance dispose d'un cadre de régulation prudentielle en assurance-vie et en assurance non-vie (faire en sorte que les assureurs aient les ressources financières pour faire face à leurs engagements c'est-à-dire pouvoir indemniser les assurés en assurance de biens et de responsabilités et faire face aux demandes de récupérations des fonds placés en assurance-vie). Il s'agit notamment des directives

européennes de 1973 (assurance non-vie), 1979 (assurance vie), 1992 et 1995 sur les principes fondamentaux et régimes de surveillance en assurance.
A cela s'ajoute le corpus dit Solvabilité 1 faisant suite à plusieurs directives adoptées en 2002.

Pour Dreyfuss (2012, p.18-19), Solvabilité I est un régime prudentiel fondé sur les directives des années 1970 et qui, bien qu'ayant été révisé en 2002, ne semblait plus adapté aux enjeux économiques, financiers et juridiques de l'assurance (mondialisation et essor des assureurs internationaux, apparition de nouveaux risques couverts par les assureurs et postérieures à Solvabilité I, développement de nouvelles exigences réglementaires dans les différents pays d'Europe et complexification des modèles mathématiques de calcul des risques, utilisation accrue de l'information et de l'ingénierie financière, évolution de la distribution d'assurance et essor de la bancassurance etc.).

Pour ces raisons, les nouvelles générations de directives ont eu pour but de faire évoluer ce cadre prudentiel pour passer d'une logique forfaitaire de calcul et de provisionnement du risque (dans laquelle le contrôle interne des risques n'était pas spécifié en tant qu'exigence face aux risques) à une logique intégrée renforçant les aspects qualitatifs de contrôle du risque et de reporting.

Les textes issus de Solvabilité I ne comportaient que peu d'exigences en matière de gouvernance et le contrôle prudentiel des groupes d'assurance n'était pas spécifié (il se limitait alors au contrôle des entités juridiques et ne prenait pas suffisamment en compte la réalité économique de groupes d'assurance ayant fusionnés successivement pour atteindre une taille critique et développer de nombreuses branches d'activités).

Face à de nombreuses critiques de ce cadre prudentiel au niveau européen (jugé trop simpliste, ne prenant pas suffisamment en compte la réalité des risques de chaque assureur ou de leur structure organisationnelle, limitant le développement du marché unique européen), la directive européenne n°2009/138 du 25 novembre 2009 a entendu modifier le régime prudentiel dans ce secteur.

La directive dite Solvabilité II (relative à l'accès aux activités d'assurance et de réassurance et à leur exercice) avait initialement pour but d'entrer en application en 2012, puis 2013. L'application de la directive est désormais applicable au 1er janvier 2016 (suite à la

confirmation dans le cadre du dispositif normatif Omnibus II) pour des raisons pratiques d'adaptation, tout comme la réforme Bâle 2 du milieu des années 2000 dans le secteur bancaire (en France adaptée par le règlement CRBF 97-02 et l'arrêté de février 2007).

Cependant, le régulateur (Autorité de Contrôle Prudentiel et de Résolution) s'inscrit dans la mise en œuvre progressive de cette directive en France dans le cadre d'un travail commun d'adaptation avec les représentants des assureurs (FFSA, GEMA, FNMF).

Le cadre prudentiel du secteur de l'assurance est fondé sur trois niveaux conformément au processus dit « Lamfalussy »[16] :

- un premier niveau relatif à la directive Solvabilité II qui prévoit une transposition identique par chaque Etat membre de l'Union Européenne sans la possibilité de maintenir des règles nationales distinctes,

- un second niveau relatif à des actes délégués issus de la Commission Européenne ou de l'Autorité Européenne des assurances et des pensions professionnelles (EIOPA, anciennement CEIOPS), via un règlement européen directement applicable dans le droit national,

- un troisième niveau relatif à des standards techniques et aux orientations réglementaires et à un ensemble de recommandations fixées par l'EIOPA.

Au-delà de ces éléments, une directive d'adaptation, dite « Omnibus 2 », a été mise en place via les instances européennes en vue d'adapter la directive Solvabilité II dans le contexte du système européen de surveillance et de stabilité financière.

[16] Du nom d'Alexandre Lamfalussy, ayant occupé des fonctions de représentations et de direction au niveau européen.

3.1.2.Objectifs et composantes de la directive Solvabilité II

- **Les objectifs de la directive** peuvent se décliner comme ci-après :

- améliorer la protection des assurés en renforçant la solidité financière des assureurs, trouvant un équilibre en protection des assurés et coût du capital pour les assureurs (coûts des fonds propres immobilisés pour couvrir les risques pris en charge),

- promouvoir une meilleure réglementation dans le secteur de l'assurance,

- harmoniser les règles prudentielles en Europe,

- responsabiliser les assureurs par une meilleure gestion des risques.

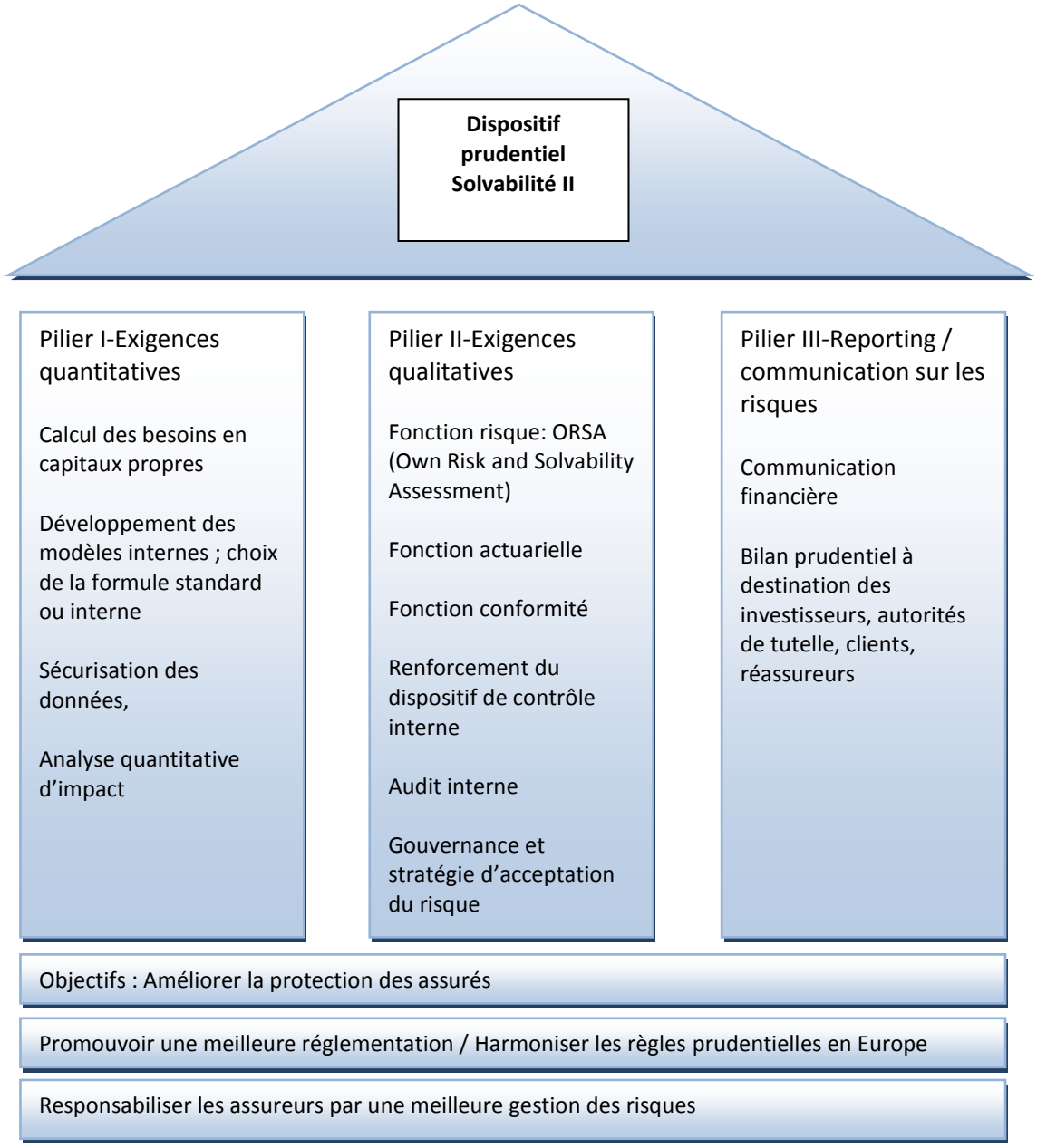
- **Les éléments clés de la directive**[17]

Afin d'assurer ces objectifs, la directive Solvabilité II comprend différents éléments relatifs au calcul des engagements, à la maîtrise des risques ainsi qu'à la gouvernance des sociétés d'assurance (Fonction AMSB pour administrative management and supervisory board[18]). Si la conformité des sociétés d'assurance est envisagée pour le 1er janvier 2016, les prises de décisions effectives relatives aux différents chantiers de cette directive doivent être prises au plus tard pour le 31 mars 2015[19]. En assurance, la gestion des risques représente un réel chantier dans la mesure où l'enquête annuelle de l'ACPR révélait à fin 2013 que 50 % des mutuelles se disaient prêtes sur ce sujet, contre 43 % de sociétés d'assurances mutuelles et 78 % de sociétés anonymes et d'institutions de prévoyance[20].

La directive Solvabilité II comporte trois piliers édictant des corps de règles à destination des sociétés d'assurance. L'architecture de ce projet en cours de mise en œuvre dans les organismes d'assurance (sociétés d'assurance, mutuelles, institutions de prévoyance etc.) est proche de la réglementation bancaire et se décline selon le schéma ci-après.

[17] Source : Site internet de l'EIOPA : rubrique « publications » – Technical Standards.
[18] Il s'agit de l'organe de contrôle et de surveillance des risques de l'entreprise d'assurance, cette fonction peut être assumée par le Conseil d'Administration ou de Surveillance, ou encore par un organe de surveillance créé ex nihilo au sein de l'entité.
[19] La Tribune de l'assurance, n°187, janvier 2014, *Quand l'évolution de la gouvernance coince*.
[20] Les mutuelles sont les sociétés affiliées au code de la mutualité. Les sociétés anonymes au code des assurances et les institutions de prévoyance au code de la Sécurité Sociale.

Figure 9. Dispositif prudentiel Solvabilité II



- **Les exigences quantitatives (pilier I)**

Les règles relatives aux exigences quantitatives concernent :

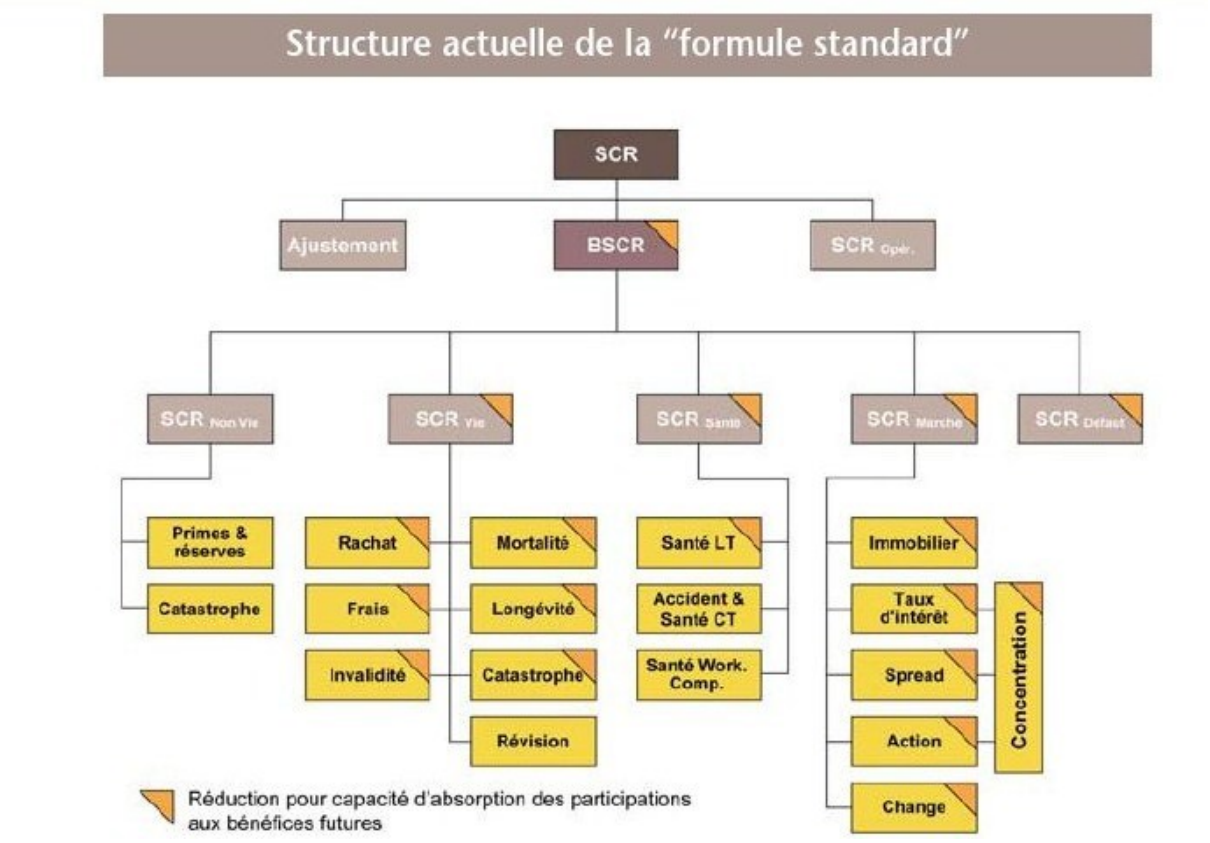
-l'allocation des fonds propres et les exigences de capital. Il s'agit d'évaluer le « capital de solvabilité requis » : cela consiste en un montant de fonds propres visant pour l'assureur à absorber des pertes non prévues, ce qui tend à garantir la sécurité de l'épargne des assurés ainsi que des garanties octroyées aux souscripteurs de contrats d'assurance. En cas de choc significatif ayant consommé ces montants de fonds propres, l'assureur doit mettre en œuvre

des plans d'actions rapides et concrets, afin de rétablir ce niveau de fonds propres en tenant compte des risques auxquels est exposé l'assureur (ce qui suppose une quantification précise de ces derniers en termes de probabilités de survenance et d'impact financier de manière prospective).
Un dernier filet de sécurité est constitué par le minimum de capital requis : il s'agit d'un montant minimal de fonds propres qui, dès qu'il est franchi (l'assureur se retrouve en dessous de ce montant), est le signe d'une atteinte réelle et sérieuse à la solvabilité de l'assureur. Une fois ce seuil franchi, il nécessite l'intervention des autorités prudentielles.

Si ces exigences s'appliquent indépendamment de modèles financiers, les assureurs ont le choix entre modèle standard, modèle interne et modèle interne simplifié afin d'optimiser l'évaluation de leurs risques et donc des fonds propres à allouer en garantie de ces derniers.
La structure de calcul des risques sous Solvabilité II substitue en effet une approche de calcul par type de risque à l'approche forfaitaire de Solvabilité I (approche globale du coût de l'exposition au risque et provisionnement agrégée). Sous Solvabilité II, on retrouve le calcul des fonds à allouer de manière agrégée mais sur la base des différentes sous catégories de risque qui suppose elles-mêmes un calcul pointu des types de risques. Le schéma ci-après illustre cet enjeu pour la formule dite standard (les formules dites internes dépendent de chaque assureur et de son exposition au risque qu'il évalue et défini selon des critères spécifiques). On constate que les principaux risques à prendre en compte pour les assureurs indépendamment sont les risques liés aux catastrophes et aux différents accidents en assurances de dommages et des responsabilités, mais aussi les risques liés aux activités d'assurance vie, de couverture santé des assurés ainsi que les risques financiers liés à la détention des actifs des assureurs (actions, obligations, risque de change, taux d'intérêt etc.)

Ces risques sont pris en compte par des montants de fonds propres par type de risques : les risques financiers (risque action, de contrepartie, de taux, de spread, risque immobilier), les risques de catastrophe (impact d'une pandémie, catastrophe technologique majeure etc.), les risques liés à la souscription en assurance vie, non-vie, santé, les risques opérationnels. Un ajustement est également pratiqué (notamment pour tenir compte des impôts différés et de l'effet de diversification en risque de marché).

Figure 10. Le calcul des risques sous Solvabilité II, exemple de la « formule standard »[21]



-la problématique des **provisions techniques** (sommes en garanties des engagements des assureurs telle que définie à l'article 45 de la directive Solvabilité II). Les exigences relatives aux provisions techniques supposent que ces dernières soient prudentes, fiables et calculées de manière objective. Les provisions doivent donc être calculées sur la base de leur valeur actuelle en tenant compte également des informations du marché (valeur actuelle probable des flux futurs calculée sur la base d'hypothèses devant être réalistes : évolution crédible et réaliste de la courbe de taux sans risque).

Dans ce cadre, l'assureur doit déterminer une marge de risque qui a pour but de couvrir les risques liés aux passifs et de permettre la liquidité de l'assureur face à ses engagements[22].

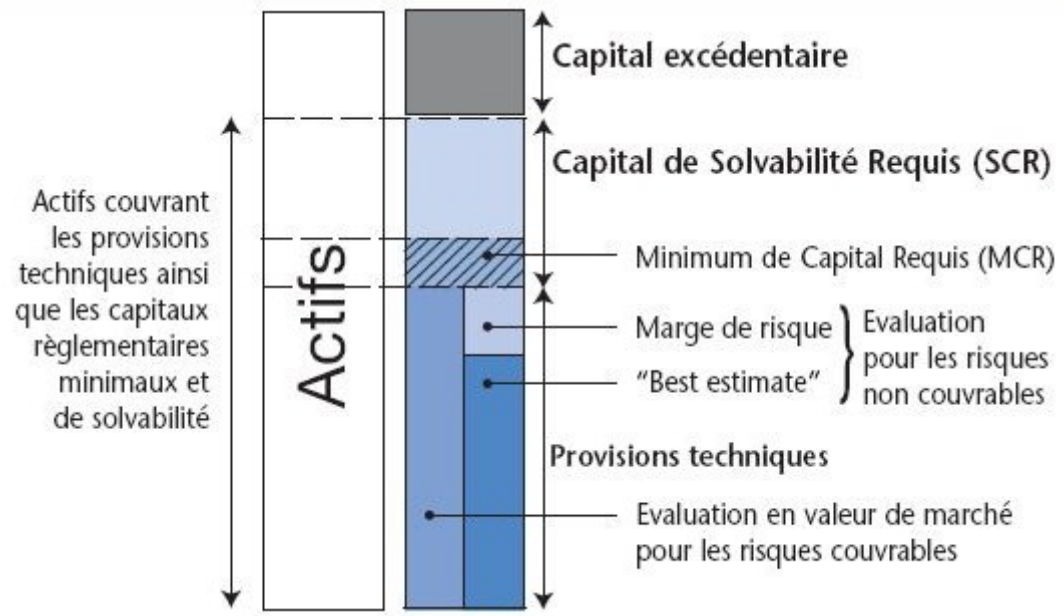
-les actifs à détenir par les assureurs pour couvrir leurs différents risques (équilibrage entre actifs et passifs). La gestion actif-passif des assureurs doit être renforcée afin de mieux

[21] Source : *Aon Risk Consulting, Etude Solvabilité II*

[22] Plusieurs méthodes statistiques ont existé pour calculer la marge de risque basées sur les distributions de probabilité et sur différentes estimations : current estimate, central estimate et best estimate. Une méthode basée sur le coût du capital face à la liquidation des engagements a été retenue in fine.

prendre en compte les flux futurs auxquels ces derniers sont confrontés (retraits massifs des épargnants, vagues importantes d'indemnisation ou de résiliation à échéance, catastrophes majeures ou d'ampleur couverte par l'assurance). Il s'agit de voir dans quelles mesures les actifs compensent les différents passifs de l'assureur.
Ces différents éléments du pilier quantitatif se résument selon le schéma ci-après :

Figure 11. Exigences quantitatives sous Solvabilité II (source Aon Risk Consulting Report)



- **Les exigences qualitatives (pilier II)**

Le second pilier de la directive insiste sur la capacité des sociétés d'assurance à maîtriser leurs risques tout en veillant à une adéquation entre leur capitalisation et leur exposition à ces derniers. Cela implique de prendre en compte les calculs réalisés dans le cadre du pilier I et d'identifier si les risques pris en compte sont en concordance avec la réalité de l'exposition de l'entreprise. Cette approche, plus qualitative des risques, cherche encore à déterminer le profil de risque de l'assureur, eu égard à sa stratégie commerciale et financière.

Ce pilier, visant la protection des assurés, se fonde sur les éléments suivants :

- mettre en place un processus d'identification et d'évaluation des risques de manière dynamique et évolutive dans le temps : en réalisant une cartographie globale des risques et des cartographies des risques par périmètre d'activité et type de risque ainsi

qu'en collectant les pertes de manière chronologique au sein de l'entreprise (base incidents).

- des fonctions dédiées à formaliser, participant à la maîtrise du risque : il s'agit notamment d'avoir une fonction risque dédiée (l'ORSA ou Own Risk and Solvability Assessment), de formaliser les fonctions clés en matière de risques. Il s'agit de la fonction actuarielle ainsi que l'audit interne, de la fonction de conformité et la fonction de gestion des risques (comprenant le dispositif de contrôle interne de l'entreprise souvent préexistant aujourd'hui). Ces fonctions dédiées constituent le système de gouvernance de l'assureur tel que défini par le considérant 29 de la directive, lequel précise que certains risques sont difficilement quantifiables et supposent des mesures de traitement passant nécessairement par une gouvernance formalisée au travers des fonctions risques, audit interne, actuariat et conformité.

- l'assureur doit encore se doter d'une méthodologie de contrôle dédiée (définir des plans de contrôle en fonction des risques identifiés ainsi que des procédures de contrôles, documenter les différents contrôles).

A titre illustratif, telle que l'Autorité de Contrôle Prudentiel et de Résolution (ACPR) le définit sur son site: *« L'ORSA est un processus interne d'évaluation des risques et de la solvabilité par l'organisme (ou le groupe). Il doit illustrer la capacité de l'organisme ou du groupe à identifier, mesurer et gérer les éléments de nature à modifier sa solvabilité ou sa situation financière. Aussi, sa déclinaison opérationnelle en fait-elle un outil stratégique de premier plan ».* L'exercice ORSA, ou évaluation prospective des risques propres, consiste à décrire la situation de l'assureur à une date donnée, sa stratégie globale et la déclinaison de ses anticipations stratégiques au travers d'hypothèses (en matière d'activité courante, en matière financière, concernant sa structure de gouvernance, son organisation en matière de gestion et de suivi des risques). Différents scénarios de risques sont ainsi décrits. Ces scénarios sont relatifs à des risques sur le cœur de métier de l'entreprise d'assurance (dérive de la sinistralité en santé, impact de la réglementation, hausse des frais de gestion etc.) ainsi que des risques financiers (risque de taux, risque action, risque sur le marché immobilier). Des projections sont réalisées afin d'étudier l'impact de ces risques sur la santé financière de l'assureur.

Sur la base des scénarios de risques précités, il s'agit d'étudier la résilience de l'assureur (au sens de sa capacité à faire face à des évènements dommageables) au travers d'actions adaptées et compte tenu de sa situation financière. Pour chaque scénario de risque, des actions sont à mettre en œuvre sont détaillées et une couverture des risques en montants de fonds propres est évaluée.

L'évaluation de l'ORSA est fondée sur la cartographie globale et transversale des risques, qui confronte les approches « top down » et « bottom up », à travers :
- un exercice au moins annuel visant à évaluer la solvabilité de l'organisme au regard de son profil de risque ;

- un exercice préalable à chaque décision stratégique, selon des critères propres à l'organisme ou consécutif à une évolution significative de l'environnement de l'organisme (ORSA « ponctuel »). L'objectif vise à s'assurer de la cohérence de la décision avec l'appétence au risque défini par l'organisme.

Au-delà des orientations globales fixées aux articles 41, 44 et 45 de la directive Solvabilité II, l'EIOPA a entendu fournir des orientations afin de guider les sociétés d'assurance dans la mise en œuvre de leurs modèles d'évaluation et de gestion interne des risques (EIOPA, 2013). Ces recommandations insistent notamment sur le rôle organisationnel et de sensibilisation des fonctions clés garantissant la maîtrise des risques. Dans le cadre du pilier II de la Directive Solvabilité II, sont définies et décrites ci-après :

-**Fonction gestion des risques** : La fonction de gestion des risques, telle que décrite à l'article 44 de la directive cadre, fait partie des structures dites de « pilotage », qui apportent une garantie sur la gouvernance des risques au sein de l'entreprise d'assurance. Elle fournit une vision transversale et synthétique des risques majeurs auxquels est exposée la société et veille à ce que le niveau de risque pris soit cohérent avec les orientations et les objectifs définis par le Conseil d'Administration (ou le Conseil de Surveillance le cas échéant). Elle assume, à ce titre, les aspects suivants de la politique de gestion des risques :

- relation avec les directions opérationnelles, « propriétaires des risques » ;
- coordination / réalisation de la cartographie des risques pour l'ensemble des risques ;
- suivi de la mise en œuvre des dispositifs de maîtrise des risques ;

- information des dirigeants ;
- organisation de la continuité des activités concernées par des risques dont la gravité remettrait en cause le fonctionnement pérenne de l'entité.

Également, au sein de la fonction gestion des risques, la fonction centrale de contrôle interne s'appuie sur un réseau de référents de maîtrise des risques (référent pour chaque activité, ayant une autorité reconnue), en charge des risques sur leurs activités, les actions de maîtrise associées, leurs plans de contrôle, mais constituent aussi des relais d'information / formation et des forces de proposition et un support de l'audit interne et des directions relativement aux enjeux de conformité.

-**Fonction actuarielle :** La fonction actuariat, telle que décrite à l'article 48 de la directive cadre, est en charge de :

- coordonner le calcul des provisions techniques ;
- contribuer à la mise en œuvre du système de gestion des risques (notamment dans le cadre de l'ORSA) ;
- donner un avis sur la politique générale de souscription et sur l'adéquation des accords de réassurance.

-Fonction conformité : La fonction conformité, telle que décrite à l'article 46 de la directive cadre, est en charge de la gestion du risque de non-conformité (Vérification de la conformité aux lois, règlements, procédures) :

- identification / évaluation, mise en place d'un plan de conformité et animation ;
- conseil aux dirigeants / formation des collaborateurs,
- veille interne / externe.

Les missions de la fonction de vérification de la conformité sont les suivantes :

- veille sur les obligations réglementaires en matière de contrôle interne ;
- assurance sur la maîtrise des risques opérationnels (base incidents) ;
- cohérence d'ensemble de la cartographie des processus et des risques ;
- communication interne et externe ;

- diffusion de glossaire et de guide méthodologique du contrôle interne ;
- proposition de grands axes pour la formation (salariés et administrateurs).

-Fonction d'audit interne : La fonction d'audit interne, selon l'article 47 de la directive cadre, constitue une structure de supervision : elle exerce une fonction de vérification sur la gouvernance, les systèmes et les opérations de l'assureur, pour apporter une expertise indépendante sur la conformité de l'organisme aux dispositions réglementaires et aux orientations données par l'assemblée générale.

Son rôle consiste à réaliser des diagnostics et à émettre des recommandations, synthétisées et communiquées à son entité de rattachement au moins une fois par an. En cas de défaillance significative, la cellule a un devoir d'alerte immédiat. Elle exerce ainsi les contrôles dits de « 3ème niveau ». Les auditeurs fonctionnent sur la base d'une charte d'audit interne. Chaque mission fait l'objet d'une lettre de mission (thème, périmètre, objectifs, intervenants, date de début et durée prévue de la mission, moyens spécifiques alloués le cas échéant) cosignée par un Directeur et le Comité d'audit. Les rapports d'audit sont soumis à revue contradictoire par les entités auditées.

Sous Solvabilité II, l'organisation de la gestion des risques est donc conçue en plusieurs phases : une structuration au niveau des dirigeants qui doivent avoir une vision des risques de l'entreprise lors des décisions stratégiques. Ces derniers doivent recevoir des recommandations de la fonction gestion des risques (dont le rôle est de coordonner les actions de réductions/préventions du risque) et de contrôler la bonne application de la politique de maîtrise des risques définie au sein de l'entreprise. Cela constitue un premier niveau. Un second porte sur le contrôle des risques des activités opérationnels et supports.

Le rôle de la politique de maîtrise des risques dans la philosophie globale de Solvabilité II : L'article 44, de la directive Solvabilité II, étant relatif à la fonction de gestion des risques précise que ladite fonction doit être mise en place de manière à faciliter la mise en œuvre du système de gestion des risques, de contrôles dédiés ou non mais intégrant le facteur risque et une stratégie globale de gestion du risque (Dreyfuss, 2012).

Ses principaux axes sont : le contrôle de l'application des politiques de gestion des risques, l'identification des déficiences potentielles et avérées du système de gestion des risques, la coordination des actions de gestion et de réduction des risques et son adéquation à l'exposition de la société d'assurance aux situations génératrices de pertes.

A cet effet, la directive prévoit la formalisation de politiques écrites assorties de procédures claires de prise de décision en matière de gestion des risques (et des crises). Cette politique doit préciser les objectifs de gestion du risque (objectif de la fonction mais aussi orientation du système global de gestion dédié), les principes clés et les limites de tolérance par catégorie de risque.

La politique de risque doit également comprendre une répartition des responsabilités au sein de la société d'assurance.

Le document écrit de politique de risque doit classer les risques par catégories mais aussi par seuil de tolérance. Il doit également être fait référence aux périmètres d'activités concernés pour chaque catégorie ainsi qu'aux fonctions en charge de chaque périmètre.

En indiquant notamment qu'il est indispensable de prendre en compte chaque catégorie de risque, que celle-ci ait fait ou non l'objet d'une quantification, en précisant la nécessité d'une approche prospective du risque, favorisant l'anticipation des risques dans l'organisation, l'EIOPA insiste sur le rôle central des actions de gestion des risques ainsi que la promotion d'une gouvernance effective des risques. L'EIOPA précise alors les contours de la politique d'évaluation prospective des risques (EIOPA, 2013, p.8). Cette politique doit comprendre notamment le fait de :

- définir et mettre en œuvre une politique d'évaluation prospective des risques (politique ORSA),
- décrire et mettre en place les processus et procédures pour mener à bien cette évaluation prospective,
- établir des corrélations entre le profil de risque de l'établissement et les limites de risque fixées dans le cadre de la politique.

- **Les exigences en matière de reporting et de communication (pilier III)**

La directive Solvabilité II distingue la communication à destination du superviseur et la communication en direction du public. Ce troisième pilier (parfois appelé « Reporting et discipline de marché ») suppose en effet d'établir une communication concernant son exposition au risque ainsi que les mesures prises chaque année en vue de la réduire. Il s'agit d'informations prudentielles harmonisées (ne relevant toutefois pas du domaine public) permettant au superviseur de réaliser aisément des comparaisons entre assureurs mais surtout de pouvoir être certains que tout est mis en œuvre pour garantir une gestion prudente des risques au sein de chaque société d'assurance. Ces informations concernent le système de gouvernance appliqué par les sociétés d'assurance, les principes d'évaluation mis en œuvre pour mesurer la solvabilité face aux différentes activités de l'entreprise, la structure du capital, le besoin en capital et sa gestion, l'exposition aux catégories de risques. Ces informations, à destination du superviseur, doivent permettre de répondre au besoin accru de contrôle du superviseur (aux niveaux macro et micro-prudentiels) et faciliter la réalisation des contrôles (Buckham et al., 2010).

En réalisant ces reporting sur des éléments de gouvernance des risques, de techniques de calcul du risque et de mise en ouvre des dispositifs de contrôle, l'assureur doit établir de manière claire au superviseur les démarches réalisées en interne en vue de maîtriser les risques. Cela comprend également la mise en œuvre dans le temps des recommandations faites par le superviseur.

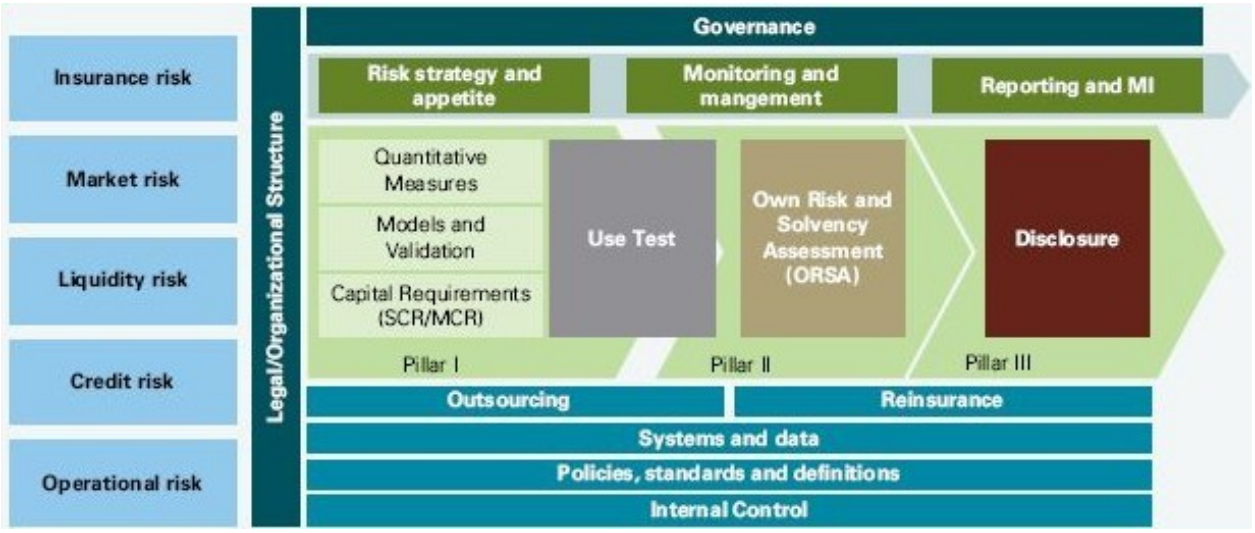
La communication vers le public (investisseurs et actionnaires, agences de notation, presse spécialisée, assurés) telle qu'évoquée au considérant 38 de la directive poursuit un objectif de transparence. Les sociétés d'assurance doivent ainsi rendre publiques les informations relatives à leur solvabilité et à leur situation financière ainsi que les dégradations ou améliorations ayant pu affecter ces éléments. Les assureurs peuvent, au-delà de ces informations obligatoires, publier davantage d'informations sur une base volontaire.

3.2.Focus sur la gestion des risques opérationnels en assurance

Le risque opérationnel sous Solvabilité II est défini comme *« le risque de pertes résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'évènements extérieurs ».* Il s'agit d'une définition sensiblement proche de celle du domaine bancaire.

La directive Solvabilité II apporte toutefois peu d'éléments quant à la question spécifique des risques opérationnels et à sa gestion. Cette dernière est principalement envisagée au travers des politiques de gestion des risques telles que définie dans le paragraphe précédent. Elle est fréquemment intégrée en tant qu'enjeu transverse mais néanmoins distinct à côté des différents risques d'une entreprise d'assurance : risques d'assurance (risques de l'activité non-vie, de l'activité vie ou risques en assurance santé), risques en matière financière (liquidité, marché, crédit).

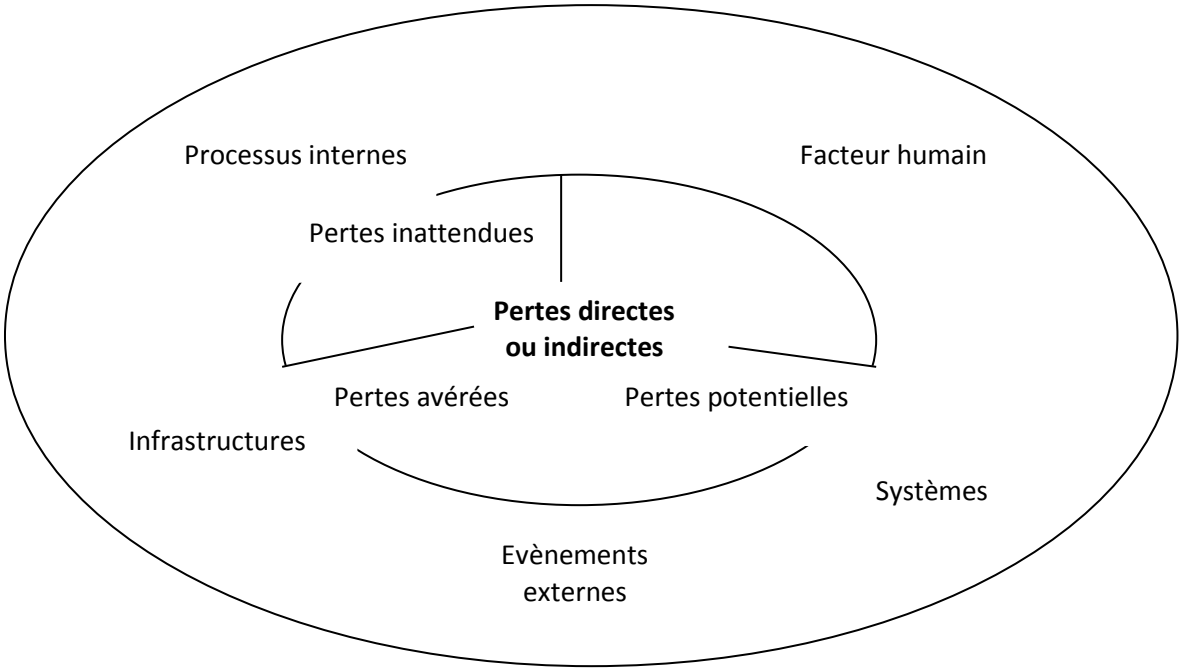
Figure 12. Positionnement du risque opérationnel dans l'architecture risque (Etude 2011 KPMG, Solvency II



Pour Torre-Ensico et Barros (2013) le risque opérationnel en assurance, bien que n'étant pas nouveau, doit être envisagé à la lumière de la réglementation Solvabilité II comme un sujet bien plus détaillé que ce à quoi renvoient les rares précisions sur ce sujet. Le risque opérationnel, même s'il fait consensus quant à sa définition en assurance, suppose bien des débats quant à son périmètre (voir la figure ci-après). Les auteurs insistent notamment sur le champ élargi qu'il recouvre : problématiques environnementales, enjeux de ventes et de

manquement au devoir d'information et de conseil, discrimination, harcèlement au travail, réalisation d'alliances entre assureurs, problématiques de chaine de valeur et de maîtrise de la distribution des contrats, gestion des ressources humaines et risques psychosociaux, maîtrise de la politique de souscription et de ses procédures, bonne application et adéquation des traités de réassurance, risques sur les activités externalisées (courtage et intermédiation d'assurance, gestion déléguée des contrats).

Figure 13. Risques opérationnels en assurance, d'après Torre-Ensico, Barros, 2013



Ce périmètre élargi comprend donc plusieurs catégories que l'on retrouve en matière bancaire (voir le second paragraphe du chapitre) et peut se diviser entre les risques liés aux processus internes (inadaptées, non précisés), aux enjeux de facteur humain (erreur de traitement d'information, non transmission d'information, comportements frauduleux), aux infrastructures et systèmes (inadaptés) ainsi qu'à des évènements externes.

On saisit ainsi la diversité des enjeux que recouvre le risque opérationnel : des risques de fréquences, très nombreux et de faible coût unitaire, tels que les risques relatifs aux défauts de qualité interne ou externe, aux impacts des réclamations clients, aux fraudes aux prestations d'assurance ; mais aussi des risques opérationnels majeurs à l'instar des risques de type pandémie, des risques d'interruption durable de l'activité suite par exemple à une catastrophe naturelle, à un incendie d'ampleur, à une fraude majeure etc.

Tableau 8. Périmètre du risque opérationnel en assurance

Périmètres	Exemples de risques opérationnels
Processus internes	Processus de souscription non formalisés, acceptation et interdiction de couverture d'assuré non précisée ou mal définie, plafond d'indemnisation non appliqué/équivoque, gestion des contrats défaillantes/non structurée.
Infrastructures	Infrastructures inadaptées suite à une réorganisation, locaux vétustes/insuffisants, architecture SI mal conçue.
Evènements externes	Catastrophes naturelles : cru centennale, incendie affectant les locaux de l'assureur.
Facteur humain	Fraude interne (complicité d'un collaborateur), fraude d'un intermédiaire d'assurance (agent, courtier), participation d'un collaborateur aux pratiques de blanchiment d'argent.
Systèmes	Systèmes d'information inadaptés, non opérationnels, présentant une défaillance de longue durée ou de multiples défaillances sur courte durée.

Exemple : le risque opérationnel lié à la fraude

Dans cette optique de gestion des risques, une société d'assurance mettra en œuvre des moyens afin d'identifier et de mesurer son risque de fraude.
La fraude peut se définir comme tout acte ou comportement commis intentionnellement par une personne ou un groupe de personnes afin d'obtenir un avantage ou un bénéfice de façon illégitime, illégale ou illicite.

Une fraude à l'assurance sera par exemple :

- **Fraude interne :**

- Un collaborateur de la société d'assurance ayant connaissance des procédures internes contourne ces dernières en vue d'obtenir une somme de manière indu.
- Un collaborateur en charge de l'indemnisation fera profiter à des proches ayant subis un sinistre, d'une indemnisation supérieure à ce que leur contrat stipule en maquillant l'action réalisée.
- Un intermédiaire de la société d'assurance fera profiter uniquement à des proches des rabais tarifaires dont il dispose.
- Un intermédiaire vendra des produits plus rémunérateurs (commission) au détriment de l'intérêt du client.
- Usage par un collaborateur du système d'information de l'assureur pour vendre à un concurrent des informations client.

- Versement à tort d'indemnités journalières en prévoyance à une entreprise n'étant plus cliente de l'assureur.

- **Fraude externe :**

- Un assuré fera une fausse déclaration suite à un sinistre incendie. Il déclarera non seulement des biens ayant réellement brulés lors du sinistre mais aussi d'autres biens non touchés par ledit sinistre, prétextant avoir également perdu les factures lors de l'incendie.
- Un assuré n'ayant subi aucun vol fera une fausse déclaration en vue d'être indemnisé.
- Emission de faux justificatifs pour obtenir une réduction de cotisation d'assurance.
- Omission de fournir des documents permettant de mettre à jour la situation d'un assuré (reprise d'activité non déclarée pour un assuré bénéficiant d'une indemnisation en retraite).

Le coût de la fraude pour les assureurs : D'après Audouin et Ricchiuto (2013)[23], le coût de la fraude à l'assurance dépasse aujourd'hui les 130 millions d'euros chaque année (contre une cinquantaine de millions d'euros il y a dix ans). Cependant il s'agit du coût des fraudes effectivement démontrées. Les assureurs estiment que le coût réel des fraudes subies dépasserait chaque année les 2,5 milliards d'euros, soit près de 5% des cotisations d'assurance perçues annuellement (principalement en assurance automobile et en dommages aux biens plus largement).

En conclusion, on constate donc que tout comme pour les établissements bancaires, le risque opérationnel en assurance présente une forte diversité de cas et reste encore un sujet exploratoire dans la réglementation comme dans l'étude pratique de ce sujet de gestion et de contrôle.

[23] Audoin O., Ricchiuto (2013), *Organiser et piloter le risque de fraude en assurance*, l'Argus de l'assurance.

4. Analyse critique : Une approche gestionnaire de la régulation, le contrôle par la norme dans un monde post-crise

L'impact économique des enjeux de contrôle n'est pas récent (Eisenhardt, 1985). Toutefois, la dimension organisationnelle tend à prendre de l'importance en tant que facteur d'intégration et d'adaptation de la norme.

Dans un monde d'après-crise, une approche efficace de la régulation implique de repenser la norme, de voir celle-ci comme un vecteur d'information et non comme une contrainte pesant sur l'activité (Brammertz, 2010). Cela est d'autant plus important qu'il existe une pluralité de normes et de contrôles y étant associée se traduisent par des conflits de normes mais aussi par des complémentarités parfois non prises en compte donc sources potentielles de redondances et de sous-efficacité du dispositif global de contrôle.

Ainsi, concernant la thématique du risque opérationnel, on distingue une diversité de contrôle entourant cette catégorie : contrôle interne, contrôle de conformité, contrôle qualité, contrôle comptable et de gestion, contrôle des risques (direction des risques opérationnels), audit interne (Fernandez-Laviada, 2007 ; Dufour, Teneau, 2013).

Dans ces différents cas, il est question de répondre aux enjeux posés par les normes de régulation du risque mais aussi par les autres normes (soft comme hard law[24]). Le contrôle interne et la gestion des risques se sont fortement développés sur le plan national en France et international plus globalement. La prolifération de normes sur ce sujet conduit progressivement à se concentrer sur le « comment mettre en œuvre » en pratique cette régulation plutôt que sur la question du « pourquoi » développer celle-ci (Cordel, 2013). L'une des dérives de ce contrôle par la norme relevée fréquemment dans les études de cabinet tel Ernst & Young ou encore de la Federation of European Risk Management (FERMA) est que la raison principale de la mise en œuvre de système de contrôle des risques est le souci d'être en conformité avec la réglementation au sens large. Les raisons de type réponse au besoin des parties prenantes ou encore enjeu de RSE et de pression des marchés étant désormais secondaires.

On distingue ainsi les normes traitant du risque opérationnel en tant que tel (Bâle II, Solvabilité II) et les normes répondant à une problématique de risque donnée de risque opérationnel mais ne faisant expressément référence au risque opérationnel (les obligations en

[24] Le système de Hard Law définit les lois et règlements s'imposant aux agents économiques là où la Soft Law concerne des dispositifs n'étant pas d'application stricte (normes professionnelles sectorielles, référentiels etc.).

matière de protection de la clientèle, de lutte anti-blanchiment par exemple). Il faut également ajouter à cela les normes engendrant des risques opérationnels sans y faire référence spécifiquement : il s'agit de l'ensemble des normes impactant de manière forte un établissement financier et engendrant des réorganisations ou une mise en conformité de l'entité dans un délai court.

Comme l'évoque Cohen (2010), qu'il s'agisse des normes comptables, des règles prudentielles, des règles sur la transparence ou l'information financière, des réformes ont eu lieu depuis la crise de 2007-2008.
Paradoxalement, si ces normes ont été changées, la référence au risque opérationnel n'a pas été renforcée et la critique du Risk Management ne s'est pas traduite par une réelle rupture, quant à la nécessité d'une prise de conscience du rôle essentiel du contrôle des risques dans les activités financières qui sont, en banque comme en assurance, des métiers du risque.

Le dépassement de la norme, en vue d'une recherche d'effectivité du contrôle, s'inscrit dans une préoccupation de notre temps. Les recherches menées en sciences de gestion montrent que le Risk Management, en tant que politique organisationnelle, doit viser avant tout la responsabilisation des acteurs, de manière globale (Boatright, 2011). Une politique de risque efficace sera presque tacite : chaque acteur de l'établissement financier se préoccupera de cette question dans son activité opérationnelle ou managériale, ne cherchant pas uniquement à l'éluder car il existe un montant de fond pour couvrir le risque inhérent (Mikes, 2009). L'essence même d'un Risk Management efficace est de déceler les risques futurs, non encore survenus dans le passé (McGrew, Bilotta, 2000), de développer une architecture organisationnelle permettant de positionner les dispositifs de contrôle sur les enjeux réels de l'organisation. Cela de manière dynamique, c'est-à-dire adaptée à la réalité changeante du profil d'exposition au risque de l'organisation (Pathak, 2005 ; Fraser, Henry, 2007). Une telle posture permet non seulement une réactivité renforcée en cas de crise par une meilleure préparation de l'organisation (la notion de résilience), mais elle correspond aussi à une approche responsable de la gouvernance d'entreprise qui implique d'intégrer ce qu'Hans Jonas qualifie d'obligation à l'avenir : pouvoir communiquer sur la base d'informations adaptées (Drott-Sjoberg, 1991).

Les recherches récentes et post-crise sur le Risk Management tentent d'expliquer les approches inadaptées de gestion du risque. Au titre de ces dernières figurent

principalement des travaux sur la recherche d'effectivité des dispositifs prévus par les normes. Concernant le Risk Management ces approches renvoient notamment au rôle des managers, et de la gouvernance d'entreprise, dans la diffusion de principes et de zones d'enjeu prioritaire mais aussi des limites de risques acceptables (Buehler, et al., 2008a). En ce qui concerne le risque opérationnel, cela se traduit par la nécessité de développer une approche culturelle du risque (Ospital, 2006), soit un environnement où la variable risque est une composante du processus de décision. Cette approche se retrouve notamment dans la philosophie de Solvabilité II au travers des principes tels que le principe de prudence (en matière de placements financiers), le principe d'accountability (obligation de rendre des comptes, au travers des reportings prudentiels dans le cadre des piliers III des directives précitées en banque et assurance), ou encore le principe dit des « 4 yeux » (concernant la gouvernance partagée des risques de l'entité par la présidence et la direction générale par exemple dans leurs domaines respectifs d'intervention).

La diffusion de cette approche culturelle suppose une vision partenariale de la norme de contrôle, laquelle n'est pas nécessairement incompatible avec une recherche de conformité aux normes (Edwards, Wolfe, 2006). Cette vision culturelle a souvent était détournée en une culture du risque devenant avant tout une culture du calcul du risque et de la collecte de données historiques. L'écueil a été de rechercher dans les données passées les zones de risque futur, ce qui a une efficacité relative pour des risques opérationnels de fréquence mais reste limité pour des risques extrêmes rares. Les entreprises doivent tirer comme enseignement de la crise que le risque est avant tout le fait du facteur humain, et qu'une approche axée sur les pratiques opérationnelles et les comportements aura plus d'efficacité qu'une approche par le reporting et l'auto-déclaration (Stulz, 2009), même si celle-ci est longue et complexe à mettre en œuvre.

Enfin, d'autres recherches remettent le rôle clé des normes et des mécanismes de régulation au centre de ces travaux sur les facteurs d'acculturation au risque. Pour Andersen et al. (2011), la dérégulation des pratiques dans le secteur financier, mais aussi les enjeux de conflits de normes, ont permis, non seulement la créativité d'experts sur des produits complexes mais aussi une certaine ambigüité quant au rôle de la norme et à son interprétation. Il existe en effet des débats récurrents sur la manière d'intégrer et de transposer en pratique la norme de contrôle du risque opérationnel, chaque groupe d'acteur en ayant sa propre lecture (Wahlström, 2009).

Ces différentes recherches sur le rôle des normes de régulation en Risk Management nous amènent à envisager l'enjeu que représente le cadre émergent de la tétranormalisation ainsi qu'à considérer la pertinence du système de régulation du secteur financier.

4.1.Une approche réactive de la régulation prudentielle

La littérature académique en économie et en gestion a abondamment étudié les dernières crises financières en vue d'expliciter leurs facteurs de survenance et d'envisager des moyens de traitement. La littérature gestionnaire penche largement, non pas pour une refonte du capitalisme moderne, mais dans le sens d'un « Risk Management » de l'après-crise (Amri et al., 2011 ; Kaplan, Mikes, 2012).

La critique du Risk Management moderne se situe notamment dans la recherche d'une plus grande effectivité des dispositifs de contrôle (Cappelletti, 2006, 2009a) mais aussi d'une meilleure prise en compte de catégories encore émergentes de risques, à l'instar des risques opérationnels (Maurer, Lamarque, 2009 ; Bon-Michel, 2011). Un tel enjeu n'est pas récent et il implique de repenser les leviers du contrôle, au sens de Simons (1995), pour dépasser une approche du risque s'étant institutionnalisée voire industrialisée tout en ayant perdu son sens (Bon-Michel, Dufour, 2013).

La réglementation prudentielle relative au risque opérationnel dans les établissements financiers envisage ce sujet en premier lieu comme un enjeu de provisionnement de fonds propres en vue de se couvrir contre le risque futur (Foot, 2002 ; Guegan, Hassani, 2013). Comme le relèvent certains auteurs (Haouat-Alsi, 2011), une telle approche traite davantage des conséquences du risque que des causes racines et doit cependant être complétée en cela qu'elle n'est pas suffisante pour cerner la réalité de l'enjeu d'un risque lié au facteur humain. Une approche dynamique de type Risk Management à vocation organisationnelle, c'est-à-dire s'inscrivant dans un management actif, fréquemment évaluée et repensée, semble aujourd'hui une nécessité bien que constituant une gageure (Jednak, Jednak, 2013).

Pour d'autres auteurs, il faut également analyser la réglementation prudentielle dans le secteur financier comme un cadre général, posant des principes d'action mais dont la mise en place

s'est rapidement avérée coûteuse et complexe pour les établissements financiers. Ce coût est double : celui de la mise en place de dispositifs souvent complexes et difficilement adaptables aux nombreuses activités d'un établissement financier, et le coût de la mise en conformité avec des exigences de fonds propres renforcées (Herring, 2005). D'autres auteurs insistent sur la dimension interprétative du cadre prudentiel sensé faciliter la responsabilisation au sein des établissements financiers. Cette dimension interprétative se retrouve concernant le second pilier des dispositifs évoqués en banque et assurance, mais il importe de mentionner que le premier pilier relatif aux exigences quantitatives est d'application claire mais manque d'adaptabilité pour prendre en compte la diversité des cas d'établissements financiers ainsi que leurs activités respectives (Cornford, 2009). Les progrès réalisés depuis les premiers accords de Bâle sont sensibles, notamment en ce qui concerne le risque de liquidité mais aussi les risques opérationnels (Ojo, 2010). Pour d'autres auteurs, il s'agit d'une des limites de la régulation prudentielle qui, à elle seule, ne peut constituer une réponse : la régulation prudentielle repose avant toute chose sur la recherche de consensus entre une pluralité d'intérêts et un objectif commun qui concerne la maîtrise des risques. Cet objectif commun est partagé en théorie mais difficilement conciliable en pratique (Gordon-Hart, 2004 ; Walhström, 2009). Cela montre ainsi les limites des initiatives publiques en matière de régulation et la tendance globale à une régulation émanant des secteurs financiers eux-mêmes, évoqués comme mieux à même de se réguler de l'intérieur en présence de risques imbriqués et complexes à identifier (Miron et al., 2011). Dès lors que l'appétence des dirigeants sur la question des risques et de leur gestion est un sujet d'intérêt (Froud, 2003). Ces derniers sont mieux à même de contrôler leurs risques, dans ce postulat de « l'auto-contrôle ». De telles considérations sont bien entendu à nuancer face à la capacité des établissements financiers de contourner voire d'interpréter la réglementation prudentielle, ce qui suppose une veille constante des Etats via les instances de régulation (Gaver, Paterson, 2004).

4.2.Le risque opérationnel : une réalité de l'action, une invention du régulateur visant la prise de conscience

M.Power (2005) parle *« d'invention du risque opérationnel »* pour qualifier cette création ex nihilo d'une nécessité de se représenter un ensemble de risques distincts. Cette *« fiction instituante »* au sens de R.Shiller (2003) a pour objectif de permettre une organisation de l'incertitude (Power, 2007), une catégorisation en un ensemble de plusieurs sous-ensembles

de risque que sont notamment les catégories baloises de risque opérationnel (fraude interne, fraude externe, risque HSE-PCA, risques liés aux clients-produits et pratiques commerciales, dysfonctionnements des systèmes, dommages aux actifs corporels et exécution-livraison-gestion des processus). On retrouve bien dans la notion de « risque opérationnel » la nécessité de regrouper les nombreux risques liés à l'activité courante de l'organisation sans être le cœur du métier de prise de risque d'une banque (risque de crédit, risque de marché) ou d'une société d'assurance (risque lié à la souscription de contrats vie ou non-vie).

Avec les affaires médiatiques de risques opérationnels extrêmes, cette catégorie a fait l'objet d'une attention croissante en vue de démontrer son rôle encore émergent (au sens d'un risque nouveau et ne faisant l'objet que de peu voire d'aucune étude statistique) dans le cadre réglementaire et dans les dispositifs de Risk Management.

Cette définition appréhende le risque par sa composante négative, les conséquences du risque pour l'établissement financier. Le risque opérationnel ne repose sur aucun encours connu et ne peut s'appréhender à la lecture du bilan ou du compte de résultat par activité. Le flou de ce qu'englobe le risque opérationnel contribue à le rendre tributaire d'une certaine culture du risque et d'une expertise car il est aisé de confondre la notion de risque avec d'autres notions proches telles que les menaces, les incidents ou encore les évènements redoutés. Cette difficulté se retrouve dans les limites de l'exploitation des bases de collectes des pertes et incidents ou des cartographies des risques.

De manière plus intelligible, les risques opérationnels incluent l'ensemble des risques ayant un potentiel de désorganisation. Ces risques peuvent ainsi inclure les risques juridiques (procès suite au non-respect de certaines obligations), les risques sociaux (grève, émeute) et psychosociaux (suicide d'un collaborateur) ou encore les risques informatiques (panne d'un serveur ou de l'installation informatique paralysant l'activité) mais aussi les risques projets intégrant notamment le lancement de nouveaux systèmes d'information ou encore les projets de réorganisation de l'entreprise. Cette multiplicité de catégories de risques opérationnels implique en pratique le rapport à une pluralité de normes en vue d'une mise sous gestion. Une telle approche est cependant peu formalisée.

Si la gestion du risque opérationnel peut avoir un impact sur la réputation de l'entreprise et la confiance qui lui est accordée (Gillet et al., 2010 ; Sturm, 2013), elle est davantage une affaire de maîtrise des connaissances dans l'organisation (connaissance des processus, du fonctionnement de l'organisation, connaissance client) que d'une recherche de réponse conformiste à un dispositif normatif (Hora, Klassen, 2013). Le contrôle de l'enjeu complexe

risque opérationnel ne peut être atteint uniquement par une approche normative comme le montrent certaines recherches insistant sur l'extrême contingence de cette thématique. Le risque opérationnel et la faculté d'identification de ce dernier au sein d'une entreprise (notamment pour les fraudes internes et externes) sont ainsi contingents de nombreux facteurs tels que la composition du Top Management (Wang, Hsu, 2013), l'intérêt des dirigeants pour cette thématique, la stratégie de l'entreprise et l'expertise à disposition sur ce sujet variable et complexe (Frost et al., 2000) ou encore de la capacité de l'établissement financier à collecter les données et à les transformer en informations pertinentes et utiles (Chernobai et al., 2011 ; Jebrin, Abu-Salma, 2012).

4.3. La tétranormalisation : comment repenser la régulation des sources de risques dans un monde de normes ?

Au-delà des critiques théoriques portant sur la norme de contrôle du risque elle-même, l'analyse des normes dans le secteur financier peut s'envisager notamment dans le prolongement de la théorie néo-institutionnelle et à la lumière du cadre théorique émergent de la tétranormalisation.

4.3.1. Un prolongement de la théorie néo-institutionnelle

Nous nous inscrivons dans une approche différente mais néanmoins complémentaire aux travaux menés dans le champ de la théorie institutionnelle. Selon cette théorie (Powell, Di Maggio, 1991) : *« l'institutionnalisation est un processus par lequel les mécanismes sociaux en viennent à prendre un statut de règle dans la pensée et l'action* ». Les normes de contrôle sont donc des règles institutionnalisées aux niveaux d'un secteur, d'une entreprise, d'une fonction (Cappelletti, 2006). Ce champ théorique développé depuis les années 1980 dans l'analyse des organisations cherche notamment à expliquer les interactions des acteurs en fonction d'intérêts politiques. Il en découle que les institutions sont envisagées comme des accords entre acteurs sur une structure de coopération apportant une réponse à un problème d'action collective. En gestion, ces institutions sont le fruit de l'action humaine, nous rappellent Di Maggio et Powell (1997), mais elles ont de particulier qu'elles ne sont pas issues d'un objectif conscient. Ces institutions (habitudes, normes sociales, procédures légales) ne sont pas indépendantes : elles sont le fruit de jeux d'acteurs, de soumission à des

règles de convenance (March, Olsen, 1984). Les normes informelles et les standards de professionnalisme ont un rôle à jouer nous disent encore les auteurs. Cependant, l'approche institutionnaliste implique d'aboutir à une théorie du choix rationnel appliquée aux institutions sociales. Par la mise en avant du cadre de pensée de la tétranormalisation, nous nous inscrivons dans une posture davantage néo-institutionnelle où les institutions ne sont pas toujours le fait d'objectifs conscients. Ces mêmes institutions (les normes de contrôle de risque dans notre étude) sont la cause de choix non rationnels : l'édiction de normes en conflit entre elles, de normes trop importantes en nombre et tellement variées qu'elles sont contre-productives c'est-à-dire contraires à leur objectif premier (assurer une meilleure maîtrise du risque en ce qui concerne la norme de contrôle du risque). Notre revue de littérature révèle que les institutions à la base du contrôle des risques ont été défaillantes. Le recours au cadre théorique de la tétranormalisation nous permet de fournir une grille de lecture explicative en prolongement de l'approche néo-institutionnelle. Nous faisons écho aux travaux de Moe (1987) sur la critique des mécanismes du contrôle législatif (ayant des effets indirects et non-intentionnels au-delà des mécanismes formels de contrôle).

4.3.2. Le cadre de la tétranormalisation

Le cadre de la tétranormalisation s'inscrit dans l'axe théorique de la socio-économie des organisations, soit l'intégration des variables sociales dans les stratégies des organisations. En l'espèce il s'agit du rôle joué par les normes dans la gestion des organisations.

La tétranormalisation (Savall, Zardet, 2005b) vise à rendre compte de l'organisation des normes en quatre pôles. Ces quatre pôles de normes affectant les organisations sont les normes comptables et financières, les normes traitant des échanges commerciaux, les normes sociales et les normes relatives à la qualité et à l'environnement. Face à ces quatre corps de normes, la littérature académique fait état d'une prolifération (souvent appelée « inflation ») normative ainsi que d'une incompatibilité entre normes (Savall, Zardet, 2005b). A celle-ci, on peut ajouter une logique d'interprétativité dans un monde de normes qui explique souvent la problématique du « pourquoi », sans toutefois répondre à la question du « comment » (Brunsson, Jacobsson, 2005) pour les organisations devant appliquer ces normes.
Cette marge de manœuvre et ces conflits de normes donnent parfois lieux à ce qui est qualifié « d'hypocrisie normative » (Cappelletti, 2009a): la norme est appliquée par l'organisation pour être en conformité et ne remplie qu'en apparence ses objectifs premiers. Dans le cas de

la réglementation prudentielle, il s'agirait d'une meilleure maîtrise des risques. Dans ce même cas de figure, il s'agit de mettre en place des normes et procédures non appliquées mais étant formalisées. Expliquer les contraintes d'application des normes et définir une convergence entre normes est une difficulté croissante pour les organisations (Don Vangel, 2004), y compris lorsqu'elles se sont dotées de services de veille réglementaire et de conformité juridique.

La théorie de la tétranormalisation distingue donc quatre corps de normes en interactions :

-les **normes comptables et financières** : qui dans le cas du secteur financier sont notamment la loi Sarbannes-Oxley (pour les sociétés côtées à la Bourse de New York), la loi de NRE (Nouvelle Régulation Economique) de 2002, la Loi de Sécurité Financière (LSF), les normes IFRS et French Gaap notamment, la directive du 8 décembre 2008 sur le contrôle légal des comptes, les dispositifs prudentiels Bâle I, II (et sa transposition au travers du règlement CRBF 97-02) et Bâle III (à venir), les directives Solvabilité I et II (à venir), le règlement AMF etc.

-les **normes relatives aux échanges commerciaux** : en France le droit de la consommation et les règles édictées au code monétaire et financier, au code des assurances etc.

-les **normes sociales** : Il s'agit notamment du droit social, du droit du travail (code du travail, conventions collectives, accords de branche etc.) pour Nicholson et al., (2011) les normes sociales ont également un rôle croissant à jouer dans l'explication des mécanismes de régulation des sources de risques financiers : dès lors que des pratiques financières ont un impact sur la société, il n'est pas anormal de voir l'opinion publique (en tant que somme de contribuables, mais aussi par la voie des mandats représentatifs) influer dans le sens d'une législation plus protectrice de ses intérêts.

-les normes **Qualité et Environnement** : la norme ISO 14000 (Management Environnemental), les normes relatives à la Responsabilité Sociale de l'Entreprise, à la qualité des pratiques en entreprise (ISO 9001) et à la sécurité des processus (ISO 27000), la norme ISO 31000 sur le management global des risques, les normes Hygiène Sécurité Environnement (HSE).

En matière de contrôle du risque opérationnel, on retrouve bien les enjeux de tétranormalisation. La diversité que suppose le risque opérationnel et ses typologies est alors à rapprocher du cadre de la tétranormalisation proposé par Savall et Zardet pour comprendre les sources de crises en entreprise (2005b, 2013, p.18).

Les risques opérationnels comprennent ainsi des sources de risques dans les 4 corpus de normes :

-des **risques comptables et financiers** : la fraude interne et externe,

-des **risques relatifs aux échanges commerciaux** : le risque client, le risque de la chaine de valeur, le devoir d'information et de conseil, LAB-LAT-LAF[25],

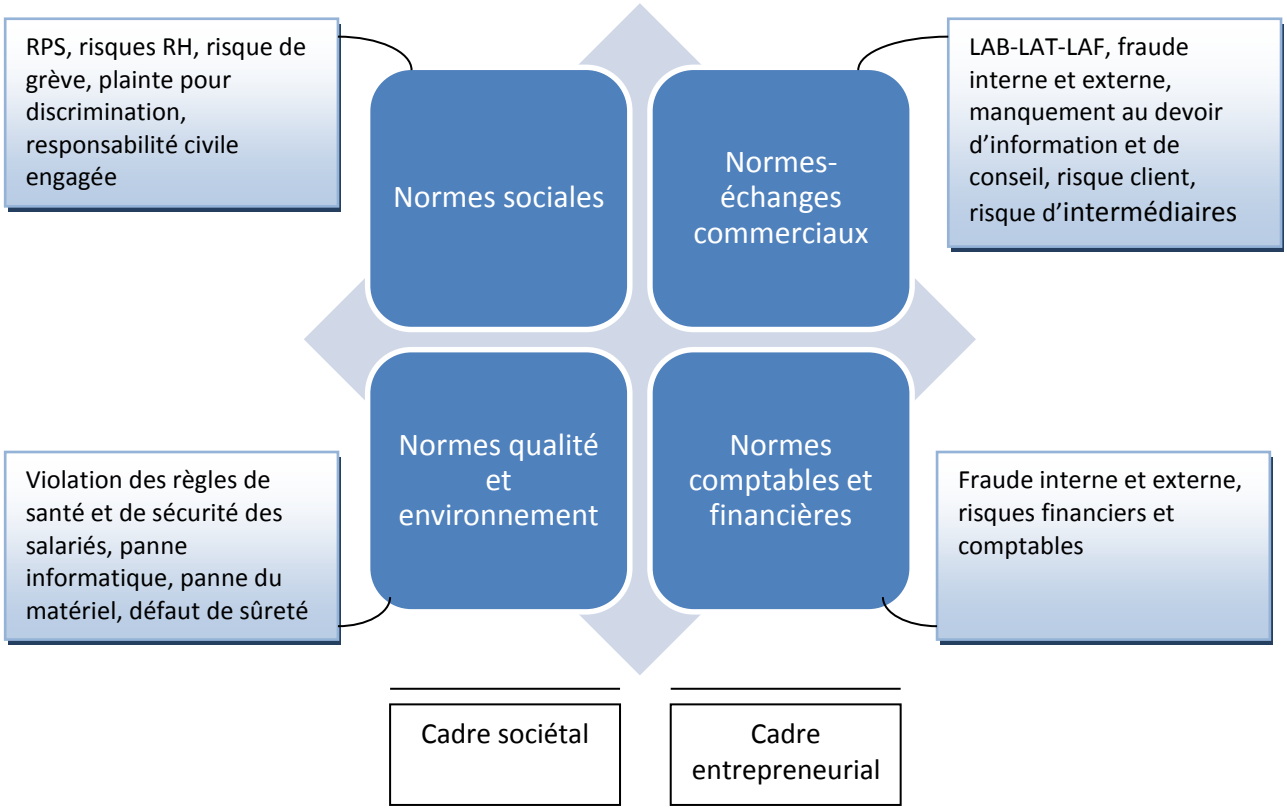
-des **risques sociaux** : les risques psychosociaux (RPS), les risques liés à la gestion des Ressources Humaines et au cadre social de fonctionnement de l'entreprise (le risque de grève)

-des **risques sur l'environnement externe** : la sécurité au travail, le risque de réputation (parfois exclu mais a un impact risque opérationnel), le risque de cyberattaque, le risque politique d'une filiale (ou risque pays-risque filiale).

Ces catégories de risques se retrouvent dans les typologies de risques opérationnels. Le tableau présenté en annexe établit un rapprochement entre typologie baloise de risque opérationnel et enjeux récurrents de tétranormalisation (Voir annexe 7 - Correspondance des enjeux de tétranormalisation et des catégories de risque opérationnel).

[25] Respectivement les dispositifs de lutte anti-blanchiment, de lutte anti-terrorisme, de lutte anti-fraude.

Figure 14. Tétranormalisation et risques opérationnels dans le secteur financier



Conclusion du chapitre deux- Un rôle croissant des normes dans la production de contrôles socialement organisés

Depuis les accords de Bâle en banque et les premières directives sur la solvabilité en assurance, de nombreux corps de règle ont été ajoutés en vue de définir le cadre prudentiel des établissements financiers. Ces corpus de normes ont pour vocation de renforcer la confiance dans lesdits établissements en mettant sous contrôle les différents types de risques pouvant survenir. Le cadre prudentiel, tel que défini aujourd'hui, comprend à la fois des éléments quantitatifs dans une logique réactive de provisionnement, ainsi que des dispositions de nature qualitative visant à développer l'anticipation et la proactivité ainsi que l'information du public. Ces éléments de nature qualitative, concernent la gestion et le contrôle des risques. Si en banque les accords de Bâle II et les recommandations du Comité de Bâle ont permis d'objectiver le risque opérationnel, ce sujet reste émergent en assurance dans la réglementation prudentielle. Force est de constater, à la lumière des critiques évoquées concernant ces normes, que le secteur financier nécessite des repères théoriques et conceptuels face à des notions interprétatives et aussi englobante que le risque opérationnel et la gestion des risques.

Conclusion de la première partie – Diversité des risques institutionnalisation de l'évènement non encore survenu qui guide l'action future

Les politiques de maîtrise des risques, bien que formalisées dans la réglementation prudentielle et mise en place en pratique, restent un sujet émergent dont la compréhension pratique et théorique s'impose (Baldwin, Cave, 1999). De tels constats s'inscrivent dans la continuité des recherches réalisées quant au rôle des normes dans les différents secteurs d'activité, lesquelles se situent entre autonomie et sanction (par les pouvoirs publics). Ainsi, pour Demortain (2011), la régulation des risques dans notre époque moderne est davantage le fait des standards internationaux et des experts que des organes Etatiques. Ces experts sur les thématiques de risque forment un « collège invisible » (Demortain, 2011, p.8) caractéristique d'un niveau de contrôle à part entière. Les risques opérationnels liés aux activités du secteur financier s'inscrivent dans cette logique : une régulation étant davantage le fait des experts internationaux formalisant des corpus de règles (le comité de Bâle, l'Eiopa notamment). Ces travaux conduisent peu à peu à bien distinguer les catégories de risque, les liens entre ces dernières, les facteurs aggravants de chaque catégorie ainsi que les moyens de répondre à chaque type de risque. L'objet de la partie II est d'envisager ces enjeux de gestion des risques dans le secteur financier au travers de la littérature académique.

Partie II-Partie théorique - De la Société du Risque au Risk Management des sociétés

Introduction de la seconde partie – Vers un « Total Risk Management »

Cette seconde partie aborde les principaux éléments théoriques issus de notre revue de littérature et étant relatifs aux politiques de maîtrise des risques ainsi qu'aux risques opérationnels.

Nous présentons dans un premier chapitre les principaux travaux en gestion, mais aussi dans des disciplines proches (telle que l'économie), ayant abordé l'enjeu à part entière que constitue la gestion des risques pour les organisations. Ces travaux s'inscrivent dans différents champs théoriques (théorie des organisations, comptabilité-contrôle-audit). Nous constatons qu'un cadre théorique « en construction » relatif à la gestion des risques a émergé depuis la fin du XXème siècle. Ce cadre théorique s'inscrit à la fois dans une perspective gestionnaire (management, théorie des organisations) et dans une perspective sociologique (théorie de la structuration notamment, rôle sociétal du risque et repositionnement social de la gestion des risques). Nous décrivons également dans ce chapitre les grilles de lecture les plus significatives pour étayer notre démonstration empirique dans la partie suivante (théorie de la structuration, théorie de l'acteur-réseau, théorie socio-économique).

Le second chapitre précise notre posture épistémologique (d'inspiration constructiviste) ainsi que le cadre méthodologique choisi pour notre recherche empirique. Notre protocole de recherche s'inscrit dans une triangulation méthodologique combinant recherche-action, étude documentaire et entretiens semi-directifs à visée confirmatoire.
Nous présentons dans ce chapitre les principaux matériaux de recherche collectés (cas d'entreprises, documents internes et externes aux entreprises, entretiens auprès de spécialistes risques opérationnels etc.).

Ces grilles de lecture théoriques et ce protocole de recherche visent à structurer la démarche de collecte et de traitement-analyse des données recueillies en vue de mettre en lumière, dans la troisième partie de la thèse, nos principaux résultats et constats théoriques et managériaux.

Chapitre 3 - Approche théorique des politiques de gestion des risques, une lecture organisationnelle du risque

« La science conçoit naturellement le risque sur un mode quantitatif. Elle transforme les risques en probabilité froides et objectives parfois tellement éloignées qu'elles échappent à la compréhension du profane »
Keith Hawkins

Notre revue des recherches académiques et professionnelles a consisté à étudier dans un premier temps la littérature dense concernant le risque en entreprises puis, plus spécifiquement, le Risk Management dans les organisations (secteur financier et non-financier). Si plus de deux mille cinq cent sources bibliographiques concernant des recherches académiques ont alors été recensées, nous nous sommes principalement centrés sur les recherches en comptabilité-contrôle-audit et dans le domaine de la théorie des organisations (en étudiant le rapprochement entre ces deux champs des sciences de gestion) en vue de traiter de manière théorique notre problématique de recherche.

Ce chapitre se structure en deux parties : la revue de la littérature décrivant l'état de l'art en matière de gestion du risque et de risque opérationnel. Puis, nous abordons dans un second temps les grilles de lecture conceptuelles mobilisées dans le cadre de notre étude de terrain dans les secteurs banque et assurance.

I. Cadre théorique : de la « Société du risque » à la gestion du risque des sociétés

Cette première partie de notre chapitre théorique aborde les différentes recherches menées en matière de gestion des risques et de risque opérationnel. De nombreux travaux en économie, gestion ou encore en psychologie et sociologie abordent la thématique du risque. L'objet de cette revue de littérature est non pas de prétendre à l'exhaustivité mais d'envisager les principales recherches s'apparentant ou traitant explicitement de la gestion des risques. Nous cherchons donc à dessiner les contours d'une théorie émergente de la gestion des risques. Nous insistons également sur l'importance d'une justification théorique de cet objet de recherche.

1.1. Les théories économiques et les prémices d'une recherche en gestion des risques

L'analyse des distinctions entre les notions entourant le risque a été développée par Knight dès 1921 notamment, lequel précisait que l'incertitude se caractérisait par l'impossibilité de regrouper des cas similaires en raison d'une trop grande diversité là où le risque était construit par un regroupement de cas de même nature et de même singularité. L'incertitude, pour devenir risque, se base alors sur les probabilités dites « fréquentistes » (induites de l'expérience). On parle alors d'objectivation pour ces évènements se répétant avec une certaine fréquence (Moureau, Rivaud-Danset, 2004, p.12).

D'autres économistes ont entendu compléter cette approche : Keynes, dès 1936 (dans sa Théorie Générale de l'Emploi, de l'Intérêt et de la Monnaie) abordait l'importance du facteur risque et de la recherche d'anticipation de cette notion comme facteur d'incitation ou non à l'action. Pour Keynes, l'individu ou l'entreprise ne peuvent se plonger dans l'introspection et l'analyse en permanence, il est donc nécessaire de s'en remettre aux conventions : l'approche dominante face à un risque est donc de se référer à l'avis du plus grand nombre et à la fixation de standards permettant de connaitre un niveau de risque dans le temps et dans un lieu donné (le taux d'intérêt notamment pour Keynes).

Von Hayek quant à lui aborde le risque sous l'angle de l'action rationnelle déterminée entièrement par le calcul et où l'étude du risque repose sur des connaissances, des vérités connues et démontrables. Cependant, il nous alerte également sur le fait que les individus n'ont en général qu'une connaissance partielle des faits. L'Homme est donc guidé à la fois par sa connaissance partielle des faits et par des conventions, des usages et des règles d'action. Les conséquences anticipées de nos actes et les règles sociales guident l'action pour l'auteur (Hayek, 1980).

Des auteurs plus modernes, comme Minsky en 1975 ou Davidson en 1991, refusent l'omniscience en matière d'économie. Toute action comporte un risque qu'il n'est pas possible de cerner totalement par des méthodes quantitatives ainsi que par la construction de connaissances sur la base d'évènements passés (Moureau, Rivaud-Danset, 2004).
Nous pouvons également faire référence aux travaux de J.K.Galbraith qui, en 1977, évoque la grande entreprise comme mode d'organisation le plus difficile à comprendre (bien que

structure la plus proche de l'individu) et pour lequel la complexité implique une mise sous contrôle des activités à risque.
Certains économistes soulignent encore un problème d'actualité et davantage ciblé sur une approche gestionnaire : la présence d'acteurs multiples en matière de gestion du risque et les difficultés de coordination entre ces derniers. Pour Chick (1997), les interactions macroéconomiques sont riches et complexes dans le temps, ce qui rend difficilement analysable le fonctionnement des marchés ainsi que les phénomènes d'interactions entre acteurs sur ces derniers. On s'achemine progressivement vers l'idée d'une gestion des risques en économie.

Pour Williamson (1985, 1990), les institutions guident l'action et éclairent les dirigeants sur les processus de décision à retenir dans les situations à risque. Pour ce dernier l'institution n'est pas restreinte au caractère d'autorité publique propre par exemple à la Justice : elle intègre l'ensemble des pratiques et comportements fondés sur des usages ou des règles et intègre également la notion d'organisation. L'auteur évoque comme point de départ le recours à l'organisation. Ce recours est préférable dès lors que l'appel au marché devient trop coûteux. Pour ce dernier, un environnement incertain caractérise la fréquence d'évènements dommageables et fortuits auxquels les agents économiques doivent s'adapter. Pour s'y adapter, ces derniers utilisent un ensemble de contrats types, mais cette solution s'avère souvent incomplète en matière de décision en univers incertain, les agents ne pouvant envisager toutes les éventualités lors de la rédaction des contrats. Face à l'incomplétude des contrats même les plus complexes, il importe alors de rechercher des garde-fous. L'organisation hiérarchique est évoquée par ce dernier comme la meilleure des solutions. Dans l'organisation, la formalisation de processus de décision et de dispositifs introduisant des mécanismes incitatifs permet de réduire le risque. L'organisation permet une spécialisation des individus réduisant les problèmes de rationalité étant à la fois cause et conséquence de l'incertitude.
Moureau et Rivaud-Danset (2004) résument ces apports des économistes en distinguant les approches institutionnalistes, l'économie des conventions et encore l'économie évolutionniste. Dans le premier cas, l'incertitude est vécue comme une perturbation exogène et il incombe aux agents économiques de choisir les modes de réduction minimisant les coûts (de transaction notamment). Dans le second cas, face à la complexité et à la singularité des situations, la convention est appréhendée comme le mode de réduction de l'incertitude le plus satisfaisant pour l'individu. Le troisième cas postule que face au caractère fortement

évolutionniste de l'économie (marquée par la complexité et l'évolution aléatoire des techniques et des pratiques), les acteurs utilisent des routines pour traiter une multitude d'informations et réduire l'incertitude (les routines guident la norme). Un tel cadre d'analyse décrit clairement l'évolution de la gestion des risques de l'assurance vers l'approche organisationnelle du risque (tel que décrite dans la suite de cette première partie).

Plus récemment encore, d'autres économistes ont complété ces apports : Pour Zadjenweber (2009, p.60), les pertes opérationnelles extrêmes des banques rendent nécessaire dans le secteur financier plus que dans d'autres secteurs d'activité la mise en place de politiques de maîtrise des risques : cela est notamment dû au fait que les établissements bancaires sont structurellement, et par nature, très endettés. La nature même de l'activité bancaire implique d'être soumis, plus que d'autres entités, aux risques financiers mais aussi aux risques opérationnels : fraudes externes et internes, vol, erreurs et omissions, pannes informatiques. De tels évènements sont dommageables pour toute entreprise mais plus encore en matière financière car cela affecte non seulement la solidité de l'entreprise à court terme mais son image à long terme (renvoyant à la notion de confiance).

Enfin, nous pouvons également citer Shiller ou encore Orléan (2010) qui bien que se référant à des courants de pensée distincts s'inscrivent tous deux dans la perspective suivante : la nécessité de sécuriser davantage les économies modernes dans lesquelles la financiarisation est omniprésente, ce qui induit davantage de mécanismes de circulation des actifs mais aussi des risques. Pour Shiller (2003, p.32), les grandes organisations autant que les individus sont vulnérables à une multitude de risques, souvent difficilement détectables, mais dont les conséquences sont bien réelles sur l'économie. Partant de ce constat, il prône la nécessité de développer tant des mécanismes assurantiels de transfert et de couverture de risque que des mécanismes d'incitation à l'intention des individus, ce en vue de favoriser des comportements « prudents ». Ces travaux, bien que très significatifs quant à l'étude des risques, doivent être complétés par d'autres champs théoriques pour préciser la réponse à apporter à notre problématique de recherche.

1.2. La sociologie des organisations ou le risque comme mesure de l'action humaine

Notre revue de littérature emprunte des éléments à la théorie du risque, notamment en ce qui concerne la sociologie du risque (Luhman, 1993 ; Beck, 1986, 1999 ; Bernstein, 1998 ; Peretti-Watel, 2000 ; Cingolani, 2001). Ces travaux ont pour objectif de démontrer le rôle des

organisations en matière de diffusion et de maîtrise du risque dans notre époque dite post-moderne.

Certains travaux se situent également dans le champ de la théorie des organisations et des sciences de la décision en contexte de risque (Drucker, 1973 ; Guilhou, Lagadec, 2002). La question des risques jalonne notre histoire depuis plusieurs siècles avec le souci de répondre à cet enjeu d'avenir dans le présent (Walter, 2008). Il importe de resituer dans son contexte socio-organisationnel cette recherche de réduction du risque propre à l'Homme.

Comme le précise Munier (2000, p.27) : « *la gestion des risques a beaucoup évolué pour devenir un art basé sur de vastes connaissances scientifiques ».* Du commerce maritime des origines par les marchands lombards au XIIIe siècle, couverts par des mécanismes d'assurance, jusqu'à l'actuelle gestion des risques tenant compte « *de l'évolution culturelle des individus et des sociétés, de l'évolution technologique et scientifique et encore de l'évolution interne des entreprises »,* la gestion des risques s'est trouvée transformée pour accompagner les changements de la Société.

Les premiers développements de la notion de risque remontent aux travaux de Bernouilli sur la mesure du risque (1738). Les premières apparitions d'une gestion des risques datent du siècle des Lumières lorsque le danger commence à être envisagé comme un domaine pouvant être source de connaissance et non simplement une fatalité ou le fait de forces dépassant ce que la science pouvait expliquer jusqu'alors.

L'approche humaniste et philosophique du risque remonte en effet au XVIIIème siècle. Ainsi, le tremblement de terre de Lisbonne de 1755[26] marque les prémices de l'appréhension par l'Homme de sa capacité à agir pour limiter le risque. Toutefois, c'est aux philosophes grecs que l'on doit les premières réflexions sur ce sujet. Ainsi, on citera Pythagore pour qui, si les ressources pour prévenir les évènements malencontreux manquent, il faut avoir la prudence de les anticiper.

[26] Le tremblement de terre de 1755 a complètement détruit Lisbonne, faisant plus de 100 000 morts dans une ville à forte densité et aux habitations (en bois) rapprochées. Jean-Jacques Rousseau fit alors remarquer que la responsabilité des hommes et leur intelligence sont en cause dans ce type d'évènement. Ainsi, la pertinence du lieu d'implantation des villes et le choix des procédés de construction sont déterminants. Le grand incendie de Londres de 1666 peut largement s'expliquer par des constructions en bois rapprochées les unes des autres facilitant la propagation des flammes.

L'étude du risque se développera au XIXème siècle dans une société marquée par l'essor des sciences, de la technique, de l'industrie et des dangers nouveaux qu'il importe alors de maîtriser dans le cadre d'une prise de conscience de la vulnérabilité croissante de l'Homme face à ses propres créations techniques visant à repousser les limites de la connaissance. C'est au XXème siècle cependant, avec l'essor des risques exogènes à l'entreprise que va se développer la fonction de gestion des risques.
Une telle fonction s'est développée au fur et à mesure de la prise en compte de nouvelles thématiques de risque pour l'entreprise. La fonction en tant que telle de gestion des risques nous vient des États-Unis ayant repris cette dimension philosophique du risque en y apportant une méthodologie opérationnelle, laquelle est aujourd'hui encore en évolution comme le montrent les nouvelles méthodes et outils, l'apport des *« cyndiniques »* ou sciences du danger etc. (Kervern, 1995 ; Jousse, 2009) en constitue un exemple.

Les approches du risque ont été largement abordées dans une perspective sociologique, le risque étant intimement lié au rapport qu'en ont les individus dans les différentes Sociétés et selon les époques (dimensions espace et temps) :
Ainsi, le risque a pendant longtemps était appréhendé selon des perspectives religieuses. On pense notamment au *« désenchantement du monde »* évoqué par Weber pour qualifier notre période moderne marquée par le progrès technique dans une perspective rationaliste. Cette même perspective rationaliste a rapidement laissé place à ce qui est qualifié de période post-moderne, soit une période dite de *« Société du risque »* (Beck, 1986) se caractérisant par le fait que notre monde, malgré notre savoir technique, peut laisser place à l'erreur et à la défaillance humaine (Power, 2004).

1.2.1. La pensée d'U.Beck : la sociologie du risque et la prise de décision

Pour Beck (1986, p.52) *« lorsqu'il s'agit de définir des risques, la science perd le monopole de la rationalité ».* Il s'agit d'un point crucial dans la pensée de l'auteur, la rationalité scientifique laisse place à la rationalité sociale en matière de risque. Pour l'auteur (p.52-53) : *« les différents acteurs de la modernisation et les différents groupes exposés au risque ont toujours des objectifs, des intérêts et des points de vue concurrents et conflictuels »*, lesquels sont nécessairement pris en compte lors de la définition d'un risque. Ces différents éléments sont au fondement même de la perspective de gestion des risques : la science ne cesse d'être désavouée au profit d'une approche socio-organisationnelle dans la mesure où tout pronostic

d'infaillibilité est critiquable, soit au profit d'une réalité déjà exprimée (la survenance d'un risque, d'une catastrophe, d'une crise qui s'en suit), soit du fait d'un état dans lequel différents acteurs souhaiteront éviter d'être exposés de manière durable à un risque donné.

Beck (1986, p.55) poursuit sur l'imbrication entre ces deux modes de rationalité (scientifique et sociale), ce qui a pour implication une multiplicité des définitions du risque et la conséquence pratique d'aboutir à une « surproduction » de risque : chaque groupe tente de créer ou de faire disparaitre ses propres définitions ou catégories de risque dans la défense de ses intérêts, ce qui ouvre la voie à des interprétations potentiellement infinies.

Pour l'auteur (1986, p.58) *« l'efficacité sociale des définitions du risque ne dépend pas de sa validité scientifique ».* On parle alors de validité au regard d'études scientifiques : analyses causales et argumentations étayées par de solides connaissances de terrain ayant été généralisées par des études de récurrence. Une définition efficace du risque est davantage celle pour laquelle l'interprétation sera généralisable malgré l'extrême diversité des facteurs particuliers de notre système moderne de production industrielle. En somme, l'efficacité sociale d'un risque en tant que catégorie dépend de sa faculté à être intégré comme axe de prise de décision quels que soient les facteurs de contingence d'un secteur, d'une activité, d'une organisation, d'un groupe d'acteurs etc.

Pour cette raison, Beck définit le risque comme la mesure de l'action humaine, cet *« évènement non encore survenu qui motive l'action »* (1986, p.60). L'auteur entend ainsi que le facteur à la base d'une prise de décision se concrétise par une action soit positive (le fait de mener un acte dans un but donné pour répondre à un objectif précis) soit négative (le fait de ne pas faire, car cela est jugé trop risqué par rapport à ce même objectif). Le risque ne se résume donc pas à ses conséquences et à ses dommages potentiels. Il exprime l'action future et est en soi fondamentalement dual : réel et irréel car il pourra concerner des risques déjà survenus mais dont on ne souhaite pas la survenance au regard d'une action en cours ou future, ou être l'objet d'un risque encore jamais survenu à ce jour.

Pour ces raisons, le risque devient un objet de gestion à part entière dans un rapport à l'avenir qui situe la conscience du risque comme moteur d'action et d'anticipation: *« nous devenons actifs pour éviter, atténuer, prévenir les problèmes où les crises de demain ou d'après demain, ou justement pour ne rien faire de tout cela »* (Beck, 1986, p.61).

Outre ces éléments relatifs au contexte dans lequel l'individu ou l'organisation sont à même de gérer le risque, la pensée d'U.Beck fait encore état d'une nécessaire faillibilité des individus et des organisations, remettant en cause la certitude historique sur le progrès technique comme facteur de maîtrise de l'environnement. Ce constat essentiel de l'époque

post-moderne implique une remise en cause des structures classiques de décisions politiques (Etat social, démocratie) pour permettre l'émergence d'autres modes de mise sous gestion du risque.
La gestion des risques apparaît comme une nécessité dans une époque marquée par l'importance de la composante technologique et met au centre des attentions des principes pour lesquels le décideur public trouve un rôle prégnant. Cette perspective gestionnaire de risque (Méric et al., 2009) comprend comme sous-jacent une dimension « précaution » essentielle (Godard et al., 2002) dans un monde où tout devient risque (Power, 2004). Elle suppose d'intégrer la gestion des risque dans l'organisation comme une étape incontournable.

Dans cette optique, gérer les risques est indispensable pour permettre la création de valeur (Darsa, 2011). Notre époque se caractérise alors par un effet sociétal où l'on constate une désinstitutionalisation de l'Etat comme gestionnaire de risque et une institutionnalisation des acteurs privées (entreprises, diverses organisations) en tant qu'acteurs de la gestion des risques (Ewald, 1986). Le champ de prise en compte de la gestion des risques n'est donc pas seulement scientifique et sociétal mais bien socio-organisationnel dans une logique d'élargissement du spectre de risques gérés et d'acteurs concernés mais aussi de catégorisation à outrance resituant davantage le risque dans des contextes économiques, sociaux, politiques, entrepreneuriaux à l'instar des risques informatiques, des risques clients, des impacts en termes d'image ou encore des risques RH (Edouard, 2008).

1.2.2. Réflexion sur le cadre institutionnel de la gestion des risques : les politiques de risque ou le pilotage par les risques à l'échelle globale

Il existe de nombreuses recherches traitant du contrôle social des organisations. Celles-ci prennent leur origine dans un contexte d'interdépendance où les choix organisationnels doivent être affirmés et dans lequel le contrôle est nécessairement sous influence des groupes et des coalitions (Pfeffer, Salancik, 1978). Depuis que l'organisation consomme des ressources, on cherche à évaluer l'utilité ou la légitimité d'une activité au regard de ses résultats mais aussi des conséquences qu'elle peut avoir sur les autres ou dans l'organisation (Parsons, 1956). L'étude du risque dans les organisations se situe dans ce contexte ; les fonctions dédiées à la gestion des risques étant souvent envisagées comme des centres de coûts.

Les débats sur la RSE, l'essor des principes de précaution, de responsabilité, le développement de fonctions au sein des entreprises telles que l'audit interne, le contrôle interne, la fonction Risk Management, la fonction de conformité sont autant d'éléments permettant d'attester de la place du risque au niveau des acteurs privés (Power, 1999 ; Véret, Mékouar, 2005 ; Morlaye, 2006). Ces fonctions deviennent une nécessité face à la complexification des risques au sein des entreprises ainsi que la prise de conscience du rôle de l'entreprise privée quant aux externalités (positives comme négatives) de son action sur la Société (Méric et al., 2009).
La gestion des risques est ainsi au centre d'un processus normatif la rendant incontournable pour les acteurs privés mais également pour un Etat qui serait parfois tenté de s'en défausser (Laufer, 1993 ; Bessire et al., 2010), posant la question des politiques de management public en matière de risque.

Face à cette perspective gestionnaire de risque, le management public a évolué en vue de définir de véritables politiques du risque à l'échelle globale (Borraz, 2008). Il existe, outre les risques spécifiques à la gestion des entreprises, un ensemble de thématiques de risque concernant les parties prenantes d'une société. Ces *« risques collectifs »* posent certaines difficultés et rendent inopérant le postulat d'une différence entre ceux créant les risques et ceux chargés de les gérer, il y aurait a priori convergence des buts. Quand des risques sont collectifs au point de concerner en théorie tout le monde et dans la gestion effective personne, il importe que l'acteur public définisse la conduite des politiques du risque. On pense aux cas des OGM, des risques liés à la téléphonie mobile, des déchets nucléaires, des risques chimiques, des risques géopolitiques… Comme le soulignent certains auteurs, *« la gestion des risques comme technologie politique, est au cœur de la construction de l'Etat moderne »* (Borraz, 2008, p. 279). Cette approche du risque est à ce titre au centre du processus démocratique visant à passer d'une *« Société du risque »* (Beck, 1986) à une *« Société de confiance »* (Peyreffite, 1995). L'introduction de la thématique du risque depuis les années 1970 à la fois dans la sphère privée et dans le débat public va au-delà de la simple thématique des dangers nouveaux affectant la Société. Cela pose la question du rôle de l'Etat et de sa capacité à assumer ce type de mission régalienne. La confiance dans l'Etat se matérialise alors autour de la thématique du risque. La question des risques est révélatrice de la manière dont l'Etat contrôle des activités économiques et gouverne des territoires ainsi que de la façon dont il s'accorde des différentes demandes et jeux d'acteurs. Sa capacité de

réponse face aux acteurs privés est ainsi testée par ce biais, tout en posant la question de sa faculté à assurer une action cohérente dans le temps.

Les politiques du risque se sont développées comme retour d'un Etat longtemps en recul, face à la prise de conscience qu'il n'existait pas de risque zéro et qu'un pilotage des risques au niveau le plus global apparaissait comme une nécessité. La conduite des systèmes à risque ne peut ainsi être le seul fait des acteurs privés car elle engage la sécurité de la communauté comme le montrent les domaines des transports, du nucléaire, de la chimie ainsi que les récentes crises technologiques majeures telles qu'AZF, British Petroleum, Fukushima… (Gilbert, Lascoumes, 2003).

Cette approche collaborative du risque est indispensable en vue d'éviter des erreurs d'action de management du risque : agir alors que le risque n'existait pas ou ne pas agir alors que le risque était bien réel. Dans les faits, éviter ce type d'erreurs et permettre cette approche collaborative pose la question de l'influence et du pouvoir du décideur public dans la gestion des risques intégrant les acteurs privés. Cela suppose encore de ne pas considérer technique et politique comme deux réalités autonomes mais bien comme deux composantes imbriquées. Depuis le milieu des années 1980, la Société Civile est plus présente et familière avec le débat sur les risques (Szpirglas, 2006). Cela situe au centre des attentions des pouvoirs publics comme des entités privées les dialogues et la construction de sens dans ces échanges sur le risque.

1.2.3. La société du contrôle et de l'audit : l'approche socio-organisationnelle comme caractérisation de la gestion des risques

Dans le cadre socio-organisationnel, comme le rappelle M.Power (2005), les faillites et les scandales financiers à répétition engendrent nécessairement un désir de réglementation en vue d'imposer la gestion du risque dans le cadre entrepreneurial. La substitution de l'entreprise aux pouvoirs publics telle que nous l'avons précitée a ainsi une conséquence plus générale : la Société incite de manière croissante les organisations, les entreprises à se livrer aux pratiques d'auto-observation. L'audit des organisations dans sa forme la plus répandue est donc aujourd'hui une pratique d'auto-contrôle (Spira, Page, 2003). L'audit tire son existence de la nature même des individus : il n'est pas possible de faire entièrement confiance à l'individu, lequel doit rendre compte de son action. Le cadre le plus adapté pour rendre compte de son action au sein d'une organisation étant l'organisation elle-même (Power, 2005, p. 227 et s.).

Inspirée des concepts évoqués quant à notre Société post-traditionnelle (Beck et al., 1994), la fonction d'audit correspond à une certaine vision du contrôle (reproduire une structure formelle dans une logique rationaliste visant à renforcer un système de connaissance pragmatique) et poursuit un objectif de transparence par rapport aux conséquences de l'action humaine (Power, 2005).

Cette Société de l'audit au sens de Power resitue le contrôle et l'audit non comme des systèmes basés sur la défiance mais bien comme des approches organisationnelles reposant sur la confiance, dont l'essence même est la production de confort (Power, 2005, p.230), ce qui n'exclut pas une logique critique face à la production d'information. L'audit et le contrôle peuvent créer des conflits en pratique car ils comportent une dimension de surveillance. Ils visent cependant la responsabilité et le dialogue et constituent en soi de nouvelles institutions de responsabilisation, sensées être dotées d'une plus grande visibilité dans les organisations car plus directement rattachées aux préoccupations des acteurs.

Enfin, par essence, l'un des enjeux essentiels de la société de l'audit et du contrôle est d'apporter des réponses, dans cette logique de confiance, face au risque. Ce mécanisme d'auto-contrôle de l'organisation participe aux « technologies du risque » (Ewald, 1990, p.147). Il intègre un cadre et un statut d'analyse formalisés relatifs aux catégories de risques, aux objets sur lesquels il porte, mais aussi aux tâches et besoins à formaliser et à traiter. Ce cadre s'inscrit dans un programme de gestion coordonné en tant qu'engagement normatif et pratique routinière. Ce cadre de pensée de la gestion des risques étant évoqué, il nous faut envisager la littérature émergente en sciences de gestion sur cet objet de recherche. Au-delà des approches économiques et sociologiques, centrées sur les mécanismes globaux ; notre étude théorique de la gestion des risques se situe également dans une perspective organisationnelle. Nous envisageons donc le rapprochement avec les études académiques en sciences de gestion relativement à notre objet de recherche.

1.3. La gestion des risques comme objet d'étude en sciences de gestion

Les recherches dédiées à la gestion des risques émergent pour la plupart dans les années 1980 et se développent fortement dans la décennie 2000. Notre revue de littérature aborde cependant certaines références fondatrices en sciences de gestion, renvoyant notamment au rôle des assurances comme technique gestionnaire de risque. Les recherches abordées

résument la diversité des domaines que recouvre le risque en entreprise, attestant du caractère encore largement exploratoire d'un tel sujet (approches organisationnelle, financière, comptable, étude sur le lien entre gouvernance et décision, étude des contrôles et liens entre contrôles du risque, stratégie et risque, risque et facteur humain, études par type de risque, recherches sur l'histoire de l'entreprise et l'évolution de la gestion des risques).

1.3.1. Une pluralité de recherches contemporaines sur la gestion des risques

De nombreuses voies ont été explorées par les chercheurs et les praticiens autour de la question du Risk Management et de la manière d'obtenir un dispositif de contrôle des risques efficace et effectif, ces recherches se structurent notamment autour des axes suivants :

- des recherches exploratoires en vue de caractériser le Risk Management moderne, ses méthodes et outils (Liebenberg, Hoyt, 2003 ; Fehle, F. Tsyplakov, 2005 ; Buehler et al., 2008a). Ces études distinguent les approches historiques de contrôle du risque (Vaughan, Vaughan, 1995 ; Sylla, 2003), ce notamment au regard des nouvelles formes de risques pouvant affecter l'organisation et la déstabiliser (Eccles et al., 2007 ; Bower et al., 2011). L'apport de ces travaux est de montrer qu'il existe une demande forte dans les organisations en vue de se doter d'outils et de méthodes adaptés d'identification et d'évaluation du risque. Toutefois, ces auteurs mettent en garde sur l'illusion que peuvent constituer les outils et méthodes des risques, souvent adaptés à des cas particuliers, donc peu transposables à des situations variées. Cet outillage suppose un niveau de maîtrise élevé des acteurs les mettant en œuvre ainsi qu'un regard critique de ces derniers sur les apports réels desdits outils et méthodes.

- des recherches sur la régulation, la normalisation et les thématiques de risques y étant associées (Bessire et al., 2010). Elles concernent en particulier le rôle de la régulation prudentielle comme facteur incitant à mettre en place des dispositifs et fonctions dédiées au risque à l'instar du contrôle et de l'audit interne, du contrôle de conformité et de la fonction de gestion des risques (Ojo, 2010). Il s'agit non seulement des fonctions et dispositifs mais aussi de l'exigence croissante de reporting des établissements financiers en matière de risque (Dobler, 2008). La manière dont la réglementation prudentielle envisage les failles des dispositifs de contrôle du risque est également abordée dans une logique organisationnelle (Mitra, 2009). La déclinaison opérationnelle de la réglementation prudentielle (Dedu, Nechif, 2010) est encore prise en compte dans certaines recherches démontrant ainsi le rôle du

management dans la réussite d'une réponse aux normes mais aussi aux objectifs effectifs de ces dernières (Wahlström, 2009). Ces recherches opérationnelles sur la réglementation prudentielle attestent notamment de la nécessité d'une certaine flexibilité dans la mise en œuvre des normes et dans la mise en conformité avec lesdites normes (Arnold et al., 2011 ; Lindberg, Seifart, 2011).

- des recherches en contrôle et finance sur le déploiement des dispositifs de risque et les difficultés techniques que ces derniers peuvent constituer notamment dans leur déclinaison dans l'organisation et en lien avec la stratégie d'entreprise (Beasly et al., 2005 ; Fraser, Henry, 2007 ; Zéghal, Ebondo, 2009 ; Sheehan, 2010 ; Girotra, Netessine, 2011 ; Frigo, Anderson, 2011).

- des travaux portant sur l'information sur les contrôles et la manière dont ces derniers sont utilisés et dont les acteurs en charge du contrôle utilisent l'information interne pour mieux prendre en compte le risque (Appéré, 2006 ; Chandra, Calderon, 2009 ; Kim, Park, 2009) et/ou sauvegarder la valeur de la firme (McShane et al., 2011). Ces travaux insistent notamment sur la capacité des acteurs en charge des différents contrôles et audit à innover en vue de mieux prendre en compte les risques de l'entreprise. L'objectif de ces travaux étant de déterminer comment contribuer à améliorer leur viabilité mais aussi la profitabilité des organisations grâce aux fonctions de contrôle (Thiery-Dubuisson, 2003).

- des recherches visant à définir ce que constitue un contrôle des risques efficace et effectif de manière globale (Simons, 1995) et dans le secteur financier plus particulièrement (Stulz, 2009 ; Taleb et al., 2009). En distinguant les facteurs de contingence du Risk Management (Gordon et al., 2009) et les facteurs d'effectivité du Risk Management (Danielsson et al., 2002), notamment dans un environnement financier changeant et étant le fait de nombreuses innovations (Merton, 1995). Ces innovations peuvent fragiliser une institution même réputée solide financièrement (Merton, 1995 ; Bernoth, Pick, 2011). Les recherches montrent notamment qu'un contrôle des risques efficace et effectif est celui qui repose sur la définition d'objectifs clairs de réduction des risques définis par les managers de l'entreprise dans leur périmètre de responsabilité. Ces recherches insistent enfin sur la nécessité de désigner des responsables de l'enjeu risque sur les différents périmètres de l'organisation, carence répandue quels que soient les secteurs d'activité concernés.

- le lien entre les différentes fonctions traitant de la variable risque en entreprise (Spira, Page, 2003 ; Fadzil et al., 2005 ; Sarens et De Beelde, 2006). Il concerne le lien entre Risk Management, contrôle interne et audit interne (Sarens, Christopher, 2010 ; De Zwaan et al., 2011). Les recherches sur ce sujet montrent notamment que ce lien bien que visible entre l'audit et le contrôle interne n'est pas encore suffisamment développé entre les fonctions de Risk Management et les fonctions audit et contrôle interne. Ces recherches abordent, sans les détailler toutefois, la nécessité de renforcer les interactions entre ces différents niveaux de contrôle ainsi que d'envisager d'autres acteurs du contrôle de l'organisation.

- le rôle du Risk Manager et de la fonction Risk Management au sein de l'organisation (Colquitt et al., 1999 ; Véret, Mékouar, 2005 ; Mikes, 2008b), est abordé par certains auteurs en tant que signe d'alerte sur les enjeux prioritaires de l'organisation, sur les menaces externes à celle-ci et sur ses vulnérabilités potentielles, augmentant ainsi la connaissance qu'ont les acteurs au sein de ladite organisation (Pathak, 2005), mais aussi en tant qu'acteur influent dans l'organisation (Saeidi et al., 2012).

- le positionnement du Risk Management au sein des instances de gouvernance et de son rôle dans la déclinaison et le choix des options stratégiques (Chong, 2004 ; Subramaniam et al., 2009 ; Aebi et al., 2012) et des modèles de gouvernance des risques (Bugalla et al., 2012). Ces recherches démontrent notamment le rôle essentiel que jouent les dirigeants d'entreprise et les différents membres des organes exécutifs et délibérants dans l'efficacité ou la non-efficacité d'une politique de maîtrise des risques. Ce rôle est présenté comme décisif en vue d'initier une démarche « crédible » de prise en compte du risque au sein d'une organisation. Sans perception positive des dirigeants, la démarche de gestion des risques est en effet jugée soit non prioritaire soit davantage comme étant une contrainte de reporting ou d'affichage d'une « éthique d'apparence » (Kippenberger, 1999 ; Kavcic, Bertoncelj, 2010 ; Yazid, 2012).

- des études plus récentes sur de nouvelles voies ouvertes dans le champ du contrôle, ayant une dimension comportementale voire psychologique marquée sont également à prendre en compte (White, 1995 ; Szpirglas, 2006 ; Rötheli, 2010 ; Chauvey, 2010 ; Hanlon, 2010). Ces études concernent la dimension d'apprentissage organisationnel liée à la gestion des risques ou le lien entre gestion des risques et gestion de la connaissance (Neef, 2005). Ces recherches constituent encore un champ nouveau et ouvre la voie à des travaux établissant le lien entre finance, sociologie du risque et contrôle-audit (Bricker et al., 2003 ; Moerman, Van der Laan, 2012). Ouvrir de nouveaux champs de recherche en comptabilité-contrôle-audit constitue en

effet une nécessité pour ces auteurs et cela intervient par le croisement des domaines mais aussi la prise de conscience d'une nécessité de penser autrement ce domaine académique, plus spécifiquement en ce qui concerne les enjeux de régulation (Shortridge, Smith, 2009), les comportements face au risque et le coût associé à ces derniers (Scimia, 2010), les structures décisionnelles et leur rôle en matière de réactivité et d'efficacité face au risque (Cvilikas, 2010), les différences d'application des mêmes approches de la gestion des risques selon les contextes d'entreprises ou de pays (Miron et al., 2011). Le biais culturel en gestion des risques est également revisité à la lumière de théorie sociologique pour montrer cette nécessité de penser hors des cadres conventionnels (Linsley, Shrives, 2009).

Ces travaux sont à la fois pré et post-crise de 2007-2008:

-Pré-crise: ils concernent alors la mise en place des dispositifs de contrôle et de gestion des risques et la nécessité d'institutionnaliser ces pratiques (Froot, Stein, 1998 ; Spira, Page, 2003)

-Post-crise : une étude critique de ce qui n'a pas fonctionné et de ce qui s'est avéré pertinent en gestion des risques (Kaplan et al., 2009 ; Mikes, 2011 ; Fox, 2011 ; Kaplan, Mikes, 2012 ; Power, 2009 ; Huber, Scheytt, 2013). Ces recherches montrent notamment que le Risk Management n'est pas infaillible, que les dispositifs de contrôle du risque peuvent présenter des faiblesses souvent décelées ex-post (Mitra, Hossain, 2011) à un évènement dommageable pour l'entreprise (pertes financière importante, crise médiatique par exemple). Elles se situent aussi dans une approche critique des normes comme ne permettant pas de répondre efficacement à une demande croissante de la Société quant à une exigence de meilleure maîtrise des risques (Hollingsworth, 2012).

Les éléments de littérature académique concernant le risque opérationnel sont moindres en nombre mais on note cependant une littérature émergente sur cette thématique. Cela atteste de la prise de conscience dans la communauté scientifique du rôle croissant joué par cette catégorie de risque au cœur de l'organisation et centrale comme facteur explicatif et parfois comme conséquence lors des défaillances rencontrées lors de la crise de 2007-2008. Le paragraphe « 1.4 » de ce chapitre détaille ces éléments de littérature. Nous reprenons ces éléments après avoir présenté la tendance émergente en matière de formalisation d'une théorie organisationnelle du risque, dans laquelle le contrôle des risques opérationnels s'inscrit.

1.3.2. Une évolution de la gestion des risques : d'une théorie du risque à une théorie organisationnelle du risque

L'objet du développement ci-après est d'envisager l'évolution de la théorie du risque en insistant sur l'apparition progressive d'une théorie organisationnelle du risque.

- **Une gestion des risques assurantielle et technique**

Pour P.L. Bernstein (1998, p.99 et s.) *« il est difficile pour nous aujourd'hui d'imaginer un monde ignorant les lois des probabilités ».* Il est également difficile d'imaginer un monde sans assurance, et de manière plus précise une entreprise non assurée pour les divers risques auxquels elle aurait à faire face.
L'évolution de la gestion des risques en entreprise s'est faite par le passage d'une démarche initialement tournée vars la recherche de sécurité et l'optimisation du recours aux mécanismes d'assurance vers une approche visant à accompagner la stratégie de l'entreprise.

Le risque est dynamique et en constante évolution. Dans les 18ème et 19ème siècles, la plupart des entreprises étaient de relativement faible taille et simple dans leur organisation, avec une utilisation minimale de matériaux complexes. Alors que les entreprises ont augmenté en volume, la gestion des risques est devenue plus complexe en raison du développement de nouvelles méthodes de travail. La législation et les progrès technologiques qui, sans changer les principes fondamentaux des risques, ont également eu une incidence sur la façon dont ils sont gérés. Certains risques ont disparu, de nouveaux se sont développés.

Concernant les entreprises et les organisations plus particulièrement, Fayol[27] évoquait dès 1916 la fonction de sécurité au sein des six fonctions principales de l'entreprise[28]. De nombreux économistes se sont ensuite intéressés à la thématique du risque et de la décision en univers incertain (Knight, 1921 ; Houston, 1960 ; Kahneman, Tversky, 1979).

Comme le relèvent Verbano et Venturini (2011), il faudra toutefois attendre de nombreuses années avant que des travaux émergent entre 1955 et 1963 concernant la gestion des risques.

[27] Henri Fayol, 1916, *Administration industrielle et générale.* Henri Fayol était chef d'entreprise (société de Commentry Fourchambault et Decazeville) et ingénieur civil du corps des Mines.
[28] Ces fonctions étant : la fonction technique (produire, transformer et fabriquer), la fonction commerciale (achat, vente et échanges), la fonction financière (recherche et optimisation des capitaux), la fonction sécurité (protéger les personnes et les biens), la fonction comptable (recensement des actifs, calcul de paie, statistiques) et la fonction d'administration (préparer, organiser, commander, coordonner, contrôler).

A cette période, il était question avant tout de réduire le coût des assurances en mettant en place des moyens et techniques de protection et de prévention au sein de l'organisation. Il s'agissait de rechercher grâce à l'aide des courtiers les meilleures offres d'assurance pour la firme.

Gallagher précise quant à lui, dès 1956, la nécessité d'une personne employée à temps plein pour gérer les risques de l'entreprise et réduire les pertes, mettant en place la gestion des différentes polices d'assurances de l'entreprise. Ainsi, la période préindustrielle correspondait à l'apparition des premières assurances et la période industrielle au développement des couvertures d'assurance (visant le refinancement d'activités soumises à un danger potentiel). Une telle conception de la gestion des risques visait et vise encore aujourd'hui à ce que les assureurs facilitent le financement du risque et réduisent son coût.

La gestion des risques depuis son apparition en tant que fonction à part entière, au début de la seconde moitié du XXe siècle et jusque dans les années 70-80 se veut largement préventive. Il s'agit de la gestion des risques[29] pour compte de tiers. Il incombe aux assureurs de gérer et d'assumer, les risques des grandes industries dans un premier temps, puis du secteur tertiaire en second lieu (prestataires de services, établissements financiers). Les assureurs se dotent alors de modèles permettant une meilleure connaissance (identification, évaluation) et maîtrise des risques de leurs clients, ce afin d'assurer l'équilibre de leurs activités d'assurance que de permettre une meilleure prise en compte de l'avenir des organisations face au risque.
L'approche par le transfert de risque prévaut donc jusque dans les années 1970.

Le risque était avant tout considéré au regard de la conséquence économique ou financière directe sur l'entreprise. Peu à peu se formalisa la démarche de gestion des risques en trois parties (années 60) : identifier, évaluer et traiter des risques (Mehr, Hedges, 1963).

[29] Les risques concernés sont principalement les risques accidentels et industriels. Les industriels cherchant alors à limiter les pertes découlant d'activité dont la dimension technique allait croissante et de ce fait la maîtrise du risque n'était pas totale. Transférer le risque apparaît alors comme une solution efficace dans une industrie en expansion.
Certains auteurs, tenants de cette gestion des risques à tonalité assurancielle, distinguent alors « risques purs » (l'incendie par exemple) et « risques spéculatifs » ou encore « risques fortuits » et « risques prévisibles ». (Doherty, 1985).

Dans les années 1980, la crise affectant le marché de l'assurance a rendu plus difficile le fait de pouvoir s'assurer contre les nombreux risques que peut connaitre une entreprise, le coût des assurances devenant très élevé (notamment aux Etats-Unis), cela impliqua de faire davantage appel à ces techniques et méthodes encore récentes de gestion des risques. Les années 1990 et l'essor des variables économiques et financières firent évoluer les entreprises vers une spécialisation des techniques et un accroissement du recours à la gestion des risques, en vue de se prémunir contre les fluctuations de l'économie et la volatilité croissante des marchés. Ce fut le développement de l'Alternativ Risk Transfer ainsi que de la gestion stratégique des risques (Clark, Varma, 1999).

Le début des années 2000 vit se développer la gestion des risques d'un point de vue à la fois financier et stratégique (Doherty, 2000). Cela amena progressivement une vision intégrée de la gestion des risques telle que nous la connaissons aujourd'hui et qui se développe bien au-delà du monde anglo-saxon dont elle est issue.

La gestion des risques dans cette version récente se définit comme une approche structurée intégrant les éléments de la stratégie, les processus, le personnel, la technologie et les savoirs dans le but d'évaluer et de gérer les menaces et opportunités auxquelles l'entreprise doit faire face dans le processus de création de valeur (De Loach, 2000).
Cette approche suppose de redéfinir chaque fonction en y intégrant la vision risque en vue de repousser des barrières culturelles qui supposeraient le refus du risque. Les risques clés affectant la conduite des affaires peuvent être gérés via une approche holistique, intégrée, orientée vers le futur dans le but de maximiser la valeur actionnariale de l'entreprise (De Loach, 2000).

Des accidents affectent des sociétés tous les jours, mais seule une infime partie d'entre eux est catastrophique. Les minimiser va au-delà d'une simple question d'assurance. La bonne stratégie réside dans une approche gestionnaire de risque et implique l'élaboration d'un plan en cas de catastrophe et d'une gestion de crise. Braithwaite (1989) explore la mise en place et l'organisation de ces régimes qui impliquent, entre autres choses, la relation et la coordination des risques, la définition des responsabilités, des back-up de contact, de soutien et communication, des tests réguliers, le recours à l'assurance. L'auteur insiste sur le fait qu'à long terme la viabilité d'une entreprise doit inclure un développement de la stratégie quant à la gestion du risque, la prévention des pertes de contrôle et de confinement des dommages.

On constate parallèlement un essor des typologies de risques, des méthodes et techniques dédiées à la gestion des risques ; le tableau ci-après en fournit une illustration même si d'autres auteurs[30] distinguent de manière plus précise les classes de risque.

Tableau 9. Classification des risques clés pour les organisations, d'après Verbano et Venturini (2011)

Risque d'atteinte à l'intégrité physique	Risques financiers	Risques opérationnels	Risques stratégiques
Incendie et dommages aux biens Risques naturels Perte d'exploitation, interruption d'activité Infirmité, accident de travail, risque homme clé etc. Engagement de responsabilité Risque technologique	Risque de prix Risque de liquidité Risque de crédit Risque d'inflation	Risque pesant sur la conduite des opérations (Risques psychosociaux, développement produit, risque de la chaine de valeur) Risques liés aux systèmes d'information, au défaut de fiabilité du reporting comptable et financier, risque sur l'évaluation des investissements etc.	Risque de réputation Risque client Risque de changement politique et réglementaire Risques liés aux variables démographique et socioculturelle Risques liés à la concurrence

- **Une gestion des risques participative et globale**

Cette évolution de la gestion des risques en entreprise va donc de ce qui était une gestion assurantielle du risque ou une gestion spécialisée dans un domaine de risque précis (par exemple les risques industriels) à une gestion globale du risque.

Comme l'exprime Jean-Paul Louisot (2007) : *« Dans le contexte mondial actuel, il est clair que la vision traditionnelle et réactive de l'acheteur d'assurance protégeant le patrimoine de l'organisation est obsolète. Elle doit faire place à une vision proactive, dynamique, beaucoup plus large de la gestion des risques visant la protection des objectifs ou missions de l'organisation »*[31].

[30] Voir Notamment J-D. Darsa, 2011, *La gestion des risques en entreprise*, Gereso: sur les 13 classes de risque en entreprise.
[31] Extrait de l'article paru dans RiskAssur Hebdo en 2007.

La fin du XXe siècle et le début du XXIe siècle ont vu se développer un contexte propice à l'apparition progressive de l'ERM (*Enterprise Wide Risk Management*, aussi appelé *Business Risk Management*) ou gestion globale du risque. Dans un contexte où l'entreprise n'est plus une *« boîte noire »* isolée des autres parties prenantes de son environnement, mais bien en lien avec ces dernières[32], la gestion globale des risques s'impose comme une nécessité. Le risque est aujourd'hui davantage le fruit d'une négociation que d'une simple décision par l'entreprise elle seule, car l'éthique constitue un risque à part entière.

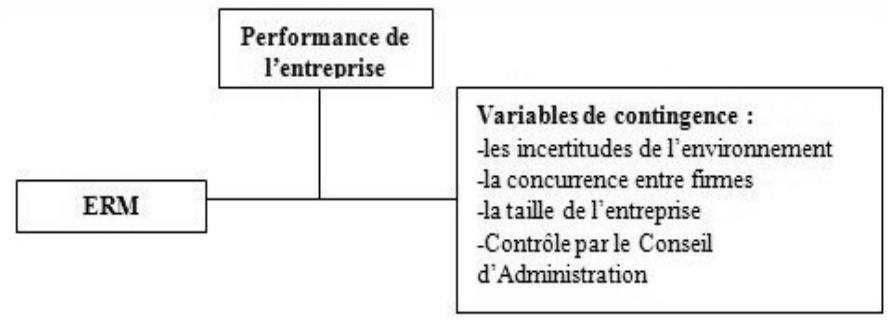
Le référentiel COSO (2004, 2013) définit l'ERM comme un processus adopté par la direction de l'organisation, le personnel, le management, appliquant la stratégie dans l'ensemble de l'entreprise et visant à identifier les évènements potentiels pouvant survenir et affecter l'entité. Ce processus est encore conçu pour déterminer l'appétence au risque tout en fournissant une assurance raisonnable quant à l'atteinte des objectifs de l'organisation.

L'ERM est fondé sur une approche organisationnelle, participative, visant à instaurer une certaine dynamique tournée vers le risque et la prise de décision (Arena et al., 2010).
Cette démarche appartient à une nouvelle vague d'approche auto-régulatrice débutant dans les années 1990 et conçue pour durer. Elle est la principale voie envisagée depuis cette période pour gérer l'incertitude entourant l'entreprise et a fait évoluer la gestion des risques d'une fonction périphérique de l'organisation à une fonction se rapprochant de la gouvernance d'entreprise. L'ERM lie la gestion des risques à la stratégie de l'entreprise et aux objectifs opérationnels de celle-ci, comprenant la prise de décision, les enjeux de contrôle et de comptabilité.
L'essor de cette fonction est lié à un environnement économique se complexifiant, une concurrence exacerbée, la recherche d'une rationalité accrue, la prise en compte de nombreux risques : interruption des systèmes d'information, fraudes, risques croissants de faillite, inflation normative et réglementaire, la surexposition financière de certaines firmes, volatilité accrue des cours de bourse (Hunt, 2003). Ces éléments sont tels qu'il existe, selon certains auteurs, des pressions convergentes se traduisant par une *« explosion du Risk Management »* au sein des organisations (Power, 2004, p.9).

[32] Voir sur ce point les travaux relatifs au modèle institutionnel de l'entreprise (Williamson, 1985 ; Jameux, Munier, 1977). L'entreprise est face à de nombreux acteurs : fournisseurs, clients, États et collectivités territoriales, associations diverses (notamment défenseurs de l'environnement), opinion publique. Voir encore l'article de Ronald Coase 1937, *The nature of the firm.*

Ces dernières années, on constate un changement de paradigme quant à la manière de percevoir la gestion des risques. Au lieu de voir la gestion des risques selon une approche en silo, celle-ci s'inscrit désormais dans une vision intégrée dite holistique. ERM et performance sont liés, la performance de l'entreprise est contingente de sa faculté à mettre en place un dispositif de management des risques efficace et suffisamment transverses pour s'appliquer a minima à toutes les fonctions stratégiques de l'entreprise (Gordon et al., 2009). Cette approche est alors vue comme le moyen le plus performant de gérer le portefeuille de risques de l'entreprise (Liebenberg, Hoyt, 2003). Beasly et al. (2005) mettent encore en avant le fait que le comité exécutif et le senior management ont un rôle critique dans la réussite d'une implémentation de l'ERM. D'autres facteurs de contingence contribuent à influencer la mise en place de ce type de processus de gestion : le rôle joué par les auditeurs, la taille et le type de l'organisation (industrie, secteur des services, secteur financier etc.), le pays d'appartenance de l'entreprise.

Figure 15. L'Enterprise Risk Management,
entre contingence et performance, d'après Gordon et al., 2009.



Ces variables de contingence montrent la dépendance, en pratique, de l'ERM aux contextes sectoriels, à la stratégie de l'entreprise mais aussi au positionnement concurrentiel. On peut aussi y voir une limite des approches actuelles, si la recherche de la performance est un objectif commun à toutes les entreprises, il n'est pas certain que les démarches d'ERM soient aussi efficaces dans tous les secteurs d'activité, comme l'illustre la crise financière de 2007-2008 dite des subprimes qui a montré le caractère vulnérable de tels dispositifs.

La dimension participative du Risk Management permet donc d'innover dans la prise en compte des risques en partageant de nombreuses expériences et en soulevant des propositions de solutions. Toutefois, uniquement communiquer sur le risque présente des limites. Les employés doivent avoir une compréhension des risques liés à l'activité de l'entreprise, la nécessité de les prendre ainsi que la manière dont ils sont gérés et réduits. Les risques ne sont pas uniquement l'affaire des dirigeants dans le cadre d'une stratégie d'ensemble de gestion des risques. L'un des rôles du Risk Manager est donc de fédérer les différents membres du management autour de cette notion de risque afin que ces derniers fassent redescendre la sensibilisation au niveau des entités leur étant allouées. En ce sens, intégrer la réflexion sur la culture comme instrument au service du contrôle des risques est une des conditions de réussite du Risk Management. Il s'agit du moins de l'un des objectifs que doit poursuivre une politique pertinente de gestion des risques. Une communication intégrée sur les risques est donc essentielle et ne peut être découplée du Risk Management (Niestat, 2005). Elle consiste à savoir dicerner parmi la multitude de connaissances et d'informations dans l'organisation, celles réellement utiles quant à l'objectif de maîtrise des risques. A cet égard, la gestion des risques s'inscrit en tant qu'enjeu de savoirs construits voire « coconstruits » (Revet, 2013).

Ladite communication visera alors une sensibilisation aux différents risques avec des adaptations selon les classes de risques. Des formations complémentaires s'avéreront pertinentes dans le cadre d'une démarche de sensibilisation.

En fin de compte, gérer les risques, c'est aussi gérer les relations en interne et avec l'extérieur.

D'autres auteurs développent une approche distincte du contrôle des risques. Cette dernière est fondée sur la vision du risque comme coût. Les actions de contrôle des risques auront pour principal but de réduire le coût du risque. Pour Fehle et Tsyplakov (2005), la nécessité de gérer les risques est liée aux imperfections de marché affectant les entreprises. Le Risk Management est envisagé comme un moyen de réduire les pertes financières mais aussi

l'incertitude pesant sur le prix des consommations des entreprises ou encore les variables réglementaires et fiscales.

Pour Colquitt et al. (1999), la gestion des risques suppose une véritable vision stratégique et une approche intégrée car le marché du transfert de risque n'est en soi pas une option toujours suffisante. L'approche par le financement du risque trouve sa pertinence mais également ses limites (captives d'assurances notamment, rétention des risques par l'entité via un autofinancement). La gestion des risques suppose en effet de participer à la sauvegarde et à la création de valeur en prenant en compte des variables telles que la taille de la firme, sa stratégie, son environnement concurrentiel etc.

Le Risk Management est lié à une culture du calcul dans l'entreprise, cela suppose un lien avec le contrôle de gestion et la contingence avec les variables décrites ci-après par Mikes (2009) :

Figure 16. Risk Management et culture du risque (Mikes, 2009)

L'approche quantitative et assurantielle manque à elle seule de sens, notamment en ce qui concerne les risques organisationnels (tels que les risques humains ou les risques opérationnels). Il faut passer d'une approche en silo, séparant différentes fonctions, à une approche intégrée pour mieux prendre en compte *« l'agrégation des risques dans l'entreprise »* (Mikes, 2009, p.24). On retrouve ainsi la notion de culture du risque qui doit

être diffusée via des politiques d'entreprise et donner du sens au dispositif global de maîtrise des risques.

L'auteur (A.Mikes), en étudiant plusieurs établissements bancaires, décrit ainsi différentes approches caractérisant la gestion des risques que l'on peut observer dans les organisations. On retrouve notamment outre l'approche en silo où les fonctions dédiées au risque sont séparées, une approche visant l'intégration des risques, une approche basée sur une mesure de performance incluant les risques (Risk-based Management) et enfin une approche holistique du Risk Management qui vise à tenir compte de manière significative des risques non quantifiables. Cette approche se veut encore plus englobante en intégrant la notion d'incertitude dans le processus de Risk Management.

Ces 4 idéaux-types du Risk Management se résument ainsi :

Tableau 10. Les idéaux-types de la gestion des risques
(Adaptation, d'après A. Mikes, 2009)

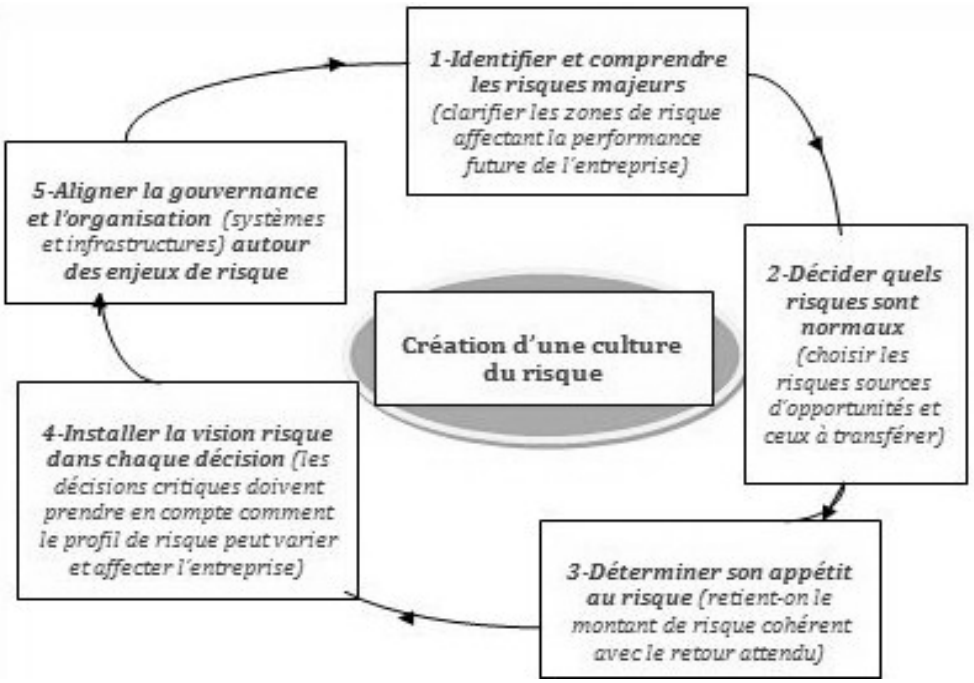
	Approche en silo	**Approche intégrée**	**Approche risque-performance**	**Approche globale (ou holistique)**
Cadre institutionnel	Régulation internationale et allocation de capital	Notation des agences et allocation e capital	Impératif d'augmentation de la valeur de l'entreprise	Essor d'une approche risque et contrôle interne dans la décision
Thématique de risque	Quantification des risques	Agrégation des risques	Approche risque basée sur la mesure de performance	Gestion des risques non quantifiables également prise en compte
Objectifs poursuivis, focus	Mesure et contrôle des risques en silo, calcul du minimum de capital requis (dans les secteurs réglementés type banque)	Assignation d'un dénominateur commun selon les différents silos (capital économique)	Calcul de la création de valeur pour les actionnaires, lien entre performance et mesure du risque	Inclusion des risques non quantifiables dans le processus de gestion des risques (sur la base d'avis du senior management)
Techniques utilisées	Loss Distributions Approach (LDA), modélisation	Capital économique	RAROC (Risk Adjust Return On Capital), transfert de risque	Analyse de scénarios, analyse de sens, revue des risques

Les techniques de gestion des risques doivent toutefois être fréquemment revues et ajustées pour ne pas devenir obsolètes comme le démontre l'auteur. Ainsi, aux approches purement techniques et financières de gestion des risques se sont substituées les approches organisationnelles en développement aujourd'hui. Cette nouvelle donne de la gestion des risques positionne les questions de culture organisationnelle au centre des enjeux de gestion des risques.

Les enjeux de la culture organisationnelle liés au risque

Dès 1986, Singh analyse la relation entre prise de risque dans le processus de décision et performance organisationnelle (Singh, 1986). Les recherches montrent alors qu'il existe une relation indirecte entre ces notions. Par une médiation, par le biais d'un management incitatif, visant le développement d'une culture organisationnelle introduisant la prise de risque et permettant une performance accrue. Dans la lignée de ces travaux, Klein (2011) démontrait que la culture d'entreprise, au même titre que la stratégie peut être développée par les managers et dirigeants d'entreprise en vue de renforcer la performance de l'entreprise. La culture est contingente de la stratégie développée ; la stratégie permet de faire émerger une certaine culture d'entreprise et cette même culture déterminera l'appétence au risque, la recherche de la performance, de revenus supérieurs etc. Construire une norme culturelle implique de développer une approche de qualité là où des normes défensives dans l'organisation ne le permettent que de manière relative. Buehler et al., dans un article paru dans la Harvard Business Review en 2008, identifient les éléments d'un état d'esprit orienté risque et de la diffusion d'une culture du risque.

Figure 17. Les risques : entre état d'esprit et culture (d'après Buehler et al., 2008b)

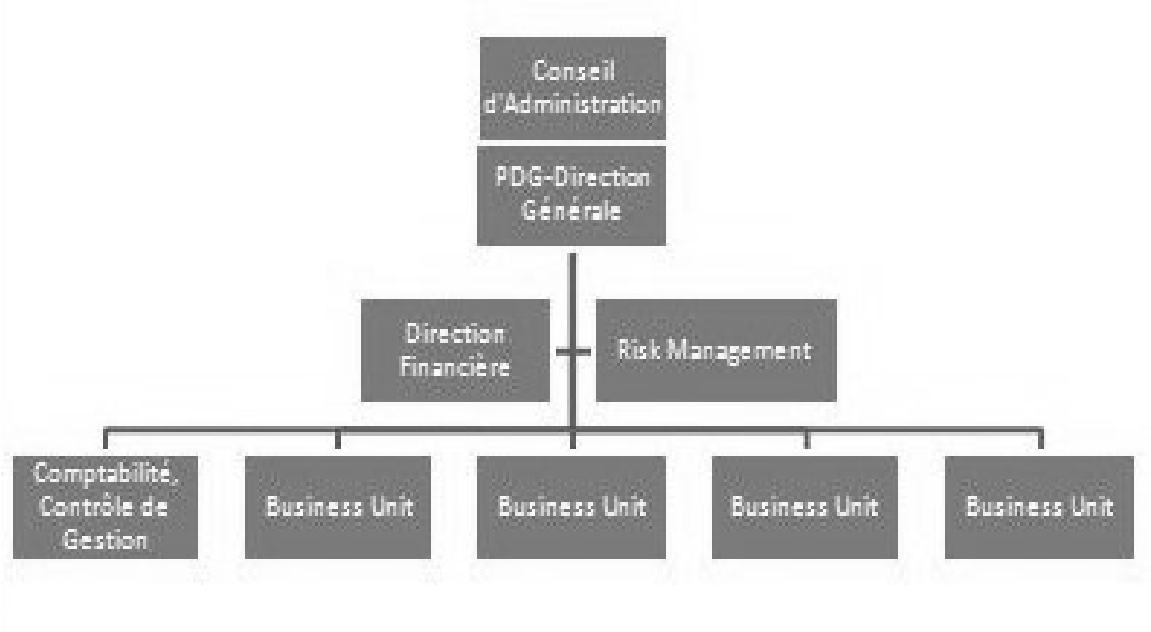


Ces mêmes auteurs démontrent alors que cette approche culturelle apparaît comme pertinente si elle implique conjointement le Chief Risk officer (CRO)[33] et le Chief Financial Officer (CFO) en vue de faire redescendre parallèlement les enjeux de risque et les enjeux financiers dans les différents centres d'activités. En outre, grâce à des outils sophistiqués, cela permet d'éviter une surexposition au risque de même qu'une couverture d'assurance excessive.

Le schéma ci-après issu de travaux de recherche de Buehler et al., (2008) traduit le positionnement que l'on retrouve le plus fréquemment de la gestion des risques (CRO) et de son rôle dans l'organisation quant à la diffusion d'une culture du risque. Ces éléments nous amènent à décrire la gestion des risques dans une approche globale qui consiste en un mouvement d'aller-retour Top Down / Bottom-Up[34].

[33] Respectivement responsable / directeur des risques et directeur financier.
[34] Descente d'informations relatives au risque entre le Top Management et les différents étages de l'organisation (Top Down) et remontée d'informations vers la hiérarchie (Bottom Up).

Figure 18. Positionnement du Risk Management dans l'organisation, d'après Buehler et al., (2008b)



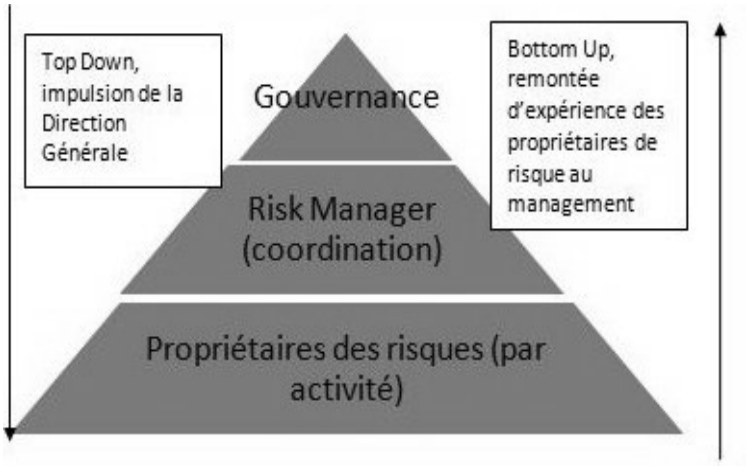
La diffusion de la culture du risque, un cadre d'institutionnalisation du risque

Le Risk Manager (ou responsable des risques) n'est pas décisionnaire, il possède un rôle largement consultatif, mais il doit néanmoins gérer les décisions une fois prises. Son champ d'action décisionnaire concerne le traitement des risques associés à ces décisions. Pour être pleinement efficace à cet égard, il se doit d'être coordinateur entre la gouvernance de l'entreprise et les différents propriétaires de risques. Cela se fait en fonction de la politique de risque déterminée par la Direction Générale et adaptée par la remontée d'informations issues des différents départements et services (par le biais du Risk Manager). Dans le cadre du processus de gestion globale des risques, notamment lors d'une étape essentielle vers la maîtrise des risques qu'est l'élaboration d'une cartographie des risques, l'approche *top down* ou *bottom up* sera privilégiée. Il s'agira alors de réaliser une cartographie des risques pour chaque entité, à chaque niveau (groupe / filiales), par activité, et de procéder à une mise en commun. Une approche Top Down aura pour avantage de mettre clairement en exergue la volonté de la Direction Générale de donner une impulsion dans la mise en place d'un processus de Risk Management. Les menaces seront mises en évidence au niveau global et l'accent sera mis sur la nécessité d'une adhésion du management décisionnel (Véret, Mékouar, 2005). Il existe clairement un rôle du comité de direction en vue de mettre en place et de bien positionner la fonction de gestion des risques, un mauvais positionnement peut avoir deux conséquences : une fonction non dotée des moyens permettant la réussite de la

démarche de gestion des risques, un désintérêt des acteurs de l'organisation pour ce sujet jugé non prioritaire à la fois pour eux-mêmes mais aussi pour la direction générale de l'entreprise (Sheehan, 2009).

L'approche Bottom Up permettra quant à elle de mieux apprécier des risques opérationnels a priori de faible impact, mais dont le cumul, l'agrégation, peut atteindre des montants non négligeable pour l'entreprise. Une telle approche permet encore de mieux détecter les risques orphelins (n'ayant pas de propriétaires de risques[35] à proprement parler, il s'agira alors de risques transverses entre plusieurs fonctions), d'obtenir davantage d'informations sur chaque risque afin d'y allouer les ressources de la manière la plus optimale qui soit (Hanssen, 2005 ; Rötheli, 2010).

Figure 19. Approche Top-Down et Bottom-Up de la gestion des risques



- **Les risques, au-delà de la culture, une question de sens**

Comme le remarque Drott-Sjoberg (1991), le risque est devenu un sujet de communication en management et dans la vie de tous les jours. Les réactions sont différentes pour les risques naturels et pour les risques liés à l'activité humaine (man-made risk). Ainsi, les risques issus de l'activité humaine sont bien souvent difficiles à percevoir en cours de survenance et parfois intangibles a priori. La question de la réaction aux risques, tout comme de la communication

[35] La notion de propriétaire de risque désigne les acteurs responsables de la gestion des risques sur un périmètre donné. Par exemple, sur la direction des ressources humaines d'une entreprise, le référent risque RH, à défaut le directeur des ressources humaines.

sur ces derniers, est avant tout une question de sens (Weick, 1995) et suppose un relativisme associant risque et bénéfice.

Certaines études démontrent que les managers sont prêts à prendre des risques, quelle que soit leur organisation, si ces risques ont un sens et sont pris dans le cadre de la stratégie de l'entreprise et en tenant compte de son cœur de compétence (Noy, Ellis, 2003).

Ainsi, la stratégie peut varier dans sa mise en œuvre au sein d'une même organisation en fonction des perceptions du risque que l'on peut avoir. La propension à prendre des risques sera ainsi plus élevée dans les fonctions de l'entreprise se trouvant dans ce cœur de compétence et supportant l'avantage concurrentiel de l'entreprise. En termes de vision, cela suppose de ne pas regarder le risque comme quelque chose à éliminer (Girotra, Netessine, 2011, p.104) mais bien comme un facteur influant sur les ressources et capacités de l'entreprise.

1.4. La gestion globale des risques dans le secteur financier, état des recherches et prise en compte du risque opérationnel

Plusieurs ouvrages et études de référence ont traité du cadre organisationnel de la gestion des risques dans le secteur financier. Les travaux de Lamarque et Maurer (2009) offrent une synthèse en la matière concernant le secteur bancaire et la division en trois axes de cette gestion des risques, proche du cadre réglementaire.

1.4.1. La constitution progressive d'un corpus de recherches relatives au risque opérationnel

Les travaux fondateurs de M.Power (2005) exposent les prémices d'un enjeu de recherche à part entière en gestion : ses apports sont notamment de formaliser la notion-même de risque opérationnel, qui bien que préexistante au cadre réglementaire dans le secteur financier, appelle des études dédiées quant à son objectivation, à la nécessité d'en faire un enjeu à de gestion intégrant identification, quantification mais aussi mesures de traitement-réduction dédiées.

L'éclairage apporté par J.C. Hull dans son ouvrage de 2007 (*Risk Management and Financial Institutions*) résume cette gestion des risques opérationnels de la manière suivante. Ses apports théoriques ont été complétés par un certain nombre d'études récentes:

-Pour J.C. Hull, il existe de multiples manières de définir le risque opérationnel. Comme d'autres auteurs avant lui (Hoffman, 2002), il l'exprime par la différence : *« ce qui n'est pas du risque de crédit ou de marché »* (Hull, 2007, p.321) ; une variation dans les résultats opérationnels résultant de pratiques à risque par exemple. L'auteur reconnait que la définition donnée par la réglementation quant au risque opérationnel est à la fois trop large (comprenant des risques externes et internes, des risques politiques et des risques liés à la régulation elle-même, les risques liés à l'intégration d'un nouveau marché, des facteurs économiques, le développement de nouveaux produits etc.) et par certains aspects trop étroite (ne comprenant que tacitement des risques majeurs tels que ceux liés au rogue trading ou excluant le risque de réputation pourtant très lié au risque opérationnel, ou encore les risques stratégiques).

-On peut mentionner des recherches ayant consisté à identifier les déterminants du risque opérationnel dans les sociétés du secteur financier en France (Maurer, Lamarque, 2009 ; Torre-Ensico, Barros, 2013) et dans le monde anglo-saxon (Chernobai et al., 2011). Certains travaux ont ainsi montré que dans un environnement post-crise les sociétés prennent davantage en compte l'enjeu de déstabilisation que constitue le risque opérationnel (Andersen et al., 2011). Elles sont notamment plus que par le passé sensibles à l'innovation financière comme facteur de risque opérationnel (Philippas, Siriopoulos, 2009).

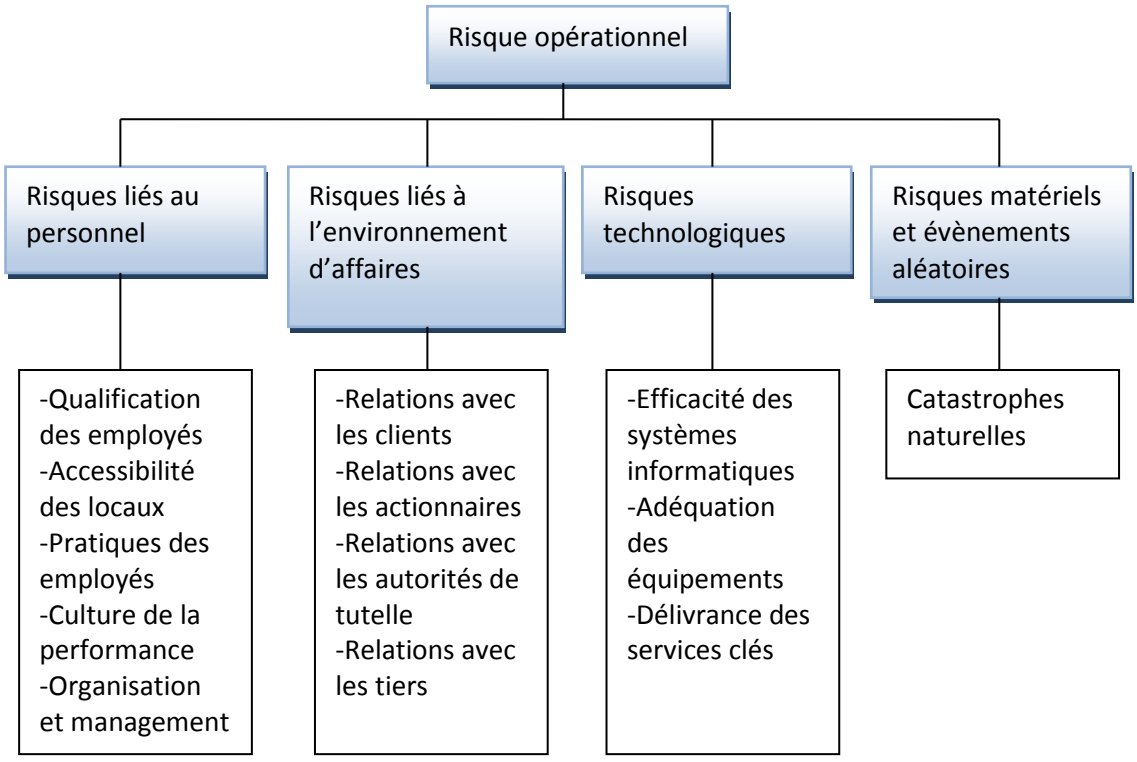
-une importance de l'approche financière comparant coût du capital au retour sur investissement. Elle consiste à identifier le coût du risque associé au capital et à la perte de ce dernier, puis à comparer cela aux perspectives de revenus futurs escomptés. Cette approche est largement connue et a fait l'objet de nombreuses études empiriques et académiques (Froot, Stein, 1998 ; Evanoff, Wall, 2002 ; Ai et al., 2011).

-le rôle croissant de méthodes complexes basées sur les simulations et modèles et mobilisant des outils telle la VaR (Value at Risk) ou cherchant encore à établir des analyses de corrélation et de causalité statistiques pour tenter de discerner les phénomènes de survenance de risque. Cette approche tend à se développer pour se rapprocher de ce qui est qualifié « d'intelligence du risque ». Une approche dans laquelle il est nécessaire de structurer l'information financière et extra-financière en vue d'un plus grand discernement à l'égard de cet objet complexe qu'est le risque (Apgar, 2006).

-un rôle encore émergent des problématiques avant tout organisationnelle de gestion des risques au titre desquelles le risque opérationnel constitue un élément moteur de prise de

conscience. L'histoire du risque opérationnel dans le secteur financier comporte de nombreux cas de banques américaines, anglaises, allemandes, françaises, irlandaises mais aussi turques par exemple, et pour lesquelles *« les défauts de structuration de la gestion des risques peuvent rapidement transformer une imperfection de marché en pertes significatives »* (Bodur, 2012, p.77). Pour Kulpa et Magdon (2012), la majorité des scandales ou des crises ayant affecté des établissements financiers lors des deux dernières décennies a débuté avec un problème opérationnel. Les problèmes opérationnels récurrents sont listés par les auteurs dans le schéma ci-après. Dans la majorité des cas, des processus inadaptés étaient en cause, viennent ensuite le personnel (fraude notamment, erreur humaine non intentionnelle, faute intentionnelle), les systèmes (brèches dans le dispositif de contrôle non révélées à temps par l'audit interne) et enfin des évènements externes (catastrophes naturelles, grèves).

Figure 20. Les formalisations fréquentes du risque opérationnel, d'après Kulpa et Magdon, 2012



Dans ces différents cas, si le risque opérationnel ne peut être complètement empêché, il existe cependant des manières de réduire son impact ainsi que sa probabilité de survenance. Cela passe par la mise de place de politiques dédiées au risque opérationnel dont l'enjeu est à la fois un enjeu de gestion du coût du risque mais aussi de développement d'une organisation

centrée sur le développement d'une réelle culture du risque tournée vers l'anticipation (Hanssen, 2005 ; Ospital, 2006 ; Bon-Michel, 2011).

1.4.2. La recherche progressive de grilles de lectures adaptées

Les cas médiatiques concernant des établissements concurrents ou d'autres départements permettent aux décideurs de voir les risques opérationnels pouvant les affecter (Hora, Klassen, 2013). L'une des difficultés reste de savoir comment ces mêmes risques pourraient les concerner dans des configurations proches.

Face à la grande diversité des formalisations du risque opérationnel, les recherches récentes relatives au risque opérationnel soulignent la nécessité de déterminer un cadre de lecture théorique adapté.

La littérature récente y répond de la manière suivante :

-Le degré d'effectivité des dispositifs de maîtrise du risque opérationnel est contingent de la capacité des entreprises à organiser une culture dédiée. Cela passe par une sensibilisation des managers et dirigeants au fait de s'informer régulièrement sur la réalité du risque opérationnel dans leurs champs de responsabilité et dans celui des autres managers. Les travaux récents insistent sur le fait que les managers ayant une approche pertinente en la matière ne sont pas nécessairement ceux qui ont une connaissance exhaustive des risques passés dans leur domaine. Il s'agit davantage de ceux développant une capacité à se tenir informés et à être en alerte de manière continue sur des risques latents. Développer cette culture orientée risque opérationnel apparait comme une solution intéressante dès lors que les informations recueillies servent la conduite de l'activité courante (Hoffman, 2002 ; Hanssen, 2005 ; Mikes, 2007).

-Les informations récoltées en matière de risque opérationnel reflètent trop souvent les risques passés de l'établissement et ne sont pas suffisamment axées sur les risques futurs (Bon-Michel, 2011). Or une telle approche permettrait de réels progrès en matière de maîtrise des risques en insistant sur les axes d'amélioration futurs dans une logique d'apprentissage organisationnel. Cette logique prospective dans la collecte d'information permettrait de gagner en pertinence en situant la gestion des risques en amont des projets et des nouvelles activités des établissements financiers. Il s'agit d'étudier les risques potentiels afin de savoir

si un projet sera lancé avec un degré de maîtrise raisonnable, ce qui suppose une culture de la communication entre acteurs de l'organisation (Bon-Michel, Dufour, 2013).

-Face à des causes de risques opérationnels disparates et à des enjeux financiers de magnitude très variable selon le type de risque opérationnel, certains auteurs insistent sur la nécessité de se doter d'outils de gestion des données plus que d'outils de gestion du risque à part entière qui correspondent à l'enjeu de réglementation prudentielle qui n'est qu'une partie du problème associé à cette catégorie de risque. Ce, d'autant plus que pour ces mêmes auteurs la réglementation prudentielle a un temps de retard sur la réalité des préoccupations en matière de risque (Kraujalis et al., 2006 ; Chernobai, 2011 ; Guegan et Hassani, 2013).

-Certaines recherches insistent encore sur le manque de partage d'information entre structures et départements d'une même organisation. Un décloisonnement est nécessaire pour avoir une information complète sur le risque opérationnel au sein d'un établissement financier. Le manque de partage effectif d'information, c'est à dire d'informations utiles aux décideurs comme aux managers de risque reste l'une des difficultés principales à ce jour. Cette difficulté explique en pratique le manque de résilience de certains établissements financiers face aux pertes opérationnelles sur de nombreux projets et produits financiers. Par manque de résilience, les auteurs entendent le défaut de capacité des décideurs à mettre en place des solutions de long terme pour des risques opérationnels considérés comme des risques subis car peu d'informations adaptées permettent de les identifier et de connaitre leur causes racines (Frost et al., 2000 ; Francis, 2011).
Un partage d'information efficace concerne les fonctions opérationnelles évoluant au sein d'un même département d'un établissement financier mais aussi les différentes lignes managériales et les fonctions supports. Les recherches mettent également en avant la nécessité d'inclure davantage les différentes fonctions de contrôle des établissements dans le processus de gestion du risque opérationnel tel que l'audit interne notamment (Fernández-Laviada, 2007).

-Au-delà de l'exhaustivité de l'information relative au risque opérationnel, il est nécessaire de progressivement structurer celle-ci pour éluder les nombreuses informations peu pertinentes en matière de risque opérationnel. Une multitude d'évènements sont en effet mentionnés en tant que risque opérationnel sans pour autant en être, ce qui rend complexe la gestion des

vrais risques opérationnels et décrédibilise la démarche globale sur ce sujet (Jebrin-Abu-Salma, 2012 ; Jednak, Jednak, 2013).

Ces différentes recherches, bien qu'encore à un stade exploratoire pour la plupart, montrent qu'il s'agit d'un enjeu de préoccupation croissant dans la communauté académique comme dans le monde professionnel. Ces dernières prennent en compte l'enjeu risque opérationnel au travers des sujets de normes, d'organisation et de stratégie, mais aussi de comportements, culture, structuration des contrôles et de l'information.

Tableau 11. Synthèse des principaux travaux relatifs au risque opérationnel

Les principales recherches en gestion relatives au risque opérationnel			
Domaines d'études	Objets de recherche	Apports	Auteurs
Notion	Définir le risque opérationnel	Le risque opérationnel concerne toutes les organisations et intègre la double composante structure-comportement.	Hoffman, 2002 ; Power, 2005 ; Hull, 2007 ; Torre-Ensico, Barros, 2013
Organisation et contrôle	Formaliser et adapter les contrôles face au risque opérationnel	Le contrôle du risque opérationnel est par principe parcellaire et réactif.	Mikes, 2007 ; Fernández-Laviada, 2007 ; Philippas, Siriopoulos, 2009 ; Andersen et al., 2011 ; Kulpa et Magdon, 2012 ; Jebrin-Abu-Salma, 2012 ; Jednak, Jednak, 2013
Stratégie	Définir les stratégies de gestion du risque opérationnel	Il existe une double stratégie à la fois financière (optimiser le coût des fonds propres), et organisationnelle (réduire durablement l'exposition au risque).	Froot, Stein, 1998 ; Evanoff, Wall, 2002 ; Ai et al., 2011 ; Hora, Klassen, 2013
Information	Déterminer les composantes du risque opérationnel	Nécessité de structurer l'information relative au risque opérationnel.	Frost et al., 2000 ; Kraujalis et al., 2006 ; Francis, 2011 ; Chernobai, 2011 ; Guegan et Hassani, 2013
Normes	Expliciter le lien entre norme et gestion du risque opérationnel	Le risque opérationnel est un enjeu de provisionnement mais aussi de gestion active.	Maurer, Lamarque, 2009 ; Chernobai et al., 2011
Culture et comportements	Comprendre et mettre en œuvre une culture du risque opérationnel	La culture du risque opérationnel repose sur un ensemble d'acteurs clairement identifiés et chargés de ce sujet.	Hanssen, 2005 ; Apgar, 2006 ; Ospital, 2006 ; Bon-Michel, 2011

En définitive, on constate que le nombre de recherches académiques dédiées au risque opérationnel restent encore limité. Cependant, la quasi-totalité de ces travaux date de la décennie 2000 dont une majorité lors des cinq dernières années (décennie 2010), signe d'un intérêt prononcé pour ce sujet de recherche.

La diversité des recherches et des sujets étudiés relatifs au risque opérationnel exprime encore la difficulté de trouver des cadres de référence en la matière et incite à penser cette thématique organisationnelle en tant que notion, et en tant que sujet de gestion. Il s'agit d'un champ de recherche à part entière sur le risque dans sa dimension organisationnelle. Ce sujet, bien que ciblé sur le secteur financier dans notre étude, dépasse même ce dernier en cela qu'il comporte des enjeux liés à la sécurité des biens et des personnes ou encore aux systèmes d'information et aux erreurs de décision et de gestion (étant des objets de recherches à part entière notamment dans le domaine industriel). Nous pouvons donc conclure en l'intérêt croissant de cet objet de recherche dans le monde académique mais aussi à la nécessité de mobiliser des grilles de lecture adaptées. Ce qui nous amène à exposer des développements en ce sens dans la seconde partie de ce chapitre.

II. Cadre conceptuel, grilles de lecture théoriques mobilisées : De la sociologie des organisations et du contrôle à la théorie socio-économique

Si la gestion des risques a fait l'objet de nombreux travaux depuis les années 1970, les risques dans le secteur financier ont principalement été envisagés dans une logique quantitative et financière (risque de crédit, de marché, transfert et couverture de risque). Le risque opérationnel, difficilement quantifiable, notion plus récente et contingente de la sphère organisationnelle, a fait l'objet de certaines études quantitatives mais reste encore peu abordé sous l'angle organisationnel et en tant que sujet de contrôle et de gestion. Cependant, de nombreux travaux concernent les fonctions traitant de ce risque, qu'il s'agisse du Risk Management, de l'audit comme des dispositifs de contrôle interne. Afin de cerner ces enjeux et en lien avec notre question de recherche, notre cadre théorique se compose des éléments suivants :

Notre recherche consiste à partir du rôle des normes traitant du risque opérationnel dans le secteur financier pour ensuite étudier les processus organisationnels qu'elles impliquent

notamment en termes de réseaux d'acteurs et de contrôles (Hanlon, 2010 ; Kaplan, Mikes, 2012). Ce cadre théorique s'inscrit à la fois dans le cadre conceptuel émergent de la tétranormalisation (Bessire et al., 2010) ainsi que dans la poursuite de travaux menés sur l'effectivité du contrôle face au risque (Cappelletti, 2009b ; Vyas, Singh, 2010 ; Jafari et al. 2011 ; Boatright, 2011).

Nous empruntons alors des éléments aux différentes grilles de lecture décrites ci-après (tableau 12).

Tableau 12. Grilles de lecture théoriques mobilisées

Théories mobilisées	**Apport de la grille de lecture dans la recherche**	**Usages par rapport à l'objet de recherche**	**Champs disciplinaires**
Théorie de la structuration (Giddens, 1984, 1994)	Mobilisation importante	Structuration des contrôles, socialisation et institutionnalisation du risque dans l'organisation	Sociologie des organisations
Théorie de l'acteur réseau, sociologie de la traduction (Callon, Latour, 1981)	Mobilisation importante	Traduction de la norme de contrôle du risque opérationnel et animation Risk Management autour de l'enjeu 'filière risque opérationnel'	Sociologie des organisations
Théories modernes du contrôle des risques (Simons, 1995 ; Power, 1999)	Mobilisation importante	Etude des leviers du contrôle face au risque (valeurs, principes, interactions, diagnostic du risque et action)	Gestion, Contrôle, théorie des organisations
Théorie du sensemaking (Weick, 1995)	Mobilisation secondaire	Etude critique du sens des contrôles de l'activité dans les secteurs banque et assurance	Gestion, Socio-psychologie des organisations
Théorie socio-économique des organisations (Savall, Zardet, 2005a, 2010)	Mobilisation secondaire	Evaluation de la sauvegarde de valeur liée au contrôle, mesure qualimétrique des coûts-performances cachés risque opérationnel, analyse structure-comportement	Gestion, Théorie des organisations

Plus particulièrement, notre thèse a recours dans un premier temps au parallèle fort existant entre théorie de la structuration (Giddens, 1984, 1994) et théorie de l'acteur-réseau (Callon, Latour, 1981 ; Callon et al., 2002 ; Akrich et al., 2006). Notre cheminement théorique cherche à expliquer les politiques de maîtrise des risques opérationnels en tant *qu'enjeu de structuration des contrôles* autour des différents axes de la confiance moderne dans

l'organisation, d'où le recours à la théorie de la structuration (Giddens, 1984). Cette grille de lecture est complétée par *les apports de la théorie de l'acteur-réseau* (Callon, Latour, 1981) notamment concernant les enjeux de traduction (des normes dans notre recherche) et d'animation d'acteurs (la filière risque opérationnel).

Ces deux théories nous permettent d'observer l'axe de structuration (théorie de la structuration) autour des quatre éléments encadrant la notion de confiance dans une organisation et l'axe des comportements au travers des quatre éléments décrits par Callon et Latour dans la théorie de l'acteur-réseau. Ces théories sont complétées par les travaux relatifs au contrôle des organisations ainsi qu'à la détermination du sens (notamment les formalisations des travaux de Simons et de Power), partant du principe que ces grilles de lecture peuvent contribuer à comprendre la recherche de structuration des contrôles face au risque opérationnel.

Nous justifions le recours à ces théories issues de la sociologie et de la sociologie des organisations au regard des recherches académiques évoquées ci-après dans le domaine des sciences de gestion et plus spécifiquement en comptabilité-contrôle-audit.

2.1. Justification et recours à la théorie de la structuration

Quelle est la raison ayant poussé à ce que notre époque moderne projette les risques liés à l'activité financière au centre des débats ? Il y a toujours eu des crises et les cas de rogue trading par exemple sont légions dans l'histoire financière. L'importance croissante du financier dans la Société est en soi une clé de lecture à expliciter. La théorie de la structuration (Giddens, 1984) nous renseigne sur cette évolution liée au financier. L'apport de la théorie de la structuration est bien de resituer les objets d'étude sociologiques (au titre desquels on peut inclure la sociologie des organisations) dans leur contexte de survenance spatial et temporel, ce que Giddens qualifie de géographie de l'espace-temps (1984). Penser cette dualité implique de se poser la question du contexte dans lequel notre objet de recherche prend forme :

-au niveau spatial : l'étude du risque opérationnel est un sujet d'attention croissante dans le secteur financier, et ce plus particulièrement en Europe et dans le monde anglo-saxon (les pays émergents prenant moins en compte cette problématique sauf pour ceux qui sont intégrés aux dispositifs bâlois dans le domaine financier).

-au niveau temporel : une époque où les normes de contrôle sont mises en œuvres en vue de donner un caractère objectif au risque opérationnel, lequel existait bien avant les régulations prudentielles en banque et assurance (on pense notamment aux fraudes à l'assurance et au fraude au crédit, au manque de connaissances clients, aux erreurs informatiques ou au défaut de conseil dans les activités de vente de produits et services financiers).

Le recours à la théorie de la structuration nous semble particulièrement adapté relativement à notre objet et à notre question centrale de recherche (le passage d'une conformité des pratiques de contrôle à une gestion effective des risques opérationnels). En effet, la théorie de la structuration s'intéresse davantage à la coordination des actions dans leurs aspects transsituationnels qu'au degré de conscience des agents (Martuccelli, 1999). Elle définit la configuration des interactions et des relations sociales au travers des dimensions espace (une organisation dans un secteur et un/des pays donnés via des mécanismes de délocalisations) et temps (la vitesse à laquelle des échanges peuvent survenir simultanément, successivement ou encore conjointement, ce dans le champ spatial étudié).

Cette époque accorde une importance croissante à la dialectique en dualité oscillant entre confiance et danger (Taylor, Gooby, 2008), soit entre confiance et risque, le risque étant pour A. Giddens (1994) une forme particulière du sentiment de danger au sein de ce que U. Beck qualifie de « Société du risque » (1986).
L'un des apports de la théorie de la structuration se situe au niveau de l'explication du phénomène de confiance. Cette grille de lecture permet de comprendre comment l'on passe du sentiment de confiance à celui de défiance par la suppression progressive des garde-fous de la finance moderne (Dufour, 2011).
En matière de contrôle des organisations, plusieurs recherches ont montré la pertinence des grilles de lecture issues de la théorie de la structuration, ces dernières explicitant l'apparition et la compréhension de phénomènes sociaux dépassant le simple cadre de l'économique et du financier (Coad, Herbert, 2009). La théorie structurationniste fournit des grilles d'analyse pour diagnostiquer les dysfonctionnements des organisations (Husser, 2010). Depuis presque trente ans, les travaux menés en comptabilité-contrôle-audit traitant des apports de Giddens (Busco, 2009) permettent peu à peu d'éclairer les sciences de gestion quant aux phénomènes de contrôle des organisations (Englund, Gerdin, 2008 ; Englund et al., 2011).

2.1.1. Eléments de la théorie de la structuration : l'organisation, un pendule qui oscille entre confiance et méfiance ?

L'objet des développements ci-après est de mettre en lumière les apports de la théorie de la structuration de Giddens (1984, 1994) en ce qui concerne plus spécifiquement la notion de confiance, structurante pour les établissements financiers.

- **La modernisation comme processus, la modernité comme aboutissement : la *« Société du risque »* comme conséquence de la modernité**

Parler de *« Société du risque »,* c'est avant tout se poser la question de l'époque dans laquelle nous vivons, l'époque moderne voire post-moderne au sens de Giddens car *« là où l'on voyait autrefois des réponses, se profilent aujourd'hui des questions »* [36]. La *« Société du risque »*, nouvelle « étiquette » (Méric et al., 2009) se situe au centre de ce questionnement. Le risque a toujours été présent, il a jalonné l'histoire de l'activité humaine. La période moderne l'a mis en exergue, en a fait un marché (Ewald, 2010) et a rendu nécessaire le fait de se prémunir contre ce dernier pour permettre le développement économique (Ewald, 1986). La modernisation [37] et la croissance des forces productives y étant associées ont été la source de risques nouveaux et de potentiels de mise en danger à « l'ampleur sans précédent »(Beck, 1986).

Dans une logique de responsabilité face à l'avenir (Jonas, 1990, p.88) ce questionnement implique de se demander comment maîtriser les risques issus du processus de modernisation afin de déterminer la part de « risque acceptable ». Cette logique sociale induit une augmentation du recours aux mécanismes de gestion des risques, envisagés comme des garde-fous de la confiance post-moderne.

-La modernité comme cadre de référence de la « société du risque » : Cette prise en charge accrue du risque découle de trois éléments liés à la modernité (Giddens, 1994) que sont : la séparation du temps et de l'espace, le développement des mécanismes de délocalisation (détacher une activité de son contexte local) et

[36] Sur la distinction entre modernité et post-modernité (Bell, 1976): la notion reprise et enrichie par Anthony Giddens réside dans l'idée que la post-modernité s'inscrit dans de nouvelles « préoccupations» sociales et écologistes.

[37] Beck U., 1986, *La Société du Risque, sur la voie d'une autre modernité*, p.35 : La modernisation se comprend par les progrès technologiques et les changements du monde du travail et de la sphère organisationnelle, des structures d'influence, des styles de vie… et se distingue de « l'industrialisation ».

l'appropriation réflexive de la connaissance (la production d'un savoir systématique portant sur la vie sociale devient partie intégrante de la vie sociale face aux fixités de la tradition). Ces trois caractéristiques de la modernité réunies sont une clé de lecture de la « société du risque », conséquence de la modernité, si l'on en croit l'approche de Giddens pour qui : *« la vie moderne ressemble plutôt à une course à bord d'un semi-remorque lancé à pleine vitesse qu'à un tranquille voyage en voiture »* (Giddens, 1994, p.59.

-La **« réflexivité du savoir »** (nul n'est sûr que chaque élément du savoir ne sera pas remis en cause) trouve toute sa pertinence et un terreau favorable quant à la problématique des risques, matrices des problématiques de changement technologique, économique, social, organisationnel, environnemental (Lagadec, 2002), la réflexivité y étant « constante » (Giddens, 1994). En ce sens, le « rôle nouveau du savoir prévisionnel » est de reconnaitre l'ignorance de l'étendue des conséquences du savoir technique et de notre « pouvoir excessif » (Jonas, 1990). Dans cette perspective de réflexivité de la connaissance, le champ de prise en compte des risques va croissant. On souhaite augmenter la connaissance du risque et réduire l'incertitude dans une optique de maîtrise.

-La **séparation du temps et de l'espace**, autre caractéristique de la modernité est encore une clé de lecture de la constitution d'une *« Société du risque ».* En effet, la dématérialisation des échanges, l'assouplissement des frontières entre marchés et territoires et la déconnexion des activités humaines ont engendrés des processus tels que les risques peuvent apparaitre 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.

-Le **développement des mécanismes de délocalisation** : autre idée clé de la modernité liée aux systèmes abstraits, elle se traduit par le recul des institutions au profit d'une pluralité d'entités privées, délocalisées dans leurs activités. Nombre d'entités non institutionnelles créent par leur activité de l'incertitude (bien que mettant sous gestion les sources de risques potentielles). Cette délocalisation procède d'un essor des risques non plus individualisés mais globaux comme menaces affectant chacun dans différentes zones et non uniquement dans un endroit identifié. Le risque trouve des terreaux favorables en dehors de sa zone de survenance et survient en de multiples lieux sous des formes nouvelles.

Les risques de la période moderne, trouvent un écho dans ces caractéristiques de la modernité. Ainsi, la mondialisation du risque, l'intensité et la fréquence des risques (augmentation du nombre d'évènements contingents), la création et le développement d'environnement à risques institutionnalisés, la conscience de la limite de la compétence et du risque en tant que risque et, in fine, la répartition de cette conscience du risque (Giddens, 1994, p.131) sont autant d'éléments issus des caractéristiques de la modernité permettant d'expliciter le paradigme *d'une « Société du risque ».*

Cela étant, il faut encore évoquer la notion de confiance pour comprendre l'émergence d'un tel cadre de pensée. La confiance s'inscrivant comme dénominateur commun des caractéristiques de la modernité.

- **La confiance, clé de lecture de la modernité, herméneutique[38] de la *« Société du risque »***

Pour A. Giddens (1994), le nécessaire développement est permis par la confiance ou dissuadé par la défiance, point de divergence entre une société frileuse regardant dans le passé et une société de projet tournée vers l'avenir. Dans les dix points qu'il aborde pour décrire la notion de confiance, A. Giddens précise que la confiance est un *« outil permettant d'affronter la liberté des autres »*, elle pallie l'insuffisance d'informations. La confiance vise à s'en remettre au hasard, à prendre des risques, car elle implique le lien avec autrui. La modernité de nos sociétés rend la confiance et le risque indissociables en instaurant des garde-fous de sécurité pour permettre d'aborder ledit risque en confiance (Giddens, 1994, p.42). Le passage de la confiance à la méfiance a lieu dès lors que les garde-fous de ladite confiance sont levés peu à peu : remises en cause des systèmes abstraits et de l'expertise, recul du sentiment de sécurité, perte de sens dans les mécanismes traditionnels en place.

-Confiance et systèmes abstraits : Les institutions modernes sont de nature telle qu'elles reposent sur des mécanismes de confiance dans des *« systèmes abstraits »,* soit des systèmes délocalisés réorganisant les activités sociales et impliquant des *« garanties de fiabilité »* pour permettre la confiance. Ces systèmes abstraits sont dans

[38] Au sens d'interprétation.

la *« géographie de l'espace-temps »* d'A. Giddens (1984) à rattacher aux mécanismes de délocalisation et de dématérialisation croissante des activités.

-Confiance et spécialités : Les experts ont un rôle important dans le maintien de la confiance car ils sont supposés avoir une connaissance aboutie d'un domaine. *« La confiance n'est en effet réclamée que lorsqu'il y a ignorance »* des spécialités techniques ou des intentions des individus (Giddens, 1994, p.94). Il s'agit de faire un *« pacte »* avec la modernité en accordant sa confiance aux gages symboliques et aux systèmes experts. Ce pacte est envisagé sous le signe d'un mélange de déférence et de scepticisme, de confort et de crainte. La confiance selon A. Giddens consiste davantage à accepter les circonstances dans lesquelles un acteur donné dans un contexte organisationnel n'a pas le choix. La confiance entre acteurs est maintenue dans la mesure où le système génère des externalités positives et laisse place à la défiance en cas d'effets négatifs non escomptés. Les experts ont ainsi un rôle dans la clarification des systèmes abstraits et de leurs enjeux (clarifier un dispositif de gestion des risques, son rôle et ses modes d'effectivité). Cette clarification est permise par l'expertise, au sens de la faculté des acteurs à mobiliser les expériences vécues et le savoir accumulé pour comprendre et définir un problème en vue d'y apporter une réponse adéquate (Lebraty, 2008).

-Confiance et sécurité ontologique : Phénomène plus émotionnel que cognitif, nombre de nos actes sont issus de notre capacité à la certitude, et a contrario, à l'incertitude. De la confiance de base propre à chaque individu ou de son opposé la méfiance (« inquiétude prémonitoire ») découle une certaine anxiété, contingente au sentiment de sécurité (Giddens, 1994, p.100, 138).

-La tradition : Ensemble organisé et structuré de croyances et de pratiques, la tradition est un élément déterminant de la confiance. Elle s'inscrit dans un horizon temporel au sens du *« temps réversible »* selon l'expression de Claude Lévi-Strauss. Cet environnement traditionnel du risque est dominé par les dangers du monde touchant à l'intégrité physique des individus. Pour Giddens, ces différents éléments de la relation de confiance sont structurants dans notre monde par le jeu des institutions sociales modernes visant à apporter les réponses face au *« nouveau profil du*

risque »[39]*,* conséquence d'un *« savoir socialement organisé »* (Giddens, 1994, p.116). Le lien entre risque et confiance, contingent d'une approche sociale et organisationnelle, suppose l'appartenance de l'individu à un groupe social donné et se comprend à la lumière de l'approche culturelle (Beck et al., 1994 ; Larkèche, 2011).

Tableau 13. Environnements de confiance et de risque dans la modernité (Giddens, 1994, p.108).

Environnement de risque	**Environnement de confiance**
Menaces et dangers issus de la réflexivité de la modernité	Relations personnelles, stabilisation des liens sociaux
Menaces liées à l'industrialisation	Systèmes abstraits : stabilisation des relations à travers des champs spatio-temporels définis
Menace de perte de sens au niveau de l'individu (réflexivité de la modernité appliquée au moi)	Connexion du présent au passé à travers une pensée futuriste, projective

2.1.2. L'invention du risque opérationnel, une recherche de confiance dans l'organisation ?

-Le risque opérationnel, un système abstrait : Les risques opérationnels restent une catégorie récente de risque notamment dans les organisations du secteur financier.
Le risque opérationnel englobe l'ensemble des risques inhérents à l'activité de l'établissement (risques informatiques, de fraude, commerciaux, juridique et de conformité etc.).

M. Power (2005) parle *« d'invention du risque opérationnel »* pour qualifier cette création ex nihilo d'une nécessité de se représenter un ensemble de risques distincts. Cette *« fiction instituante »* au sens de R. Shiller (2003) a pour objectif de permettre une organisation de l'incertitude (Power, 2007), une catégorisation en un ensemble de plusieurs sous-ensembles de risque que sont notamment les catégories baloises de risque opérationnel (fraude interne, fraude externe, risque HSE-PCA, risque lié aux clients-produits et pratiques commerciales, dysfonctionnements des systèmes, dommages aux actifs corporels et exécution-livraison-gestion des processus). On retrouve bien dans la notion de « risque opérationnel » la nécessité de regrouper les nombreux risques liés à l'activité courante de l'organisation sans être le cœur du métier de prise de risque d'une banque (risque de crédit, risque de marché) ou d'une société d'assurance (risque lié à la souscription de contrats vie ou non-vie).

[39] Le risque influe sur l'environnement matériel par le biais de l'industrialisation selon Giddens (les exemples des risques écologiques ou technologiques sont évocateurs). Il s'inscrit dans une rupture causale par rapport aux risques naturels ayant affectant l'Homme.

-Le risque opérationnel et la structuration des systèmes experts : De par son omniprésence et sa technicité, le risque opérationnel est un sujet d'expertise. Son identification et son évaluation constituent des enjeux d'expertise (Hanlon, 2010). L'exemple de la créativité d'experts en matière de produits financiers comme cause de risque opérationnel abonde dans ce sens (Méric, Sfez, 2011) tout comme les risques liés à la continuité d'activité ou encore aux évènements de fraude.

-Le risque opérationnel et la sécurisation de l'activité : La gestion du risque opérationnel répond à des objectifs de supervision (au sens de contrôle de l'activité) dont l'objectif est de permettre une stabilité du système financier : stabilité interne de chaque entité, protection des intérêts financiers des clients (Kraujalis et al., 2006). L'enjeu du risque opérationnel en matière de Risk Management réside bien dans la capacité de l'organisation à assurer une sécurisation face aux menaces potentielles pour l'entité et ses actifs (Muermann, Oktem, 2002).

-Risque opérationnel et tradition, le tiers facteur immatériel dans l'organisation : Si la gestion des risques opérationnels constitue un moyen émergent de développer une culture du risque dans l'organisation (Ospital, 2006), ces risques sont très contingents de l'organisation et de sa culture (Jobst, 2007)[40]. L'approche culturelle semble parlante pour identifier et gérer progressivement des risques opérationnels de fréquence mais le poids de la tradition est alors de faible secours en matière de risque opérationnel extrême (Sampath, 2009) tels que les crises majeures, ou la rupture de continuité d'activité pour une entreprise.

2.1.3. La réinvention et l'illusion du contrôle : du pacte envers la modernité au pacte entre acteurs

Pour U. Beck (1986), accepter de vivre dans un monde de risque, c'est constituer un pacte envers la modernité : cela revient à accepter celle-ci et ses mécanismes. C'est un moyen d'intégrer le rapport au risque et le rapport à autrui dans son activité propre.

[40] A noter qu'A. Giddens (1984) distingue à ce titre d'une part la culture moderne fondée sur la croyance dans le recours à la rationalité instrumentale et aux outils de la technè et d'autre part la culture post-moderne envisagée comme le dépassement du recours à la technè et au repositionnement du rôle de l'individu comme étant au centre des mécanismes de structuration.

Toutefois, en ce qui concerne la finance moderne, les mécanismes de délocalisation et la dématérialisation des échanges, facilités par les mouvements de dérégulation de la fin du XXème siècle, ont tendance à transformer ce pacte envers la modernité en un pacte imparfait (contrat entre acteurs). Cette vision de l'auto-contrôle est remise en cause au regard des critiques modernes du Risk Management, soit la recherche d'un nouveau contrat-parfait : le Risk Management de l'après-crise tenant compte du facteur humain et des conflits d'intérêts entre acteurs : notamment entre opérateurs de marché et clients des banques par exemple, ou manquement au devoir d'information et de conseil, type de risque opérationnel constituant une forme moderne de l'asymétrie d'information.

Comme l'évoquent certains auteurs, les scandales récents et les nombreux cas de risques opérationnels médiatisés impliquent de se demander ce qui fonctionne réellement en matière de risque opérationnel (Galloppo, Rogora, 2011). L'émergence des risques opérationnels avait rapidement entrainé une redéfinition des contrôles (Spira, Page, 2003) davantage tournés vers la logique globale du Risk Management. Toutefois, l'empilement d'une multitude de contrôles est apparu comme un moyen d'intégrer dans le champ du rationnel ce qui était largement contingent et découlant du facteur humain. Lors des cas médiatiques tels qu'AIG, Société Générale, Dexia, ou encore JP Morgan, UBS, HSBC, nous sommes passés d'une confiance forte dans les mécanismes de contrôle, *« l'explosion du contrôle »* (Maijoor, 2000) au sens de développement de ces dispositifs et fonction, à une défiance vis-à-vis de ces mêmes dispositifs, *« l'illusion du contrôle »* et le regard critique désormais porté sur cette *« Société de l'audit »* (Buehler et al., 2008 ; Power, 2009).
Le *« système abstrait risque opérationnel »* et sa gestion n'ont pas pleinement permis de conforter la confiance dans l'organisation, révélant des conceptions erronées des contrôles d'apparence (Hanlon, 2010).
Les études récentes montrent ainsi la fragilité des organisations du secteur financier (Bernoth, Pick, 2011). Cette fragilité ne se situe pas nécessairement au niveau de la solvabilité de ces organismes d'assurance ou établissements de crédit, mais au niveau organisationnel : dans le partage des informations en interne et entre structures sur les sources de risques (Francis, 2011), dans l'analyse des influences causales déterminant le risque opérationnel (Cech, 2009), dans la capacité à faire évoluer les structures de Risk Management (Martin, 2009 ; Huber, Scheytt, 2013). L'analyse de la littérature nous fournit toutefois des constats datant d'avant la crise de 2007-2008 et des cas récents de risques opérationnels extrêmes. Pour certains auteurs, les enjeux de contrôle et de management des risques comportent une dimension sociale voire

sociétale que l'on redécouvre sans cesse dès lors que les risques des entreprises affectent notre quotidien de par leur potentiel de déstructuration (Merton, 1995 ; Spira, Page, 2003 ; Hakenes, 2004).

Un Risk Management effectif intègre ce rapport à l'autre et cherchera à internaliser ces conséquences négatives sur la Société. Son objectif sera de contribuer à maintenir la confiance qu'autrui aura dans la capacité des systèmes abstraits à assurer la sécurisation de l'organisation et des individus qui la composent (Danielsson et al., 2002). Le Risk Management, de par sa dimension gestionnaire du risque, est en cela la fonction sensée maintenir et conforter les garde-fous de la confiance moderne. Cette perspective d'auto-contrôle de l'organisation a été largement décriée (Shapiro, Matson, 2008 ; Jiang, Rupley, 2010 ; Fiordelisy et al., 2011) pour son manque d'efficacité à déceler les crises et à permettre une réactivité suffisante.

2.2. Justification et recours à la théorie de l'acteur-réseau

Notre recherche mobilise également la théorie de l'acteur-réseau développée par Callon, Latour (1981) et complétée par des recherches plus récentes (Akrich et al., 2006). Le recours à cette théorie est croissant en sciences de gestion comme le montrent certaines études académiques telles que des recherches doctorales en gestion de l'innovation (Tran, 2008) et dans le domaine du contrôle bancaire (Seran-Luu, 2012). Des études dans des revues anglo-saxonnes confirment également l'intérêt du recours à cette grille de lecture théorique en comptabilité-contrôle-audit et en management des organisations, attestant du fait que la recherche en gestion dans le domaine de la comptabilité et du contrôle peut mobiliser de manière pertinente les cadres conceptuels et théoriques des sciences sociales (Vollmer, 2009). Les recherches académiques dans ce domaine mobilisent la théorie de l'acteur-réseau pour démontrer notamment le rôle de cette approche dans la formalisation des changements intervenant dans les systèmes comptables et de contrôle de gestion (Briers, Chua, 2001), dans la gestion des ressources stratégiques et les problématiques d'interactions entre acteurs (Steen, 2010), dans la déclinaison opérationnelle d'un réseau d'acteurs permettant une meilleure diffusion des informations comptables et financières (Pipan, Czarniawska, 2010) ou encore dans la diffusion des innovations en contrôle de gestion (Alcouffe et al., 2008).

Notre recherche vise donc à mobiliser cette théorie plus particulièrement en ce qui concerne le déploiement d'une filière de gestion et de contrôle du risque opérationnel.

Dans ses apports plus récents, Latour (1995) mobilise en effet la compréhension d'un réseau d'acteur en tant que « filet de sécurité » au sein d'une organisation : le réseau vient en quelque sorte permettre l'auto-expansion de l'entreprise, cette « technoscience »[41] vise à répondre au tryptique gestion, risque et organisation (Méric et al., 2009, p.121). Cette théorie est à rapprocher de la théorie de la structuration évoquée précédemment. Pour Latour, (1995, p.547), le caractère cumulatif de la science et de la compréhension de notre monde implique de tisser des réseaux d'acteurs de manière à faire coïncider les visions divergentes ou convergentes dans le temps et dans l'espace.

2.2.1. Les risques opérationnels et l'opérativité donnée aux normes de contrôle : la traduction opérée par l'acteur réseau Risk Manager

Si le contrôle et la gestion du risque opérationnel ont été envisagés sous l'angle normatif et de l'effectivité des dispositifs (Cappelletti, 2009b ; Haouat-Asli, 2011), la dimension sociale des dispositifs formels de contrôle devient un sujet d'étude incontournable dans cette recherche d'effectivité. En revanche la question de la « créativité » est encore peu abordée bien que constituant une nécessité dans un environnement où l'innovation financière induit de nombreux risques opérationnels (Méric et Sfez, 2011).

L'apport du champ théorique issu de la sociologie des organisations facilite la compréhension des enjeux de traduction par les responsables de la filière risque vers les différents collaborateurs pour transformer le risque opérationnel en un objet frontière, soit un espace de communication intergroupes. Cette traduction (Callon et Latour, 1981) est sensée faciliter la compréhension et l'appropriation du risque en un ajustement d'esprit tourné vers l'action. Notre postulat est alors qu'elle suppose une créativité dans l'application de la norme pour rendre la gestion du risque opérationnel effective.

-Naturaliser les normes, les rendre parlantes pour les opérationnels : Pour Akrich (1987), face à la profusion de règles, il importe de pouvoir « stabiliser et naturaliser » les scripts, c'est-à-dire les traduire en faisant le lien entre technique et dimension humaine. Cet enjeu de traduction est alors le fait de l'acteur-réseau, au centre d'un processus d'interaction entre les individus au sein de l'organisation.

[41] Lieu de concrétisation de l'entreprise moderne au travers de multiples réseaux d'acteurs interconnectés. Pour Latour (1995), du fait que le monde soit peuplé d'acteurs irrationnels, la logique en réseau de notre époque moderne trouve tout son sens et son fondement même : pouvoir interagir et requérir l'avis d'autrui afin de construire des métrologies adaptées.

Face à un enjeu technique, il est possible de rencontrer des zones de conflits sociocognitifs. Un même enjeu organisationnel peut alors faire l'objet d'interprétations divergentes du fait de différences culturelles. Le rôle de l'acteur réseau est alors de permettre la convergence de compréhension des enjeux techniques (Callon, 2001). Naturaliser la norme, c'est la rendre intelligible en soi mais également intelligible de la même manière pour les différents acteurs ayant à l'appliquer tout en prenant en compte le caractère situé de son application.

-Normes de contrôle et culture de la virtualité inter-groupe : Si les collaborateurs d'une organisation sont capables de discernement, la gestion des risques opérationnels est une forme de matérialisation de la complexité, un moyen commode d'intégrer le rapport à l'Autre et la part d'incertitude qui lui est inhérente. Cela permet le passage d'un processus intrapersonnel à un processus interpersonnel qui modifie l'équilibre « Nous-Je » (Elias, 1991, p.208). Le Risk Manager, acteur au centre d'un réseau d'interactions et d'informations où « espace des flux et culture de la virtualité » se conjuguent (Castells, 2001, p.473) cherche à lever les barrières psychologiques du profane que sont la complexité, la technicité ainsi que la définition des notions entourant le risque. Une telle conception s'inscrit dans le rapport aux attitudes de la psychologie sociale décrite comme « un état neuro-psychique préparant et facilitant l'action » par « un ajustement d'esprit » (Crozier, Friedberg, 1977, p.461). Cet ajustement d'esprit suppose bien d'aller de la norme à une gestion effective, empreinte d'opérativité.

-le Risk Manager au centre du processus de traduction-compréhension-action de la norme de risque opérationnel :

Pour Greimas et Courtès (1979), l'acteur s'envisage comme toute unité discursive, investi par des rôles distincts et évolutifs, non limités à l'univers humain mais cadrant aussi les enjeux techniques. Le Risk Manager est l'acteur en charge de la conduite de la politique de maîtrise des risques de l'organisation. Ses rôles sont non seulement d'animer et de fédérer une filière de parties prenantes dans l'organisation autour des enjeux de risques mais d'apporter des réponses et conseils techniques sur des problèmes précis identifiés par l'entreprise. La bonne application de la norme en matière de maîtrise du risque est une partie intégrante de son rôle. Il est en lien avec les fonctions suivantes en vue de s'assurer de la bonne compréhension de la norme afin de veiller à son application effective et au caractère adéquat de la normes aux enjeux organisationnels : fonctions juridiques, conformité, dispositifs de contrôle (contrôle interne périodique et permanent) et audit interne mais aussi avec les directions financières

ainsi que les nombreuses entités métiers (marketing, distribution, opérations, direction technique, systèmes d'information etc.).

2.2.2. De la problématisation à la mobilisation : apports de la théorie de l'acteur-réseau

La théorie de l'acteur-réseau distingue différentes étapes dans la constitution d'une logique dite en réseau. Celles-ci vont de la problématisation de l'enjeu à l'intéressement, l'enrôlement et la mobilisation des acteurs (Latour, 1995).

-La problématisation de l'enjeu : Cette première étape a trait au repérage et à la formulation de « problèmes » directement issus de la réalité (observations, constats, besoins, expériences). Il s'agit de fédérer un certain nombre d'acteurs au sein d'une organisation ou d'un groupe d'organisations. Pour Latour (1995, p.207-247), *« se forger des alliés »* implique de pouvoir synthétiser un ensemble de phénomènes, de faits, d'actions avérés en un problème concret et parlant pour ces derniers. Il faut pouvoir être *« un constructeur de faits »* et ainsi *« traduire les intérêts des autres ».* Latour précise à cet égard que les enjeux de traduction ne constituent pas à proprement parler une théorie, mais bien un cadre de compréhension de la constitution des faits.

La problématisation implique la reconnaissance, par les acteurs, d'une convergence de fait ou l'on cherche à repenser leurs intérêts comme des réponses et solutions à apporter autour d'un problème commun. Cette problématisation ne peut être assurée que par un traducteur reconnu et accepté par les acteurs du réseau. La problématisation consiste non seulement à formuler les problèmes mais aussi à proposer des solutions au travers des étapes suivantes.

-L'intéressement des autres : L'intéressement au sens de Latour (1995, p.373 et s.) réside dans la constitution concrète d'un système d'alliances. Pour cela, il faut pouvoir intéresser les autres « au laboratoire » en rendant ce dernier indispensable. L'auteur insiste sur l'intéressement en tant que démarche visant à rendre incontournable la concrétisation d'un groupe de personnes chargé d'apporter des solutions au(x) problème(s) préalablement identifié(s).
L'étape d'intéressement se caractérise par l'interprétation des faits par les acteurs en charge de construire ces derniers. Il s'agit d'inclure dans cette démarche l'ensemble des acteurs susceptibles de participer à la (co)construction d'un même fait. Le but d'une telle démarche

est de formaliser un lien étroit entre acteurs autour d'une même problématisation en définissant le rôle de chaque acteur.

-L'enrôlement des acteurs : L'enrôlement ne comprend pas ici une connotation négative, au sens de forcer un acteur à intégrer un groupe ou une organisation. Il s'agit davantage de pouvoir coordonner et faire coïncider des rôles définis ou à définir. La pertinence et l'efficacité de cette démarche dépendent de la capacité préalable des acteurs en charge de la résolution d'un problème à intéresser leurs homologues.
Nous décrivons l'enrôlement comme le fait d'aligner les différents acteurs sur des intérêts similaires en mettant en commun des moyens et en définissant des comportements et logiques d'actions semblables à adopter (dans le temps et dans l'espace). Il est question de mettre en œuvre des formes de négociations multilatérales et donc de définir les meilleurs cadres d'action pratique à adopter.

-La mobilisation des alliés : Cette dernière étape consiste à faire des acteurs d'un projet ou d'une politique commune les porte-parole des fonctions, organisations, en un mot, des groupes socio-organisationnels auxquels ils se réfèrent en tant qu'entités de rattachement. Pour que la mobilisation soit effective, celle-ci doit revêtir une réalité objective, qu'elle soit physique ou visible sous d'autres formes (formalisation lors de discours, communiqués, documentation officielle, interactions etc.) ; rendant ainsi empirique un système d'alliance.

2.2.3. Les politiques de maîtrise des risques opérationnels et l'acteur-réseau Risk Manager

Les éléments précités de la théorie de l'acteur-réseau se prêtent particulièrement à la description du rôle de la fonction en charge des risques (opérationnels) au sein des organisations :

-La problématisation de l'enjeu prudentiel risque opérationnel : le développement de la notion même de risque opérationnel en tant qu'enjeu concret auquel apporter une réponse constitue bien un sujet de problématisation-solution essentiel (Power, 2005). La filière de gestion des risques opérationnels (Comité de Bâle, 2011) implique en effet de définir le risque opérationnel en tant qu'enjeu stratégique de gestion, faisant l'objet d'une politique de maîtrise des risques dédiés, et supposant de faire interagir un ensemble d'acteurs sensés participer à sa maîtrise.

-L'intéressement à la problématique du risque opérationnel : le rôle de fédération du Risk Management autour d'une problématique commune est caractéristique de la logique de gestion globale des risques précitées dans ce chapitre. Le risque opérationnel ne fait exception à une telle logique (Mikes, 2007). La création d'une culture du risque opérationnel est bien la capacité à faire comprendre à chaque acteur son rôle exprès ou tacite par rapport à ce même sujet (Ospital, 2006 ; Francis, 2011 ; Hora, Klassen, 2013).

-L'enrôlement des acteurs au sein d'une filière commune: Il s'agit de déterminer qui sont les « correspondants risques » (Comité de Bâle, 2003b, 2011) soit un ensemble d'acteurs sensés faire remonter des informations chiffrées ou non, des alertes relatives au risque opérationnel mais aussi proposant des actions concrètes à mettre en œuvre dans leur périmètre d'activité (Hanssen, 2005 ; Fernández-Laviada, 2007). Ces acteurs doivent ainsi reporter au Risk Manager, lequel est en charge d'harmoniser, d'aligner les pratiques afin de dessiner une vision homogène et consolider de la gestion du risque opérationnel dans l'organisation.

-La mobilisation des acteurs: La mobilisation des acteurs autour de l'enjeu risque opérationnel suppose pour le Risk Manager d'animer une filière d'interactions tournée vers l'anticipation. Les concepts formalisés, les objectifs fixés, les plans d'actions à mettre en œuvre sont autant d'enjeux concrets auxquels répond cette phase de mobilisation dans la conduite de la politique de maîtrise du risque opérationnel (Galloppo, Rogora, 2011 ; Jebrin, Abu-Salma, 2012).

2.3. Le contrôle interactif des risques

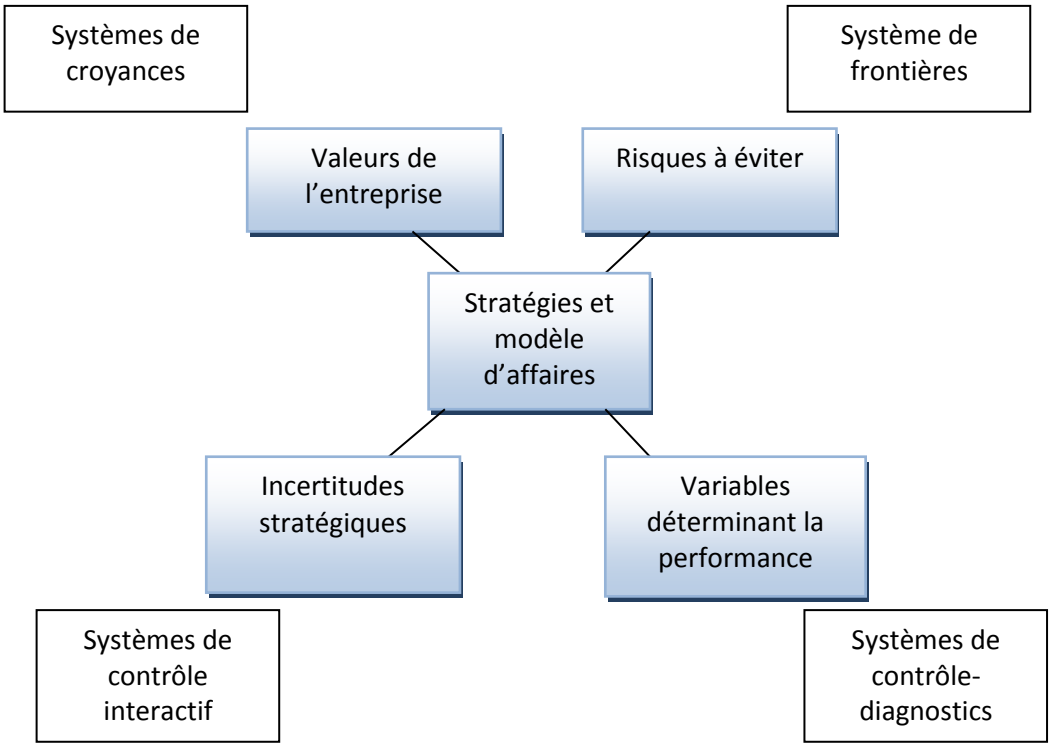
Enfin, nous pouvons nous référer aux travaux fondateurs de R.Simons (1995). Pour ce dernier, le contrôle interactif est cette forme de contrôle qui focalise l'attention des managers sur les incertitudes stratégiques. Ils favorisent l'innovation et l'émergence de nouvelles stratégies intégrant l'incertitude dans la prise de décision tout en favorisant le dialogue et les débats réguliers dans l'organisation (Renaud, 2013).

La littérature dans ce domaine (Tani, 1995) distingue ainsi le contrôle vertical (échanges intensifs et réguliers entre managers, dirigeants et opérationnels), et horizontal (via des confrontations de savoirs entre managers et fonctions de l'organisation autour d'un projet commun). Le rôle de la fonction de contrôle interne et de celle de gestion des risques s'inscrit clairement dans l'approche de contrôle interactif horizontal. Il faut néanmoins ajouter que les différents niveaux de contrôle nous permettent d'affirmer qu'il est en fait questions de

concomitance entre approche verticale (le contrôle de 1er niveau évoqué dans le chapitre 2) et horizontale (les contrôles de second niveau ainsi que l'audit interne et la gestion des risques tels que décrits dans ce même chapitre).

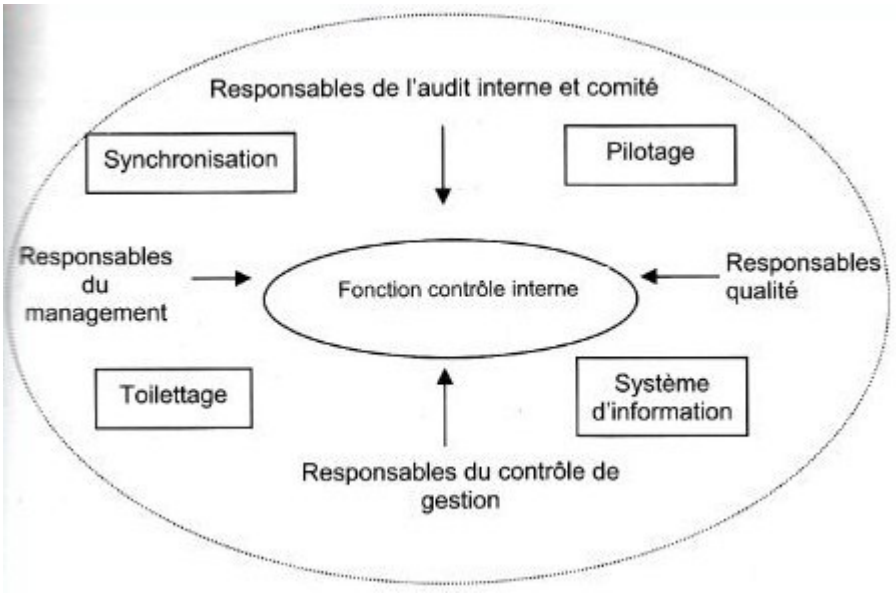
Le schéma ci-après reprend les éléments clés du contrôle interactif tels que présentés par R.Simons. Pour l'auteur, les systèmes de croyances déterminent l'axe des valeurs de l'entreprise de la même manière que les systèmes de frontières (délimitation du champ d'intervention de l'entreprise) déterminent les risques à éviter dans le cadre du modèle stratégique. Ces deux premières composantes supposent de faire cohabiter les systèmes de contrôle interactifs (de type contrôle organisationnel) et les systèmes de contrôle de diagnostics (de type audit comptable et contrôle de gestion), les premiers ayant un impact sur le niveau d'incertitude stratégique auquel est soumise l'organisation et les seconds concernant la performance de l'entreprise.

Figure 21. Système de contrôle interactif (d'après R.Simons, 1995)



Une telle approche du contrôle, loin d'être récente comme le montrent les travaux d'Ouchi (1977), a été reprise et développée récemment (Cappelletti, 2009).

Figure 22. Modèle d'animation d'une fonction de contrôle interne, d'après Cappelletti, 2009



Dans le modèle ainsi proposé dans cet article se basant sur différents cas d'entreprises, audit interne, gestion de la qualité, systèmes de management et contrôle de gestion sont en interaction avec le contrôle interne des risques de l'entreprise. La nature de ces interactions est d'ordre horizontal et contribue à déterminer ce qu'est un contrôle des risques effectif et efficace. Ce dernier est effectif dès lors qu'il s'appuie sur une réelle implication des managers de l'entreprise et mobilise également les systèmes de contrôles orientés processus mais aussi performance de l'entreprise. Dans cette approche, il revient au contrôle interne des risques d'être l'acteur clé entre ces différents contrôles et les managers opérationnels en vue non seulement de répondre aux exigences réglementaires mais aussi de contribuer à la réduction des incertitudes entourant l'organisation et par ce biais d'améliorer sa performance durable.

2.4. Une « triangulation théorique » : structuration / acteur-réseau / contrôle socio-organisationnel

Nos deux principales grilles de lecture étant exposées, il nous faut exposer les voies de rapprochement entre ces dernières.

Les grilles de lecture relatives aux théories de la structuration et de l'acteur-réseau sont complétées par *les apports de la théorie du contrôle appliquée au risque* (Simons, 1995 ; Power, 1999, 2005, 2007), mais également les recherches récentes dans le champ du contrôle des risques. Notre recherche s'inscrit dans une perspective socio-organisationnelle resituant le contrôle du risque opérationnel dans son contexte, l'organisation, en vue d'aller au-delà du sujet de la transposition de la norme, (Hanssen, 2005 ; Drott-Sjoberg, 1991 ; Beretta,

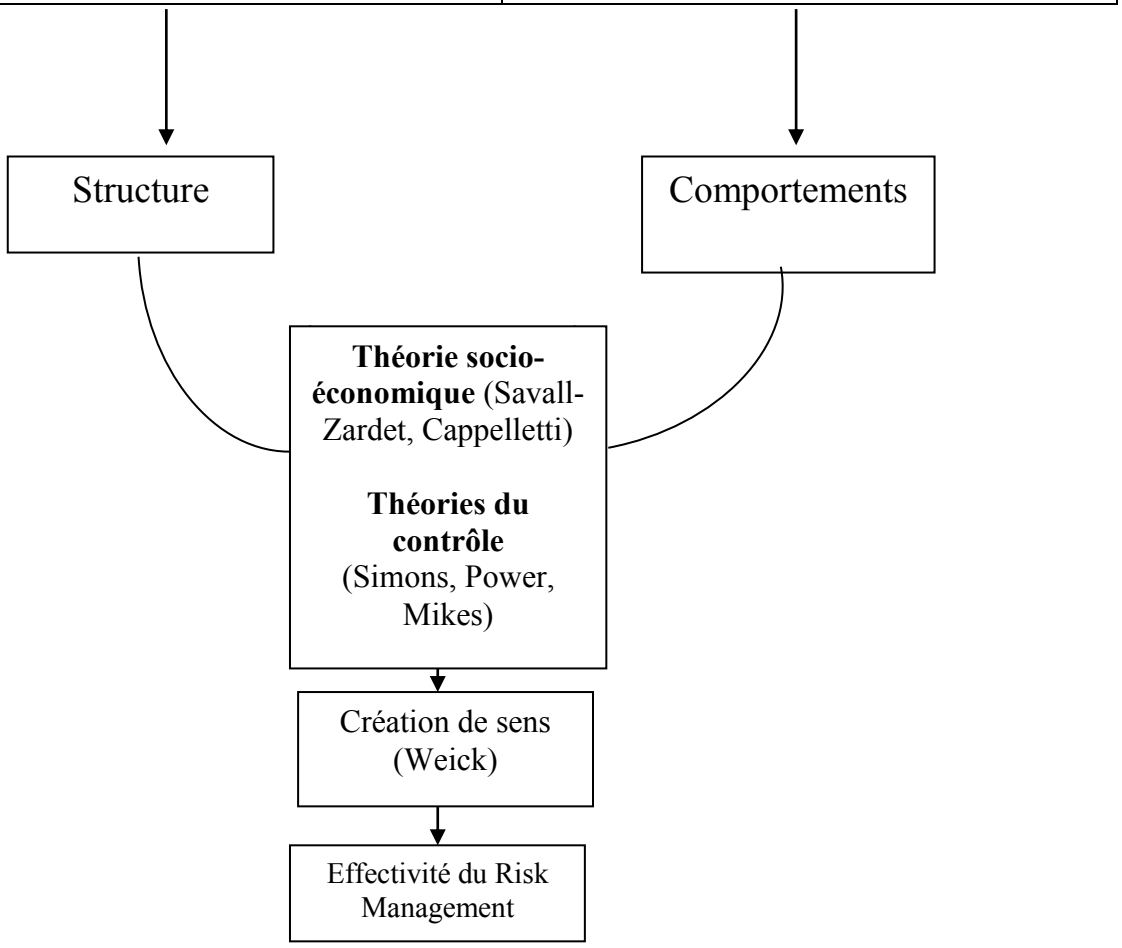
Bozzolan, 2004, Mikes, 2009, 2011 ; Linsley, Schrives, 2009 ; Scimia, 2010 ; Kaplan et al., 2009 ; Beck, Kropp, 2011 ; Battilana, Casciaro, 2012).

Le recours à ce champ théorique socio-organisationnel dans le domaine du contrôle s'inscrit dans le prolongement de recherches qualitatives en comptabilité-contrôle-audit (Parker, 2012).

Il existe en effet un rapprochement que nous souhaitons établir entre les axes de compréhension de l'enjeu de risque dans la théorie de la structuration (autour de la structuration de la notion de confiance) et dans la théorie de l'acteur-réseau (en ce qui concerne la mobilisation des acteurs). Nous nous référons à la théorie socio-économique (Savall, Zardet, 2005a) qui insiste sur le rapprochement de l'étude des phénomènes de structures organisationnels et de comportements des acteurs. Notre dualité théorique entre structure et comportement s'inscrit aussi dans le prolongement des éléments cités sur le contrôle interactif au sens de R.Simons (1995), mettant en corrélation les enjeux de valeurs, de stratégies, de contrôle et de risque. Le tableau ci-après précise le rapprochement entre nos principales grilles de lecture théoriques : les phases de la théorie de la structuration sont corrélées à celles- de la théorie de l'acteur réseau, la première explicitant les enjeux de structure et la seconde les enjeux de comportements. Ces différents éléments, et c'est du moins ce que nous souhaitons expliciter au regard de notre étude empirique, permettent de contribuer à la création de sens en tant que convergence de pratique et rendent effective la gestion des risques (en en faisant une réalité de l'action).

Tableau 14. Grilles de lecture théoriques mobilisées

Théorie de la structuration (Giddens)	**Théorie de l'acteur-réseau** (Callon, Latour)
Etude des systèmes abstraits	Problématisation et traduction
Tradition et culture du risque	Intéressement
Rôle des systèmes experts	Enrôlement
Sécurisation	Mobilisation



Conclusion du chapitre – La nécessité de grilles de lecture adaptée au contrôle organisationnel des risques

L'apport académique de notre recherche consiste donc non seulement à recenser les études encore émergentes sur le risque opérationnel dans le champ des organisations, mais aussi à formaliser les apports des recherches éparses sur le contrôle organisationnel des risques. De nombreuses études ont ainsi entendu exposer ce qu'est la gestion des risques dans les organisations tout en insistant sur les limites de telles pratiques de fiabilisation-sécurisation.

En outre, les secteurs de la banque et de l'assurance ont fait l'objet d'études sous différents angles mais la thématique de ce que nous qualifierons de « risque organisationnel » reste à ce jour un champ de recherche à développer.

Nous avons mobilisé différentes grilles de lecture se rapprochant de la sociologie des organisations car ces théories nous semblent particulièrement adaptées pour comprendre le phénomène émergent, d'inspiration réglementaire, que constitue la formalisation de politiques de maîtrise des risques opérationnels. La théorie de la structuration et la théorie de l'acteur-réseau étant des théories davantage « sociologiques », celle-ci sont rapprochées dans notre étude des recherches récentes en sciences de gestion dans le domaine du contrôle et de l'audit et en matière de gestion des risques opérationnels. Nous constatons que nombre de chercheurs de notre discipline académique s'y réfèrent car elles permettent d'expliciter la construction de phénomènes au sein des organisations mais aussi de comprendre le rapprochement entre les logiques de structure et de comportement.

Ces éléments théoriques étant exposés, avant de les rapprocher de nos cas d'études empiriques, nous abordons dans le chapitre suivant notre positionnement méthodologique et la logique d'investigation poursuivies tout au long de la recherche de terrain réalisée.

Chapitre 4 - Démarche méthodologique, la pertinence de démarches qualitatives tournées vers la pratique dans l'étude du contrôle des risques

« Adopter une épistémologie, donc des guides pour l'action et la recherche, permet de se démarquer des consultants, des dirigeants ou des journalistes qui parlent sur l'entreprise au seul titre de leur praxis ou de leur expérience » (Wacheux, 1996, p.38).

Introduction

Ce chapitre explicite et détaille la posture épistémologique qui qualifie notre recherche ainsi que les outils et méthodes de recherche retenues afin de collecter et d'analyser les données de terrain. Nous abordons également la présentation des cas d'étude et des entretiens réalisés dans le cadre de cette recherche doctorale.

Le contexte d'accélération des échanges et des interactions entre individus appelle de nouvelles approches de la recherche, plus proches du terrain et mieux à même d'en saisir le contenu, transcendant la distinction classique entre sciences appliquées et fondamentales. Ces nouvelles approches doivent favoriser la transdisciplinarité pour dépasser le caractère parfois perméable d'une recherche, surtout si celle-ci est orientée vers un but précis ou commanditée par un groupe donné. On ne peut imposer une démarche unique, les situations étant trop différentes pour que les différentes postures et devis méthodologiques soient appliqués de manière similaire (Gibbons et al., 1994). C'est dans ce contexte que s'inscrit notre recherche : un lien prononcé entre théorie et pratique et un positionnement épistémologique que nous qualifierons de *« constructiviste aménagé »* ; en référence à un recours accru à des méthodologies de collecte des données cherchant à décrire une réalité organisationnelle préconstruite et à expliquer ses conditions d'évolutions (Gibbons et al., 1994).

En effet, dans une logique constructiviste visant à expliquer la réalité sur notre objet de recherche (les politiques de maîtrise des risques opérationnels), nous avons eu recours successivement à des études de cas au sein d'entreprises du secteur financier français, lesquelles ont été réalisées en recherche-action à la *« première personne »*[42]. Ces études de cas ont été l'occasion de réaliser un ensemble d'observations participantes et non

[42] Concept explicité dans ce chapitre dans le paragraphe relatif à la recherche-action.

participantes (y compris des entretiens au sein des entités étudiées). A ces études de cas se sont ajoutées des entretiens confirmatoires semi-directifs auprès de contrôleurs des risques, Risk Managers, auditeurs internes. Les données collectées sont succinctement présentées afin d'introduire le chapitre suivant relatif aux résultats de notre recherche.

1. Conception du protocole de recherche

Notre méthodologie de recherche s'inscrit dans la continuité des travaux de l'école dite « française » de contrôle (David, 1999 ; David, 2000 ; Savall, Zardet, 2004 ; Cappelletti, 2006, 2009) développant des méthodologies qualitatives afin d'étudier les thématiques de contrôle de gestion ou encore de contrôle interne. Ces recherches sont transformatives et collaboratives, elles ont recours à des méthodologies de type recherche-intervention transformative ou encore à la recherche-action. Elles sont appropriées en cela qu'elles permettent d'étudier des terrains a priori difficiles d'accès pour des chercheurs extérieurs et pour lesquels une grande complexité caractérise les organisations (Van de Ven, Johnson, 2006).

Nous nous inscrivons tout comme ces travaux dans une rupture avec des méthodologies traditionnelles des recherches positives fondées sur la séparation entre le chercheur et son objet de recherche (Cappelletti, Baker, 2010).

Notre positionnement au cœur des organisations étudiées était celui d'acteur à part entière du processus de co-construction de connaissance et de transformation sociale de l'organisation. Ce dernier supposait cependant de respecter des conditions de rigueur dans la collecte et l'analyse-traitement des données recueillies (Cappelletti, 2010) afin de garantir la validité des observations.

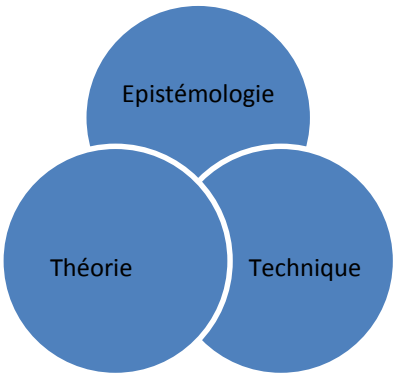
1.1. Posture épistémologique : un « constructivisme aménagé »

L'épistémologie est une science des sciences, une philosophie de la pratique scientifique sur les conditions de validité des savoirs théoriques. Elle consiste pour le chercheur à légitimer sa recherche par rapport au quotidien qu'il étudie. Elle est une autorisation de parler et de se faire entendre dans ce qui est qualifié *« d'étude de la constitution des connaissances valables »* (Martinet, Pesqueux, 2013)[43].

[43] Citant Piaget, dans *Epistémologie des sciences de gestion,* Vuibert, p.3.

L'épistémologie s'intègre en lien avec les savoirs théoriques et les techniques (au sens de méthodes, outils et articulation entre les méthodes) de recherche mobilisées.

Figure 23. La démarche de recherche, d'après Wacheux, 1996, p .37



Notre positionnement peut s'apparenter à une épistémologie constructiviste que nous qualifierons « d'aménagé », pour les raisons décrites ci-après.

L'épistémologie constructiviste suppose l'acceptation d'un univers construit avec les représentations des acteurs, ce qui oriente la démarche de recherche (Le Moigne, 1990). Elle explicite les connaissances individuelles et collectives au travers de la structuration des actions quotidiennes, il s'agit d'une explication et d'une formalisation extérieure aux individus (Giddens, 1984). Le constructivisme n'est donc pas une sociologie compréhensive mais explicative des compréhensions qu'ont les acteurs dans les organisations (Avenir, 1992). La production de connaissance et leur validation ne peuvent être dissociées. L'explication est une formalisation extérieure aux individus. Il s'agit d'une représentation dans laquelle ils doivent se reconnaitre (critère de représentativité) et dont la cohérence est appréciée par des instances extérieures (critère de pertinence).

L'épistémologie constructiviste est qualifiée par Bachelard (1934) de science en action car elle se constitue selon les éléments suivants :
-les phénomènes sont des tissus de relations,
-la pensée est un programme d'expérience à réaliser,
-la démonstration prime sur la constatation.
C'est en cela que notre positionnement est constructiviste. Il repose sur des méthodologies établissant des relations entre acteurs et entre fonctions des organisations. Le recours à la

méthodologie de recherche-action (détaillée dans ce chapitre) se situe dans une logique de démonstration par l'agir plus que dans une perspective de constatation et il a supposé la réalisation d'expériences concrètes situées dans les organisations relativement à notre objet d'étude.

Dans l'épistémologie constructiviste, la structure et les interactions se construisent d'après la réalité. Elle implique de :
-démembrer les réalités en fragments d'analyse,
-trouver des règles d'association explicatives.

Cette épistémologie travaille à observer, comprendre et proposer des explications sur les phénomènes étudiés avant de les associer puis de les interpréter dans une approche téléologique (expliquer le fondement de la construction sociale de la réalité).
Notre recherche au sein d'établissements financiers français a en effet consisté à :
-observer de manière participante et non participante les pratiques relatives au contrôle des risques opérationnels et à la déclinaison pratique de ce que serait une politique de maîtrise des risques opérationnels (contextes normatif, organisationnel et individuel).
-sur la base de ces observations et à l'aide de nombreux échanges lors d'entretiens formels et informels, nous avons ensuite cherché à comprendre les facteurs de contingence permettant de répondre à notre question de recherche (comment passer d'une politique de maîtrise des risques d'inspiration normative à une approche opérative de diffusion de la culture du risque opérationnel par l'agir et formalisée au travers de principes d'actions),
-nous avons proposé lors de ces études de cas différentes manières de rendre effectives ces politiques de maîtrise des risques opérationnels, propositions ayant ensuite été abordées expressément et tacitement lors de nos entretiens confirmatoires. Puis nous avons contribué à la mise en œuvre de ces actions pour lesquelles des échanges ultérieurs ont été réalisées.
In fine, une phase d'entretiens confirmatoires a eu lieu dans le cadre de cette recherche.

Dans cette optique, l'accumulation des connaissances est progressive et se fait par la constitution de recherches successives (Wacheux, 1996).

Le tableau ci-après résume les principales postures épistémologiques et situe ainsi notre positionnement d'inspiration constructiviste par rapport aux autres clés de lecture des approches scientifiques (positivisme, sociologie compréhensive, fonctionnalisme etc.)[44].

Tableau 15. Les principales postures épistémologiques, d'après Wacheux, 1996, p.42-44.

Epistémologies	**Approches du réel**
Positiviste	Recherche des lois et régularités qui gouvernent les faits sociaux par l'observation de données d'expériences.
Sociologie compréhensive	Expliquer le sens de l'activité sociale des individus, des groupes ou de la collectivité par la réalisation des intentions conscientes ou inconscientes des acteurs.
Fonctionnaliste	Repérer les formes permanentes de la vie sociale et culturelle, par l'émergence des rôles, des normes et des structures sociales
Constructiviste[45]	*Repérer et expliquer les propriétés intrinsèques de certains ordres sociaux et poser les problèmes en termes de méthodes et d'approches à retenir.*

Nous qualifions cette épistémologie de « constructivisme aménagé » en raison du recours aux méthodologies de type recherche-action comme fondatrice de notre recherche (et suivant un principe de contingence générique) ainsi qu'aux entretiens semi-directifs à visée confirmatoires s'inscrivant quant à eux dans une logique de généralisation analytique (Thiétart, 2003). La *contingence générique* caractérise le positionnement épistémologique de notre étude. Ce concept est proche du concept d'*engaged scholarship* (Van de Ven, Johnson, 2006) en cela qu'il suppose une révision, un toilettage régulier des hypothèses de recherche au regard de l'interaction avec le terrain étudié et de l'action au sein de ce dernier (Savall, Zardet, 2004).

Cependant, malgré ces précisions quant à notre positionnement épistémologique, il nous faut nuancer ces propos en précisant à l'instar de Pesqueux et Martinet (2013) que chaque travail

[44] A noter que d'autres postures épistémologiques existent, à l'instar du réalisme critique notamment.

[45] Le constructivisme est parfois qualifié de « structuralisme » (en cohérence avec la sociologie de la structuration). Le constructivisme est une notion davantage applicative en sciences de gestion (Wacheux, 1996, p.38).

scientifique et sa qualification ne peut etre envisagé comme définitif et ayant un caractère universel. Une recherche est nécessairement située et contextualisée. Elle est également évolutive et au carrefour de plusieurs approches, lesquelles, bien que répondant à un souci de cohérence (entre les méthodes employées et les grilles de lecture mobilisées notamment), empruntent nécessairement à différents courants ou positionnement de recherche.

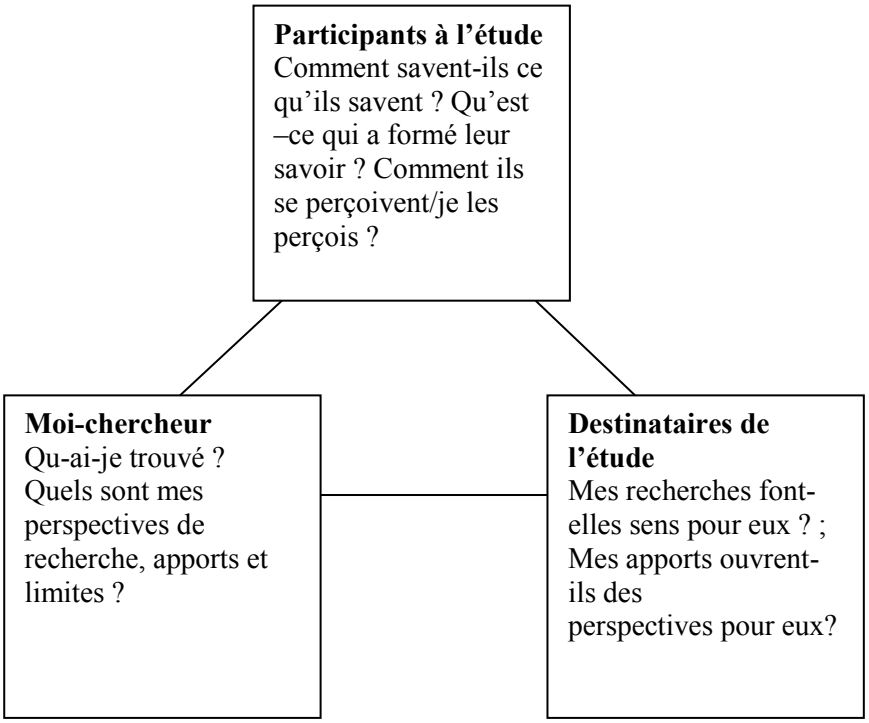
1.2. Epistémologie constructiviste et triangulation au sein de notre recherche

Dans la logique constructiviste qui caractérise notre recherche, tous les sujets de compréhension sont constructivistes. Ils sont forgés dans l'inter-personnel et donc nécessairement limités (Patton, 2002, p.96).

L'auteur, reprenant Crotty (1998, p.58), distingue constructivisme (création de sens par le biais de l'action individuelle de recherche) et constructionnisme (génération collective et transmission de sens).En parlant de *« constructivisme aménagé »,* nous répondons à un souci de clarifier notre positionnement épistémologique tout en attirant l'attention sur les limites de cet exercice par rapport à notre recherche.

La triangulation vise à répondre aux questions suivantes (Patton, 2002, p.66) :

Figure 24. Triangulation et constructivisme



Notre recherche, tant dans les interactions avec les acteurs des entreprises étudiées (études de cas) que durant les entretiens confirmatoires réalisés avait comme sous-jacent le triptyque de questionnements décrit par le schéma ci-dessus : des questions relatives aux participants à notre recherche, des questions relatives à notre positionnement en tant que chercheur et enfin des interrogations concernant les destinataires de notre étude (monde académique mais aussi professionnels concernés par cet objet de recherche). Ce triptyque de question s'inscrit dans la recherche de cohérence tout au long du déroulement de notre recherche et ce dans le but de garder une posture de recherche identique sur les différents terrains de recherche étudiés (deux cas d'entreprise sur des périodes de longues durée et une vingtaine d'entreprises lors de nos entretiens confirmatoires).

2. Méthodologie de recherche

« Nous sommes passés d'une sociologie qui se limitait à l'analyse des aspects institutionnels de la science à l'investigation détaillée de la recherche comme activité située. L'essor de cette investigation détaillée s'est faite pour en venir à l'examen réflexif du discours analytique lui-même voire à la participation effective du chercheur aux pratiques » (Sormani et al., 2006, p.201). Ce contexte d'évolution des recherches caractérise également les sciences de gestion où de nombreux colloques et congrès scientifiques insistent sur la nécessité de recherche d'une approche à la fois transdisciplinaire et davantage enracinée dans la pratique tant par les objets et méthodes d'études qu'elle mobilise. Nous nous inscrivons dans ce souci de lier des outils et méthodes permettant une forte proximité avec notre terrain de recherche, y compris des méthodologies issues historiquement d'autres disciplines (sociologie notamment dans notre recherche).

2.1. Le choix d'une recherche qualitative

« La recherche qualitative de terrain, en particulier, comporte de nombreuses inconnues, car ses opérations ne sont pas aussi prévisibles, que disons, une recherche expérimentale ».
Elle se définit comme *« la recherche qui implique un contact personnel avec les sujets de la recherche, principalement par le biais d'entretiens et par l'observation des pratiques dans les milieux mêmes où évoluent les acteurs »* (Paillé, Mucchielli, 2012, p.13).
Elle peut être définie par ses outils et méthodes de collecte de données (notes, témoignages, images…) et d'analyse (codage, matrices de corrélations) visant à en extraire le sens plutôt que les transformer en pourcentage ou en statistiques.

Cela signifie également que la recherche est menée de manière *« naturelle »,* sans appareils sophistiqués ou mises en situations artificielles. La logique suivie est proche des personnes, de leurs actions et de leurs témoignages (dans une visée de proximité).
La recherche qualitative vise donc la compréhension et l'interprétation des pratiques plutôt que la mesure de variables à l'aide de procédés mathématiques (par exemple à la différence de l'enquête quantitative par sondage qui est de l'ordre de la vérification par le biais d'études de fréquence, de distribution et de compilation des résultats).

2.1.1. Les conditions de rigueur en recherche qualitative

En recherche qualitative la collecte de données est toujours en partie ouverte (comme cela peut être le cas pour les entretiens en profondeur ou les observations participantes). Cette approche n'est donc pas dans la posture de vérification d'une théorie mais bien dans la recherche d'équilibre entre théories et pratiques, ce que Paillé et Mucchielli qualifient *« d'équation intellectuelle du chercheur »* (2012, p.21). Tout chercheur aborde son sujet avec des connaissances et des apports théoriques mais en matière de recherche qualitative aucune lecture rigide de ces connaissances n'est souhaitable (il n'est pas nécessairement question d'adopter une posture théorique de départ avant même le développement de l'ensemble de la recherche).

Il faut cependant distinguer en recherche qualitative :

-les invariants dans la conduite d'une recherche scientifique en sciences humaines et sociales. Ces invariants sont notamment l'objet précis de la recherche, le fait de dégager une problématique claire autour de cet objet (par la disposition de premières « sondes » sur le terrain ainsi que par l'étude des principaux écrits et recherches sur ce même sujet, le cas échéant). La collecte et l'analyse (ainsi que les lectures théoriques) se succèdent en un aller-retour, formant ainsi une boucle récursive.

-Les différentes étapes de la recherche et les prescriptions s'y rattachant sont également à spécifier, de même que les suggestions sur les opérations à mener et la logique d'ensemble de la recherche.

-Les opérations à mener ont concerné le renouvellement des connaissances (la problématisation de l'objet, la problématique doit reposer en partie sur la prise en compte des réflexions antérieures : faire le lien avec les recherches antérieures par rapport aux données qualitatives recueillies).
-Nous avons enfin précisé les conditions de l'enquête (la méthode de recueil de l'information, le choix des sites et des participants, la durée des séjours de recherche, l'importance et la variété des entretiens. Puis, nous avons procédé à l'explicitation des opérations d'analyse qualitative des matériaux et les avons présentées clairement dans le cheminement de la recherche.

Dans notre étude, l'objet de recherche et la problématique centrale (ainsi que les questionnements sous-jacents) ont évolué lors d'une première phase dite exploratoire (les entretiens réalisés au sein même des cas d'étude en recherche-action). Une fois cette phase dite exploratoire finalisée, ces éléments ont constitué des invariants, excepté pour notre objet de recherche, lequel est resté inchangé en raison de sa nature relativement claire et précise en pratique et dans la littérature académique.
Les différentes étapes de notre étude ainsi que les conditions de l'enquête décrites dans les paragraphes suivants ont également été spécifiées clairement à l'issue de cette phase exploratoire en vue d'obtenir un cadre clair de collecte et d'analyse.
Se pose également la question de la validité des données collectées, afin de contribuer à la rigueur et au caractère reproductible de notre recherche. La validité de la recherche se base alors sur la validité de l'instrument de mesure ainsi que sur la validité interne et externe des données. Toutefois, la question des critères de validité d'une recherche, bien que disposant de cadres généraux, ne convient pas nécessairement pour décrire chaque recherche, ainsi il n'est pas toujours possible de mettre en œuvre des tests permettant de valider toutes les recherches dans leur globalité (Drucker-Godard et al., 2007, p.263 et s.).

- **La fiabilité de la mesure**

Il s'agit d'avoir recours à des méthodes similaires pour collecter et analyser des données multiples. Dans notre étude, la notion d'instrument de mesure, telle qu'exprimée dans certaines formalisations de recherche, semble peu adaptée. Néanmoins, et en vue de répondre à ce critère de validité, nous avons mobilisé une méthodologie de recherche-action (décrite ci-après) similaire dans différents cas d'études et une grille unique lors de nos différents

entretiens. La méthode d'analyse des données collectées en recherche-action est également la même dans nos cas d'études et nos entretiens ont été codés et analysés (en thèmes, sous-thèmes et idée-clés) selon le même procédé.

- **La validité interne des données**

Les données collectées forment un tout cohérent sur les groupes de personnes rencontrés et les évènements observés (Paillé, Mucchielli, 2012, p.455).

Il s'agit en outre de chercher à limiter les différents biais ayant pu affecter la validité de la recherche : biais d'histoire, biais issus d'effets de maturation, biais de sélection, biais issus d'effets de contamination entre acteurs de l'étude[46] etc. (Drucker-Godard et al., 2007, p.279-280).

Au sein de notre recherche, nous avons entendu garantir la fiabilité interne des données recueillies en concentrant notre période d'étude sur une durée limitée et fixée préalablement (afin de ne pas voir notre objet de recherche changer brutalement du fait d'évolution réglementaire affectant les politiques de maîtrise des risques par exemple). Nous avons également soumis à différents avis d'académiques et d'experts sur notre objet de recherche nos questions de recherches et hypothèses (dans une phase exploratoire) afin de limiter les effets d'instrumentation (questions mal formulées). En outre, notre expérience empirique sur ce sujet ainsi que le caractère formalisé du recueil de données nous ont permis d'assurer la significativité des questions posées ou problèmes traités lors des entretiens et études de cas.

Bien que les différents collaborateurs rencontrés en étude de cas ou responsables risques et contrôles interviewés puissent se connaitre, nous avons entendu réaliser nos différents entretiens dans une période de temps restreinte afin de garantir une certaine confidentialité de notre étude. En outre, les données collectées n'ont été diffusées qu'ex post à leur analyse aux différentes parties prenantes.

Enfin, nous avons également cherché à réduire les biais de sélection des données en diversifiant les profils de personnes rencontrées lors des cas d'étude et entretiens (des responsables risques, contrôles, audit interne, des responsables métiers, managers et opérationnels issus d'horizons distincts et ayant des expériences variées). Si des biais peuvent

[46] Il s'agit notamment de biais liés au fait que des acteurs, apprenant que d'autres acteurs ont participé à l'étude, souhaitent savoir ce que ces derniers ont répondu avant même d'y participer personnellement. On citera également des biais liés à l'évolution même de l'étude et aux adaptations de l'objet d'analyse, à la survenance d'évènements extérieurs modifiant l'objet d'étude ou les questions posées (changements réglementaires, économiques, bouleversements organisationnels affectant l'un des cas d'entreprise étudié etc.).

subsister quant à ce critère, c'est davantage en raison d'un manque de temps de certains interlocuteurs n'ayant pas pu répondre à notre étude, que du fait d'une carence dans la sélection des profils d'interlocuteurs rencontrés. En outre, les collaborateurs experts sur le sujet du risque opérationnel étant relativement peu nombreux par organisation, nous avons cherché, lors de nos entretiens confirmatoires, à rencontrer des collaborateurs de structures différentes (sociétés d'assurance, mutuelles, banques de détails, banques d'affaires, consultants indépendants, consultants-experts issus de structures spécialisées) et variées (environ une vingtaine de structures d'appartenance différentes pour les collaborateurs rencontrés lors des entretiens). Cela nous a permis d'avoir une vision complémentaire par rapport aux études de cas réalisées en recherche-action. Le choix des entretiens, malgré un effort pour diversifier les profils et les entreprises étudiées, est en partie guidé par la possibilité empirique d'accéder aux terrains de recherche, tant dans les études de cas que lors des entretiens.

- **La validité externe des données**

Le chercheur vérifie que les données qualitatives collectées viennent de multiples sources d'information en vue de répondre à un critère dit de *« validité écologique »* (Paillé, Mucchielli, 2012, p.455). Il s'agit de déterminer dans quelle mesure les résultats exposés pourront être généralisés à l'ensemble de la population mère puis de voir si cette recherche pourra être réappropriée par d'autres chercheurs ou transposées à d'autres cas d'études similaires en vue de répondre aux mêmes questionnements (Drucker-Godard et al., 2007, p.286).

Dans notre étude, nous avons eu recours à deux recherche-action au sein de deux structures différentes. Une entreprise du secteur assurance et un établissement bancaire français. Ces deux cas d'étude, bien que présentant des spécificités, sont représentatifs dans le secteur financier des entreprises soumises aux problématiques fortes posées par le risque opérationnel et le contrôle de ces risques par le biais de politiques dédiés.

Dans ces deux cas, la contrainte réglementaire prudentielle est présente et il est question d'y répondre par la mise en place de politiques de maîtrise du risque opérationnel dédiées. En outre, ces établissements ayant des positionnements qualifiés de « généralistes » dans la distribution de produits financiers (multi-produits), ils sont représentatifs de la diversité

d'activités présentes dans le secteur financier français. Nos entretiens répondent également à ce critère de représentativité de la population mère dans la mesure où nous avons réalisé cinquante-cinq entretiens semi-directifs à visée confirmatoires (le critère de représentativité statistique pour des entretiens de ce type étant fixé à trente entretiens à minima)[47].

Nous pouvons également ajouter à l'appui de cette validité externe que le recours à la triangulation méthodologique (développée ci-après) tend à conforter le caractère représentatif de nos données en ce qui concerne les pratiques du secteur financier français en matière de contrôle du risque opérationnel. Pour ces raisons, notre présence en tant que chercheur-acteur, tend à être un biais limité dans la mesure où de nombreuses sources d'informations (actions réalisées, documents internes et externes aux entreprises étudiées, entretiens) viennent compléter, conforter voire contredire nos constats.

Enfin, le caractère reproductible de notre recherche sur d'autres cas d'étude est permis par la formalisation de notre méthodologie et le descriptif des périodes et moyens de collectes de données. Nous avons eu recours à une méthodologie usitée en sciences de gestion (la recherche-action) en employant les différentes étapes de collecte évoquées dans la littérature académique sur ce sujet. Nos grilles d'analyse théoriques sont exposées et mises en relation (voir le chapitre théorique et le chapitre relatif aux détails des cas d'étude). Nos entretiens confirmatoires obéissent encore à une grille de lecture et à un questionnaire fournis dans le cadre de cette recherche doctorale. La validité externe de notre recherche, bien qu'ayant été une préoccupation sous-jacente durant toute la période de collecte, d'analyse et de restitution des données, pourra cependant sembler perfectible en raison du caractère qualitatif de notre recherche. Laquelle, mais cela dépasse le cadre d'une recherche doctorale, pourrait être envisagée sous un angle quantitatif plus poussée, à condition d'avoir un accès au réel permettant une telle analyse. Cela n'était à ce stade pas le cas de notre étude (pour la partie qualitative), ni notre souhait pour des raisons de faisabilité dans une période de temps étant celle d'une recherche doctorale. Les données disponibles en matière de risque opérationnel posent en pratique de nombreuses difficultés en matière d'homogénéité, de fiabilité ainsi que de disponibilité d'une base suffisamment importante pour être exploitable via des méthodes statistiques fiables[48].

[47] Critère de convergence le plus souvent évoqué en recherche qualitative.

[48] Les bases de données existantes en matière de risques opérationnels sont ORX en banque et ORIC en assurance. Toutefois, ces bases de données ne sont accessibles que par les établissements financiers abonnés et

2.1.2. Les limites de l'approche qualitative : quelles difficultés posées par notre méthodologie ?

L'une des limites de notre recherche est résumée notamment par Wacheux (1996) et Lawrence Neuman (2011). Ils insistent sur le fait que l'observation passive ou participative dans une logique qualitative peut entrainer le chercheur vers des détails parfois sans importance ou en marge même de l'objet de recherche. Dans ces cas de figure, la dimension affective implique le chercheur et peut perturber les observations. Il existe des nuisances propres à la collecte mais aussi à l'analyse des données qualitatives que sont les biais d'ancrage et le manque de distanciation que peuvent impliquer ces données ou encore la difficulté à distinguer ce qui constitue les éléments réellement représentatifs ou explicatifs de plusieurs contextes croisés (Miles, 1979).

La recherche qualitative implique donc des garde-fous que nous évoquons dans notre descriptif méthodologique au travers des approches par distanciation et un codage ad hoc permettant de passer de la contingence spécifique à une contingence générique dans la lignée du principe de généralisation analytique.

L'une des limites du recours aux méthodologies de type recherche-action est également que le chercheur vit avec les acteurs au sein de l'organisation et peut donc faire preuve d'un « syndrome d'empathie ». Il devient alors le défenseur des actions du groupe où il se situe. Lors de notre recherche cette seconde limite s'avère peu opérante dans la mesure où nous avons entendu préciser le rôle de chaque acteur et notre rôle par rapport à chacun d'entre eux afin d'éviter une confusion des actions et un rapprochement des positionnements biaisant nos constats. Il subsiste nécessairement certains biais de collecte de données liés à l'expérience même des interviewés ou à des non-dits ou points de vues dont le caractère subjectif est parfois difficile à décorréler des propos à vocation plus générale étant tenus.

---

contribuant à alimenter lesdites bases. Les données présentent dans ces bases sont toutefois trop éparses et présentent des problématiques de confidentialité les rendant difficilement exploitable dans le cadre d'une recherche extérieures aux entités ayant renseigné ces données (nos entreprises de rattachement en recherche-action n'étant alors pas adhérentes à ces bases de données).

Tableau 16., Approches quantitative et qualitative, d'après Lawrence Neuman (2011, p.17)

Approche quantitative	Approche qualitative
-Mesure des faits objectifs	-Construire une réalité sociale/culturelle
-Focus sur les variables	-Focus sur les processus interactifs/évènements
-Fiabilité des données comme facteur clé	-Authenticité des données comme facteur clé
-La valeur des données est exogène	-La valeur des données est contingente
-Sépare théorie et données	-Théories et données sont liées
-Indépendance par rapport au contexte	-Situations contraintes (temps, contexte)
-Nombreux cas et sujets d'étude	-Quelques cas et sujets d'études
-Analyse statistique	-Analyse thématique
-Chercheur détaché de son objet de recherche	-Chercheur impliqué, engagé dans sa recherche

2.1.3. La recherche qualitative dans notre champ de recherche

Dès 1979, Van Maanen insistait sur la nécessité d'un recours plus prononcé aux méthodologies de recherche qualitative. Le recours à des méthodologies de recherche qualitative n'a pas toujours fait l'unanimité, notamment en raison des problèmes d'analyse et de généralisation de la connaissance auxquelles sont souvent confrontés les chercheurs face à des données qualitatives (Miles, 1979) ; ce qui constitue un paradoxe pour des sciences appliquées (Denzin, Lincoln, 2011). Des études récentes tendent à démontrer qu'il est pertinent de prendre davantage au sérieux les recherches qualitatives dans les sciences du management et en ce qui concerne l'étude des organisations même si le statut de ce type de méthodologie est souvent décrié au profit de méthodologie quantitatives ayant historiquement montré leur validité scientifique, comme l'expliquent Cassell et al. (2006).

Le recours aux méthodologies de type qualitative peut cependant s'avérer pertinent pour répondre à des problématiques encore émergentes, exploratoires, ne faisant pas l'objet d'un consensus et pour lesquelles l'accès à des données formalisées fait en partie défaut[49] (Parker, 2012 ; Ter Bogt, Van Helden, 2012). Certains auteurs défendent la nécessité de dépasser une simple logique de quantification et de modélisation de tout phénomène organisationnel, a

[49] Comme cela est le cas pour les risques opérationnels dans de nombreux établissements financiers. D'où le recours à des bases de données externes en vue de réaliser des études comparatives.

fortiori quand ces derniers concernent et font interagir des attitudes et comportements ou qu'ils impliquent des processus complexes (Lee, Humphrey, 2006).

D'autres auteurs insistent sur la nécessité de proposer des approches de recherche mixant méthodes qualitatives et quantitatives en vue de dépasser cette dichotomie (Hofstede et al., 1990 ; Savall, Zardet, 2004 ; Cappelletti et al., 2007 ; Jogulu, Pansiri, 2011 ; Grafton et al., 2011).

Les recherches qualitatives abordant l'objet de recherche 'Risk Management' : De nombreuses études (principalement en économie et finance) abordent la thématique du risque, au travers de l'enjeu de probabilité de survenance dans une logique assurantielle (Morlaye, 2006 ; Vaughan, Vaughan, 1995) ou la logique comptable associée au risque (Gardener, 1983). Toutefois l'enjeu que constitue le risque pour la société a fait l'objet d'études montrant la nécessité de développer de réelles politiques de risque (Kessler, 2000 ; Gilbert, Lascoumes, 2003 ; Pradier, 2006 ; Borraz, 2008). Les études du risque ayant recours à une approche qualitative visent notamment à décrire le lien entre cette notion et d'autres notions similaires telles que les notions de confiance et de menaces (Nooteboom et al., 1997), le lien entre risque, processus organisationnels, gestion des risques et stratégie (Jemison, 1987), le lien entre risque et responsabilité (Knechel, 2007 ; Murphy, 2011), la description pratique des limites du Risk Management (Crawford, Stein, 2002). Pour ces différents sujets, une recherche qualitative semble mieux à même de permettre la collecte et l'analyse des données relativement aux normes de contrôle des risques opérationnels.

2.2. La triangulation méthodologique

La recherche qualitative permet et suppose le recours à de nombreuses méthodes pour collecter la matière empirique. Ces dernières incluent l'interview, l'observation directe, l'analyse des artefacts et des éléments culturels ou encore le recours à des matériaux *« visuels »* et à l'expérience personnelle (Denzin, Lincoln, 2005, p.25). Notre positionnement méthodologique s'inscrit dans ce contexte en mobilisant différents outils complémentaires.

La méthodologie de recherche retenue s'inscrit dans une triangulation méthodologique (Jick, 1979) comprenant le recours à des études de cas menées en recherche-action (Barbier, 1996) et à une analyse de contenu sur la base de documents internes aux études de cas réalisées ainsi qu'à la littérature sur la gestion et le contrôle des risques. Enfin, des entretiens semi-directifs

sont conduits en vue de compléter les études de cas réalisées. L'objectif de cette triangulation méthodologique est de cerner par différents moyens les enjeux exprès et tacites liés à la gestion du risque opérationnel (notamment les freins et leviers que présentent une telle approche du contrôle issue à la base de la réglementation prudentielle). Le schéma ci-après (figure 25) précise les différents modes de collecte de données et leurs rôles respectifs et spécifiques dans la recherche de confirmation de nos hypothèses.

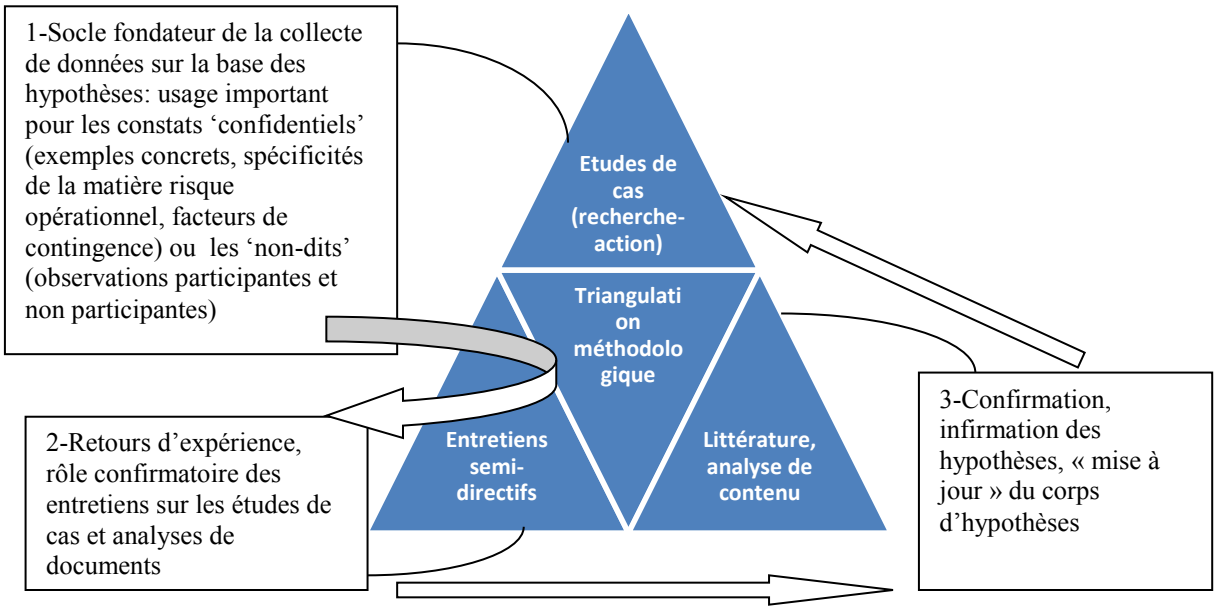
Comme l'explique Lindsay (2012), la tendance actuelle en gestion est désormais d'envisager davantage l'usage de méthodologies tournées avant tout vers l'action pour rendre la recherche en comptabilité-contrôle-audit plus utile, tout en gardant les critères de rigueur nécessaires à la production de connaissances et à la validation des questions et hypothèses de recherche.

C'est à cette préoccupation que répond le choix du recours à la triangulation méthodologique : utiliser une pluralité de méthodes complémentaires en vue de cerner un objet complexe, ce qui caractérise particulièrement les nouveaux champs de recherche en contrôle (Hoque et al., 2013). Le recours à une diversité de méthodes apparait de surcroit adapté en ce qui concerne des thématiques de recherche comprenant un diagnostic organisationnel : cela explique la pertinence de méthodologies typiquement académiques, mixées à des méthodologies davantage tournées vers la pratique telle que la recherche-action ou la recherche-intervention, ce qui caractérise le champ émergent des *'consulting science'* (Paul, 1996 ; David, 2000). La triangulation autour d'un objet complexe usant plusieurs méthodologies convient en outre pour des recherches exploratoires visant à faire émerger un cadre de pensée autour d'une thématique de recherche (Kekäle, 2001).

Le recours à la triangulation méthodologique dans notre recherche se caractérise de la manière suivante :

Plusieurs types de données ont été collectés entre 2010 et 2013. Des données primaires (entretiens semi-directifs et observations participantes et non participantes lors de deux études de cas en recherche-action) et des données secondaires (recueil de documents internes : compte-rendu de réunion, rapports internes et externes aux entreprises, études sectorielles, réglementation prudentielle et rapports sur ladite réglementation etc.).

Figure 25. Triangulation méthodologique



-Descriptif et justification de la méthodologie employée : Notre recherche basée sur une « triangulation méthodologique » (Jick, 1979) vise à établir le lien entre notre revue de littérature, notre recherche-action ainsi que des entretiens qualitatifs exploités via un codage manuel (renforcé grâce à l'utilisation d'un logiciel d'analyse de contenu). Cette méthode se veut de percevoir l'approche du contrôle développée quant au risque dans une logique « humaniste », soit la recherche d'une cohérence des actions par rapport aux buts que se fixent les individus (Burlaud et al., 2004). Face à cela, la posture constructiviste résumant nos études de cas vise à retranscrire une réalité du contrôle des risques reprenant le modèle des usages de la recherche-intervention en contrôle de gestion : interactivité cognitive, intersubjectivité contradictoire et contingence générique (Cappelletti, 2010).

2.3. Le recours à des études de cas en recherche-action

L'objet de ce paragraphe est d'appréhender la logique de réalisation d'études de cas utilisées dans le cadre de notre recherche. Nous présentons également les spécificités liées au recours à une méthodologie de collecte et d'analyse de données en recherche-action.

2.3.1. Justification du recours aux études de cas

L'étude de cas est définie par Yin (2012) comme une enquête empirique à propos de phénomènes contemporains survenant dans le monde réel dans des contextes spécifiques.

Cette approche méthodologique trouve sa justification dans l'étude des cas pour lesquels la frontière entre phénomène et contexte n'est pas clairement établie[50].

Le choix de l'étude de cas dépend de la question de recherche: dès lors qu'il s'agit d'une question à caractère descriptif (comment et pourquoi quelque chose est survenu ?), il est alors pertinent de pouvoir alterner les méthodes de recherches pour discerner ce qui relève du cas particulier de ce qui a vocation à être généralisé. L'étude de cas est donc un outil méthodologique précieux en début de recherche pour comprendre la survenance de certains phénomènes (comme l'apparition de politiques de maîtrises dédiées au risque opérationnel dans notre recherche).

L'étude de cas peut permettre de limiter certains biais que l'on retrouve parfois dans les questionnaires d'entretiens (caractère précis et partiel des questions et donc des réponses qu'elles suscitent ; les approches quantitatives et le caractère fini des données recueillies). Cela permet encore de mieux cerner le contexte « naturel » de survenance d'un fait ou d'une série de faits. Pour ces raisons, la méthode de l'étude de cas est aujourd'hui couramment utilisée en « comptabilité contrôle audit » notamment et a permis de documenter de nombreuses problématiques appliquées (Yin, 1994). Nous nous inscrivons dans cette démarche.

Comme l'évoque Yin (2012, p.7-9), l'étude de cas repose sur:

-la définition claire d'un cas : dans notre recherche il s'agit d'étude de cas de longue période en tant que chercheur-acteur interne à l'organisation,

-le choix d'un design spécifique d'étude de cas (entre une approche holistique consistant à réaliser une recherche complète et à visée exhaustive d'un ou plusieurs cas d'étude et une approche intégrée consistant à étudier un ou plusieurs cas en répondant successivement à des questionnements interconnectés) : dans notre étude il est question d'étudier plusieurs cas d'entreprises (un établissement bancaire et une société d'assurance) en répondant à plusieurs questionnements imbriqués (descriptifs, explicatifs, prescriptifs),

-le fait d'établir un lien entre le cas d'étude et la théorie (l'étude de cas s'inscrit dans une perspective théorique) : dans notre recherche, notre positionnement (décrit ci-après) de type

[50] Traduction libre de l'auteur.

chercheur interne / praticien réflexif nous permet de lier certains cadres théoriques (théorie de l'acteur réseau, théorie de la structuration, théorie du contrôle interactif ou encore théorie émergente du contrôle des risques) à nos constats empiriques, et ce par le prisme de retours successifs entre théorie et pratique,

-la recherche d'une variété de sources de données lors du cas : nos études de cas répondent à cette logique car nous mobilisons de nombreuses sources internes (observations directes et indirectes par le biais de notre pratique, de témoignages et entretiens internes, de documents internes et externes),

-l'accès à des observations directes : dans nos deux études de cas, nous avions un accès direct aux terrains de recherche, eu égard à nos positionnement en tant que contrôleur des risques (société d'assurance) et de Risk Manager (établissement bancaire).

-des interviews ouvertes : les différentes réunions et échanges au sein des services et départements de rattachement lors de nos études de cas nous ont permis de réaliser un nombre important d'entretiens non directifs mais aussi d'entretiens davantage formalisés, ce tout au long des études de cas. Nous orientons en effet les échanges en lien avec notre question de recherche.

-le recueil de données d'archives et historiques de l'entité étudiée : nos deux études de cas nous ont permis d'avoir accès aux nombreuses données internes des entreprises étudiées (rapports de contrôle, d'audit, notes d'analyses de risques, notes de services, compte-rendu de comités produits, comités risques etc.),

-un protocole claire de recherche de données (Yin, 2012, p.13)[51], l'une des difficultés de l'étude de cas est de pouvoir vérifier en permanence la pertinence des données collectées à partir d'une même source (Strauss, 1987). La triangulation méthodologique mobilisée dans le cadre de cette recherche doctorale permet de confronter ces données. Dans la lignée des apports de Yin (2012), le rôle de la revue de littérature dans la triangulation méthodologique (et de l'analyse de documents) est d'aider à anticiper les situations où les données vont se corroborer entre elles sans pour autant enlever les biais (car elles proviennent des mêmes

[51] Traduction libre de l'auteur.

acteurs ou d'acteurs différents mais répondant à une même problématique expresse ou tacite). Ces données feront ainsi écho à la même logique sans pour autant permettre de décrire la réalité de l'organisation,

-une présentation spécifique des cas (Yin, 2012, p.15), laquelle suppose d'avoir un cheminement clair de collecte de données qui, sans être indispensable, peut être d'une aide efficace pour guider le chercheur face à une situation de « prolifération de données ». Il est clairement question de ne pas mixer ce qui relève du cas, du résultat réel, de l'exemple, et de l'interprétation, a fortiori lorsqu'il y a plusieurs cas, cela créé un biais dans la comparaison inter-cas, il faut donc bien scinder des éléments distincts issus de la même collecte de données. Notre recherche prête attention à ces éléments en reprenant les apports méthodologiques de Savall et Zardet (2004) dans la présentation des cas d'étude,

-une analyse dédiée aux études de cas, laquelle, sans être routinière, suppose le recours à des méthodes précises et/ou des logiciels d'analyse de contenu constituant une aide pour définir une logique d'interprétation décuplée dans chaque cas (Exemples : approche chronologique, approche par récurrence, approche narrative).
Comme le précise Yin (2012) relativement à ces méthodes, le fait de répliquer la même approche méthodologique peut avoir le risque de conduire au même résultat. Il faut donc conserver l'idée dans l'analyse qu'il peut subsister des biais et que la généralisation statistique ou la codification thématique, aussi poussée soient-elles, ne constituent pas le statut de preuve. Lors de nos études de cas, nous avons entendu nous inspirés des travaux menés mobilisant notamment l'approche narrative (Boje, 1994, 2001, 2004). Le recours à cette approche suppose toutefois, dans une logique pragmatique, des adaptations pour tenir compte de la spécificité du vocabulaire employé lors de nos études de cas, mais ce tout en gardant une rigueur méthodologique afin de retranscrire la réalité des terrains de recherche.

2.3.2. Justification de l'approche méthodologique de type recherche-action

La recherche-action est définie comme : *« une double opération de formalisation et de modélisation des pratiques sociales »*. La formalisation de ces pratiques consistant à extraire des contenus vécus (sous formes institutionnelles, langagières, communicantes, affectives, cognitives, économiques, pratiques) qui servent de références implicites aux acteurs sociaux tels que les chefs d'entreprises, les cadres et les employés/ouvriers (Resweler, 1995, p.8). Elle

permet de comprendre comment les pratiques sociales et à visée d'apprentissage sont localisées et émergent dans des circonstances empiriques (Kemmis, McTaggart, 2005). La recherche-action nous semble particulièrement adaptée eu égard au caractère exploratoire de notre recherche, s'agissant d'une *« méthodologie expérimentale en vue de l'action »* (Barbier, 1996, p.23)

Le terme de recherche-action appelle des précisions car il est par nature imprécis et ambigu : il concerne ce qui, bien que théorique, reste empirique et réalisé sur le terrain avec une finalité pratique. La recherche-action vise à clarifier un sujet, à définir des priorités, à restructurer une entreprise ou à permettre de voir les conditions dans lesquels reconquérir un marché donné.

La démarche est d'emblée codée car il s'agit d'une réflexion sur l'action menée et sur les actions à mener dans une logique prospective. Elle peut également être qualifiée de processus social, participatif et collaboratif à visée d'émancipation : permettre le recul sur l'irrationnel, le non-productif, l'injuste et les problèmes dont les solutions ne sont pas satisfaisantes. Elle est également critique par le langage, le discours et l'interaction, elle pose des questionnements sur les différences entre acteurs et fonctions, les inclusions et exclusions et les affiliations-relations sur des points donnés. Elle est enfin réflexive car elle aide les individus à *« investiguer »* la réalité dans le but de la faire évoluer (Kemmis, McTaggart, 2005, p.565 et s.).

En tant que fondateur de la recherche-action, K.Lewin explique dès 1946 que ce type de méthodologie s'est développé en réaction contre la séparation des logiques de connaissance et d'action.
Il définit cette méthode comme une « recherche impliquée » étant un compromis entre recherche appliquée et recherche pure. *« Elle vise à pallier le morcellement du savoir en repositionnement le chercher sur la cité »* (Resweler, 1995, p.8).

Pour Reason et Bradbury (2001, p.2)[52], *« le but premier de la recherche-action est de produire un savoir empirique utile aux individus dans la conduite de leur vie de tous les jours. Elle intègre un enjeu plus large qui est de contribuer à travers un savoir pratique à*

[52] Traduction libre de l'auteur.

accroitre le bien-être (économique, politique, psychologique, spirituel) des individus et des communautés ».

La recherche-action s'inscrit dans un cadre de pensée post-moderne où l'on cherche davantage les moyens de poser des questions nouvelles dans une logique exploratoire que de répondre à des questionnements dans une visée confirmatoire (Harvey, 1990). Le chercheur en recherche-action a un rôle de facilitateur, il agit comme un consultant sur les processus et les hommes et facilite l'évolution des cadres socio-organisationnels en posant des questions, en expliquant des situations et en permettant un débat à des fins de compréhension de sujets non solutionnés ou nouvellement posés.

Dans notre étude le choix des cas s'explique pour les raisons suivantes :

-le sujet exploratoire « risque opérationnel » et l'étude de la mise en œuvre pratique des politiques de maîtrise dédiée à cette catégorie supposaient de mobiliser des cas d'entreprises suffisamment long pour que l'observation soit représentative de la réalité (des études de cas de six mois minimum semble crédible sur un sujet de ce type, alliant des problématiques réglementaires aux enjeux organisationnels internes aux structures). Une période de six mois minimum (respectée dans nos deux études de cas) nous permettait clairement d'identifier les freins et leviers dans la mise en œuvre des politiques de maîtrises des risques opérationnels ainsi que d'envisager notre sujet central (le passage de la normativité à l'effectivité du contrôle des risques).

-nous avons également orienté notre choix sur deux structures différentes, une société d'assurance et un établissement bancaire, en vue d'étudier les différents degrés de maturité par secteur pour ces entreprises françaises et de nous livrer à des comparaisons inter-cas,

-le choix des études de cas était également orienté par la nécessité d'être en face de situations d'entreprises représentatives du secteur français et présentant une réelle diversité de cas de survenance de risque opérationnel, ces entreprises étant généralistes de par leurs activités,

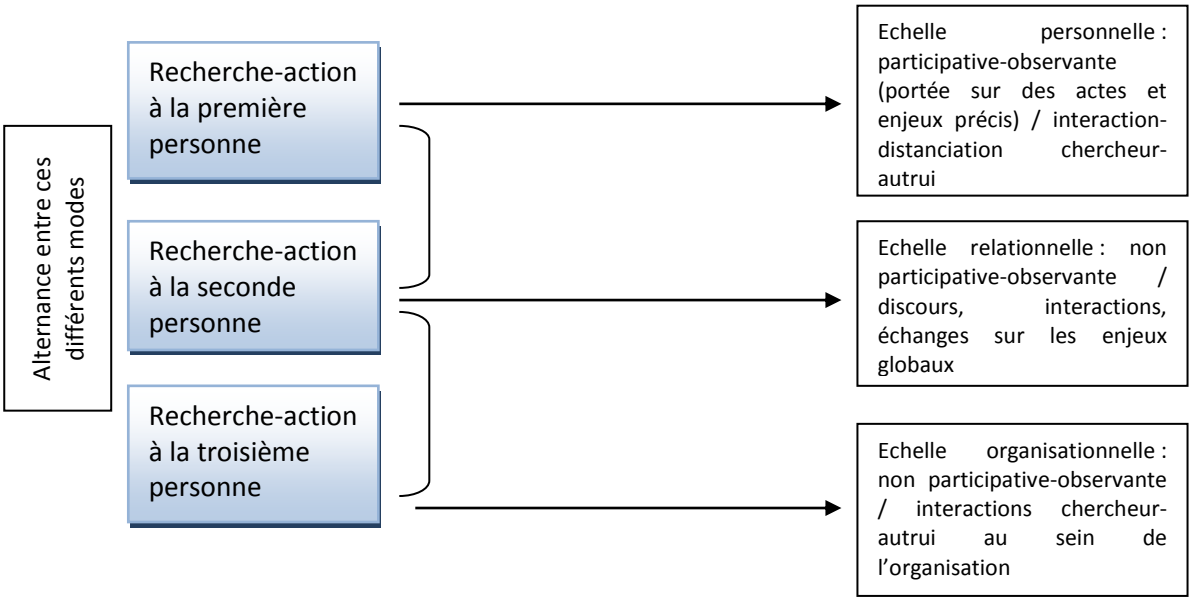
-enfin, le choix des cas est également le fait des contraintes d'accès au réel, nous nous sommes centrés sur les cas d'entreprise dans lesquels une étude appliquée était réalisable, tant pour des questions d'accessibilité de l'entreprise que d'intérêt accordé au sein des structures au sujet constituant notre objet de recherche.

Pour Gustavsen (2001, p.15) une recherche limitée à quelques cas d'étude et à un périmètre restreint peut très bien convenir dans une logique fondatrice d'une recherche sur un sujet émergent. La recherche-action est en outre adaptée pour cerner une perspective « en réseau » dans un cas d'étude.
Notre recherche se concentrant sur deux cas d'entreprises, une telle perspective est donc en cohérence avec la logique exploratoire que nous poursuivons.

2.3.3. Notre positionnement en recherche-action

Parmi les différents positionnements en recherche-action (décrits dans le schéma ci-après), notre recherche au sein des entreprises étudiées se caractérise par un positionnement principal de type recherche-action à la première personne (dans une logique fortement participative mais aussi observante). Concomitamment, notre approche de la recherche-action a été un enjeu d'échanges et d'interactions avec de nombreux acteurs rencontrés (recherche-action à la seconde personne). Dans une moindre mesure, et de manière tacite, la recherche-action a pu être de type troisième personne (non participative et observante). Cette dernière posture était ponctuelle (journée de séminaires dédiées « risque », rôle de reporting sur certains comités).

Figure 26. Positionnement en recherche-action d'après Torbert, 1999



Dans le même temps, S.Kemmis et R.McTaggart (2005, p.559 et s.) distinguent différentes postures en recherche-action :
-la recherche-action participative (participative research), laquelle est axée vers la transformation sociale sur un ou des projets et sur une communauté donnée,
-la recherche-action critique (critical action research), qui est orientée vers l'analyse sociale et l'étude des pratiques, du langage et des organisations en vue d'améliorer la réalité,
-la recherche-action en groupe (de type classroom action research), à visée d'enseignement et d'améliorer des méthodes d'enseignement et d'apprentissage (apprendre les uns des autres en travaillant en groupe),
-la recherche-action de type consultation scientifique (action science), dans laquelle les enjeux académiques et les problèmes pratiques sont complètement imbriqués.

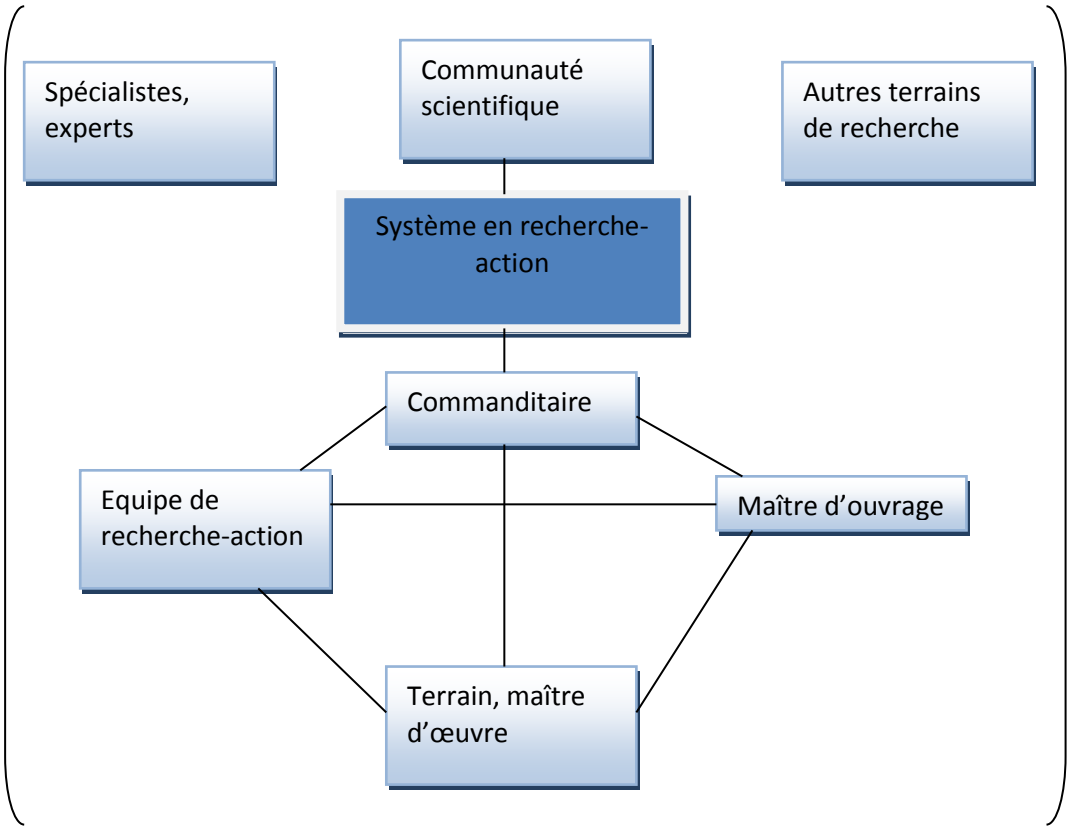
Les deux premières postures (participative et critique) caractérisent notre positionnement. En effet, notre recherche visait une communauté donnée : celle des contrôleurs des risques et des acteurs en lien avec ces derniers. Elle avait pour but l'explication et la conduite de projets visant la mise en place de politiques de maîtrise des risques. En cela, elle est donc participative. Egalement, elle concernait l'étude des pratiques de contrôle et de traduction de la norme relative au risque opérationnel à des fins de meilleures compréhensions et d'adaptation pratique de ladite norme. Cela donne à notre recherche son caractère critique. Si la recherche-action de type consultation scientifique pourrait sembler adaptée, dans notre recherche les enjeux pratiques ont en premier lieu pris le pas sur la dimension académique. Si certaines grilles de lecture théoriques et études ont inspirés notre démarche d'analyse, la dimension académique intervenait en second lieu après une phase de distanciation et à des fins d'analyse en vue de ne pas biaiser la collecte de données.

Notre positionnement en recherche-action est donc à la fois :
-caractérisé par une approche à la première personne, (à la seconde personne dans une moindre mesure),
-situé entre l'approche participative et critique de la recherche-action.

2.3.4. Sur quoi repose la recherche-action ?

La recherche-action repose sur l'interprétation d'un vécu dans un contexte situé. Elle est à la fois compréhensive, explicative et comparative. En effet, la recherche-action ne vise pas uniquement l'interprétation, elle cherche à corriger, infléchir ou transformer la réalité.
En fonction de cela, le rapport recherché relève soit de l'implication, soit de la concentration du chercheur sur une thématique donnée.

Figure 27. Les interlocuteurs de la recherche-action (d'après Liu, 1997, p.152)



Liu (1997, p.155) distingue ainsi les interlocuteurs directs (sur le terrain) des interlocuteurs indirects (hors du terrain tels que les membres de la communauté scientifique, les autres chercheurs le cas échéant, les parties prenantes d'autres terrains de recherche).
La recherche-action dans cette optique repose ainsi sur la création de réseaux d'interactions, ce en plusieurs phases que sont :
-la découverte et la mise à jour des interlocuteurs pertinents (connaître les réseaux d'interactions),

-l'animation du réseau et l'information des interlocuteurs,
-l'établissement de lieux d'échanges et de négociations.

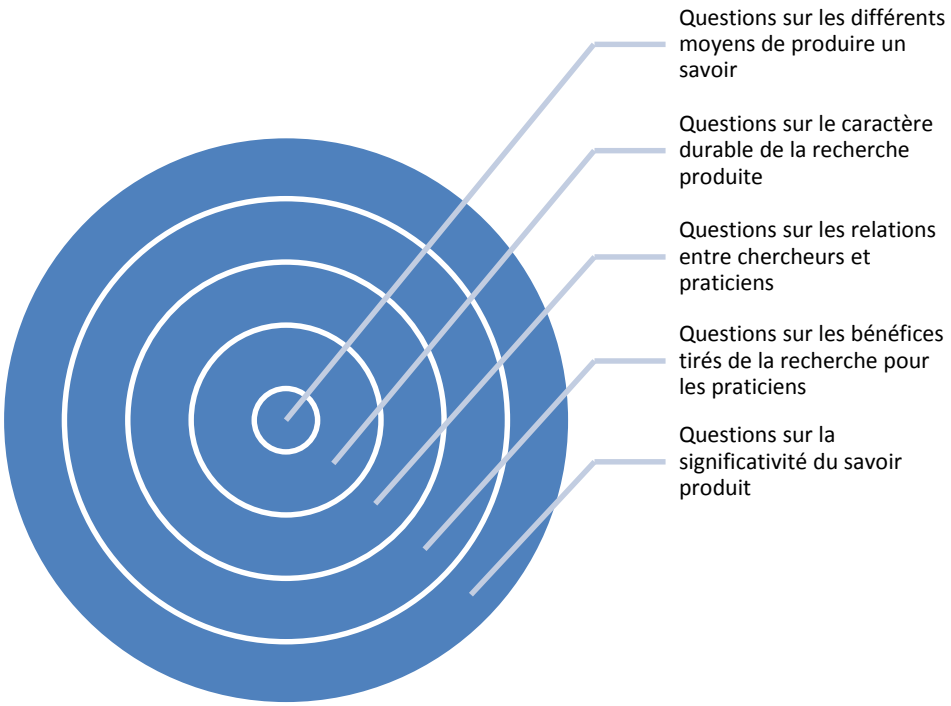
Les matériaux sur lesquels reposent la recherche-action portent sur ce qui est vu ou entendu lors de l'étude de terrain tels que des conférences internes, des discours, les retours d'expérience et échanges de groupes d'acteurs (y compris les relations entre ces derniers, les rapports et notes internes, les nouvelles pratiques et modes d'organisation. (Gustavsen, 2001, p.21). Cela comprend également :
- les lectures internes ou externes sur une organisation donnée,
- les histoires décrites ou racontées par les acteurs de l'entité étudiée sur celle-ci, y compris des déclarations particulièrement originales,
- les retours d'expérience lors de monologues ou d'entretiens avec les acteurs rencontrés dans l'organisation,
- les enquêtes publiées sur le cas d'étude,
- les retours et évaluations des chercheurs et de la communauté scientifique le cas échéant,
- les échanges avec un groupe choisi (de managers notamment),
- les données diverses produites dans l'entreprise et les plans internes engageants les collaborateurs de l'organisation étudiée et les participants directs ou indirects de l'étude au sein de celle-ci.

- **La validité de la recherche-action**

Pour être valide une recherche-action doit répondre aux critères de falsification évoqué par Popper (1973). Il y a une résistance en pratique qui fait que le caractère contextuel subsiste. Une étude de cas présente nécessairement un caractère contingent qu'il convient de mettre en exergue en vue de démontrer qu'il s'agit bien d'une étude dont on cherche à extraire ce qui est générique du contingent sans pour autant prétendre que le cas d'étude fait « science » sans remise en cause ou démonstration possible au travers d'un cas contraire. La phase de distanciation suivant toute recherche-action rend possible tout amendement aux schémas et descriptions réalisés. Cela suppose clairement de définir les éléments analysés et le contexte de l'étude pour pouvoir démontrer potentiellement l'inverse ou confirmer les constats réalisés à l'aide d'un cas proche voire similaire.

La validité d'une recherche-action telle que définie par Reason et Bradbury (2001) repose sur le fait de poser les questionnements suivants :

Figure 28. Questionnements en recherche-action, d'après Reason et Bradbury, 2001



- **L'élaboration des connaissances dans la recherche-action**

Resweler (1995, p.255) détaille les différentes phases permettant l'élaboration des connaissances dans le cadre d'une méthodologie de type recherche-action, cela consiste à choisir une problématique :

-propre au terrain de recherche (un terrain différent n'aurait pas les mêmes implications sur les résultats escomptés),

-propre à la méthodologie de recherche-action, (une autre méthodologie n'aurait pas permis d'étudier ce terrain ou tout du moins d'obtenir ces résultats),

-propre aux enjeux sociaux et de changement socio-organisationnel (le questionnement est ancré dans la réalité, il doit sous-entendre des préoccupations plus larges pour les acteurs d'une société ou d'un groupe organisationnel donné).

« Exemple : Quels sont les conditions pour qu'un groupe prenne en charge un problème donné ? Quels sont les résistances à cette prise en charge ? »

La phase suivante concerne le choix d'un sujet d'étude : là-encore propre au terrain, à la démarche de recherche-action et aux enjeux socio-organisationnel dans lesquels celle-ci s'inscrit.

L'élaboration de la connaissance suppose une perception claire des situations et changements en cours, aussi elle implique de réaliser :
-un diagnostic des situations initiales,
-une formulation des problématiques,
-une mise en œuvre d'actions expérimentales,
-l'élaboration des conclusions de chaque cas d'étude.

Pour Treleaven (2001, p.266), plusieurs étapes en recherche-action permettent une traduction des concepts émergents et donc la production de connaissance. Ces dernières sont :
-la contextualisation des cadres théoriques enracinés dans la pratique,
-le fait de situer les questions et enjeux collaboratifs au sein de ces cadres théoriques et pratiques,
-intégrer les pratiques de type *« story-telling »* en ce qui concerne plus spécifiquement les évènements marquants ou *« critiques »* lors de la recherche-action.

2.3.5. Les différentes phases d'une recherche-action

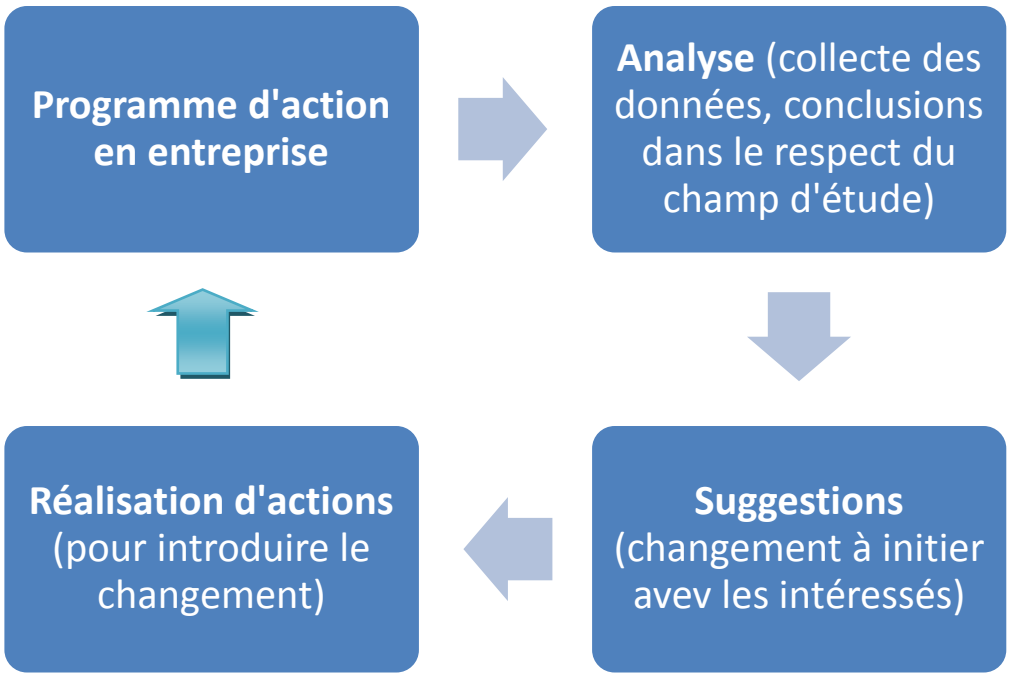
-La période exploratoire (définir le problème) : elle consiste en l'énoncé de la problématique, à l'analyse des demandes, à l'identification de la manière de résoudre le problème par la détermination de valeurs partagées (il s'agit par exemple des déterminants des logiques de responsabilités et d'approches préventives propre à ce qui est qualifié de « culture du risque », de la recherche de conciliation entre performance de l'activité et maîtrise des risques, etc.).

-l'analyse du champ d'action possible de la recherche-action et des rapports de forces (choisir les solutions et les modes de résolution) : il est important de ne pas laisser le système dans une situation de crise à l'issue de la recherche-action. Aussi, l'analyse de la faisabilité de la recherche-action dépend du degré de liberté accordé au chercheur. Dans notre étude il s'agit de savoir si la mise en œuvre « opérative » des politiques de maîtrise du risque opérationnel est réalisable.

-L'analyse des conditions de réalisation et des résultats (mise en œuvre des solutions).

Le processus de recherche-action tel que décrit est ainsi résumé par le schéma ci-après (Kumar, 2005, p.109) :

Figure 29. Processus de recherche-action, d'après Kumar, 2005



2.3.6. Détail du protocole de recherche-action au sein de notre étude :

Nous nous sommes basés sur des études de cas en entreprise. L'étude de cas a comme fondement des observations des pratiques professionnelles comme mode de collecte des données, ce sur la base d'une implication du chercheur au sein de l'entreprise étudiée (Jönsson, Lukka, 2005). Nous nous inscrivons dans le prolongement de certaines recherches attestant qu'en matière de gestion et de contrôle, il existe plusieurs modes de création de connaissance : l'observation et la contribution directe par l'action en tant que participation à l'action collective (David, 2003). Ce positionnement tend à justifier le recours à la triangulation méthodologique (Jick, 1979). Nous avons observé de nombreuses pratiques par des entretiens ainsi que des données secondaires (rapports, notes de service etc.) mais avons également eu comme démarche la contribution directe au processus étudié concernant les politiques de risques opérationnels.

La recherche-action est envisagée par Argyris et al., (1985) comme l'un des meilleurs moyens d'observer un processus de changement et d'y contribuer. Il s'agit de l'une des méthodologies de recherche transformative au même titre que la recherche-intervention (Jönsson, Lukka, 2005 ; Kaplan, 1998).

La recherche-action est une méthodologie de transformation intentionnelle de l'organisation et de ses composantes. Elle a pour objectif de préparer un groupe d'acteurs au changement, lequel peut être initié par ledit groupe et pouvant inclure le chercheur lui-même. Elle comprend deux axes que sont la formalisation du changement et sa contextualisation dans un cadre organisationnel donné.

Comme le résument certains auteurs, la recherche-action a pour objectif de préparer un groupe au changement par des processus participatifs et démocratiques qui aideront les acteurs à se libérer de l'emprise des structures. Il leur reviendra de transformer l'organisation selon leurs visions et objectifs, potentiellement en dehors de l'action du chercheur (Cappelletti, 2010, p.7 ; David, 1999 ; Reason, Bradbury, 2001). Une telle approche apparait comme particulièrement justifiée au regard de notre objet d'étude : le déploiement de politiques de risque opérationnel dans les établissements financiers en vue de répondre aux exigences prudentielles.

Nos études de cas menées en recherche-action concernaient deux entreprises. Une filiale française de compagnie d'assurance de dimension internationale ainsi qu'un établissement bancaire d'ancrage national.
La première recherche-action (menée sur un an) concerne le déploiement d'une politique de gestion des risques opérationnels au sein de la société d'assurance. L'objectif est d'intégrer au sein du dispositif de contrôle interne la logique de gestion des risques opérationnels dans un souci de conformité aux exigences du régulateur du secteur financier en vue de l'application de la norme à venir Solvabilité II (directive européenne).
La seconde recherche (d'une durée de six mois) a pour objectif l'application de la politique de maîtrise des risques opérationnels au sein d'un établissement bancaire. Cette politique, alors en cours de redéfinition, se devait d'être clarifiée au regard des exigences du règlement bancaire CRBF 97-02 dans plusieurs périmètres de la banque pour lesquels des écarts voire des retards avaient pu être constatés dans la collecte des données et la mise en place du dispositif de gestion des risques.

La recherche-action a permis de procéder à un ensemble d'observations à la fois participantes et non participantes (retours issus des comités risques opérationnels, comités produits, comités moyens de paiement, réunions de filière risque opérationnel, construction du plan de contrôle, missions de contrôle ciblées par produits et zones de risque) afin de cibler au mieux les multiples enjeux organisationnels pouvant conduire à l'inefficacité et au manque d'opérativité d'une politique de risque. Les points d'attention concernaient la mise en œuvre de dispositifs de contrôle des risques de manière commune avec plusieurs contrôleurs internes (structure n°1) et la conduite d'une politique de risque (structure n°2) conjointement avec d'autres Risk Managers. Il ne s'agissait pas seulement de mettre en œuvre des dispositifs pour respecter la réglementation, l'objectif essentiel de cette recherche-action était bien la sensibilisation à la culture du risque et la manière dont on pouvait prendre en compte le risque dans une activité opérationnelle quotidienne (logique de réduction du coût du risque) tout en visant l'atteinte des objectifs stratégiques de l'organisation. Les études de cas menées sont intégrées dans notre recherche par le biais de monographies.

Notre cadre méthodologique, inspiré de travaux menés en recherche-action, peut être décrit selon le schéma ci-après.

Figure 30. Cadre de la recherche-action mise en œuvre, d'après Cappelletti, 2010

La recherche-action est à rapprocher dans le cas présent du concept *d'engaged scholarship* proposé par Van de Ven et Johnson (2006) qui décrivent clairement le processus de production-traitement de connaissance réalisé : poser des problématiques de recherche enracinées dans la pratique et la réalité, concevoir un projet de recherche selon un mode d'apprentissage collaboratif dans et en dehors de l'organisation, développer un projet de recherche de longue durée, mobiliser des théories et des méthodes de recherche variées, réviser régulièrement les hypothèses de recherche.
La recherche-action nous a permis un accès aux données facilité afin de mieux cerner la complexité de cette thématique de manière réflexive. Si cette immersion était nécessaire, elle implique un certain parti pris et engagement dans l'organisation concernée. L'enjeu de généralisation et de validité de la connaissance produite suppose alors une nécessaire distanciation et une phase ex-post d'échange avec les collaborateurs rencontrés : phases de perception, introspection, action (Lallé, 2004 ; Cappelletti, 2010). Les constats réalisés sont en partie contingents des cas d'étude mais ces derniers restent porteurs de questionnements plus larges (Schön, 1983) quant à notre objet de recherche.

Les phases d'immersion en entreprise ont été l'occasion de réaliser de nombreux échanges avec les membres des filières risques et contrôle et de récolter un nombre important d'informations qui ont pu être traitées et analysées par la suite (distanciation). Les constats et analyses ainsi faites lors des échanges avec les collaborateurs (interactivité cognitive) sur le terrain ont ensuite été soumis ex-post à ces derniers pour avis et critiques (intersubjectivité contradictoire). La phase d'entretiens confirmatoires réalisée (voir ci-après) a ensuite été l'occasion de réaliser des généralisations (contingence générique).

2.4. Le détail des cas d'étude

La description faite de nos études de cas suit les principes de recherche-action et de formalisation des situations rencontrées dans la lignée des recherches anglo-saxonne sur les méthodes narratives de recherche de terrain (Boje, 1994). Cette méthode est fondée sur une approche narrative du discours de chaque acteur (Boje, 2001 ; Cunliffe et al., 2004). La communication sur le risque étant essentielle dans notre recherche, cette méthodologie semblait appropriée : dans nos recherche-action, lors de chaque réunion de service, échanges formels et informels, comités risques (dans une moindre mesure), notre objectif était de pouvoir faire émerger pour chaque acteur rencontré un retour d'expérience sur le sujet risque

opérationnel et politique de maîtrise des risques. Ces retours d'expérience étaient alors formalisés selon une approche narrative et temporelle : dans le temps, quels sont les éléments marquants pour les personnes rencontrées dans chaque étude de cas. Cela permettait de faire dégager les problématiques récurrentes ou émergentes ayant marqué les acteurs rencontrés.

Le recours au *« story-telling »* dans nos études de cas (Boje, 1994) :
Il s'agit d'une approche narrative facilitant la compréhension par chacun et permettant un gain de temps dans l'explication de la diversité d'éléments étudiés lors d'une recherche. Cela permet également aux individus, lors d'une recherche appliquée au sein d'une entreprise, de prendre un temps pour l'échange et les questions sur des points que ces derniers n'auraient pas compris ou intégré auparavant (Treleaven, 2001). Dans l'approche narrative, l'objectif est de faire se rencontrer les savoirs et intérêts de chacun afin d'expliciter une information donnée et obtenir des interprétations convergentes.
Dans notre étude en recherche-action, nous avons appliqué cette approche, ce qui nous a conduit à :
-identifier les histoires « symptomatiques » (là où sont les problèmes et leurs causes racines),
-rédiger en groupe, collaborativement, l'histoire propre à chacun de nos cas d'entreprise en cohérence avec notre objet d'étude sur les politiques de maîtrise des risques,
-établir des connections sur les sujets communs d'analyse et construire des alliances stratégiques entre acteurs, (le rôle de la filière risque et contrôle dans le déploiement d'une politique de maîtrise des risques),
-recadrer enfin les enjeux organisationnels concernant les politiques de maîtrise des risques et les pratiques qu'elles comprennent et suscitent.
Cette approche, tournée vers l'action affirmée, la planification des possibles et leur réalisation, nous permet à la fois de décrire nos cas d'étude mais aussi d'en analyser le contenu pertinent par rapport à nos questions et hypothèses de recherche.

2.4.1. Le choix des études de cas en recherche-action

La construction d'éléments théorisables en faisant appel à des études de cas a été évoquée par plusieurs auteurs de référence (Huber, Van de Ven, 1995). Pour H.Mintzberg, (1979, p.585), peu importe si l'échantillon est plus faible que dans des recherches quantitatives où quelle que soit la thématique retenue, il importe d'étudier les organisations avec un angle clairement défini et un mode de collecte de données systématique.

Le recours à l'étude de cas est une méthodologie critiquée comme insuffisante pour son manque de généralisation et son caractère trop souvent contingent. Cependant, avec des éléments de rigueur et une méthodologie claire, elle permet davantage que d'autres méthodes d'accéder au réel et d'interpréter l'agir (Yin, 1981). Ce, tout en distinguant ce qui est générique de ce qui est contingent en utilisant des critères d'analyse similaires d'un cas d'étude à un autre.

Nous nous sommes en effet limités à deux études de cas. Si le nombre restreint des études peut prêter à débat, nos recherche-action sont en revanche de longues périodes et nous ont permis de rencontrer un nombre importants d'acteurs des organisations étudiées et de nous livrer à une séries d'entretiens avec certains d'entre eux afin d'approfondir des constats et observations réalisés. Nous ajouterons, dans la lignée de Giddens (1979), qu'un nombre de cas restreint, limité à deux cas d'étude, peut suffire dès lors qu'une analyse se centre sur la sélection et l'étude des cas par paire, en vue de lister leurs différences et similarités. Des groupes de trois à quatre cas maximum peuvent cependant être utilisés pour des comparaisons fiables et suffisamment approfondies (Eisenhardt, Bourgeois, 1988, p.77).

2.4.2. Les entreprises étudiées, données primaires

- **Cas C1 - Société d'assurance française, assureur généraliste**

Notre première étude de cas concerne une filiale française de société d'assurance présente en France depuis la révolution industrielle. Elle s'est développée durant la seconde moitié du XXème siècle et a fait l'objet de plusieurs rapprochements et fusions avec des entreprises concurrentes. Cette structure, qui compte plus de 10 000 collaborateurs en France (et plusieurs milliers à l'étranger) a atteint une taille critique, compte plus de cinq millions de clients et distribue des produits d'assurance de biens et de responsabilités mais aussi des produits d'assurance de personnes (assurance vie, santé, épargne, retraite, prévoyance). Son positionnement de « généraliste » se traduit aussi par la distribution de services bancaires simples (compte courant, livrets d'épargne réglementés).

Les activités de l'assureur sont les suivantes : assurances automobile, habitation, risques d'entreprises (TPE, PME, Artisans, grandes entreprises) et des collectivités pour les garanties de dommages aux biens et de responsabilités civiles et professionnelles. Cela représente un tiers de son activité. L'assureur a également une activité de gestion et de distribution des

contrats d'assurance vie (fonds euros et unités de comptes), de placements de produits d'épargne, d'assurance prévoyance et santé, obsèques, invalidité (assurances individuelles et collectives). Cela représente les deux tiers restant de son activité. Ces différents produits sont distribués par le réseau d'agences de l'assureur (plus de 1000 agences) ainsi que par des réseaux de courtiers partenaires (plus de 2500).
La stratégie de l'assureur est clairement orientée vers la constitution de partenariats et d'alliances stratégiques ainsi que sur la recherche de relais de croissance en France mais aussi à l'étranger.
Son chiffre d'affaires annuel dépasse les 10 milliards d'euros, pour un résultat net de moins d'un milliard d'euros en 2013.
L'assureur C1 est soumis aux règles européennes sur la solvabilité et le contrôle des risques des sociétés d'assurance (notamment le cadre prudentiel de la directive Solvabilité II).
Son organisation est centralisée : une décomposition en un groupement d'intérêt économique détenue par une holding et une structuration en deux filiales (assurance vie et assurance non-vie suivant le principe de spécialisation en vigueur en France qui sépare ces deux activités).
Son organisation est la suivante :
-une filiale d'assurance vie (dont santé-prévoyance),
-une filiale d'assurance non-vie (dont assurances de biens et de responsabilités),
-une filiale de services d'assistance (aux particuliers et aux entreprises),
-une filiale de gestion d'actifs (gestion des actifs et des passifs, activité de placements pour compte propre et compte de tiers),
-une filiale dédiée aux risques des grandes entreprises (dont couverture des risques industriels et des grands risques : aviation, flottes de véhicules, flottes de bateaux, ouvrages d'art, etc.),
-une filiale centrée sur la couverture des risques de crédit aux entreprises et aux particuliers (credit risk, affacturage et recouvrement de créances commerciales, etc.)
-une filiale de gestion de patrimoine immobilier (investissement et valorisation de patrimoine immobilier, promotion immobilière, etc.).

Parallèlement à cette organisation en filiale, l'assureur C1 dispose d'une structure avec des entités fonctionnelles communes à chaque filiale :
-une fonction distribution centralisée entre ses différentes filiales en vue de réaliser des économies d'échelle en matière de distribution de produits et services,
-une direction marketing et développement de l'activité commune aux différentes filiales,
-une direction financière et administrative centralisée,

-une direction logistique et une fonction ressources humaines toutes deux centralisées au niveau de l'entité de rattachement des deux principales filiales (assurance vie et non-vie),
-une direction opérationnelle centrale (comprenant des sous-directions dans chacune des filiales de la société d'assurance),
-une direction du contrôle et une fonction gestion des risques centralisée au sein de l'assureur mais comprenant des départements et sous-directions dans chacune des filiales.

L'assureur C1 a développé en 2007-2008 les prémices d'un dispositif de contrôle interne et s'est dotée d'une politique de maîtrise des risques en 2009 dont la mise en œuvre était envisagée à l'horizon 2010-2011 en vue d'anticiper le cadre réglementaire européen Solvabilité II.
Cette politique de maîtrise des risques avait pour but :
-de développer des contrôles en interne sur les différentes activités de l'organisation,
-de se doter de pratiques d'identification et d'évaluation des risques harmonisées au sein des différentes filiales et des fonctions centrales,
-de mettre en œuvre des outils efficaces de mesure du risque (cartographie des risques, collectes des pertes) et traitement-suivi par catégories de risques (risques couverts par des solutions financières dont risques assurables, risques faisant l'objet de mesure de protection-prévention, risques opérationnels ciblés par le contrôle interne).

Notre étude de cas au sein de cette structure se résume ainsi : nous étions rattachés aux fonctions centrales au sein de la direction en charge du contrôle interne, et ce pour la mise en place de la politique de maîtrise du risque opérationnel ainsi que la déclinaison pratique de cette dernière au travers de contrôles internes.

La recherche-action au sein de cette structure s'est donc faite sur le poste de contrôleur interne des risques, sur une période d'un an à temps plein courant 2010.
Notre périmètre de contrôle interne des risques concernait différents produits sur les segments des particuliers (ensemble des risques des particuliers : risque automobile, habitation, garanties complémentaires souscrites par les assurés, assistance, etc.) et sur les risques entreprises (PME, risques divers en entreprise, risques des artisans et professionnels). Ces missions de contrôle des risques opérationnels par produits et par processus ont occupé 80% de notre temps à raison de 35 heures par semaine durant une année (soit environ 1300 heures sur ce sujet).

La mission connexe à ces contrôles concernant la conception et la mise en place pratique d'un dispositif de maîtrise du risque opérationnel, soit 20% du temps de présence en entreprise (soit environ 250 heures dédiées à cette implémentation sur notre périmètre).

La recherche-action sur ce poste a été l'occasion de réaliser un ensemble d'entretiens dont la liste est fournie dans les tableaux ci-après. Le détail de nos constats et entretiens au sein de l'assureur C1 est évoqué dans le chapitre relatif aux résultats de recherche.

Ces 22 entretiens avaient vocation à confirmer/infirmer nos observations participantes.

Tableau 17. Liste des entretiens spécialistes « risques et contrôle » réalisés au sein de l'assureur C1

Entretiens	**Code entretien**	**Renseignements personnels**	**Durée de l'entretien**	**Date de réalisation**
Directeur du contrôle	C1-1	56 ans, Femme, expérimentée	30 minutes	Janvier 2010
Responsable du contrôle interne	C1-2	55 ans, Homme, senior	30 minutes	Janvier 2010
Contrôleur interne	C1-3	58 ans, Homme, senior	30 minutes	Février 2010
Contrôleur interne	C1-4	54 ans, Homme, senior	30 minutes	Février 2010
Contrôleur interne	C1-5	42 ans, Homme, confirmé	25 minutes	Février 2010
Contrôleur interne	C1-6	43 ans, Femme, expérimentée	25 minutes	Février 2010
Contrôleur interne	C1-7	55 ans, Homme, senior	30 minutes	Février 2010

Tableau 18. Liste des entretiens « opérationnels et managers » réalisés au sein de l'assureur C1

Entretiens	**Code entretien**	**Renseignements personnels et expérience dans le poste**	**Durée de l'entretien**	**Date de réalisation**
Directeur de l'organisation	C1-8	46 ans, Homme, senior	30 minutes	Mars 2010
Directeur des ressources humaines	C1-9	47 ans, Homme, confirmé	30 minutes	Février 2010
Directeur commercial	C1-10	52 ans, Homme, senior	40 minutes	Mars 2010
Directeur commercial	C1-11	49 ans, Homme, senior	30 minutes	Mars 2010
Responsable commercial	C1-12	43 ans, Femme, confirmée	25 minutes	Mars 2010
Intermédiaire d'assurance (agent général)	C1-13	35 ans, Homme, confirmé	30 minutes	Mars 2010
Intermédiaire d'assurance (agent général)	C1-14	56 ans, Homme, senior	45 minutes	Mars 2010
Intermédiaire d'assurance (courtier)	C1-15	45 ans, Femme, confirmée	30 minutes	Avril 2010
Intermédiaire d'assurance (courtier)	C1-16	27 ans, Homme, novice	30 minutes	Avril 2010

Intermédiaire d'assurance (courtier)	C1-17	50 ans, Homme, senior	30 minutes	Avril 2010
Intermédiaire d'assurance (courtier)	C1-18	35 ans, Femme, confirmée	25 minutes	Avril 2010
Gestionnaire de contrat	C1-19	53 ans, Femme, confirmée	30 minutes	Avril 2010
Gestionnaire de contrat	C1-20	55 ans, Femme, Senior	30 minutes	Avril 2010
Gestionnaire de contrat	C1-21	23 ans, Femme, novice	40 minutes	Avril 2010
Gestionnaire de contrat	C1-22	22 ans, Femme, novice	30 minutes	Avril 2010

- **Cas C2 - Banque de détail française**

Notre deuxième étude de cas concerne un établissement bancaire (banque de détail) présent uniquement en France, et ce depuis le XIXème siècle sous une forme organisationnelle différente du statut d'établissement bancaire. Dotée depuis plusieurs années d'un statut de banque à part entière, la banque C2 est soumise aux contraintes réglementaires de Bâle II (et de la réforme à venir Bâle III). La banque C2, qui compte plus de 10 millions de clients sur ses différentes activités, comprend plus de 5000 points de vente pour plus de 30 000 collaborateurs et réalise un chiffre d'affaires annuel supérieur à 5 milliards d'euros pour un résultat net de plus de 500 millions d'euros en 2013.

La banque C2 a mis en place une stratégie dite « multimétiers » visant à être présente sur l'ensemble du territoire français au travers de différentes activités que sont :

-une activité de banque de détail dont les principaux services financiers distribués sont les moyens de paiement (cartes de crédits, chèques, virements, mandats, banque en ligne, etc.), les livrets réglementés (livret A, livret de développement durable, plan épargne logement), les produits financiers grands publics (assurance vie, fonds communs de placement, SICAV monétaire et financière), le crédit aux entreprises, aux collectivités et aux particuliers (crédit à la consommation, crédit immobilier, crédit structuré).

-une activité d'assurance de biens et de responsabilité grâce à une filiale dédiée (couvrant les risques des entreprises et des particuliers sur de l'assurance automobile, habitation, protection juridique, accident de la vie, etc.),

-une activité d'assurance de personnes (dont assurance santé et prévoyance) également grâce à une filiale dédiée,

-une activité de placements pour les investisseurs particuliers et professionnels via des filiales dédiées en capital-investissement, en gestion privée ainsi qu'en gestion d'actifs,

-une activité de promotion immobilière et de financement du secteur du logement et du bâtiment via une filiale dédiée,
-une activité de courtier en ligne et d'intermédiaire de placement pour le compte de ses clients particuliers et professionnels.

L'organisation de la banque C2 se structure autour d'une maison mère assurant la gouvernance des différentes filiales et des nombreux centres de gestion et d'opérations financières répartis dans les principales régions françaises. Cette maison-mère est rattachée en tant que filiale à un groupe d'entreprises dont l'approche multimétiers situe les services financiers comme un socle essentiel de la stratégie du groupe.

L'organisation comprend donc outre cette maison-mère et les nombreuses filiales :
-une direction des opérations segmentées par région et dont la gouvernance est centralisée,
-des fonctions supports centralisées (direction des risques, direction du contrôle interne, direction de l'organisation, direction du marketing, direction financière, direction des ressources humaines, etc.).
La politique de maîtrise des risques et de contrôle interne de la banque C2 se structure autour de différents axes :
-la maîtrise des risques par principales catégories (risques de marché, risques de crédit et risques opérationnels), en dotant la fonction dédiée au Risk Management d'outils d'identification, de collecte et mesure du risque et d'acteurs en charge du suivi des actions de réduction-évitement du risque,
-une organisation de la maîtrise des risques centralisée au niveau de la maison-mère et comprenant différents relais dans chaque filiale et chaque direction et fonction de l'organisation,
-un dispositif de contrôle interne à plusieurs niveaux (contrôle périodique, contrôle permanent) et complété par les fonctions en charge de l'audit interne et de l'inspection générale.

L'étude au sein de la banque C2 a été réalisée de la manière suivante : notre rattachement était celui de Risk Manager-Analyste risques. Nous étions en charge de la mise à jour et de la diffusion des méthodologies d'analyse de risque (identification, évaluation, traitement et suivi), ce auprès des acteurs opérationnels de la banque et des collaborateurs en charge du contrôle interne. Cette activité a été menée sur une période de six mois à temps plein en 2011.

Notre périmètre comprenait également l'étude des risques sur le pôle métier « moyens de paiement » : comptes courants, monétique (cartes bancaires), virements et prélèvements, banque en ligne, chèques, mandats et titres optiques.

Ces missions d'analyse des risques opérationnels par produits et par processus ont occupé 50% de notre temps à raison de 39 heures par semaine durant six mois (soit environ 450 heures sur ce sujet). Les 50% restant concernant l'activité d'animation de filière sur les enjeux méthodologiques et de sensibilisation aux objectifs de la politique de maîtrise des risques opérationnels (450 heures également).

La recherche-action au sein de la banque C2 a également été l'occasion de mener des entretiens dont la liste est fournie dans les deux tableaux ci-après. Le détail des constats figure dans le chapitre relatif aux résultats de recherche.

Au total, une vingtaine d'entretiens ont été mobilisés dans le cadre de cette recherche-action pour appuyer et confirmer/infirmer nos observations participantes.

Tableau 19. Liste des entretiens « Risk Management-Contrôle interne » au sein de la banque C2

Entretiens	**Code entretien**	**Renseignements personnels**	**Durée de l'entretien**	**Date de réalisation**
Directeur des risques opérationnels	C2-1	45 ans, Femme, expérimentée	40 minutes	Août 2011
Risk Manager	C2-2	35 ans, Homme, confirmé	30 minutes	Août 2011
Risk Manager	C2-3	36 ans, Femme, confirmée	45 minutes	Août 2011
Responsable risque informatique	C2-4	56 ans, Femme, expérimentée	40 minutes	Août 2011
Responsable Sécurité - PCA	C2-5	55 ans, Homme, expérimenté	30 minutes	Août 2011
Risk Manager	C2-6	40 ans, Homme, expérimenté	1 heure	Septembre 2011
Risk Manager	C2-7	42 ans, Homme, expérimenté	1 heure	Septembre 2011
Directeur du contrôle interne	C2-8	50 ans, Homme, expérimenté	1 heure	Septembre 2011
Contrôleur interne	C2-9	30 ans, Femme, confirmée	45 minutes	Octobre 2011
Contrôleur interne	C2-10	53 ans, Homme, expérimenté	45 minutes	Octobre 2011

Tableau 20. Liste des entretiens « opérationnels et managers » au sein de la banque C2

Entretiens	**Code entretien**	**Renseignements personnels**	**Durée de l'entretien**	**Date de réalisation**
Directeur de l'organisation	C2-11	54 ans, Homme, expérimenté	1 heure	Septembre 2011
Manager moyens de paiement	C2-12	40 ans, Homme, expérimenté	40 minutes	Octobre 2011
Manager moyen de paiement	C2-13	52 ans, Femme, expérimentée	40 minutes	Octobre 2011
Manager distribution	C2-14	56 ans, Femme, expérimentée	30 minutes	Octobre 2012
Conseiller financier	C2-15	26 ans, Femme, novice	30 minutes	Novembre 2012
Conseiller financier	C2-16	28 ans, Homme, novice	30 minutes	Novembre 2012
Conseiller financier	C2-17	25 ans, Homme, novice	30 minutes	Novembre 2012
Conseiller financier	C2-18	32 ans, Femme, confirmée	40 minutes	Novembre 2012
Manager centre financier	C2-19	50 ans, Homme, expérimenté	1 heure	Novembre 2012
Manager centre financier	C2-20	52 ans, Homme, expérimenté	1 heure	Novembre 2012

Outre ces entretiens, le déroulement de nos études de cas peut être résumé selon plusieurs étapes allant du lancement de l'étude de cas à sa formalisation comme élément de recherche en lien avec notre revue de littérature, ce en passant par les étapes de sélection des instruments et données de recherche, de leur analyse en vue de la révision des hypothèses (voir le tableau ci-après).

Tableau 21. Déroulement des études de cas, adaptation d'après Eisenhardt, in Huber,Van de Ven (1995)

Etapes	**Activités**	**Raisons**	**Cas 1 (C1)**	**Cas 2 (C2)**
Lancement	Définition des questions de recherche et intégration dans les cas	Centrer la recherche sur l'objet d'étude	Choix de l'objet d'étude: la mise en œuvre des politiques de maîtrise des risques opérationnels.	
Sélection des cas	Choix d'une population spécifique	Flexibilité théorique / Contraintes sur l'évaluation des données et leur validité externe	Nécessité de mobiliser des éléments de terrain en assurance (Operational risk management	Nécessité de mobiliser des éléments de terrains en banque (politiques de maîtrise des risques opérationnels)
Choix des instruments et du protocole de recherche	Collecte de données multiples combinant quantitatif et qualitatif	Triangulation des cas, synergies inter-cas et complémentarité	Recherche-action critique-participative 1ère, 2ème personne	Recherche-action critique-participative 1ère, 2ème personne
Collecte des données	Recherche de saturation des données	Permettre une analyse aussi large que possible, incluant les différentes notes prises, permettre une analyse	-Collecte de données primaires : actions réalisées en tant que contrôleur et chargé de projet	-Collecte de données primaires : actions réalisées en tant que Risk Manager

		révélant les ajustements à réaliser, les thèmes émergents, etc.	risque opérationnel -données secondaires : entretiens et documents internes collectés	responsable méthode risque opérationnel -données secondaires : entretiens et documents internes collectés
Analyse des données	Analyse intra-cas, Analyse inter-cas	Familiarité avec les données, générer des données préliminaires Force le chercheur à aller au-delà de ses impressions initiales et voir les cas et exemples sous de multiples scopes	Familiarité forte avec les données : retours d'expérience. Proximité forte avec les acteurs interviewés. Comparaison intra-cas et inter-cas réalisées ex-post aux études.	
Formalisation, révision des hypothèses	Révision itérative des hypothèses grâce aux données, Réplication logique à travers les cas, Recherche de relation (validation/invalidation)	Construire la validité et la mesurabilité des données, Construire, étendre, formuler des théories, Construire la validité interne des données	Les deux cas d'étude en recherche-action nous ont amené à redéfinir les hypothèses en lien très étroits avec notre pratique. Nous avons émis un ensemble de recommandations et de constats sur les freins et leviers lors de la mise en œuvre des politiques de maîtrise du risque opérationnel remobilisés lors de la confrontation avec les entretiens confirmatoires.	
Rapprochement avec la littérature	Comparaison avec la littérature conflictuelle, Comparaison avec la littérature similaire	Construire la validité interne, Formuler des généralisations, améliorer les définitions	Nos deux cas d'étude se rapprochent de la littérature sur le contrôle interactif ainsi que sur certaines théories (théorie de la structuration et théorie de l'acteur-réseau). Le choix des grilles de lecture théorique s'est fait ex-post aux études de cas en vue de désigner celles se rapprochant fortement de nos constats de terrain et permettant une analyse cohérente et claire.	
Finalisation de la recherche	Saturation théorique	Finaliser le process quand les améliorations sont marginales ou peu importantes	22 entretiens et un an de recherche-action nous amènent à une saturation théorique sur le contrôle interne	20 entretiens et 6 mois d'étude de cas nous amènent à une saturation théorique sur la gestion des risques opérationnels.

2.4.3. Analyse de contenu et sources de documentation mobilisées, données secondaires

Ces études de cas en recherche-action ont été complétées par une analyse documentaire sur la base des rapports de contrôle interne et d'audit interne, de la documentation réglementaire, des notes internes, des communiqués et documents de référence « politique de risque » mis à disposition ou pour lesquels une contribution a été réalisée.

Tableau 22. Documentations collectées lors des études de cas (données secondaires)

Origine	Catégories	Provenance	Etude de cas 1- société d'assurance	Etude de cas 2- établissement bancaire
Interne à l'organisation	Organisationnelle	Compte rendu, contrats, produits, documentation de formation, journal interne	Ensemble de contrats par type de produits, descriptifs des processus et procédures internes, bases de collectes des données et risques, rapports de contrôle interne	Cartographie des risques, base de collecte des pertes, référentiels de risque, documentation internes moyens de paiement, fiches d'analyse de risque, rapports d'audit interne
	Personnelle	Notes en réunion, mémo, lettre préparatoire, réflexion personnelle		
Externe à l'organisation	Juridique, économique	Lois, règlements, décrets, procès	Réglementation prudentielle Solvabilité II	Réglementation prudentielle Bâle II
	Journalistique	Journal professionnel, interviews, discours des dirigeants, annonces	Notes et documentation de référence de l'autorité de régulation et des instances européennes (EIOPA)	Notes et documentation de référence de l'autorité de régulation et des instances européennes (Comité de Bâle)
	Administrative	Rapport officiel, suivis administratifs, contrôles et audits externes	Presse professionnelle assurance (Argus de l'Assurance, Tribune de l'Assurance)	Documentation Banque de France Presse professionnelle banque (Revue Banque)

2.5. La réalisation d'entretiens confirmatoires

Notre méthodologie est également basée sur un ensemble d'entretiens semi-directifs réalisés auprès de responsables risques opérationnels, contrôle interne, audit interne, mais aussi de managers opérationnels dans les secteurs banque et assurance (plusieurs entités dans chaque secteur).

2.5.1. Les entretiens semi-directifs, justification de données confirmatoires

Un entretien s'envisage comme une suite de références sociales par le discours, le recueil de *« traces de comportements »* et les interactions comme sources de perceptions des acteurs (Wacheux, 1996, p.204). Les entretiens semi-directifs se caractérisent par le fait que l'acteur s'exprime librement face au chercheur, mais ce face à des questions précises et sous le contrôle dudit chercheur. L'implication entre chercheur et acteur interviewé est partagée. Il se distingue en cela des entretiens directifs (l'acteur répond à une suite de questions courtes et précises sur des faits, options ou représentations), non-directifs (une conversation libre et ouverte sur des thèmes préalablement définis avec intervention potentielle du chercheur à des fins de recadrages sur l'objet de recherche) ou encore des entretiens de groupe (qui s'intéresse à la construction groupale d'explications et de représentations au travers d'échanges directs entre acteurs).

Le recours à des entretiens semi-directifs semblait approprié eu égard au caractère en partie exploratoire de la thématique (le risque opérationnel reste un sujet diffus, voire confus, dans les organismes du secteur financier, chaque spécialiste du sujet ayant une lecture qui lui est spécifique). Ces entretiens nous permettaient ainsi d'infirmer et de confirmer les différents constats réalisés lors de nos études de cas en recherche-action.
En outre, la thématique du risque opérationnel peut faire l'objet de non-dit lors d'entretiens trop directifs, notamment lorsqu'elle est rattachée à des enjeux politiques et d'image de l'établissement financier (exemple : capacité à enrayer les fraudes aux moyens de paiement, capacité à contrôler des activités à risque).

Notre recherche, dans un objectif descriptif, mais aussi explicatif, du phénomène de structuration des politiques de maîtrise du risque opérationnel, suppose d'étudier cet objet de recherche à la fois en situation et dans son contexte de survenance. La nécessaire empathie à ce type de démarche suppose de s'approprier le langage et la terminologie des acteurs dans le cadre de leur pratique (Girod-Séville, Perret, 2000). Plus encore que cette démarche, notre objectif de cohérence entre l'objet de recherche, notre problématique centrale et la stratégie d'accès au réel nous a guidé vers l'usage d'entretiens semi-directifs. Comprendre et interpréter le rôle des acteurs en charge du déploiement d'une politique de risque opérationnel implique une analyse en profondeur, tout en s'imprégnant du contexte et en comprenant la structuration (Bon-Michel, 2010). Le recours à cette méthodologie qualitative vise dans notre

étude de cas à dépasser la dimension quantitative (Lee, Humphrey, 2006) caractérisant les métiers associés au contrôle dans les établissements financiers pour la resituer sur notre objet d'étude relatif aux politiques dédiées au contrôle du risque opérationnel. Elle constitue un moyen approprié de mieux cerner un objet complexe et exploratoire (Cassell, Symon, 2006) comme cela est le cas dans notre étude.

Cette méthode de collecte s'inscrit dans une approche de type exploratoire-inductive. Nous partons des faits en vue de cerner cet objet complexe et d'en tirer des conclusions à vocation générale, lesquelles pourront être développées dans des recherches ultérieures et ce de manière incrémentale (Van de Ven, Johnson, 2006 ; Cappelletti, 2010). La dimension exploratoire de cette recherche suppose le recours à des entretiens semi-directifs de longue durée (1h30 environ) avec une grille d'entretien détaillée mais restant toutefois ouverte à des prises de positions et à un développement sur certaines thématiques semblant plus centrale aux acteurs interrogées. L'objectif des questions est d'amener les interviewés à se prononcer sur des thèmes récurrents en suivant un principe de généralisation analytique (Thiétart, 2003). Nous devons conséquemment écouter les acteurs rencontrés et les faire parler de leurs savoirs implicites afin d'établir des observations pertinentes et ainsi modifier en conséquence les concepts actuels (Bird, 2002). Seules les entrevues peuvent répondre à cette demande. Bien que certains observateurs aient démontré que les gestionnaires et contrôleurs des risques, managers, opérationnels ne s'expriment pas aisément sur de nombreux aspects implicites de leurs actions, nous croyons tout de même que l'entrevue force à l'écoute et permet de briser le silence (Bird, Waters, 1989). L'entrevue nous apparaît l'outil adéquat car elle se présente comme un instrument pertinent *« lorsque l'objectif est d'explorer le sens subjectif que les répondants attribuent aux concepts et aux événements »* (Gray, 2004, p. 217, traduction libre de l'auteur). Cet outil offre la possibilité de faire une diversion dans l'entrevue afin de couvrir de nouvelles voies d'enquête qui n'ont pas été considérées originellement par l'intervieweur (Gray, 2004). Pour ce faire, nous avons décidé d'adopter la technique des entretiens semi-structurés (Patton, 2002) afin de laisser place à l'exploration de certains éléments et affects vécus par les personnes questionnées (pour mieux les confronter ensuite entre eux et avec nos cas d'études).

Guide d'entretien

Synthèse des thématiques abordées en entretiens : (entretiens d'une heure à une heure trente)

-Parcours, positionnement et expérience de l'interviewé sur la thématique risque opérationnel
-Quelle compréhension des politiques de maîtrise des risques opérationnels (freins et leviers),
-Risques opérationnels : quelles confusions en pratique sur la notion et entre les différentes fonctions qui en traitent (retour d'expérience dans les contrôles réalisés), ces fonctions travaillent-elles principalement en silo ?
-Le risque opérationnel est-il pour vous un risque subi / diffus ?
-Le risque opérationnel reste-t-il le « parent pauvre » par rapport aux autres risques (très liés au cœur d'activité) ?
Quels sont les principaux freins et leviers lors de la mise en œuvre des politiques de risques opérationnels ?

Normes :
-Existe-t-il un besoin et manque de « guidelines », de bonnes pratiques quant aux normes de contrôle des risques opérationnels ?
-Quelles sont les difficultés d'interprétation du risque opérationnel dans la réglementation ? Marges de manœuvre ?
-Contrôle des risques opérationnels et rapport à la réglementation prudentielle, rapport régulateur-entité.

Sens des contrôles :
-Qu'est ce qu'un contrôle qui a du sens par rapport au risque opérationnel ?
-Qu'est ce qu'un contrôle interne cohérent face au risque?
-Créativité et design du contrôle ? Est-ce le vrai sujet pour cerner le risque opérationnel?

Responsabilisation des acteurs des filières risque opérationnel :
-Qu'est ce que la responsabilité face au risque ? Quand a-t-elle lieu ? Sur quoi peut-on jouer pour la rendre effective face au risque?
-Le risque opérationnel est-il un enjeu de contrôle budgétaire et de gestion des coûts ?
-Qu'est ce que la culture du risque opérationnel pour vous ?

Notre questionnaire a pour objectif de révéler les freins et leviers rencontrés par les acteurs interviewés en matière de contrôle des risques opérationnels. Nous souhaitions révéler dans leur perception et leur expérience respective ce qui faisait sens concernant ce type de contrôle spécifique et comment il percevait la norme dédiée au risque opérationnel et sa transposition effective. Comment y parvenir ? En guidant à la fois la conversation vers ce qui est soumis à l'étude (thèmes) tout en étant assez ouvert avec les répondants et qu'ils puissent s'exprimer librement. Avec les exigences de l'entrevue exposées par Kvale (1996), nous estimons que ce questionnaire a permis aux Risk Managers et aux contrôleurs de fournir des explications spontanées et pertinentes sur les sujets abordés. Les questions étaient courtes, mais elles ont sollicité la clarification du sens de certains aspects dans les réponses. Certaines questions pouvaient donner lieu à des demandes de précisions ou à une orientation vers un approfondissement de la thématique abordée.

2.5.2. Le panel des entretiens

50 entretiens concernant 55 personnes ont été réalisés au total (voir le tableau ci-après). Ces entretiens codés via un logiciel d'étude de contenu (NVivo) ont été traités et analysés en termes de discours en vue de voir les vrais sujets de préoccupation de ces responsables risques et contrôle. Il s'agissait également de mettre en lumière la dimension traduction des normes et l'enjeu de structuration des contrôles face au risque parfois tacites dans les retours d'expérience réalisés.

Tableau 23. Tableau synthétique des entretiens confirmatoires réalisés

Fonctions des personnes interviewées		
Entretiens centrés sur le risque opérationnel en assurance	Entretiens centrés sur le risque opérationnel en banque	Autres entretiens (croisement problématique de risque opérationnel dans le secteur financier)
-1 directeur des risques -2 directeurs du contrôle interne et contrôle permanent -1 directeur du pilotage et reporting - 2 contrôleurs internes -1 responsable référentiel risque opérationnel -1 directeur d'audit interne	-1 responsable veille et réglementation prudentielle -1 responsable cartographie risque opérationnel -1 directeur risque opérationnel -1 directeur contrôle interne -2 directeurs métiers (informatique, marketing) -5 Risk managers spécialisés par métiers	-7 consultants séniors et experts risques opérationnels -8 contrôleurs Autorité de Contrôle Prudentielle -2 directeurs sécurité financière et conformité -5 directeurs d'audit interne -6 directeurs du contrôle interne -8 directeurs des risques opérationnels et Risk Manager
Nombre et type d'entretien (55)		
8 entretiens en assurance	11 entretiens en banque	36 entretiens (banques, compagnies d'assurance et cabinets de conseil)

(*) L'annexe 8 détaille les fonctions précises des personnes interviewées.

Le détail des entretiens réalisés (profils, âge, sexe, structure de rattachement, date et durée de l'entretien) figure dans le tableau disponible à l'annexe 8. Au total 63 heures et demi d'entretiens confirmatoires ont été réalisées.

- **Le choix et le déroulement des entretiens**

Nos entretiens confirmatoires ont été réalisés à la fois en fonction des contacts obtenus au sein du secteur financier mais aussi dans une logique permettant de diversifier le nombre de structures étudiées (une dizaine d'établissements bancaires et une dizaine de sociétés d'assurance) afin d'avoir une vision représentative des pratiques sur le marché français de la banque et de l'assurance en matière de gestion du risque opérationnel.

Le déroulement des entretiens a suivi un processus usuel allant de l'explication du but de la recherche, de la présentation de la personne interviewée à une phase de debriefing et de description post-entretien du contexte de l'étude.

Tableau 24. Déroulement des entretiens, adaptation d'après Wacheux, 1996, p.208

Etape 1	**Etape 2**	**Etape 3**	**Etape 4**	**Etape 5**
Explication, interaction, échanges et rôles	Déroulement, 1er discours conventionnel	Déroulement, discours personnel	Terminaison, débriefing de l'acteur et derniers propos	Terminaison, 1ère analyse et description du contexte
Présentation de l'objectif de l'étude, du parcours de recherche suivi, présentation de la personne interviewée et de son expérience professionnelle.	La personne interviewée aborde les problématiques récurrentes affichées dans l'organisation relativement à l'objet d'étude « politique de risque opérationnel ».	La personne interviewée aborde ensuite en détail les éléments de réponse relatifs aux sujets les plus parlants pour elle-même et sur lesquels des exemples sont plus intelligibles (en fonction de son recul et de ses vécus). Le cas échéant, l'interviewé est guidé et orienté vers les concepts souhaités via des reformulations de questions.	La personne interviewée conclut sur les éléments les plus marquants pour elle en insistant sur les principales difficultés rencontrées sur l'objet d'étude « risque opérationnel, politique de maîtrise des risques ».	Nous présentons ensuite à l'interviewé les résultats émergents de notre étude et le contexte détaillé dans lequel s'insert notre recherche (suite à des recherche-action). La plupart des entretiens ont donné lieu à un débat contradictoire d'une quinzaine de minutes liant nos partages d'expériences respectifs.

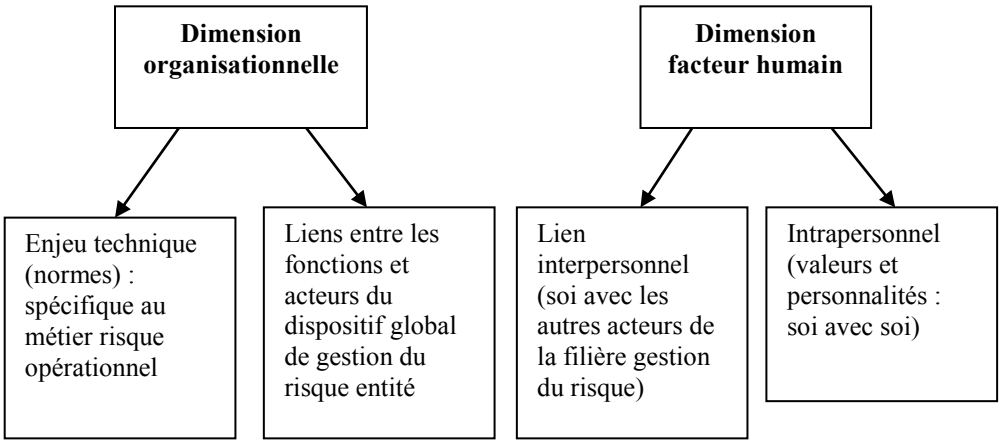
2.5.3. La grille d'analyse des entretiens

La grille d'analyse des entretiens utilisée et décrite ci-après suit un principe de généralisation analytique (Thiétart, 2003) ayant permis le codage des données. Les thématiques abordées sont décrites figure 30. L'interviewé est guidé à travers les questions afin de l'aider à articuler sa pensée autour de thèmes préétablis. Une telle grille de lecture a par ailleurs été mobilisée pour certaines recherches dans le domaine du contrôle (Ducrocq et al., 2012).

Cette grille d'entretien intègre les multiples dimensions qualitatives associées à la thématique du risque opérationnel et se structure ainsi : présentation de l'interviewé et de son parcours, perception de la notion de risque opérationnel et regard critique sur les normes et définition

utilisée, rôle par rapport au risque opérationnel et à sa gestion, comparaison avec les autres acteurs de la filière risque opérationnel (ainsi que le rôle du régulateur), perception de sa responsabilité quant au risque opérationnel ainsi que de la responsabilité d'autrui, vision du risque opérationnel en tant que priorité dans l'organisation (rapprochement avec la vision de l'interviewé, les visions d'autrui, les valeurs et la stratégie de l'entreprise). L'effectivité des politiques de risques opérationnels a aussi été envisagée lors de ces entretiens.

Figure 30. Grille d'analyse des axes techniques et humains en management du risque opérationnel



- **L'analyse et le traitement des données recueillies :**

L'ensemble des données, les entretiens retranscrits, les observations, les documents collectés ont été analysés via l'outil informatique de codage d'éléments qualitatifs NVivo (recherche, tri, analyse de contenu, visualisation). Nous avons effectué un codage des éléments relevés, en répertoriant les entretiens semi-directifs et les notes prises lors des phases de collecte de données durant les travaux en recherche-action. Nous avons réalisé un codage thématique, consistant à rattacher des verbatim liées aux quatre phases de la théorie de la structuration et la théorie de la traduction ainsi qu'aux normes prudentielles, référentiels de risque, méthodes et modèles utilisés. Nous avons par ailleurs effectué un codage analytique qui s'appuie sur une analyse explicative du contenu des entretiens et sur la réflexion sur le sens à attribuer aux données collectées. Par le recours à un logiciel d'analyse de contenu (NVivo), nous avons réalisé un double codage : à la fois thématique (en vue d'extraire des thèmes récurrents de nos entretiens ainsi que des sous-thèmes) et un codage que nous qualifierons « d'axial » en vue d'envisager de manière transverse à chaque thème de recherche des axes privilégiés de réflexion (Lewins, Silver, 2007). Eu égard à l'importance du nombre d'entretiens réalisés, le

recours au logiciel d'analyse de contenu, bien que non indispensable, permettait un gain de temps dans le traitement des données. Toutefois, et comme l'évoquent certains auteurs (Bryman, Bell, 2011, p.618 et s.), un logiciel de contenu, aussi perfectionné soit-il, ne saurait se substituer au jugement du chercheur ayant réalisé la collecte des données. Nous envisageons donc l'analyse de contenu selon l'angle de l'analyse thématique, soit le fait d'examiner de manière attentive, détaillée et systématique, un corps particulier de données composées de thèmes récurrents entre chaque entretien mais aussi de biais et de faits et exemples porteurs de sens. Notre analyse est assortie d'une interprétation en lien avec la grille de lecture théorique que nous avons mobilisée. Nous rapprochons ainsi les données présentées dans le chapitre suivant (résultats de la recherche) en fonction du rapprochement avec nos grilles de lecture théorique et à des fins de structuration des données recueillies (Leedy, Ormrod, 2005). Les codes sont réalisés de manière inductives en se basant sur les données recueillies, dans une logique allant de la collecte de données au développement des codes pour analyser et identifier les récurrences dans les éléments retranscrits. Notre analyse thématique vise à décrire et dénommer, à situer et à catégoriser, dans une logique explicative de la réalité socialement préconstruite (Neuendorf, 2002). Nous avons cherché à identifier les similarités, les éléments communs et les disparités mais aussi les relations dans les propos tenus lors des entretiens. Notre analyse visait enfin à isoler les éléments porteurs de sens (identifier ce qui se distingue des recherches précédentes ou ce qui les confirme, ce qui peut être le fait de généralisations).

3. Résumé du protocole de recherche

Notre protocole de recherche étant décrit, nous pouvons synthétiser la démarche par étape que nous avons poursuivie durant cette recherche doctorale.

Le tableau ci-après explicite les différentes étapes de collectes de données mais aussi de rapprochement avec notre revue de littérature et enfin la phase d'analyse que nous avons réalisée.

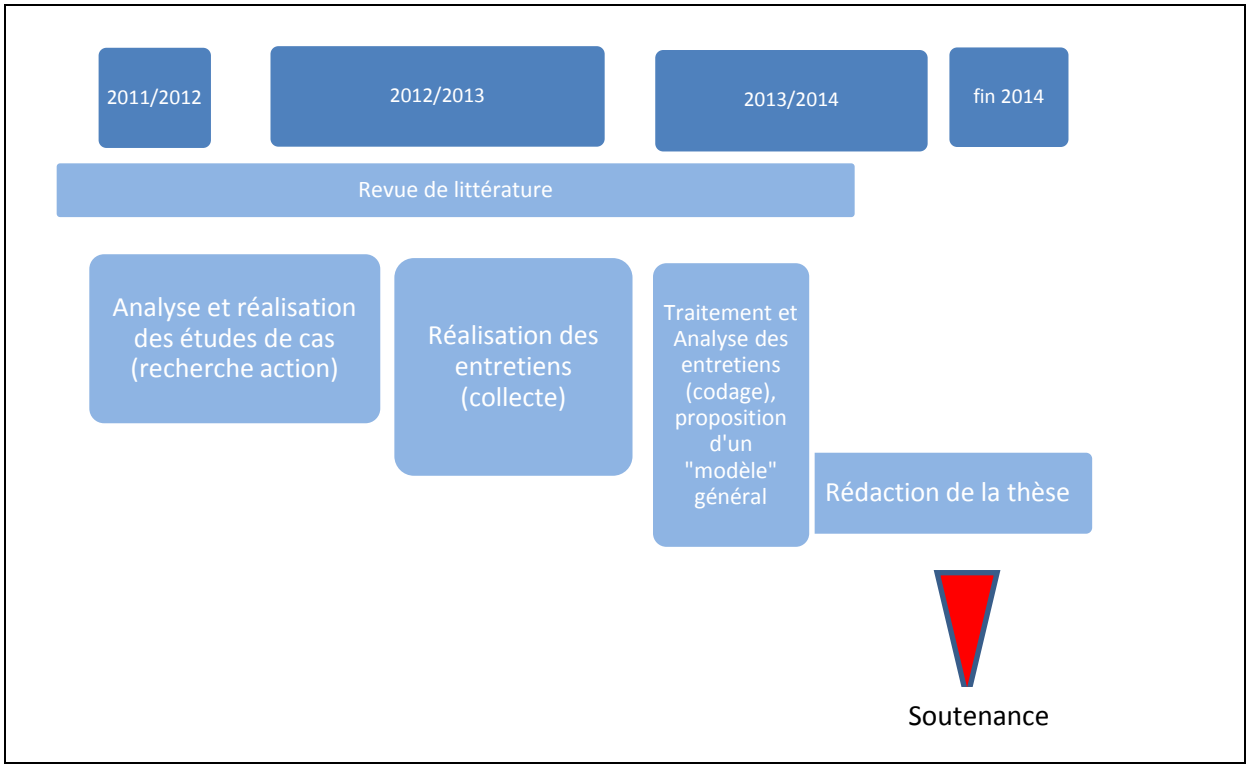
Tableau 25. Déroulement : dates clés de la recherche

Phases de la recherche	Périodes
Etude de cas n°1 (C1), société d'assurance, recherche-action, contrôle interne	**1 an, fin 2010 à 2011**
-Réalisation de contrôle par produits et ligne d'activité	5 mois
-Etude des résultats des contrôles et de leur dimension risque opérationnel	1 mois
-Définition et mise en œuvre d'un référentiel de risque opérationnel et d'une approche Operational Risk Management	1 mois
-« Toilettage » des contrôles au regard de cette approche risque opérationnel	1 mois
-Réalisation de contrôles repensés	2 mois
-Etude qualitative d'impact, quantification du rôle des contrôles (retour sur investissement /risque)	2 mois
Etude de cas n°2 (C2), établissement bancaire, recherche-action, Risk Management Opérationnel	**6 mois, fin 2011 à début 2012**
-Définition Politique de Maîtrise des risques opérationnels	1 mois
-Déploiement de la politique, filière risque opérationnel	5 mois
-Etudes risques opérationnels et formations	
Revue de littérature	Mi-2011 à fin 2013
-revue de la littérature sur le risque et le Risk Management, théorie des organisations, contrôle	1 an
-revue des grilles de lecture théorique	6 mois
-recherche littérature risque opérationnel	1 an
Analyse des études de cas et traitement des données	Début 2012 à mi-2012 6 mois
Réalisation des entretiens confirmatoires	Juillet 2012 à mai 2013 1 an
Analyse des résultats des entretiens	Mi 2013 à fin 2013 6 mois

Analyse inter-cas	Mi-2013 à fin 2013
Rédaction de la thèse, finalisation	Janvier 2014 à septembre 2014

Afin d'affiner ces éléments, il nous faut également préciser que la phase de revue de littérature s'est étendue durant toute la période de collecte de données. En fonction des constats issus de notre recherche de terrain, nous avons peu à peu précisé cette revue de littérature. La phase de « rédaction de la thèse proprement dite ayant quant à elle débuté à partir de janvier 2014.

Figure 32. Déroulement chronologique de la thèse



Conclusion du chapitre - Des méthodologies pragmatiques face à un objet de recherche émergent

Notre cadre méthodologique est issu des travaux menés en recherche-action (Reason, Bradbury, 2001 ; Baker, 2007) explicitant le processus de production-traitement de connaissance réalisé : établir des problématiques et un projet de recherche enracinés dans la pratique, selon un mode d'apprentissage collaboratif dans l'organisation et développé sur une longue durée (David, 2003 ; Van de Ven, Johnson, 2006). Avec la recherche-action, l'accès facilité aux données a permis de cerner la complexité de cette thématique de manière réflexive. La généralisation et la validité de la connaissance produite supposent ensuite une phase de distanciation et une phase d'échange avec les collaborateurs rencontrés (Savall, Zardet, 2004). La phase d'immersion au sein de la société d'assurance et de l'établissement bancaire a permis de réaliser de nombreux échanges avec les membres des directions où les études ont eu lieu. Nous avons ainsi récolté un nombre important d'informations traitées et analysées par la suite (distanciation). Les constats et analyses faites lors des échanges avec les collaborateurs (selon le principe épistémologique dit d' « interactivité cognitive ») ont été soumis ex-post à ces derniers pour avis (selon le principe dit d' « intersubjectivité contradictoire »). La phase d'échanges contradictoires via des entretiens ainsi qu'une analyse des résultats au regard de la littérature vise à repérer des premières généralisations analytiques (selon le principe dit de « contingence générique »).

Le recours à la recherche-action constitue en soi un apport spécifique eu égard à notre objet de recherche. Cette méthodologie d'étude exploratoire (complétée par des entretiens) est encore peu mobilisée dans le secteur des services financiers, lequel se prête davantage aux études quantitatives qu'aux enquêtes de terrains. Les études réalisées dans ce secteur visent en effet davantage à analyser des activités précises qu'à expliciter une réalité préconstruite en se basant sur une double étude interne (recherche-action) / externe (entretiens confirmatoires).

Nos résultats de recherche, présentés dans le chapitre suivant, visent ainsi à apporter une compréhension du phénomène en cours de développement que sont la formalisation de politiques de risque dédiées à la maîtrise du risque opérationnel.

Conclusion de la partie théorique – Emergence de l'enjeu risque opérationnel et positionnement théorique enraciné

Notre partie théorique présente donc à la fois le cadre de pensée dans lequel s'inscrit cette recherche doctorale ainsi que l'approche méthodologique retenue. Ces deux éléments de notre étude sont liés. Nous avons en effet eu recours à des théories et à une méthodologie de recherche d'inspiration « sociologique ». Les théories de la structuration et de l'acteur-réseau, l'approche socio-économique sont des théories mobilisées en sciences de gestion, plus particulièrement en sociologie des organisations. Toutefois, leur recours dans des domaines tels que le contrôle des organisations et plus spécifiquement concernant la gestion des risques, bien qu'émergent, semble pertinent car il est bien question de comprendre une réalité sociale encore relativement méconnue et peu formalisée académiquement.

La méthodologie de type recherche-action et le recours aux entretiens semi-structurés sont des pratiques usuelles en sociologie. L'étude des pratiques dans le secteur financier via ce protocole de recherche semble ainsi pertinent car permettant, en lien avec nos cadres théoriques, de recueillir des données et de formaliser des constats sous une autre forme que l'analyse quantitative. L'approche quantitative, bien qu'ayant fait ses preuves, implique également des compléments, lesquels peuvent consister dans le recours à une diversité d'outils méthodologiques de nature qualitative, a fortiori en l'absence de données quantitatives suffisamment fiables ou disponibles comme cela peut être le cas pour le risque opérationnel.

Les deux chapitres structurant cette partie théorique sont donc, en cohérence, caractérisés par une transdisciplinarité incontournable en sciences de gestion, à fortiori pour un objet de recherche aussi transverse que les politiques de maîtrise des risques opérationnels.

Partie III- Cadre empirique et discussion des résultats : De la norme de contrôle à son effectivité, traduction de la norme et structuration du contrôle

Introduction de la partie III – Vers une approche interactionniste du contrôle des risques

Cette troisième et dernière partie de notre thèse présente les principaux résultats de recherche issus de la collecte et du traitement des données recueillies en recherche-action lors des études documentaires et des entretiens confirmatoires réalisés.

Un premier chapitre présente les résultats des études de cas, études documentaires et entretiens confirmatoires envisagés à la lumière de nos principales grilles de lecture théorique. Une analyse est ensuite réalisée en vue de tirer des enseignements à vocation plus générique (ainsi qu'en vue d'extraire les principaux facteurs de contingences liés à nos données et à notre méthodologie de recherche).

Ces principaux constats étant présentés, nous réalisons dans un second chapitre un rapprochement avec la littérature académique en gestion des risques et en matière de risques opérationnels. Ce rapprochement nous permet d'aborder les principales perspectives théoriques issues de nos études de terrain ainsi que les recommandations managériales caractérisant notre recherche.

Nous abordons également dans cette dernière partie les principales limites de notre recherche. Il s'agit à la fois de limites intrinsèques aux données collectées mais aussi des limites méthodologiques liées à l'exercice contraint dans le temps d'une recherche doctorale.

Enfin, nous précisons les perspectives de recherches futures issues de ce travail de thèse, étant considéré comme un point de départ au regard de la nécessité de généraliser nos constats (voire de les contredire) dans des contextes empiriques différents (autres types d'établissements financiers telles que les mutuelles d'assurance ou courtiers ; autres secteurs d'activités que le secteur des services financiers ; autres contextes tels que les contextes de survenance de risques opérationnels en gestion de crise etc.) ou via des grilles de lecture distinctes (théorie de l'erreur humaine, théorie institutionnelle etc.).

Chapitre 5 - Résultats de la recherche - L'effectivité du contrôle des risques sous le prisme des approches organisationnelles

« Il faut constamment réaffirmer la mission du contrôle systémique face à des évènements qui menacent sa crédibilité »

Michael Power

Introduction

Le présent chapitre expose les principaux résultats de notre étude empirique relative au déploiement des politiques de maîtrise des risques opérationnels, d'inspiration normative, au sein du secteur financier français.

Nous avons eu recours à deux études de cas réalisées au sein d'une filiale française de société d'assurance ainsi que d'une banque de détail française. Outre ces études de cas de longue durée (plus de 6 mois dans chaque cas), nous avons également réalisé un ensemble d'entretiens à visée confirmatoire auprès de directeurs des risques, responsables d'audit interne, directeurs du contrôle interne, Risk Manager, consultants et experts des risques opérationnels (plus de soixante heures d'entretiens confirmatoires).

Les principaux résultats des documents et actions menées propres à chacune des études de cas, ainsi que les entretiens confirmatoires, sont formalisés dans la première partie de ce chapitre. Une seconde partie présente les résultats des entretiens réalisés en complément de ces cas (et analysés via nos grilles de lecture théoriques).

A noter que ce chapitre présente également le lien avec les grilles de lecture théoriques retenues précédemment, qui permettent de structurer les résultats des données collectées.
Pour les différents entretiens réalisés, nous avons choisi de formaliser les principaux constats étayant notre recherche par le biais de verbatim clés. Il s'agit des phrases extraites des entretiens étant les plus représentatives des problématiques relatives aux politiques de maîtrise des risques opérationnels et permettant de répondre à notre question de recherche (Comment la structuration du contrôle permet-elle de passer d'une simple recherche de conformité aux normes à une gestion effective du risque opérationnel ?).

I-Les résultats issus des études de cas

Cette première partie présente les principaux résultats issus des deux études de cas réalisées en recherche-action.

1. Recherche-action : Phases du processus de gestion des risques opérationnels.

Nous exposons ci-après en premier lieu la logique de recherche-action sous-jacente à nos deux études de cas.

Leur déroulement, reprenant les méthodologies usuelles en recherche-action telles que décrites dans notre chapitre méthodologique, est fondé sur différentes étapes :

-la description de chaque activité, des processus, des actifs et personnels concernés, le recensement des différentes étapes par processus. Cette première phase était propre à clarifier les enjeux de chaque activité et à permettre aux opérationnels et managers de s'intégrer progressivement dans la démarche de gestion des risques par la description de leur activité.

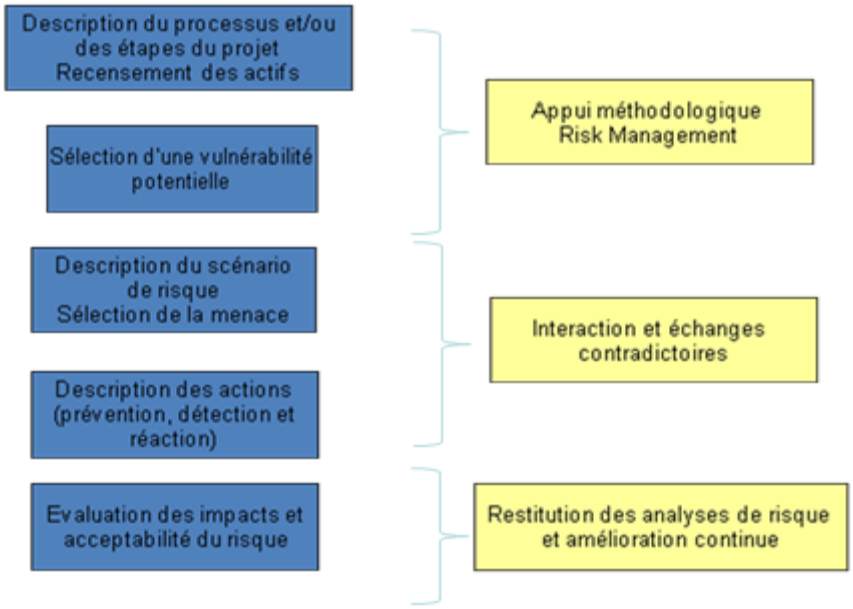
-pour chaque étape des activités des managers et opérationnels, une seconde phase de détermination des vulnérabilités internes pour l'entreprise ainsi que des menaces externes à celle-ci. Cette phase d'identification du risque opérationnel s'est faite avec l'appui des contrôleurs et acteurs des fonctions opérationnels et supports (appui méthodologique sur les objectifs poursuivis, la sémantique risque, les référentiels utilisés et les manières d'identifier le risque opérationnel dans leur activité spécifique).

-une phase d'accompagnement dans la rédaction de la politique de gestion des risques opérationnels a ensuite marqué l'aboutissement et la concrétisation de l'analyse de risque faite par les managers et opérationnels. Cette approche visait à construire progressivement une base de données d'exemples de risques opérationnels dans chaque activité. Ces exemples permettent ainsi d'objectiver le sujet risque opérationnel, le rendant concret, matérialisant ainsi progressivement la culture du risque, que celle-ci soit ou non préexistante et intégrée dans l'activité de contrôle interne.

-la dernière phase est une phase d'échange sur les impacts de ces risques, leur acceptabilité et les mesures à mettre en œuvre pour prévenir ces derniers (mesures de prévention) et les contrôler (dispositif de maîtrise des risques). Cette phase intègre un dispositif de suivi régulier par ces opérationnels et managers en vue de voir si les dispositifs mis en place ont été

efficaces, si les risques résiduels[53] sont maîtrisés et si les méthodologies et l'analyse-traitement des risques restent effectives : répondant aux objectifs fixés en matière de maîtrise des risques et faisant l'objet de mises à jour régulières.

Figure 33. Descriptif de l'accompagnement méthodologique mis en œuvre dans les cas d'études



La mise en œuvre de ces recherche-action nous permet de réaliser les constats suivant quant à l'effectivité des dispositifs de contrôle des risques opérationnels issus de la réglementation prudentielle. Si ladite démarche de gestion des risques suit comme objectif la diffusion d'une culture du risque, nous constatons en pratique des difficultés à la fois propres à la notion même de risque opérationnel, mais également à l'organisation des différents types et niveaux de contrôles existants dans les deux cas étudiés.

2. Les cas de risques opérationnels : la nécessité de politiques dédiées

Nos échanges avec différents collaborateurs des deux entités étudiées (l'assureur C1 et l'établissement bancaire C2) nous ont permis de prendre la mesure, au-delà des dispositions réglementaires, de l'extrême diversité des cas de risques opérationnels pouvant affecter un établissement financier.

[53] Risques résiduels : parfois aussi qualifiés de risques nets, par opposition aux risques bruts, il s'agit de l'impact du risque après application des dispositifs de maîtrise des risques (moyens de protection, de prévention, contrôle, transfert de risques tels que les polices d'assurance).

Ces cas de risques opérationnels peuvent ainsi aller, à titre illustratif, du cas de figure où un assureur se retrouve seul à assurer les dommages potentiels d'un barrage, car les commerciaux et actuaires ayant travaillé sur ce dossier n'avaient pas pris en charge le programme de réassurance et de coassurance[54] d'un tel dossier. En cas de sinistre, l'assureur avait donc clairement sous-estimé ses engagements.

Autre-exemple, lors de nos échanges avec des collaborateurs d'établissements bancaires, il nous a été remonté un cas de survenance de risque opérationnel atypique. Dans ce cas précis, un employé de la direction des systèmes d'information a fait tombé un porte-manteau sur des câbles d'alimentation, coupant ainsi l'alimentation des serveurs informatiques sur un site sensible de l'établissement. Une telle inattention engendra une interruption des serveurs pendant plusieurs heures. Couplée à un dysfonctionnement du serveur de secours, cela engendra un arrêt d'activité de ce site sensible et donc un manque à gagner sur une période d'activité d'une journée.

Autre évènement de risque opérationnel : le fait pour un juriste d'agrafer à un contrat de réassurance la mauvaise annexe. L'assureur, une fois le contrat signé et en l'absence de contrôle, se retrouva alors engagé sur la couverture d'un risque à hauteur de 50 millions d'euros de plus qu'initialement prévu du fait de cet erreur de traitement d'un dossier.

Nous pourrons également citer les cas de fraudes à l'assurance (plus de 130 millions d'euros par an en assurance santé selon les associations de consommateurs) et plus de 4 milliards d'euros en assurance de biens selon les fédérations de sociétés d'assurance. Les fraudes aux moyens de paiement, l'interruption des SI, les risques opérationnels majeurs (flash crash, rogue trading), les risques opérationnels à fort impact image (risques RH, corruption, fraude fiscale, amendes pour non respect de la réglementation) constituent également des cas significatifs pour les établissements financiers.

Ces quelques exemples illustrent la diversité et le caractère insidieux du risque opérationnel qui, bien que n'étant pas nécessairement une priorité au regard d'autres risques (financiers, assurantiels, de crédits), constitue une catégorie potentiellement coûteuse pour les établissements financiers.

Ces différents cas illustrent la nécessité de politiques dédiées aux risques opérationnels. Le déploiement de telles politiques est traité au travers des deux cas d'études ci-après.

[54] La coassurance consiste en la couverture d'un même risque par plusieurs assureurs (avec un assureur principal couvrant le risque). La réassurance consiste pour un assureur à faire appelle à une société de réassurance pour transférer la couverture d'une part des risques pris en charge par ce dernier.

3. L'étude de cas C1-Société d'assurance

Notre première étude de cas au sein d'une société d'assurance a duré sur une période d'un an et se structure en différentes phases. Une première étape a consisté à dresser un diagnostic de la situation initiale de la **société C1** (définition du risque opérationnel, formalisation des principaux cas de survenance de risques opérationnels). La seconde étape de cette étude de cas visait la formulation des problématiques essentielles de la société C1 face au risque opérationnel (définir une politique de maîtrise des risques opérationnels adaptée au métier d'assureur généraliste, répondant aux exigences réglementaires, fixant des limites d'acceptation de ce risque et intégrant la diversité des acteurs concernés : répartition des rôles et responsabilités). La troisième étape de l'étude de cas impliquait la mise en œuvre d'actions expérimentales répondant aux problématiques identifiées (outils, méthodes mobilisées, désignations des acteurs et mise en œuvre opérationnelle de la politique de maîtrise des risques). La dernière étape consistait en l'élaboration des conclusions de l'étude (principaux retours d'expérience en termes de freins et leviers, bonnes pratiques à pérenniser, erreur à éviter).

3.1. Le diagnostic de la situation initiale : la notion de risque opérationnel chez un assureur généraliste

Lors de notre étude de cas au poste de contrôleur interne, la première problématique consistait à définir clairement la notion de risque opérationnel et son contour.

La définition réglementaire retenue par l'EIOPA[55] a dans un premier temps été retenue *(« le risque de pertes résultant d'une inadéquation ou d'une défaillance attribuable à des procédures, personnels, systèmes internes ou à des événements extérieurs »).* Celle-ci appelait d'emblée une précision : *« le risque opérationnel, ainsi défini, inclut le risque juridique, mais exclut les risques stratégique et de réputation »*[56].

[55] EIOPA, 2010, Solvency 2, Technical Standards. https://eiopa.europa.eu/en/publications/index.html / https://eiopa.europa.eu/en/publications/sii-final-l2-advice/index.html

[56] Ainsi formulé, le risque opérationnel peut comprendre la notion de risque juridique, ainsi que le risque de non-conformité, sans pour autant inclure les risques stratégiques, par définition liés à la prise de décision stratégique, alors que le risque opérationnel concerne principalement la mise en œuvre de telles décisions. Le risque d'image ou de réputation est davantage envisagé comme une conséquence d'autres risques : un risque juridique ou un risque de fraude peut porter atteinte à l'image de l'établissement financier en cas de survenance, il s'agit davantage d'une conséquence associé à un risque (impact image) qu'une cause racine dans la majorité des cas.

Au sein de la société C1 un chantier stratégique a été mis en place en vue de se doter d'une politique de maîtrise des risques opérationnels reposant sur :

-une fonction dédiée à la gestion des risques opérationnels,

-un dispositif de contrôle à plusieurs niveaux incluant des fonctions de contrôle permanent (contrôle des managers et opérationnels) et de contrôle périodique (audit interne et contrôleurs internes).

La société C1 s'est dotée d'une politique de maîtrise des risques opérationnels reposant sur les éléments suivants (extraits de documents internes : politiques de maîtrise des risques opérationnels, rapports de contrôles internes, référentiel des risques de l'entreprise C1).

Décomposition du risque opérationnel en 7 catégories :

- fraude interne, - fraude externe, - pratiques en matière d'emploi et de sécurité sur le lieu de travail,	- clients, produits et pratiques commerciales, - dommages aux actifs corporels, - dysfonctionnements de l'activité et des systèmes, - exécution, livraison et gestion des processus

Face à une telle définition, jugée extensive voire trop générale et peu compréhensible par les collaborateurs, il est apparu rapidement nécessaire d'y apporter des précisions, de l'objectiver au regard d'exemples pour la rendre parlante et ainsi mieux cibler pour les managers et dirigeants les attentes en termes de définition d'une politique de maîtrise des risques.

Les échanges avec plusieurs cadres de la société d'assurance via une série de réunions menées sous forme de groupe de travail, permettent de faire remonter les constats suivants quant à la notion de risque opérationnel pour la société C1:

« Le risque opérationnel, c'est quelque chose de complexe pour un assureur généraliste, en assurances de personnes on comprend l'intérêt du sujet car il y a des mouvements de fonds, des problématiques d'épargne etc. mais en assurance de biens et de responsabilités à part des fraudes à l'assurance on ne voit pas bien de quoi il peut s'agir » nous explique ce responsable du contrôle interne (C1-2). Ce que confirme ce contrôleur interne (C1-5) : *« La difficulté avec le risque opérationnel c'est que quand on voit la définition, on a le sentiment que cela se retrouve partout, mais en pratique intégrer cette définition et en faire quelque chose cela relève de l'impossible : au moins être informé des risques informatiques ou des vulnérabilités de l'entreprise en amont des nouveaux projets reste une démarche à construire. Le risque opérationnel c'est une révolution dans l'entreprise, pourtant on a des contrôles depuis presque dix ans ».*

Les différents contrôleurs rencontrés sur cette problématique évoquent ainsi en début d'entretien la difficulté liée à la méconnaissance de la notion de risque opérationnel. Les contrôles réalisés sur les périmètres historiques de la société d'assurance permettaient de faire remonter des alertes, des cas spécifiques de fraudes ou le plus souvent des non-conformités aux procédures ou non-qualité dans la délivrance des services aux assurés.

L'un de nos constats clés est que la contrainte réglementaire liée à Solvabilité II contraint la société d'assurance à tenir compte du risque opérationnel. Toutefois, les différents contrôleurs en charge de ce sujet reconnaissent les nombreuses difficultés auxquels ils ont été confrontés face à cette notion :

-le risque opérationnel est une notion vague, à périmètre élargie,

-aucune recommandation ou bonne pratique n'a été formalisée ni dans l'entreprise ni par l'autorité de tutelle du secteur, en vue d'établir un référentiel réellement adapté aux risques de l'assureur C1,

-l'évolution des activités de l'entreprise et les nombreuses réorganisations donnent le sentiment que les contrôles sont inadaptés face à l'enjeu global que constitue le risque opérationnel, sans que pour autant des décisions soient prises pour réduire cette source de pertes avérées et potentielles pour l'entreprise.

« La notion de risque en soi ce n'est pas difficile, mais savoir ce qu'on doit faire et surtout comment le faire pose un vrai problème » nous révèle ce contrôleur interne (C1-6). *« Nous avons la définition du risque opérationnel mais peu d'autres éléments méthodologiques sur lesquels nous appuyer, il y a pourtant beaucoup de techniques d'analyse de risque tirées de l'industrie ou des sciences de l'ingénieur mais on voit mal comment les adapter dans notre secteur sur des métiers que nous connaissons pourtant »* nous rapporte ce responsable du contrôle interne (C1-1).

Dans le cadre de l'étude de cas C1, de multiples cas de risques opérationnels ont été identifiés tout au long de la période d'observation. Le tableau ci-après répertorie des exemples de risques opérationnels auxquels nous avons été confrontés lors de l'étude.

Tableau 26. Risques opérationnels identifiés dans le cadre de l'étude de cas C1

Risque opérationnel	Descriptif du risque / exemples
Risques liés au système d'information	-Pertes de données clients suite à la fusion entre la société C1 et un autre assureur : les données clients ont été perdues pour une partie du portefeuille client lors de la migration des données d'un SI à l'autre. -Indisponibilité du SI durant plusieurs jours engendrant des retards dans l'indemnisation des assurés (risques sur l'image et la qualité de service).
Fraudes massives sur un portefeuille de contrats-assurance automobile	De nombreuses fraudes à l'assurance automobile ont été identifiées a posteriori via des contrôles de cohérence. Des indemnisations ont été faites sans fondement juridique ou sur des montants dépassant ceux prévus.
Erreurs de traitement des informations clients assurance automobile	Des informations sur les antécédents (sinistres antérieurs) des assurés n'ont pas été renseignées : ces derniers étant plus enclins à avoir des sinistres : manque à gagner pour l'assureur car aucune répercution sur les tarifs des contrats.
Nouveaux produits non maîtrisés	-De nouveaux produits ont été commercialisés sans maîtrise suffisante : les assurés disposent d'informations peu lisibles et résilie leurs contrats au terme. Une vague de réclamation importante des assurés a été identifiée (surcoût pour l'assureur). -Des tarifs inexacts ont été appliqués aux assurés : leurs primes ne couvrent pas les sinistres à payer. -Le commissionnement des commerciaux n'est pas maîtrisé et la compagnie verse des commissions supérieures aux pratiques habituellement fixées (surcoût pour l'assureur).
Réclamations clients non traitées	Plusieurs réclamations d'assurés n'ont pas été traitées du fait d'une surcharge des services recours et réclamations. Face à des délais jugés trop longs, les assurés ont intenté des actions en justice.

3.2. La formulation des problématiques, les éléments clés de formalisation d'une politique de maîtrise des risques opérationnels

Face à ces constats relatifs au risque opérationnel, notre rôle de contrôleur interne en charge de la déclinaison d'une politique de maîtrise des risques opérationnels a consisté dans un premier temps à formaliser les « expressions de besoins » au sein de la société d'assurance C1 face à cet enjeu émergent. Les principales problématiques analysées sont les suivantes :

- **La nécessité de définir une politique de maîtrise des risques opérationnels pour donner un sens aux contrôles**

Si la notion de risque opérationnel était identifiée au préalable, de nombreux risques opérationnels étaient remontés à la direction des contrôles et des actions de contrôles nombreuses étaient préexistants sans cohérence ni objectifs précis formalisés en termes de

maîtrise des risques[57]. Les contrôles servaient l'identification des risques mais la logique inverse n'était pas formalisée. Nos différents entretiens en interne à la société C1 ont permis de faire remonter la problématique centrale face au risque opérationnel : le besoin de formaliser une politique de maîtrise des risques opérationnels adaptée à la société.

Les objectifs de cette formalisation étaient pluriels : mieux maîtriser les risques (en les identifiant et les évaluant de manière cohérente et homogène), structurer les contrôles existants, adapter les contrôles et intégrer leurs résultats dans la prise de décision des managers, passer d'une logique de contrôle de conformité (analyse des non-conformités) à une vision orientée vers la maîtrise des décisions et du coût du risque y étant associé ; l'objectif de conformité à la réglementation étant tacite (auparavant la politique de maîtrise des risques se limitait au rappel des règles prudentielles et de contrôle).

« Il y a une vraie nécessité de donner du sens à nos contrôles, les contrats ce n'est pas le problème, le vrai souci c'est la volumétrie des périmètres ou des portefeuilles clients à contrôler » ; « Nous sommes face à un problème de taille : une multitude de risques, une multitude de contrôles et un vrai souci pour savoir comment prendre le problème du risque opérationnel ; Il nous faut une politique et un référentiel dédié. » nous indiquent ces contrôleurs internes (respectivement C1-3 et C1-7). *« On a toujours eu des remontées sur les risques, des contrôles de faits, mais dire si cela a permis de mieux maîtriser nos risques, personne n'en est capable. On est sur des actions au coup par coup. On identifie des fraudeurs mais on ne sait pas si nos actions ont permis de réellement enrayer le phénomène »* précise également cet autre contrôleur interne (C1-4).

- **La définition d'une politique de maîtrise des risques opérationnels**

La politique de maîtrise des risques opérationnels a donc été construite via différents entretiens mobilisant des contrôleurs des risques ainsi que des directeurs, managers et opérationnels de l'entreprise. La phase de validation par la direction de l'entreprise a permis de tenir compte d'adaptations intégrant les objectifs opérationnels de l'entreprise.

Les principales mesures de cette politique de maîtrise des risques opérationnels sont les suivantes[58] :

[57] Ces risques alors remontés par les différentes fonctions de l'entreprise sont consolidés dans la base de collecte des pertes et incidents de l'assureur C1. La « base incidents » constitue un moyen de tracer l'ensemble des risques opérationnels avérés (étant survenus) au sein de l'entreprise. Il s'agit de constituer progressivement un historique de pertes opérationnelles liées aux risques.

[58] Source : Principaux extraits de la politique de maîtrise des risques opérationnels de l'assureur C1.

L'objectif de la politique de risque (Operational Risk Management) est de répertorier, de manière exhaustive, tout incident lié à un risque opérationnel ayant une conséquence financière.

Cette politique doit intégrer l'exercice de collecte des risques, lequel a pour objectif :

- d'alimenter les modèles statistiques qui permettent de dimensionner les montants de fonds propres à mobiliser pour couvrir le risque opérationnel dans le cadre de Solvabilité II.
- de contribuer à la connaissance des risques de la compagnie et d'identifier les zones de vulnérabilité et par la suite permettre la mise en place de dispositifs de contrôles adéquats. (…)

Le processus de collecte de pertes et d'alimentation de la base d'historique des risques s'articule autour de quatre étapes :

Etape 1 : identification des sources de pertes

- Géographie des risques à partir de la cartographie,
- Utilisation de toutes sources d'information disponibles en vue d'identifier des pertes,
- Utilisation des bases de recensement d'incidents existantes.

Etape 2 : définition des pertes

- Définition précise de l'événement au regard du processus,
- Définition de la catégorie du risque en lien avec le référentiel risque,
- Renseignement des champs permettant de qualifier la nature de la perte.

Etape 3 : Evaluation des conséquences financières des pertes

- Chiffrage des pertes en fonction d'une méthodologie commune des processus métier,
- Alimentation des champs permettant de chiffrer la perte,
- Qualification de la perte

Etape 4 : Reporting et contrôle

- Modalité d'alimentation de la base,
- Contrôle des données de pertes par le contrôle interne permanent,
- Traçabilité des données saisies par la définition d'une piste d'audit,
- Analyse et diffusion des données par un reporting adéquat.

On peut détailler la nature des éléments attendus en deux grandes composantes :

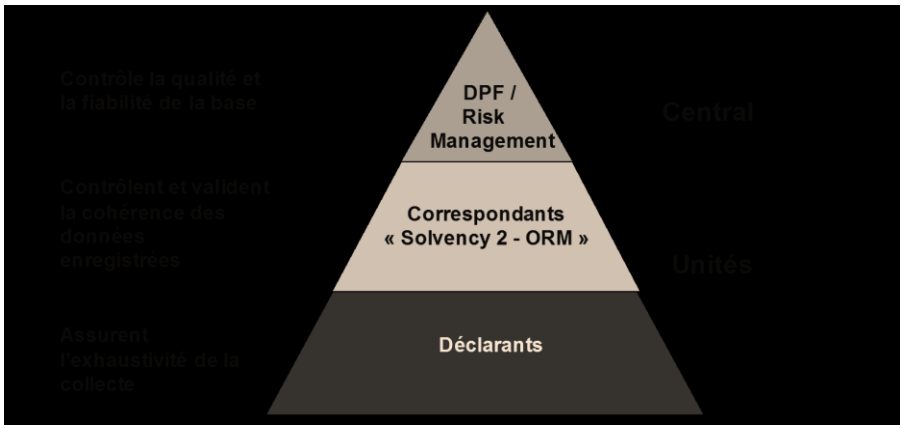
- les éléments relatifs à l'identification, la définition et l'affectation de l'événement de perte,
- les éléments relatifs à l'évaluation financière de la perte

Il a été convenu de privilégier la date de détection pour déterminer l'exercice d'affectation de la perte, sous réserve que cette date corresponde bien à une reconnaissance du risque à travers la dotation d'une provision.

Décomposition des impacts par nature : Un incident lié à un risque opérationnel peut se traduire par une perte financière principale à laquelle sera associée des pertes connexes qu'il sera aussi nécessaire d'identifier. La base prévoit de gérer quatre niveaux d'incidence.

Les rôles et responsabilités dans l'identification, l'évaluation et la réduction des risques sont décrits selon le schéma ci-après[59].

Figure 34. Rôles et responsabilités dans la politique de maîtrise des risques opérationnels de l'assureur C1



Cette répartition des rôles est réalisée en trois étapes :

- La direction centrale (dont direction financière) et la fonction Risk Management contrôlent la qualité des reportings sur le risque (formalisés par le référentiel de risques opérationnels).

[59] Dans le schéma : DPF : Direction Financière.

- Les contrôleurs des risques sont rattachés au Risk Management et se répartissent le travail d'animation des correspondants risques (managers des unités opérationnels, référents techniques ou opérationnels dans les différentes unités).
- Les correspondants risques ont pour mission de recueillir les évènements de risques opérationnels identifiés auprès des différents collaborateurs ou par leurs managers. Il s'agit en général de managers ou de référents techniques consacrant une partie de leur activité (en moyenne une journée voire deux journées au maximum par semaine) à l'activité de reporting et de contrôle.

Cette répartition des rôles est l'un des éléments clés de la politique de maîtrise des risques opérationnels. Elle vise à bénéficier pour les contrôleurs « en central » de l'appui de correspondants dans chaque unité métier de l'entreprise (directions financière, comptabilité, Direction RH, Direction des Systèmes d'Information, Direction des Opérations (dont direction de l'Indemnisation et Direction Souscription des contrats), Direction Commerciale, Direction Technique et Actuariat etc.

3.3.La mise en œuvre d'actions expérimentales pour gérer le risque opérationnel

La déclinaison de la politique de maîtrise des risques opérationnels au sein de l'assureur C1 s'est fondée sur :

-un référentiel de risque opérationnel basé sur un glossaire (voir l'annexe 9-1 Exemple de référentiel de risques opérationnel), permettant d'harmoniser l'identification des risques opérationnels entre les différents acteurs de la société C1,

-la mise en œuvre d'une cartographie des risques opérationnels et d'une base de collecte des incidents et des pertes associées au risque opérationnel (fondées sur une matrice d'évaluation des risques figurant à l'annexe 9-2),

-la réalisation d'un plan de contrôle associé au risque opérationnel fondé sur le référentiel COSO (voir l'annexe 9-3).

Outre ces dispositifs méthodologiques associés à la démarche de maîtrise des risques, nous avons également insisté sur la nécessité d'interroger le dispositif de contrôle préexistant :

Nous avons ainsi procédés à la réalisation de grilles d'évaluation des dispositifs de contrôle (évaluation du dispositif de maîtrise des risques). Cette démarche, bien qu'usitée dans les travaux théoriques en gestion des risques était alors nouvelle au sein de l'entreprise étudiée.

L'assureur C1 privilégiait une application des normes en vigueur sans toutefois avoir mis en place des éléments lui permettant d'évaluer la pertinence et l'effectivité des dispositifs existants face aux risques.
Pour adapter la mise en œuvre d'un dispositif nous permettant de nous assurer de l'effectivité des contrôles mis en place, au-delà des dispositifs formalisés, nous avons ainsi eu recours à différents échanges auprès des collaborateurs de l'entité. Plusieurs entretiens internes (précités) ont ainsi été réalisés.

Entretiens gestionnaires :
« Les Contrôleurs des risques, nous avons eu à faire à eux effectivement, mais les contrôles se sont concentrés sur des aspects formels » explique ce gestionnaire de contrat (C1-22).
« Certains contrôleurs nous parlaient brièvement de risques opérationnels mais sans pour autant nous détailler de quoi il s'agissait, ils voulaient surtout s'assurer que l'on respectait les procédures internes » déclare encore ce gestionnaire (C1-19).
« Nous avons fait l'objet de contrôles mais de la à parler de risques, cela semble excessif, certains contrôleurs nous ont même confié qu'ils se doutent que l'on connait notre métier, mais qu'ils doivent quand même faire remonter des risques à la direction » explique cette intermédiaire d'assurance (C1-16).
« Sur le risque opérationnel, on fait remonter des éléments dans des tableaux de bord, cela correspond surtout à des risques potentiels que l'on nous demande d'évaluer en cas de survenance, mais on nous demande en fait peu de choses sur l'avéré car les seuils ou les montants sont très élevés et donc nos cas de pertes ou de réclamations clients ne sont pas pris en compte, on ne comprend pas quel est l'intérêt si cela ne change rien lorsque l'on remonte un problème » confirme ce directeur commercial (C1-11).

Outre ces retours quant à l'effectivité des contrôles réalisés et à leur rapprochement en termes d'analyse de risque, une seconde série d'interviews auprès de collaborateurs de l'entreprise nous a permis d'identifier les causes de ce manque d'effectivité.

Il ressort plusieurs constats de cette seconde série d'entretiens :
-La plupart des contrôles en place ont été intégrés directement aux procédures et ce de manière incrémentale.
-L'absence de revue de l'ensemble des contrôles (absence de référentiel de contrôles) induit la présence de contrôles en surnombre, parfois redondants et peu structurés.

-Les entretiens réalisés pointent un défaut de communication en interne sur le rôle des contrôles et une absence de communication sur les résultats de ces contrôles.
-Nos échanges révèlent encore le manque de lien avec la démarche de gestion des risques.

Suite des entretiens, vision des gestionnaires :
« Nous avons été contrôlés mais le rapport de contrôle ne pointent que des pourcentages de non-conformités ou des actions curatives à mettre en œuvre, on ne sait même pas pourquoi on doit améliorer tel ou tel dispositif, on se doute qu'il y a un lien avec la réglementation mais pour nous ce n'est pas clair » confie ce directeur de l'organisation (C1-8).

« Les contrôles nous voulons bien y participer mais on devrait peut-être nous expliquer la cohérence de tout cela, nous avons déjà communiqué plusieurs fois les mêmes informations à plusieurs entités différentes » explique ce directeur des ressources humaines (C1-9).

Nous avons ensuite confrontés ces résultats aux avis d'experts des différents contrôleurs des risques en vue d'évaluer (à dire d'expert) le degré d'effectivité des contrôles face au référentiel de risque de la société.

Nos principaux constats nous orientent vers :

-la nécessité d'une mesure de l'effectivité du dispositif via une revue complète des contrôles en place,
-l'importance d'une revue critique des contrôles en lien avec la politique de maîtrise des risques (ORM) précitée pour identifier les écarts et repositionner ces dispositifs de maîtrise des risques.

En conclusion, les nombreux échanges avec les différents gestionnaires nous permettent d'insister sur des incompréhensions récurrentes sur l'enjeu des contrôles, sur une impression de lourdeur et sur un manque de visibilité sur le bien fondé des contrôles réalisés en termes de sécurisation des activités opérationnelles.

Entretiens experts :
« Ce qu'il nous faudrait c'est une revue de la cohérence et de l'intérêt des contrôles au regard de notre exposition au risque. L'audit interne ne s'appui pas suffisamment sur les

risques aujourd'hui et ne peut à lui seule revoir l'ensemble des contrôles en place » explique ce responsable du contrôle interne (C1-2).

« Le dispositif ORM a l'air intéressant mais nous n'avons pas encore franchi le pas entre une politique de risque écrite et une application concrète de ces méthodes de management des risques par les différents contrôleurs » explique ce contrôleur interne (C1-5).

Ces différents échanges, via un groupe de travail interne ont ensuite permis d'aboutir à la mise en œuvre d'un audit du processus de contrôle des risques au sein de l'assureur C1. Cet audit avait pour objectif de rapprocher les axes de contrôle interne des référentiels de risques opérationnels retenus dans le cadre de la politique de maîtrise des risques opérationnels.
Au-delà des éléments formalisés, l'objectif de l'audit était de rapprocher ces différents éléments.

Nous avons ainsi mené cet audit sur différentes bases :

-Outre les entretiens internes, réalisation d'une revue des procédures et modes opératoires intégrant des contrôles,

-Etude des rapports de contrôle interne produits sur les 3 dernières années et extraction des informations sur l'identification et la mesure du risque opérationnel,

-Etude des risques par ligne métier tels que présentés dans la cartographie des risques opérationnels,

-Phase d'échanges post-audit documentaire auprès de 5 contrôleurs et 10 représentants des entités métiers et supports.

Le résultat de cet audit ressort au travers du tableau ci-après.

Tableau 27. Analyse de l'effectivité du dispositif de contrôle des risques. Rapprochement risques opérationnels / Effectivité des contrôles

Catégories de risque opérationnel de niveau 1	**Catégories de risque opérationnel de niveau 2**	**Exemples générique secteur assurance**	**Axes de développement contrôle interne des risques UMC** (source : diagnostic de contrôle interne)	**Degré d'effectivité de la procédure de contrôle (2013)**
Clients, produits et pratiques commerciales	-Conformité (lois, règlements, normes) -Défaut de production -Service conseil -Pratiques commerciales incorrectes	Défaut d'information sur les éléments de tarification ou le détail d'une offre vendue à un adhérent Clauses abusives, peu claires ou illicites dans un contrat. Exclusion de garantie ruinant l'économie du contrat	-Le contrôle des procédures CNIL -Le contrôle des nouveaux produits (conception et développement-lancement) -Le contrôle du respect de l'obligation d'information et de conseil -Le contrôle des procédures de réclamation -Le contrôle du processus veille réglementaire -Le contrôle du processus LAB-FT	◪ ■ □ ■ □ ■
Dommages aux actifs corporels	-Catastrophes et autres sinistres	Catastrophes naturelles (inondation, tempête endommageant les locaux dont la salle informatiques et les serveurs), incendie, vol, dégradation	(PCA-PRA)	◪
Dysfonctionnement de l'activité des systèmes	-Sécurité des systèmes	Indisponibilité du SI rendant difficile le versement des prestations aux adhérents, erreur dans le calcul des fonds à provisionner pour indemniser les adhérents	-Le contrôle du dispositif de gouvernance de la qualité des données (traçabilité et gestion des données) -Le contrôle des procédures informatiques (protection des équipements et données, gestion des autorisations et cartographie	□ ■

			informatique)	
Exécution, livraison et gestion des processus	-Admission et documentation clientèle -Contreparties commerciales -Fournisseurs -Saisi, exécution et livraison des transactions -Surveillance et notification financière	Contrat santé/prévoyance comprenant des informations parcellaires (antécédents de risque, facteur de risque, éléments de prévention etc.). Mauvaise exécution des processus (gestion, souscription etc.)	-Le contrôle du formalisme des procédures (formalisation, documentation, complétude des dossiers) -Le contrôle des activités de gestion -Le contrôle de l'actuariat (conception et tarification) -Le contrôle des procédures d'achats	◪ ◪ □ ■
Fraude externe	-Vol et fraude	Fausse déclaration adhérent, prestataire, déclaration excessive	-Le contrôle de la fraude (procédures et incidents)	□
Fraude interne	-Activité non autorisée	Fausse déclaration collaborateur, déclaration excessive avec complicité interne de collaborateurs	-Le contrôle des procédures comptables et budgétaires -Le contrôle des procédures de placement et d'investissements	■ ■
Pratiques en matière d'emploi et sécurité sur le lieu de travail	-Égalité et discrimination -Relations de travail -Sécurité du lieu de travail	Prise en compte des risques psychosociaux (stress, fatigue, harcèlement etc.) Sécurité des locaux (notamment accès) et des données	-Le contrôle du PCA-PRA -Le contrôle des activités sous-traitées (PCA, contractualisation) et déléguées (externalisation sur/hors site)	◪ □

Nous avons ainsi recensé trois niveaux d'effectivité :

-effectivité complète (le rapprochement entre contrôles et risques opérationnels est réel. Les contrôles permettent bien d'identifier des risques opérationnels et d'envisager leur traitement).

-effectivité partielle (les contrôles permettent d'identifier des risques sans toutefois qu'un rapprochement avec les risques opérationnels identifiés dans le cadre de la politique de maîtrise des risques soit clairement établi)

-effectivité nulle (les contrôles sont avant tout formaliste et remontent des non conformités aux procédures internes. Lorsque des risques sont identifiés, ils sont remontés en tant que dysfonctionnement interne, sans lien avec la politique de maîtrise des risques opérationnels).

Bien que simpliste dans son fonctionnement, une telle analyse a permis de déterminer les zones pour lesquelles les contrôles semblaient insuffisants en termes d'effectivité et donc à repenser sur le fond ou sur la manière de les réaliser. Ces résultats ont été soumis pour échanges contradictoires aux différentes entités métiers et supports concernées.

3.4.L'élaboration des conclusions de l'étude

Les échanges contradictoires sur ces résultats ont permis de faire remonter différentes remarques dont nous avons précisé ci-après les illustrations les plus significatives.

La pertinence d'un rapprochement entre politique de risque et contrôles :

« On sera en présence d'une politique de risque efficace si elle nous permet de réussir à identifier clairement nos risques sans partir dans toutes les directions, et surtout si on arrive à remonter les causes d'un problème et à les traiter rapidement mais aussi durablement » déclare ce contrôleur des risques (C1-6).

« Une politique efficace doit balayer les problématiques suivantes : une maîtrise du coût du risque (dont les rapports entre sinistres et primes), tenir compte de la stratégie et des changements organisationnels, du lancement de projets et de nouveaux produits dans l'entreprise. On doit aussi avoir une vision des contrôles antérieurs et construire des plans de contrôle intégrant prévision et prévention des risques opérationnels futurs, avec ces résultats on voit bien que cela était loin d'être le cas » précise ce directeur du contrôle interne (C1-1).

D'autres interlocuteurs étaient alors plus nuancés sur les apports de ce rapprochement risques opérationnels / contrôles internes :

« On voit l'évolution du dispositif de contrôle non pas au fait qu'il devient parfait, il sera toujours perfectible. Cela se voit quand les contrôles ont permis de lever des incompréhensions…après, les risques, ce n'est pas une fin en soi » précise ce directeur commercial (C1-10).

« Quand on peut chiffrer un risque on le fait, cela aura toujours une certaine significativité, mais on aimerait généraliser ces pratiques, même si cela semble illusoire » confie ce contrôleur interne (C1-7).

Vers un rapprochement vers d'autres entités :

« Quand on voit ces listes de risques et les listes de contrôles, on se dit qu'il y a un lien fort avec la qualité : dès qu'on a de nouveaux commerciaux, de nouveaux responsables d'agences, on envoi un contrôleur les former aux bonnes pratiques, aux erreurs à éviter, il faut faire du contrôle qualité, pas du contrôle de sanction, ainsi on anticipe mieux des risques opérationnels, notamment ceux liés aux erreurs de traitement et de saisie des informations, aux dossiers clients incomplets etc. » déclare le directeur de l'organisation (C1-8).

Enfin, d'autres acteurs du dispositif de contrôle ont, à la lumière de ce résultat, insisté sur des constats complémentaires :

-le fait pour les acteurs du dispositif de contrôle des risques de devoir se baser sur le contrôle permanent et le contrôle périodique ainsi que sur d'autres types de contrôles.

-le fait que les différents contrôles en interne étaient à ce jour trop cloisonnés et qu'il existait en pratique peu de liens entre le contrôle interne et le contrôle de gestion, voire pas de vision partagée sur le coût du risque. Les remontées et redescentes d'informations consolidées sur le risque semblaient encore largement insuffisante pour que la filière contrôle des risques soit perçue comme autrement qu'une filière de contrôle « administrative ».

L'importance de la communication :

« On sait que le contrôle de gestion pourrait nous apporter beaucoup, notamment dans le pilotage des contrôles et des risques, cela permettrait de voir où il y a des pertes, d'avoir des alertes pour nous adapter ou refondre nos plans de contrôle, mais en pratique tout est cloisonné, on communique peu alors qu'ils sont au même étage. » déclare ce contrôleur interne (C1-6).

« Il nous faut des acteurs dédiés sur ce sujet des risques opérationnels pour faire le lien entre les services, formaliser une politique c'est bien mais cela ne suffit pas, sans incitation, c'est une déclaration de bonnes intentions. Avoir pu échanger avec un contrôleur chargé

d'instaurer la démarche risque nous permet de voir le travail autrement » déclare ce contrôleur interne (C1-4).

« Les acteurs en charge de la politique de risque ne doivent pas être isolés, beaucoup se dit en dehors des comités ou des réunions. Il faut faire du transverse : si cette notion est dans les valeurs de notre entreprise, ce n'est pas sans raison, c'est bien qu'on doit progresser sur ce sujet… » reprend ce contrôleur interne (C1-6). Ce qu'illustre cet autre contrôleur interne (C1-3) : *« Le vrai problème au-delà de la complexité, c'est un problème de communication, on ne pense pas à aller vers les fonctions supports, on veut forcément passer par les responsables hiérarchiques car les luttes de pouvoir risquerait de se retourner contre nous, cela paralyse toute la démarche. »*

A l'issue de tels échanges, la phase de recherche-action a permis de mettre en place une approche pilote au sein de l'assureur C1. Cette approche visait à intégrer dans les dispositifs de contrôle une démarche de pilotage par les risques déclinée sur la base du référentiel de risques opérationnels (identifiés dans le cadre de la politique de maîtrise des risques opérationnels). Cette phase pilote a ainsi concerné l'identification des risques opérationnels liés aux produits commercialisés, l'identification des risques opérationnels liés aux pratiques RH et enfin l'identification des risques de fraudes à l'assurance.
Sur ces périmètres les aspects d'identification et de mesure du risque opérationnel ont été intégrés.

Plusieurs apports de cette démarche ont pu être constatés :
-Le rôle essentiel de la fonction centrale « risque » dans la refonte des contrôles existants, lesquels[60], étaient devenus inadaptés et sans corrélation avec le niveau de risque par activité. Des contrôles ont ainsi été supprimés car étant sans relation avec les enjeux de risques opérationnels.
-L'impact positif du rapprochement avec le contrôle de gestion, alors mis en place, a permis d'identifier comptablement des surcoûts au sein de l'organisation. La possibilité de mesurer le coût du risque fut alors perçue comme un véritable levier.
-Une approche culturelle plus facile à mettre en place en abordant la thématique du risque au lieu et place de la thématique des contrôles et du respect des procédures.

[60] Contrôles préexistant à la politique de maîtrise des risques opérationnels.

La réduction du nombre de contrôle et le recentrage sur les risques de l'entreprise, ainsi qu'un rapprochement avec les pertes avérées et potentielles, ont permis de changer la perception par les différents collaborateurs quant à cette démarche de contrôle des risques.

En résumé, l'apport de la recherche-action quant au déploiement de la politique de maîtrise des risques opérationnels résidait à plusieurs niveaux :
-souligner l'importance de l'enjeu du risque opérationnel et clarifier cette notion, perçue comme peu parlante car d'inspiration réglementaire,
-repenser le dispositif de contrôle interne en lui donnant du sens pour les entités contrôlées et les entités en charge des contrôles, par le recours à l'approche par les risques,
-au-delà des méthodes et approches par les risques, mettre en lumière la nécessité d'avoir des acteurs en charge de la coordination et de l'animation d'un dispositif de contrôle du risque opérationnel au sein de l'organisation. Si nous avons rempli ce rôle tout au long de la recherche-action, après notre départ, un collaborateur a été nommé au sein de la société C1 pour remplir ce rôle d'animation et de communication transverse. Cette communication et cette animation concernaient principalement les métiers (commerciaux, gestions) et les autres fonctions supports (contrôle de gestion, contrôle qualité, conformité des opérations). Les conclusions de l'étude ont permis d'insister sur le fait qu'il s'agit d'une condition de réussite de la démarche de gestion des risques.

4. L'étude de cas C2-Établissement bancaire

Notre seconde étude de cas s'est déroulée au sein d'un **établissement bancaire (C2).** Cette recherche-action a eu lieu sur une durée de six mois. Tout comme pour l'étude de cas C1, une première étape a consisté à dresser un diagnostic de la situation initiale de la société C2 (définition du risque opérationnel, formalisation des principaux cas de survenance de risques opérationnels). La seconde étape de cette étude de cas visait la formulation des problématiques essentielles de la société C2 face au risque opérationnel (définir une politique de maîtrise des risques opérationnels adaptée au métier d'établissement bancaire, répondant aux exigences réglementaires, fixant des limites d'acceptation de ce risque et intégrant la diversité des acteurs concernés : répartition des rôles et responsabilités). La troisième étape de l'étude de cas impliquait la mise en œuvre d'actions expérimentales répondant aux problématiques identifiées (outils, méthodes mobilisées, désignations des acteurs et mise en

œuvre opérationnelle de la politique de maîtrise des risques). La dernière étape consistait en l'élaboration des conclusions de l'étude au sein de l'établissement bancaire C2 (principaux retours d'expérience en termes de freins et leviers, bonnes pratiques à pérenniser, erreur à éviter).

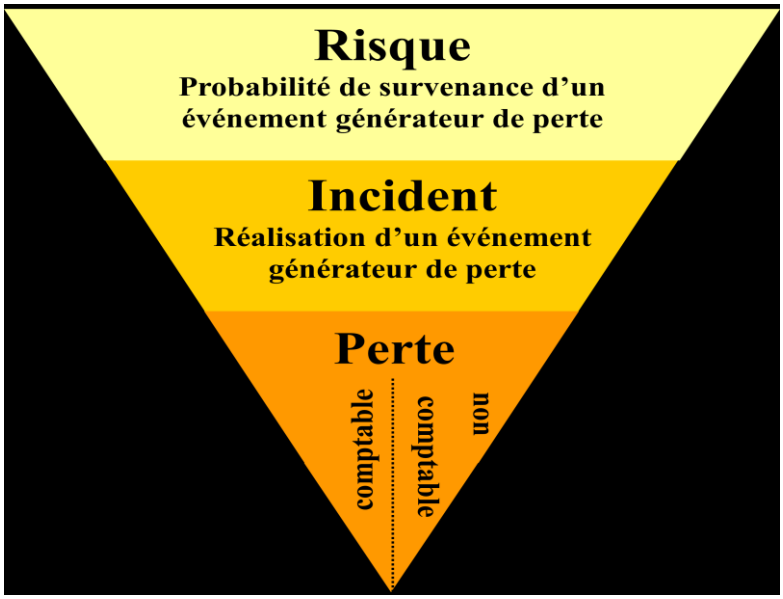
4.1.Le diagnostic de la situation initiale : la notion de risque opérationnel en banque

L'étude de cas au sein de l'établissement bancaire C2 a consisté, à la différence de C1, non pas au déploiement d'une politique de maîtrise des risques opérationnels créée ex nihilo. Il existait déjà lors de notre arrivée au début de la recherche-action une politique de maîtrise des risques opérationnels. Cependant, cette politique était jugée peu effective et impliquait un redéploiement. L'objectif premier de cette étude de cas était donc d'agir sur le redéploiement d'une telle politique, en cours de redéfinition. Notre action en tant que Risk Manager a donc consisté à redéfinir les contours de cette politique.
La définition réglementaire du risque opérationnel étant déjà appliquée en interne, nous sommes partis de cette approche (en cherchant toutefois à la clarifier).

« Le risque opérationnel se définit comme le risque de pertes dues à une inadéquation ou à une défaillance des procédures, personnels, systèmes internes ou à des événements extérieurs, en y excluant les risques stratégiques et en y incluant les risques d'atteintes à la réputation ».

Une telle définition était affinée en interne pour distinguer un élément de risque, d'un incident puis d'une perte effective (comptable ou non comptable).

Figure 35. Déclinaison de la définition du risque, étude de cas C2



Au sein de la société C2, le chantier réalisé consistait à redéfinir les contours organisationnels de la politique de maîtrise des risques opérationnels.

Après plusieurs échanges internes avec le directeur de risques, le directeur du contrôle interne et plusieurs Risk Managers, une redéfinition de la politique de maîtrise des risques a ainsi été réalisée (voir l'annexe 10 - Exemple de politique de maîtrise des risques opérationnel, illustration avec la banque C2).
Cette politique de maîtrise des risques reposait alors sur :
-une direction des risques du groupe d'appartenance de la banque C2,
-une direction des risques opérationnels à laquelle nous étions rattaché en tant que Risk Manager,
-une direction de l'audit interne,
-une direction veille et conformité,
-une direction du contrôle interne (centralisée et décentralisée).

Egalement, la politique de maîtrise des risques opérationnels reprenait le référentiel de risques issu de la réglementation prudentielle Bâle II (transposée via le règlement CRBF 97-02).
La décomposition du risque opérationnel au sein de la banque C2 est donc la suivante :
-Fraude interne,
-Fraude externe,
-Pratiques en matière d'emploi et de sécurité du lieu de travail,

-Risques liés aux clients, produits et pratiques commerciales,

-Dommages aux actifs corporels,

-Interruption d'activité et dysfonctionnements des systèmes,

-Exécution, livraison et gestion des processus.

La perception des dispositifs de contrôles issus du risque opérationnel (inspiration normative) lors d'échanges préliminaires:

Ce directeur du contrôle interne (C2-8) nous explique ainsi: *« dans la banque, quel que soit l'interlocuteur, celui-ci n'aura jamais une vision exhaustive des résultats de son action sur le risque opérationnel. Les opérationnels sont le nez dans le guidon. Notre rôle au contrôle et au Risk Management c'est de leur faire voir s'ils sont assis ou non sur une bombe ».* Ces propos sont étayés par ceux de ce Risk Manager (C2-7). *« On permet aux métiers de voir à quoi correspondent les risques chez eux, cela passe par des analyses, des cartographies, faire l'interface entre deux directions opérationnelles pour voir quels risques incombent à qui ».*
Il ressort de ces entretiens une vision relativement limitée des actions à réaliser quant à la notion même de risque opérationnel.

Egalement, ce Risk Manager (C2-2) nous indique que : *« 80 % de notre travail et de nos échanges ne sont pas formalisés par nos liens dans l'organigramme, il y a beaucoup d'informel, d'échanges via des réseaux internes que l'on a mis sur place avec le temps. Ce n'est que s'il y a vraiment un problème insurmontable qu'on passe par la hiérarchie ».* Enfin, nous citons ce Risk Manager (C2-3) : *« Le problème c'est qu'on parle du négatif et de ce qui peut arriver à l'avenir, cela ne rassure pas, il faut avoir le bon argumentaire, ce qui est compliqué car on a toujours un temps de retard avec le risque opérationnel »* précise ce Risk Manager. On voit donc au regard de ces entretiens l'importance de mettre en œuvre un argumentaire adapté pour faire face aux enjeux du risque opérationnel.

Si des efforts importants et une certaine maturité quant à la démarche de gestion des risques caractérisent les échanges internes en début de recherche-action, nous constatons également que la diversité de risques opérationnels laisse démuni l'équipe centrale en charge de coordonner le pilotage des risques opérationnels. Les différents outils et méthodes (présentés en annexe 12), notamment la cartographie des risques sont alors présentés comme des outils en théorie utile pour piloter les risques, mais pour lesquels les Risk Managers sont très vite confrontés à une surcharge d'information sur les risques opérationnels remontés par les

différents acteurs des fonctions métiers et supports (acteurs émanent de la DRH, de la direction des opérations, de la direction financière, de la direction des systèmes d'information, des centres de traitement des moyens de paiement, de la direction du Marketing).

Dans le cas de l'étude C2, ces multiples évènements de risques opérationnels remontés peuvent être illustrés au travers du tableau ci-après.

Tableau 28. Risques opérationnels identifiés dans le cadre de l'étude de cas C2

Risque opérationnel	Descriptif du risque / exemples
Fraude interne	-Transactions financières non notifiées intentionnellement, -Transactions financières non autorisées, -Evaluation intentionnellement erronée d'une position financière -Falsification de chèques, contrebande, -Usurpation de comptes, d'identité, -Fraude au crédit, absence de provisions, -Détournement de fonds, corruption.
Fraude externe	-Dommages dus au piratage informatique, -Falsification de chèques, -Intrusion banque en ligne, -Vols d'informations (avec pertes financières).
Pratiques en matière d'emploi et de sécurité du lieu de travail	-Risques relatifs aux contrats de travail, droit social, -Risque sur l'administration, rémunération du personnel, -Chute collaborateurs, -Activité syndicale engendrant une désorganisation de la banque -Discrimination.
Risques liés aux clients, produits et pratiques commerciales	-Manipulation de marché, -Blanchiment d'argent, -Activité réalisée sans agrément, -Vente agressive, -Opérations fictives, -Utilisation abusive d'informations confidentielles, -Atteinte à la vie privée, non respect secret bancaire client.
Dommages aux actifs corporels	Pertes humaines ou matérielles résultant d'une catastrophe naturelle ou d'une catastrophe majeure affectant la banque.
Interruption d'activité et dysfonctionnements des systèmes	-Interruption, arrêt, perturbations des SI, -Dysfonctionnement du plan de secours informatique.
Exécution, livraison et gestion des processus	-Erreurs de modèles (paramétrage), -Erreurs d'exécution d'une opération financière, -Conflits avec les fournisseurs, -Accès non autorisés aux comptes, -Documents juridiques absents, incomplets.

4.2.La formulation des problématiques, les éléments clés de formalisation d'une politique de maîtrise des risques opérationnels.

Le redéploiement de la politique de maîtrise des risques opérationnels au sein de la banque C2 s'est ainsi appuyé sur plusieurs axes.
-Un axe relatif à la refonte des méthodologies d'étude des risques opérationnels (évolution des définitions et objectifs de la filière risque).
-Un axe relatif à l'organisation de la filière risque opérationnel (évolution de l'organisation de la filière risque).
-Un axe communicationnel relatif à la démarche de gestion du risque : identification-évaluation-traitement et suivi des risques opérationnels (Evolution de la démarche de maîtrise des risques et de la cartographie des risques).

4.3.La mise en œuvre d'actions expérimentales pour gérer le risque opérationnel

Afin de répondre aux problématiques préalablement identifiées, nous avons donc mis en place les différentes actions d'évolutions du dispositif de maîtrise des risques opérationnels décrit ci-après.

- **L'évolution des méthodologies d'étude du risque opérationnel, vers une traduction des enjeux de risques opérationnels**

Ce premier axe a consisté, via des groupes de travail internes, à redéfinir les objectifs de la fonction de gestion des risques opérationnels ainsi qu'à transposer la définition réglementaire du risque opérationnel, alors peu parlante, dans un langage commun accessible à tous. Ces actions devant permettre d'adapter la politique de maîtrise des risques opérationnels, alors très axée sur le rappelle de règles et abordant peu des principes d'actions et de gestion.
Le groupe de travail comprenait des membres de la fonction d'audit interne, du contrôle interne, de la fonction conformité, du Risk Management, ainsi que des référents risques des entités métiers et supports (Direction RH, Marketing, Opérations, Finances, Comptabilité, Contrôle de Gestion, Qualité et organisation, gestion d'actifs, banque privée, Direction SI).
La notion de risque opérationnel, s'inspirant d'une définition du risque issue du domaine des systèmes d'information, a été envisagée comme la conjonction d'une menace externe à l'entreprise et d'une vulnérabilité interne à celle-ci, impactant les actifs ou le personnel de l'entreprise (« Possibilité qu'une menace donnée exploite une ou plusieurs vulnérabilités en

impactant un actif (ou un groupe d'actifs) »)[61]. Une menace étant alors définie comme tout évènement ou acte (délibéré ou accidentel) pouvant causer un dommage à l'organisation. Une vulnérabilité consistant en une faiblesse ou une faille pouvant être exploitée par une menace. Un actif étant enfin un élément identifiable du patrimoine de la banque C2 (dont processus, organisation etc.).
La gestion des risques a également été redéfinie de manière commune selon la définition suivante comme un *« processus continu d'amélioration qui commence avec la définition de la stratégie et se poursuit avec l'exécution de celle-ci. Elle devrait traiter systématiquement de tous les risques qui entourent les activités de l'organisation, que celles-ci soient passées, présentes et surtout futures »*[62].

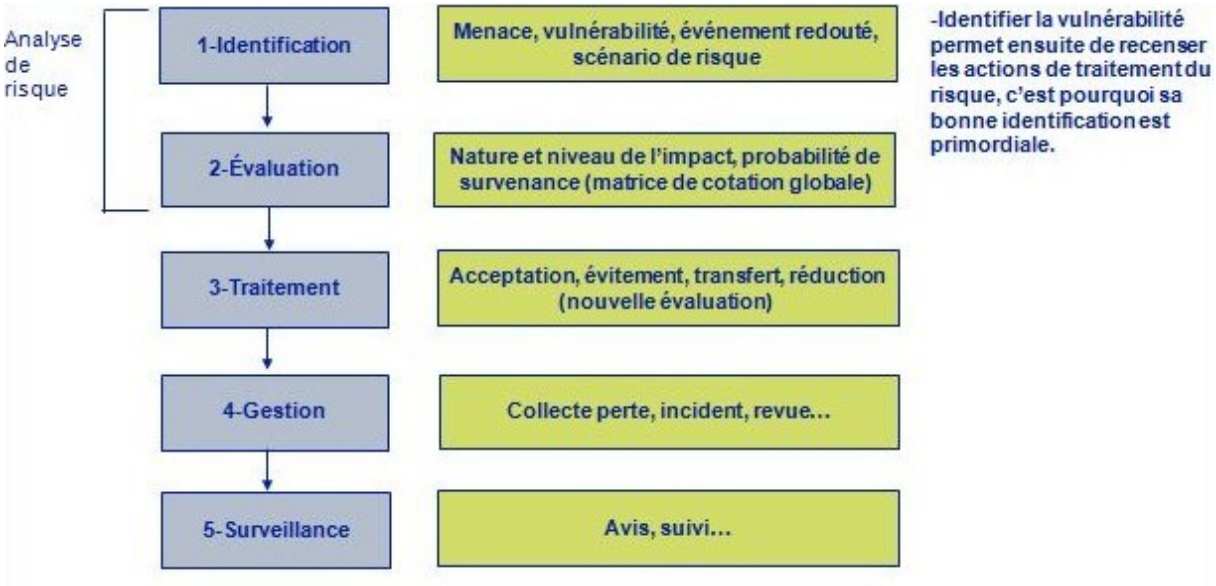
La refonte des méthodologies issues de la politique de maîtrise des risques opérationnels de la banque C2 s'appuya encore sur la détermination des facteurs de risques opérationnels potentiellement destructeurs de valeurs.
La détermination des facteurs destructeurs de valeur comprenait notamment les risques pouvant causer l'arrêt de l'activité, la dégradation de l'image de l'entreprise, la perte de marchés, la perte de chiffre d'affaires, ainsi que les éléments engendrant une chute du cours en bourse ou le non respect des exigences réglementaires.

Cette nouvelle méthodologie a été présentée aux différents acteurs comme une démarche intégrée et commune visant à fédérer les métiers autour du risque opérationnel.

La gestion du risque opérationnel fut également présentée comme un processus transversal de sauvegarde de la valeur qui, grâce à des méthodes et outils (analyse de risque, cartographie, collecte des incidents et des pertes), a pour objectif d'aider la gouvernance de l'entreprise dans la prise de décision face à la potentialité de survenance d'un risque opérationnel voire en cas de survenance d'un évènement de risque opérationnel.
La méthode commune retenue par le groupe de travail « Risque Opérationnel » suivait alors les étapes décrites dans la figure ci-après.

[61] Source : Politique interne de sécurité des systèmes d'information de la banque C2.
[62] Reprenant ainsi la définition de la Federation of European Risk Management Associations.

Figure 36. Méthode commune d'analyse du risque opérationnel, banque C2



L'objectif de ces approches méthodologiques redéfinies de manière partagée était de pouvoir redécliner ensuite ladite méthodologie une fois la seconde étape également revue (évolution de l'organisation de la filière risque de la banque C2).

- **L'évolution de l'organisation de la filière risque, vers une structuration du contrôle**

La notion de filière risque, également redéfinie clairement comme une filière organisationnelle au sein de la banque, commune à plusieurs fonctions et activités de la banque, et ayant pour objectif de s'assurer de la bonne maîtrise des risques opérationnels sur les différentes activités. L'enjeu de cette filière annoncé était de faciliter l'atteinte des objectifs de la banque sur les différents périmètres en s'assurant de la bonne maîtrise du risque opérationnel.

Auparavant la filière risque comprenait un référent par direction mais cette organisation ayant peu évoluée en 5 ans, semblait ne plus correspondre aux réorganisations nombreuses de la banque. Ainsi, de nouveaux processus et de nouvelles activités ont émergé. Ces activités nouvelles, peu maîtrisées, étaient fortement génératrices de risques opérationnels alors même qu'elles se trouvaient hors champ de la filière risque précitée.

Aussi, pour faire face à ces changements, la nouvelle filière risque, en accord avec la gouvernance de la banque C2 a été redéfinie pour comprendre les éléments suivants :

- Le Responsable de chaque activité (nouvelle ou préexistante) est responsable des risques opérationnels sur son entité (responsable de filiale, de direction). Il délègue à un membre de son équipe la gestion et le traitement des risques opérationnels.

- Le Risk Manager (fonction dédiée), rattaché à la direction des risques opérationnels, met en place une coordination dans son domaine métier (exemples : Risk Manager en charge des risques RH, Risk Manager en charge des risques SI). Il assure la supervision de la gestion des risques mais n'est pas propriétaire des risques de chaque fonction métier ou support (les responsables de chaque activité l'étant). Il fournit un accompagnement technique et méthodologique aux entités métiers et ce notamment aux référents risques et aux contributeurs risques.

- La filière risque, est basée sur des référents risques. Les référents sont chargés du reporting sur les risques opérationnels sur leur entités de rattachement (exemple : le référent risque Titre Financiers est en charge de remonter les différents risques opérationnels survenant sur les activités de titres de la banque). Les référents se basent sur des contributeurs risques opérationnels, collaborateurs de chaque entité, le plus souvent experts dans un métier précis. Ils sont en charge du traitement opérationnel des risques en cas de survenance et contribue directement à l'analyse détaillée de chaque risque (exemple : pour les risques opérationnels sur les moyens de paiement, il s'agira de l'expert technique monétique sur les cartes de paiement ou de l'expert technique sur les chèques).

Le tableau ci-après fournit une illustration de la filière risque au sein de la banque C2.

Tableau 29. Illustration[63] de la filière risques opérationnels au sein de la banque C2

Collaborateurs filière	Rattachement	Missions premières	Missions connexes
Risk Manager Banque de détail +Responsable sécurité moyens de paiement +Experts chèques, experts banque en ligne, experts monétique	**Direction des risques opérationnels** Direction des moyens de paiement Direction des moyens de paiement	Identification et évaluation des risques relatifs aux moyens de paiement, aux comptes bancaires, à la banque en ligne Suivi des plans d'actions de traitement-réduction des risques	*Coordination relation autorités de régulation* *Maintien/ évolution de la méthodologie* *Sauvegarde et structuration des données* *Veille réglementaire risques opérationnels*
Risk Manager RH +Référents risques RH +Expert droit social +Expert administration du personnel	**Direction des risques opérationnels** Direction des ressources humaines	Identification et évaluation des risques relatifs aux RH (suivi des compétences, climat social, sécurité du personnel) Suivi des plans d'actions de traitement-réduction des risques	*Elaboration tableaux de bord incidents à fort impact clientèle et analyse*
Risk Manager Finance +Expert Gestion d'actifs, +Expert Opérations Financières	**Direction des risques opérationnels** Direction gestion d'actifs Direction financière	Identification et évaluation des risques relatifs aux activités financières et de gestion d'actifs Suivi des plans d'actions de traitement-réduction des risques	*Mise à disposition des tableaux de bord* *Déploiement analyse stress test* *Elaboration tableaux de bord* *Coordination reporting réglementaire risque opérationnel* *Coordination relation contrôle de gestion*
Risk Manager Assurance +Expert Assurance Vie +Expert Assurance de biens et de responsabilités	**Direction des risques opérationnels** Direction des assurances de personnes Direction des assurances de biens et de responsabilités	Identification et évaluation des risques relatifs aux activités d'assurance (fraude interne, externe, provisionnement-tarification) Suivi des plans d'actions de traitement-réduction des risques	*Devoir de conseil* *Déontologie / fraude interne* *Interlocuteur de la Direction de la Qualité* *Coordination reporting réglementaire risque opérationnel*
Risk Manager SI-PCA +Expert Systèmes d'information +Expert cybercriminalité +Expert PCA	**Direction des risques opérationnels** Direction des systèmes d'information Direction de la sécurité informatique Direction des moyens généraux	Identification et évaluation des risques relatifs à la continuité d'activité et à la sécurité SI Suivi des plans d'actions de traitement-réduction des risques	*Méthodologie mise à jour de cartographie* *Définitions KRI[64]*

[63] Le présent tableau n'est pas exhaustif et présente une illustration de la structuration de la filière risques opérationnels au sein de la banque C2.

[64] KRI : Key Risk Indicators, ou indicateurs clés de risques. Il s'agit d'indicateurs (tout comme les KPI) permettant d'évaluer un niveau de risque sur une activité ou les sources de non performance d'une entité ou d'un processus en termes de risques.

La gouvernance de la filière risques opérationnels : Au-delà des aspects de refonte de l'organisation de la filière risques opérationnels, la redéfinition de la filière de maîtrise des risques opérationnels a consisté à préciser le rôle de la gouvernance des risques, lequel se structure autour de différentes entités que sont les comités des risques opérationnels au niveau local (par entité) et au niveau global (ensemble de la banque).

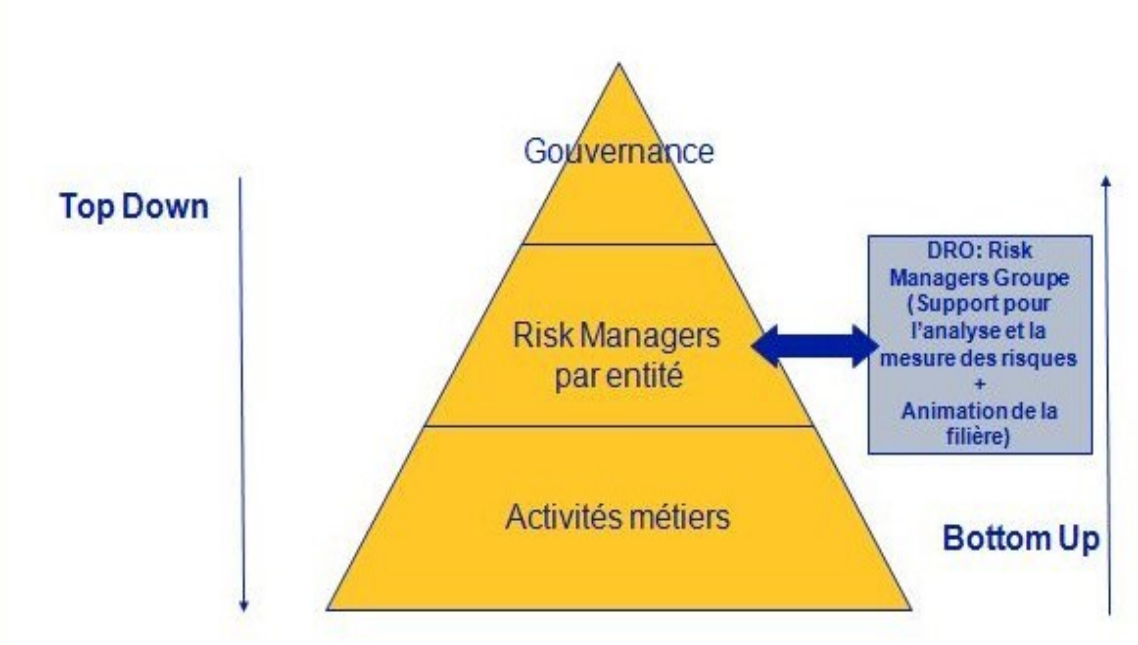
Le Comité des Risques Opérationnels : est présidé par le Directeur des Risques et animé par la Direction des Risques Opérationnels. Il comprend une représentation de chaque Direction, via la présence de Risk Manager pour chaque entité de la banque.

Le comité a pour missions le suivi du déploiement du dispositif risques opérationnels au sein des directions de la banque et de ses filiales, l'analyse régulière des risques majeurs et critiques de la banque, l'examen des incidents critiques détectés, la validation des normes et procédures en matière de risques opérationnels, le suivi des projets sensibles ou structurants en matière de risques opérationnels.

Les Comités des Risques Opérationnels locaux sont mis en place au niveau de chaque entité comportant un Risk Manager et ont des missions identiques au comité des risques global, sous la direction du responsable de chaque entité.

La filière risque opérationnel, ainsi repensée se structure suivant le schéma ci-après :

Figure 37. Filière risques opérationnels de la banque C2[65].



[65] Le cigle DRO correspond à la Direction des Risques Opérationnels au sein de la banque C2.

- **Un axe communicationnel relatif à la démarche de gestion du risque :**

Une autre étape relative à l'évolution de la démarche de gestion des risques opérationnels au sein de la banque C2 a consisté à réaliser plusieurs actions de communication autour des réalisations de la filière risques opérationnels ainsi repensée. Cette étape s'est déroulée tout au long de la recherche-action avec toutefois un investissement temps plus important en fin de mise en place de la nouvelle filière risques opérationnels.
Cette communication a concerné les différentes étapes de la démarche de gestion des risques pour lesquels des réalisations avaient eu lieu (réalisations en matière d'identification des risques, d'évaluation et de priorisation[66] des risques, de traitement et d'actions de suivi des risques).
Ladite communication a été formalisée au travers de :
-newsletters régulières sur les risques opérationnels,
-remontées et redescentes d'informations entre la filière risques opérationnels et les comités risques opérationnels,
-actions de formation-sensibilisation au sein de la filière et en dehors concernant des activités évaluées comme étant davantage sources de risques opérationnels.

Au-delà des aspects organisationnels précités relatifs à la filière risques opérationnels. Cette axe communicationnel visait à renforcer les interactions entre les différents niveaux de contrôles (contrôle interne, Risk Management, Audit interne et inspection) et entre les différents types de contrôles de la banque C2 (contrôle de gestion, contrôle de conformité, contrôle interne, contrôle qualité-réclamations et gestion des risques).

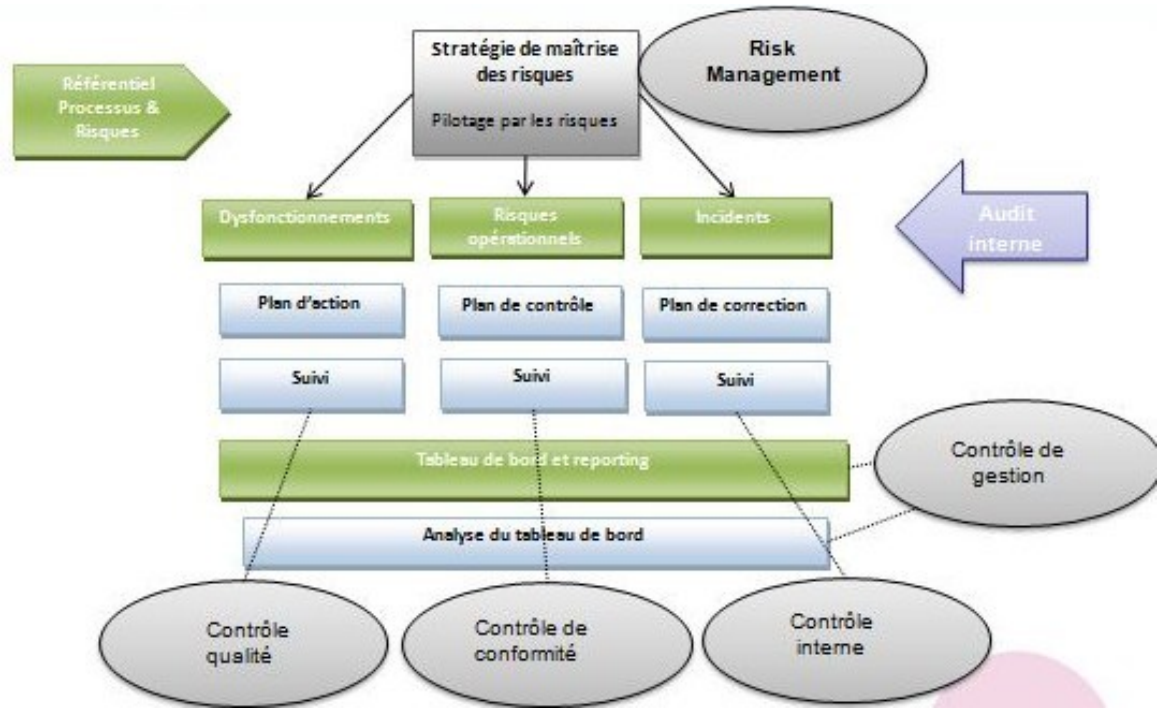
Les différents contrôles au sein de la banque, outre les échanges formalisés dans le cadre de la filière risques, ont alors fait l'objet d'échanges plus importants relativement aux risques opérationnels. L'objet de la recherche-action a été d'instaurer des interactions régulières en vue d'une part, de collecter des informations sur les résultats des activités de contrôles et d'autre part, sur les éléments de risques opérationnels spécifiques à chaque contrôle. Dans cette optique, progressivement, les contrôles ont ainsi été réorientés en vue de s'intégrer à la démarche de gestion des risques opérationnels.

[66] Au sens de la hiérarchisation opérée entre les différents risques, il s'agit de déterminer les risques identifiés et évalués étant les plus critiques (risques majeurs, risques jugés non tolérables dont on souhaite éviter la survenance pour des raisons de coûts en termes financier, d'image ou de qualité de service).

A cet effet le contrôle de gestion a eu pour rôle de structurer les informations comptables et non extracomptables relatives au coût du risque opérationnel. Le contrôle interne, par sa présence dans chaque métier, et en interaction avec les Risk Managers, a permis de collecter des éléments d'identification et d'évaluation des risques opérationnels avérés et potentiels. Le contrôle de conformité a également eu pour rôle d'alerter sur des sources potentielles de risques opérationnels. Le rôle du contrôle qualité a été d'informer la direction des risques opérationnels sur les dysfonctionnements en qualité susceptibles d'être des risques opérationnels.

De telles interactions ont été permises par la clarification des éléments sémantiques et méthodologiques relatifs au risque opérationnel.

Figure 38. Interactions entre types de contrôles banque C2



De tels résultats sont toutefois à nuancer dans la mesure où ces interactions restent variables d'une direction à une autre.

Les actions menées ont permis de faire évoluer le dispositif de maîtrise des risques opérationnels d'une filière principalement axée sur le reporting réglementaire à une filière intégrée de maîtrise des risques.

Cependant, des écueils demeurent dans cette organisation. Sans animation et relances

périodiques des Risk Managers, les différents responsables d'activités et référents risques opérationnels[67] ainsi que les différents acteurs des autres types de contrôles accordent rapidement un temps décroissant aux activités de risques opérationnels pour se concentrer sur leurs autres activités, souvent jugées davantage prioritaires. Une des limites clairement identifiées de la notion de filière risques opérationnels est que celle-ci fonctionne sur la base d'une animation régulière. Sans cette animation, nous avons constaté que les remontées et échanges sur les risques opérationnels avaient tendance à se réduire fortement voire à être laissés en attente au bout de quelques semaines (dans l'attente d'une relance des Risk Managers animant ce dispositif).

4.4.L'élaboration des conclusions de l'étude

A l'appui de cette recherche-action, nous pouvons formuler plusieurs conclusions relativement à l'étude réalisée au sein de la banque C2 sur une période d'intervention de six mois.

Les résultats de l'étude ont été présentés en fin de recherche-action à différents collaborateurs de la banque C2 par ailleurs impliqués dans la filière risques opérationnels ainsi redéployée.
-Nos résultats nous permettent ainsi d'insister en premier lieu sur l'importance de déterminer de manière claire la notion de risques opérationnels ainsi que les notions voisines de celle-ci. Sans cela, il n'y aura pas d'appropriation commune du sujet.

-Egalement, nous constatons que le sujet « risque opérationnel », s'agissant d'un sujet d'inspiration réglementaire, reste peu fédérateur pour les différents collaborateurs de la banque. La nécessité d'une animation régulière du dispositif de maîtrise des risques opérationnels est visible, s'agissant de risques souvent techniques et dont l'impact financier est souvent sous-estimé voire non évalué. Hormis le cas des risques opérationnels extrêmes, pour lesquels la gouvernance est fortement impliquée, nous constatons un faible intérêt pour cette problématique concernant les risques opérationnels de faibles montants unitaires.

[67] Les référents risques opérationnels sont des collaborateurs désignés au sein de chaque organisation pour gérer l'activité de maîtrise des risques. Ils contribuent à l'activité de la filière risques à hauteur de 25 à 30 % de leurs temps d'activité. Le reste de leur temps d'activité est attribué aux activités métiers de leur secteur de rattachement. Un référent RH occupera ainsi 70% de son temps sur des activités de gestion des ressources humaines et 30 % de son temps (en moyenne) sur des activités de gestion des risques opérationnels.

-Autre conclusion importante, au-delà des aspects réglementaires et de formalisation, la réussite de la mise en œuvre d'une politique effective de maîtrise des risques opérationnels passe par des actions de sensibilisation-communication régulières. Ces actions permettent d'objectiver le sujet « risque opérationnel », de le rendre concret et de donner une visibilité à cette problématique qui, sans une communication adaptée, restera un sujet de conformité normative.

L'importance donnée au Risk Manager :

« La direction des risques opérationnels nous apporte une meilleure connaissance de notre activité, des failles existantes. La démarche qui a été initiée est efficace. Celle-ci passe par un recensement exhaustif des incidents et défaillances, de leur quantification afin d'opposer au besoin les coûts engendrés par la non réalisation d'un objectif (et la réalisation d'un risque). Le Risk Management nous apporte une vision transversales des sujets et une facilitation des priorisations à partir de règles partagées » explique ce directeur de l'organisation (C2-11).

« Les gens nous demandent souvent des outils : les cartographies, la base de collecte des pertes et des incidents, la cartographie des procédures. Ces outils ne servent pas sans management réel: personne ne trouve le temps ou l'intérêt de remplir ces outils si on est pas là pour expliquer l'utilité ou pour guider dans la démarche afin de leur faire gagner du temps » confirme ce Risk Manager (C2-7).

« Il y a une interaction forte entre les différents contrôles, sans la direction des risques, on aurait quand même des échanges, mais on parlerait des sujets risques sans le savoir, ou sans faire de véritable analyse » explique enfin ce contrôleur interne (C2-09).

En résumé, l'apport de la recherche-action quant au redéploiement de la politique de maîtrise des risques opérationnels au sein de l'étude de cas C2 se décompose en plusieurs axes :

-mettre en lumière l'importance d'une traduction adaptée à tous de la démarche d'inspiration réglementaire qu'est la gestion des risques opérationnels.

-faire échanger les différents niveaux et types de contrôles autour de se langage commun, cette approche organisationnelle permet ainsi une complémentarité des retours via des spectres d'analyse différents (le contrôle de gestion étant axé performances organisationnelles, le contrôle interne davantage orienté sur la maîtrise des procédures

internes et la conformité étant positionnée sur la veille et le respect des règles internes et externes).

-comme pour l'étude de cas C1, nous soulignons au regard de cette recherche-action l'importance d'une coordination du dispositif de contrôle des risques. Bien que différents acteurs composent ce dispositif et qu'il fut préexistant, nous constatons qu'il s'agit d'un sujet d'amélioration continue concernant le management actif. Ce pilotage semble essentiel pour rendre la démarche de maîtrise des risques opérative et pour ne pas la limiter à une réponse normative.

II-Les résultats issus des entretiens confirmatoires : une critique convergente de la norme de contrôle, un besoin partagé de structuration

Cette seconde partie présente les principaux résultats issus des entretiens confirmatoires. Ces entretiens avaient pour but d'expliciter les constats initiaux réalisés lors de nos études de cas.

Les résultats issus de nos entretiens se structurent selon plusieurs thématiques de recherche que sont :
-le rôle essentiel des normes dans le contrôle des risques opérationnels (dont le sous-thème est l'enjeu de responsabilisation des acteurs)
-l'enjeu majeur de structuration du contrôle (dont les sous-thèmes évoquées sont ceux issus du cadre de pensée structurationniste),
-le thème de recherche relatif à la théorie de l'acteur-réseau (dont les sous-thèmes concernant la traduction des normes et rôle du Risk Manager en tant qu'acteur-réseau).

Vis-à-vis de ces différents thèmes plusieurs axes transverses ressortent de notre analyse de contenu :
-un axe central relatif au sens des contrôles et au sens des normes de contrôle,
-un axe de recherche relatif aux interactions entre fonctions de contrôles de diverses natures,
-un axe concernant le rôle de l'enjeu de gestion des risques comme facteur permettant d'initier le changement organisationnel.

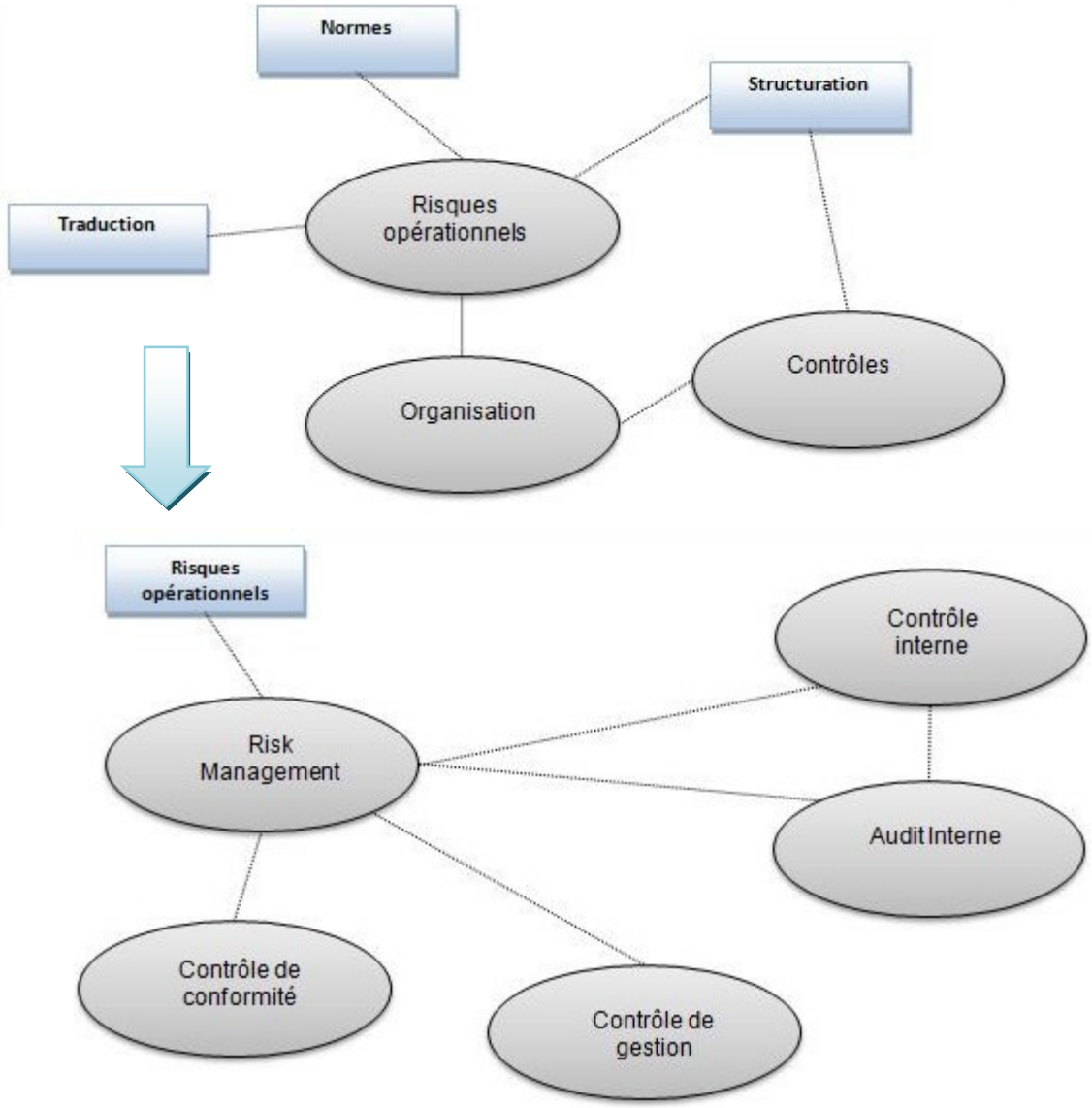
A titre indicatif l'annexe 11 présente plusieurs exemples d'entretiens retranscrits. Pour des raisons de présentation des annexes, l'ensemble des entretiens n'a pas pu être ajouté au document de thèse.
Les tableaux et figures ci-après résument les extractions faites du logiciel NVivo sur la base des entretiens réalisés et retranscrits.
Au total 63 heures et demi d'entretiens confirmatoires ont été réalisées et retranscrites (près de 260 pages d'entretiens restranscrites).

Le tableau ci-après résume les résultats de la requête faite sous le logiciel Nvivo quant aux termes les plus fréquents en lien avec le rôle du Risk Manager au regard du contrôles des risques opérationnels.

Tableau 30. Résultats de la requête sous NVivo (fréquence des mots, synonymes inclus)

Termes employés	Nombres d'entretiens concernés (sur 50)	Mots similaires
Analyse	18	Analyse causes-conséquences, causes racines, solutions
Animation	36	Animer, coordonner, coordination
Audit Interne	16	Contrôle périodique, inspection
Communication	41	Communiquer, échanger, échanges
Contrôle de gestion		Performance
Contrôle interne	36	Contrôle permanent, contrôle de 1er niveau, contrôle de second niveau
Coûts cachés	5	Performances cachées
Décision	23	Aide à la décision, facilitateur, fédérateur
Effectivité	28	Effectif, Effective
Efficace	16	Efficacité
Efficience	17	Efficient
Filière	22	Filière risque, Filière risque opérationnel
Fonction	31	Fonctions clés, fonction risque, fonction d'audit interne, fonction de contrôle interne, fonction conformité
Formation	24	Former, faire comprendre, information
Gouvernance d'entreprise	32	Politique, dirigeants
Incidents	29	Pertes opérationnelles, dysfonctionnements, incidents majeurs, incidents significatifs
Interactions	33	Interagir, actions inter-groupes, mobiliser
Méthodes	21	Méthodologies, outils, appui méthodologique
Normativité	17	Normatif, normes
Organisation	46	Organisationnel
Qualité	16	Gestion de la qualité, contrôle qualité
Régulation	47	Réguler, prudentiel, réglementation
Risk Manager	50	Risk Management, gestionnaire de risque, contrôleur des risques
Risque opérationnel	50	Risques opérationnels, risques organisationnels
Sensibilisation	38	Sensibiliser
Stratégie	11	Stratégique
Traduction	20	Clarification, explication, traduire
Valeur	17	Sauvegarde de la valeur, limitation des coûts

Figure 39. Synthèse des thèmes en lien avec le contrôle des risques opérationnels



Les résultats des entretiens confirmatoires, ainsi présentés, sont décrits ci-après en abordant successivement l'apport de notre recherche relativement à la compréhension de la notion de risque opérationnel, les enjeux de traduction que recouvrent les normes de contrôles des risques opérationnels ainsi que la perspective de structuration du contrôle.

1. La notion de risque opérationnel : l'apport de la recherche pour comprendre comment appréhender un objet complexe

De nos différents entretiens confirmatoires, il ressort en premier lieu des éléments relatifs à la compréhension même de la notion de risque opérationnel telle qu'elle découle de la réglementation prudentielle.

-Une tentative de définition du risque opérationnel : Nos différents entretiens nous orientent vers les difficultés principales posées par la définition réglementaire du risque opérationnel.

Ces difficultés sont doubles :

-couvrir l'étendue du périmètre qu'englobe la notion de risque opérationnel eu égard à sa définition extensive,

-comprendre la réalité des dispositifs de maîtrise des risques et de contrôles qu'implique une telle définition.

La notion de risque opérationnel explicitée lors de nos entretiens :

« Le risque opérationnel ce n'est pas tant un problème de définition que de traduction concrète de ce qu'attend le régulateur : avoir des dispositifs de maîtrise des risques qui répondent à l'exposition réelle de l'entreprise » résume ce directeur de la sécurité financière, EC-26, janvier 2013.

« Quand vous avez plus de 90 000 alertes sur près d'un million d'opération, on constate que votre dispositif risque opérationnel est en place, mais très vite on s'aperçoit qu'il faut de vrais moyens et une logique implacable pour filtrer ce qui est vraiment du ressort du risque opérationnel, appelant des actions concrètes, de ce qui est considéré comme 'normal' » conclu ce directeur des risques, EC-4, septembre 2012.

Ainsi, selon ces entretiens, la notion même de risque opérationnel est à dépasser pour s'orienter vers l'interprétation qui peut en être faite au travers de dispositifs opératif et clairement mis en œuvre.

Certains entretiens nous amènent à insister sur l'idée qu'une telle notion reste source de confusion. La notion de risque opérationnel peut constituer un frein.

Difficulté de traduire la notion de risque opérationnel :

« On est dans le risque opérationnel à chaque opération, la complexité de notre métier c'est de retraduire ce risque dans les métiers concrets » explique ce directeur des risques, (EC-15, novembre 2012) ; ce que complète ce consultant-expert risque, EC-2, juillet 2012, *« le risque opérationnel reste un sujet récent, cela date de 1998, avec le comité de Bâle. On a commencé à en parler vraiment à partir de 2001, le risque opérationnel est un sujet très vaste, qui couvre tous les domaines de l'entreprise. »*

Nécessaire interprétation de la notion issue du cadre réglementaire :

Face à cette difficulté, il existe donc un vrai enjeu d'interprétation de la notion telle qu'elle découle de la réglementation. *« Par rapport au risque opérationnel, notre vrai souci est de pouvoir être en sécurité dans la durée, pas seulement si l'on avait l'équivalent de " Kerviel ", mais sur les moyens de paiement, sur les crédits, sur les SI, on cherche à montrer en interne comme en externe que tout est sous contrôle, en permanence, qu'il n'y a pas de zone d'ombre et que l'on est réactif »* évoque ce directeur du contrôle interne (EC-28, janvier 2013). Egalement, pour ce Risk Manager (EC-22, décembre 2012), *« identifier les risques opérationnels, c'est beaucoup de formalisation et de formation à la prévention, on considère que l'on répond à l'esprit de la réglementation si les opérationnels font attention aux risques dont ils sont propriétaires. »*

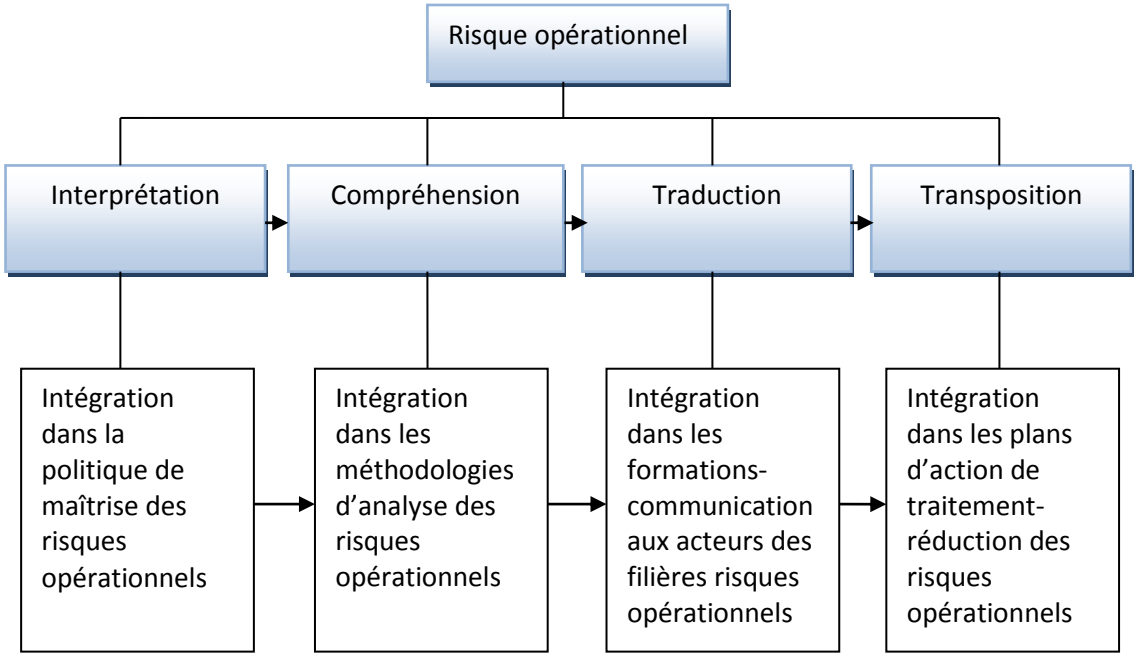
Pour d'autres experts de cette thématique, l'explication est encore à rechercher dans le niveau d'expérience des contrôleurs des risques, préparés à la survenance de ces risques.

« La gestion des risques opérationnels est un sujet d'expertise, on doit être passé par les activités opérationnelles auparavant car il faut montrer qu'on connaît les préoccupations métiers et managériales et surtout savoir quand et sur quoi apporter de la valeur : service, conseil, rentabilité de notre fonction par rapport à son coût. On doit avoir une bonne connaissance de notre activité et de ses failles et mettre en lumière ce à quoi les métiers n'ont pas pensé » explique ce risk manager (EC-36, février 2013).

« Le risque opérationnel est inéluctable car lié au facteur humain, on ne pourra jamais vraiment le mettre sous contrôle mais juste envisager des postures et des habitudes de raisonnement par rapport à ce dernier » résume encore cet analyste risque (EC-44, mars 2013).

La figure ci-après résume ainsi les différents questionnements posés par l'enjeu de risque opérationnel tels qu'ils ressortent de nos entretiens. La prise en compte de la norme de contrôle du risque opérationnel suppose différentes étapes dont, en premier lieu, l'interprétation faite par les acteurs de la notion. Cette interprétation arrive au préalable, après-même la compréhension (et non l'inverse) car en l'absence d'une compréhension claire et partagée dans le secteur financier celle-ci reste interprétative d'une entité à l'autre (quant à son périmètre principalement). La compréhension qu'en ont les acteurs permet ensuite une traduction au sein de l'entreprise puis sa transposition au travers d'action concrètes.

Figure 40. Les questionnements posés par le risque opérationnel, résultante des entretiens confirmatoires



2. Le rapprochement entre terrains de recherche et grilles de lecture théoriques

2.1.L'enjeu de structuration en matière de risques opérationnels

Ces constats relatifs aux enjeux de normes et de contrôle sont complétés dans nos entretiens par des retours expériences afférents au besoin réel de structuration de l'enjeu de contrôle des risques opérationnels. Reprenant la grille de lecture issue de la théorie de la structuration, les éléments ci-après nous fournissent une certaine compréhension de ce besoin de structuration.

-Le risque opérationnel, un système abstrait à objectiver

Nos entretiens tendent à étayer les constats précédemment évoqués relativement aux enjeux de structuration du contrôle des risques opérationnels. Ces constats renforcent l'idée que face aux mécanismes de la modernité (cités dans le chapitre théorique), la pédagogie par l'exemple permet de *« concrétiser »* une matière parfois obscure du fait de sa variabilité intrinsèque (variabilité selon le département et le métier abordé, variabilité de la notion entre risque de fréquence, de sévérité, risque frontière à plusieurs départements et concernant plusieurs processus etc.).

<u>L'étendue de la notion de risque opérationnel :</u>

Pour ce directeur d'audit interne, EC-3, septembre 2012, *« La variabilité du risque opérationnel est le plus dur à comprendre. Peu d'organisations ont compris ce qu'est le risque opérationnel. Au-delà des catégories baloises, il y a des catégories de risques opérationnels spécifiques pour chaque entreprise : entre une banque et son GIE le risque opérationnel n'est pas forcément le même. » ; « Nous sommes sur des postes qui demandent beaucoup d'abstractions, de schémas et de représentations. C'est l'un des postes qui demande le plus de vision de l'organisation. Il y a un vrai enjeu de capitalisation des connaissances et de maturité »* nous confie également un directeur des risques opérationnels, EC-9, octobre 2012.

« Les risques opérationnels, c'est très confus, c'est difficilement explicable même dans la banque de détail. Même au niveau des tops managers ou des auditeurs, il faut passer par des exemples pour que cela devienne plus clair » précise encore cette directrice du contrôle interne, EC-42, mars 2013.

Outre la dimension de système abstrait que revêt le risque opérationnel, nos entretiens nous orientent également vers un second enjeu de structuration qu'est la dimension expert du risque opérationnel.

-Le risque opérationnel et le poids des systèmes experts, une structuration des contrôles

Nos études de cas ainsi que les différents entretiens auprès de directeurs risques opérationnels et Risk Manager tendent à confirmer qu'il existe un enjeu fondamental de compétence de la fonction gestion des risques opérationnels. Cet enjeu de compétence implique une double contingence :

-une bonne connaissance de l'organisation, de l'histoire de l'entreprise, de sa stratégie et de sa structure de gouvernance. Cet enjeu de connaissance de l'organisation est indissociable du second axe, l'expertise opérationnelle.

-l'expertise métier sur le domaine d'activité (portefeuille d'activité) géré par le Risk Manager. Le Risk Manager doit avoir une bonne compréhension des enjeux techniques et managériaux propres à chaque métier pour lequel lui pilotage des risques lui est attribué, raison pour laquelle en banque et en compagnie d'assurance les Risk Manager sont spécialisés par métier ou par pôle d'activité (par exemple : les moyens de paiement, le plan de continuité d'activité, la sécurité des biens et personnes, les risques SI, les risques liés à la distribution de services financiers, la fraude interne et externe, les risques opérationnels liés à la gestion d'actif et aux activités de marché ou encore de crédit, les risques liés à l'assurance vie et non-vie).

On retrouve également cet enjeu de compétence en contrôle et audit interne : la nécessité de connaitre le métier contrôlé ou audité en vue d'émettre des recommandations ou actions curatives pertinentes et intelligibles pour les entités opérationnelles. La différence concernant le Risk Management Opérationnel est que cette compétence *« expertise et connaissance interne »* est le levier principal de création de valeur pour une fonction souhaitant être perçue comme ayant un rôle partenarial d'animation et non un rôle coercitif de contrôle.

L'enjeu d'expertise trouve alors du sens pour réduire les conflits entre acteurs : notamment sur des catégories de risque opérationnel telles que l'obligation de conformité (risque de conformité), le respect du devoir d'information et de conseil (risque juridique), ou les conflits d'intérêts par une double prise de position antinomique (placement compte propre/compte de tiers par exemple). Le recours à des experts est structurant comme le confirment nos entretiens.

<u>Le risque opérationnel une affaire d'experts :</u>

« La gestion des risques opérationnels est un sujet d'expertise, on doit être passé par les activités opérationnelles auparavant car il faut montrer que l'on connait les préoccupations métiers et managériales et surtout savoir quand et sur quoi apporter de la valeur : service, conseil, rentabilité de notre fonction par rapport à son coût. On doit avoir une bonne

connaissance de notre activité et de ses failles et mettre en lumière ce à quoi les métiers n'ont pas pensé » explique ce Risk Manager, EC-36, février 2013.

Pour cette directrice des risques opérationnels, EC-37, février 2013, l'enjeu d'expertise implique une indispensable présence d'acteurs fédérateurs : *« Nous avons une nécessaire présence et des relais dans les différents métiers et fonctions mais notre direction comprend des profils experts variés issus de l'audit, du marketing, des différents métiers opérationnels. Un adjoint direction des risques de manière plus globale. Des profils MOA pour la partie outil et des anciens consultants risques opérationnels* ».

L'enjeu d'appui par l'expertise est également important pour comprendre la norme comme l'évoque ce directeur du contrôle interne, EC-21, décembre 2012 : *« De plus, le régulateur n'offre pas toujours une compréhension claire du sujet, on se situe dans un carcan politique. Les comités risque opérationnel sont l'affaire de quelques experts en France. »*

Toutefois, l'expertise face au risque est davantage un enjeu de compréhension des bonnes attitudes à adopter et se formalise davantage par un rôle d'influence plus que de coercition des acteurs en charge de la politique de risque. *« Fondamentalement, le rôle de la Direction des risques opérationnels est un rôle d'influence. Sauf à ce que la Direction lui confie l'entière propriété des enjeux et des responsabilités associées, le Risk Management conseille, évalue, identifie, préconise, propose et met en œuvre sur certains sujets »* nous précise cette consultante-spécialiste des risques opérationnels, EC-1, juillet 2012.

Nos entretiens permettent d'insister sur l'importance de la technicité comprise dans le contrôle des risques opérationnels, à la fois pour discerner les vraies sources de risques opérationnels, mais aussi pour comprendre et adapter les exigences de contrôle à chaque métier / fonction / processus. Cette adaptation suppose une vraie connaissance des activités. Pour certains des interlocuteurs rencontrés, le meilleur expert en risque opérationnel est encore le collaborateur dans chaque métier, un bon expert risque opérationnel est un expert « métier », d'où l'importance des enjeux de filières risques reposant sur des référents métiers et sur des contributeurs techniques dans chaque fonction de l'entreprise.

-Le risque opérationnel et le sentiment de sécurité ontologique

L'un des objectifs des dispositifs de contrôle et de gestion des risques opérationnels est de contribuer à la sécurisation des activités dans l'entreprise par la construction progressive d'une traçabilité des informations et d'une formalisation des processus et activités. Cette sécurisation pour les opérationnels et les managers consiste à déterminer quels sont les risques de chaque activité pour savoir quand les accepter en l'état, quand les réduire et quand les accepter après mise en place de dispositifs de prévention et de protection voire quand refuser de s'engager dans une activité pour lesquels les risques sont inacceptables (par exemple lorsque le risque de réputation est fort ou que le risque de fraude est impossible à maîtriser ou à un coût dépassant la rentabilité escompté d'un produit).

Cette sécurité est permise par une interaction entre les acteurs du dispositif de gestion des risques : notamment entre les différents Risk Managers au sein des entités et les acteurs en charge du contrôle. Les premiers s'assurant, par leur influence et leur proximité avec la Direction Générale, du respect des processus mis en œuvre et de la réduction des intérêts divergents pouvant empêcher ou freiner cette mise en œuvre. Cette contribution au sentiment de sécurité a également lieu par la diffusion des conseils et méthodologies de maîtrise des risques par la direction des risques. Il s'agit des méthodologies inspirées des dispositifs normatifs tel ISO 31000 : *« Management du risque, principe et lignes directrices »* ou encore sur des axes spécifiques tel ISO 27001 : *« Management de la sécurité des systèmes d'information ».*

Pour ce directeur des risques, EC-4, septembre 2012*, « Le risque opérationnel, c'est plus un problème de traçabilité que de conformité à la norme, on est conforme mais le problème est de prouver qu'on l'est. Le problème c'est d'avoir la piste d'audit, dans l'ère du reporting, nous n'avons plus le choix. »* Elles permettent de clarifier des méthodologies d'identification de risque en vue de se prémunir contre les menaces de l'environnement externe (fraude externe aux moyens de paiement ou aux assurances venant de réseaux organisés, tentative de blanchiment d'argent, cybercriminalité et intrusion dans les systèmes d'information en vue de récupérer des données clients etc.).

Comme ce directeur des risques opérationnels, EC-32, février 2013, nous le précise : *« sur le risque opérationnel, ce qui compte ce n'est pas tellement les outils ou le fait d'avoir bien tout*

renseigné, on estime que l'on a fait notre travail quand on sait qu'un projet lancé est sous contrôle ou que sur un périmètre on a enrayé les pertes. »
Ces méthodologies et conseils d'implémentation diffusés par périmètre métier sont encore le moyen de réduire les vulnérabilités internes de l'entreprise (déterminer où introduire des visas informatiques bloquant, réguler la politique d'habilitation des traders entre le front, middle et back office en vue de réduire les pratiques de type « rogue trading ».

Outre ces pratiques de conseil interne, les directions des risques opérationnels contribuent à ce sentiment de sécurité par la réalisation d'analyses détaillées sur les sujets sensibles de l'organisation en lien avec les périmètres de contrôle fonctionnels (contrôle de conformité, contrôle de gestion, contrôle interne etc.) ; analyse servant de rôle d'alerte de la gouvernance le cas échéant.

Nos différents entretiens abondent dans le sens d'une sécurisation plus grande de l'activité comme apport de la fonction risques opérationnels, il s'agit d'un apport perçu comme essentiel en complément de la réponse à la norme de contrôle.

-Tradition et risque opérationnel : la création de routine comme moyen de contrôle

La tradition en tant qu'ensemble structuré et organisé de croyance et de pratique constitue en matière de risque opérationnel la manière dont le Risk Management va créer, instaurer et développer des habitudes de fonctionnement et des usages face au risque. Il s'agira de la réalisation de fiche d'analyse de risque avant tout lancement de nouvelles activités, de nouveaux produits. Un produit financier devra être analysé en termes de risque et faire l'objet d'un regard critique sur ce point en comité nouveau produit voire en comité risque opérationnel. Si les directions des risques n'ont pas un rôle officiellement bloquant, nos études de cas et entretiens révèlent qu'il s'agit davantage d'un rôle d'influence dès lors que les conseils fournis par les Risk Managers sont reconnus, un avis leur est demandé sur l'opportunité de ces nouveaux projets ou produits. En pratique, cet avis peut s'apparenter à un « droit de veto » sur le lancement de ces activités nouvelles lorsque les risques sont jugés non acceptables ou non maîtrisés. Cette pratique de reconnaissance tacite par l'usage tend à créer une tradition consistant à se tourner systématiquement vers la direction des risques en tant qu'aide méthodologique pour la réalisation de l'analyse de risque et en tant « qu'expert

conseil » pour l'étude d'opportunité (arbitrage gains/coût du risque). In fine, il revient au métier opérationnel et aux différents managers de prendre la décision.

« Notre préoccupation vis-à-vis des contrôles c'est de rester pertinent, le risque évolue en permanence, on doit cependant maintenir un équilibre et une certaine stabilité dans nos pratiques. La gestion des risques, c'est prendre en compte la somme des déséquilibres, stabiliser mais aussi challenger dans le même temps » nous explique cette directrice des risques opérationnels, EC-39, février 2013.

De telles pratiques sont aujourd'hui développées afin de construire des habitudes managériales. L'un des écueils consiste en la « routinisation » desdites pratiques liées à leur trop grande industrialisation. Nos entretiens révèlent qu'il est illusoire de vouloir développer cette habitude de reporting et de conseil dans toute l'organisation et sur toutes les lignes métiers : cela suppose des lourdeurs de gestion et des moyens importants en termes d'effectifs que n'ont pas nécessairement à ce jour les directions des risques opérationnels. L'industrialisation du contrôle constitue en outre un frein à cette logique d'influence car elle donne une dimension « administrative et bureaucratique » au travail de gestion des risques sensé être basé sur l'échange, la communication et le partage d'informations sur des sujets stratégiques.

Pour ce Risk Manager, EC-16, décembre 2012, *« Identifier les risques opérationnels, c'est beaucoup de formalisation et de formation à la prévention, on considère que l'on répond à l'esprit de la réglementation si les opérationnels font attention aux risques dont ils sont propriétaires. »*

Ce que confirme ce directeur d'audit interne, EC-31, février 2013 : *« Le travail sur le risque reste administratif et technique pour beaucoup, mais on peut penser qu'il y a une part de créativité et de réflexion pour aller chercher les risques non identifiés. C'est en partie de la Recherche & Développement. »*

Nos entretiens illustrent clairement la réponse aux enjeux de confiance moderne tels que décrits par Giddens (1994). En cela qu'elle répond aux différents critères de maintien de la confiance dans l'organisation, la fonction de gestion des risques opérationnels contribue à

structurer la réponse attendue de la norme de contrôle du risque opérationnel en termes de sécurisation de l'activité.

2.2. Enjeux de traduction et positionnement du Risk Manager en tant qu'acteur-réseau

Outre ces enjeux de structuration du contrôle des risques opérationnels. Nos entretiens révèlent également un axe essentiel relatif à la nécessité de traduire la norme relative à l'application des politiques de maîtrise des risques opérationnels. Il apparait à cet égard que le Risk Manager joue un rôle clé (traduction de la norme de contrôle) d'acteur au centre d'un processus d'interaction et de co-construction de connaissances.

-Le risque opérationnel : une zone de confusion, un enjeu de discernement du contrôle

Il ressort des entretiens réalisés que la notion de risque opérationnel recouvre pour les managers et opérationnels plusieurs réalités distinctes. Une confusion du rôle de certaines fonctions est parfois observée et la définition même du risque opérationnel apparait comme source d'ambiguïté dès lors qu'elle ne s'accompagne pas d'un référentiel clair et intelligible pour des non spécialistes. Ce type de constat a un impact important sur la compréhension de l'usage des outils et méthodes (scoring, cartographie, bases d'incidents et de pertes) mais aussi du rôle de chacun au sein de la filière de gestion du risque opérationnel.

<u>Le nécessaire encadrement de la notion de risque opérationnel :</u>
Cette directrice d'audit interne, EC-43, mars 2013, évoque ainsi : *« Le risque opérationnel nécessite toujours beaucoup de pédagogie pour ne pas perdre les collaborateurs dans des débats interminables. Les métiers ont conscience de leurs risques mais ils ne savent pas toujours mettre une étiquette sur ce sujet ou même apporter une solution efficace. »*

Pour ce directeur des risques, EC-15, novembre 2012, *« Pendant longtemps le contrôle n'a pas eu beaucoup de sens, l'objectif était de mettre en place un contrôle de premier et deuxième niveau, quelque soit le risque derrière, pour faire plaisir au régulateur. Cela explique que tous les contrôles étaient vus de la même manière sans vrai lien avec le risque et entre les risques ».*

Ce que complète cet autre directeur des risques, EC-48, avril 2013 *« L'un des vrais problèmes avec le risque opérationnel, c'est que les définitions données et la typologie de Bâle sont vastes et que l'on y confond causes et conséquences ».*
Des propos relayés par ce consultant expert risque, EC-6, septembre 2012, *« Si le référentiel de risque est trop large, il ne parle plus aux métiers, s'il est trop précis, il est rapidement inexploitable et l'on confond de nombreuses notions…on ne parle plus de risque opérationnel au final. »* ainsi que par ce directeur de l'audit interne, EC-13, novembre 2012 *« On tente de s'appuyer sur les référentiels existants et sur les best-practices de la place mais dans l'entreprise on se pose encore trop peu la question de leur adaptation. »*

L'une des difficultés à laquelle doivent répondre les dirigeants d'une entreprise est de faire travailler ensemble plusieurs fonctions distinctes qui ont toutes un intérêt à la gestion des risques opérationnels : l'audit interne, la conformité, le contrôle interne, le Risk Management. Si les fonctions sont distinguées par les métiers, ceux-ci ne perçoivent pas de manière claire le rôle de chacun en matière de gestion du risque opérationnel, ce qui leur donne l'impression de répondre de manière redondante aux différentes questions posées.

<u>Nécessité d'une réelle collaboration entre les différentes fonctions :</u>
Ces constats sont confirmés par ce directeur des risques, EC-14, novembre 2012, *« Les métiers ont souvent beaucoup de mal en pratique avec les nombreuses fonctions auxquelles ils doivent faire remonter des reporting, en plus de leurs objectifs business courants. »* ainsi que par ce Risk Manager, EC-20, décembre 2012, *« On déplore le manque voire l'absence de relations entre contrôle interne et contrôle de gestion. Ce fonctionnement en silo nui à notre efficacité et l'on se retrouve à produire de l'information que le contrôle de gestion pourrait nous fournir rapidement. Les métiers s'en rendent parfois compte, il nous demande pourquoi on se marche sur les pieds au lieu de gagner du temps »* ou encore par ce directeur d'audit interne, EC-33, janvier 2013, *« Nos métiers manquent souvent de communication sur les orientations du contrôle alors que c'est fondamental pour qu'ils en voient l'intérêt. Quand ils s'y intéressent, il faut reconnaître qu'il est dur de voir qui fait quoi, déjà pour nous, a fortiori pour ceux dont ce n'est pas la spécialité. »*

Au-delà de ces aspects de confusions que doit lever le Risk Manager en charge d'animer la filière de gestion des risques opérationnels, un réel aspect contribuant à rendre effective ladite filière concerne la co-construction de connaissances sur un sujet encore émergent.

-Le Risk Manager et la co-construction de connaissances tournées vers l'action : un enjeu de traduction

Face aux multiples confusions constatées, le Risk Manager a pour mission de faciliter la traduction de cet objet frontière qu'est le risque opérationnel (processus comprenant : confusion => traduction => compréhension) mais aussi l'appropriation par la mise à disposition de clé de lecture et d'action tels que la construction d'un référentiel, la mise à disposition et la co-construction de connaissances du risque via des scénarios d'occurrence (compréhension => appropriation => action et anticipation). Une telle approche vise à transcender la simple approche de contrôle conformiste, empreinte de routinisation, et parfois trop axée vers la description des risques passés de l'entreprise.

« On est très vite confronté à une surcharge de données difficiles à traiter car chronophage et parfois sujettes à interprétation. Notre rôle est donc de permettre de réduire le travail pour les métiers en les faisant aller à l'essentiel » précise ce Risk directeur des risques, EC-40, mars 2013. Propos étayés par ce directeur de la sécurité financière : *« On a beau sensibiliser les métiers aux dangers de la mer, cela n'empêchera pas la tempête mais l'on pourra se mettre à l'abri. Il faut garder en tête que pour les opérationnels, cette notion et ces règles, c'est compliqué, on doit rendre cela parlant pour eux. »* EC-26, janvier 2013 ou encore par ce consultant expert risque opérationnel, EC-35, février 2013 *« L'objectif à ce stade, ce n'est plus tellement de déployer des contrôles, c'est d'aller vers une vraie intelligence du risque, que cela serve les opérationnels et réponde à la norme. »*

La traduction des enjeux de risques opérationnels implique une certaine compréhension des actions à réaliser relativement au risque opérationnel. A cet égard, la créativité dont doit faire preuve le Risk Manager est alors un sujet clé contribuant à l'effectivité de la démarche de gestion des risques opérationnels.

-De la traduction à la compréhension des actions à mettre en œuvre pour gérer le risque opérationnel : la créativité du Risk Manager comme compétence clé

Nos études de cas nous amènent à préciser le fait que si les risques opérationnels font l'objet d'un reporting important dans les entreprises étudiées, ce simple reporting doit être dépassé

pour aller vers une vraie intelligence du risque qui suppose une créativité dans les démarches et méthodes.

Comme le confirment nos entretiens, cette créativité se retrouve au stade de la pédagogie déployée par le Risk Manager pour faire comprendre les enjeux rattachés au besoin réglementaire de reporting. Fédérer et sensibiliser implique des méthodes simples et claires mais aussi le fait de pouvoir tester et remettre en cause fréquemment les contrôles et les actions mises en œuvres pour cerner le risque opérationnel.

Le risque opérationnel comme vecteur de créativité :

« La créativité peut servir pour penser la diversité des risques opérationnels, imaginer ce qui ne serait pas encore survenu, ou pour sortir du factuel et du constat qu'on est sur un risque subi », commente ce directeur de l'organisation, EC-24, janvier 2013.

Pour ce directeur des risques, EC-7, septembre 2012, *« Le contrôle doit rester factuel et objectif, mais être créatif en la matière c'est penser de nouvelles formes de contrôle, changer nos critères, nos délais, nos périmètres de contrôle, on doit en permanence challenger le contrôle. »*

Propos que confirme ce Risk Manager-analyste risques, EC-44, mars 2013 *« Il faut arriver dans une logique où l'on contrôle par motivation, en se disant que c'est utile : on a recours aux scénarios, on fait participer les dirigeants mais aussi les opérationnels, en faisant appel à leur imagination mais surtout à leurs regards critiques sur leur travail, c'est très proche des cercles de qualité en fait et on ne parle expressément de la réglementation que si le métier le demande. »*

Ce consultant risque opérationnel, EC-8, octobre 2012, développe ainsi le fait que : *« Vendre le risque opérationnel et sa gestion au métier, c'est un sujet complexe de marketing, il faut être à la fois des communicants, des data miner, des créatifs, qui rendront ce sujet intelligible, mais aussi attrayant et utile. »*

Un directeur du contrôle interne, EC-47, mars 2013, nous précise encore *« Nous avons créé un groupe collaboratif où nous échangeons sur les problèmes risques opérationnels. On fait des newsletters, on propose des outils simples et clés en main, surtout nous faisons un retour régulier avec des sortes de notes d'analyse permettant aux métiers de se forger une réelle*

compréhension de ce sujet technique. » De tels constats sont corroborés par cette contrôleuse interne, EC-18, décembre 2012, *« La créativité dans le contrôle c'est de ne jamais faire la même chose, de ne pas céder à une routine. Mais aussi de savoir choisir ses mots : que cela soit clair pour tout le monde sans heurter des susceptibilités ou susciter des craintes. »*

Outre ces éléments, nos données de terrains issues des entretiens confirmatoires confirment également la nécessité d'appréhender le rôle du Risk Manager en tant qu'acteur réseau agissant sur les 4 axes développés dans la théorie de l'acteur-réseau.
Concernant ces différents axes, nous développons également les principaux retours d'expériences issus des entretiens.

Par ailleurs, en cohérence avec les apports de Callon et Latour (1981), les résultats de nos entretiens abondent dans le sens d'une transposition de la théorie de l'acteur-réseau, figure interprétée ici par le Risk Manager.

-La problématisation de l'enjeu prudentiel « risque opérationnel » réalisé par le Risk Manager

Le rôle du Risk Manager face à la problématique du risque opérationnel est pluriel comme le confirment nos entretiens avec différents spécialistes de cette thématique. Ce rôle va ainsi de la réponse aux exigences réglementaires et de reporting prudentiel à la définition de véritables politiques orientées vers une gestion réelle des risques, en lien avec la stratégie d'entreprises et en fonction du contexte organisationnel de chaque entreprise.

Ce rôle est ainsi décrit comme celui d'un acteur proactif, ayant non seulement des compétences techniques une bonne connaissance de l'organisation et des capacités relationnelles avérées. Ce dernier agit comme un « organisateur » en vue de révéler des problématiques internes pour lesquelles l'organisation est exposée aux risques.

<u>Le Risk Manager un juste impératif :</u>

« Un Risk manager c'est avant tout un poil à gratter, il insiste sur les problèmes de chacun mais sans stigmatiser un manager ou un dirigeant. Ce consultant interne se contente d'être influent et d'insister là où il y a des zones de perfectionnement », nous confie ce Risk Manager, EC-17, décembre 2012.

« Le risque opérationnel c'est un sujet où la frontière est poreuse avec d'autres risques, c'est transversal et sans Risk Manager pour soulever la question, personne ne s'en occuperait » précise également ce contrôleur bancaire, EC-53, mars 2013.

« Il n'existe pas toujours de vision partagée sur les risques opérationnels, alors le Risk Manager met en musique les différentes compétences pour vraiment gérer ce risque, il fait coïncider l'ensemble des informations pour faire apparaitre des problématiques récurrentes. Le but n'est pas uniquement d'avoir une image des risques passés, mais on cherche vraiment à savoir où seront les problèmes » expose cette directrice des risques, EC-51, avril 2013.

La problématisation opérée par le Risk Manager se caractérise également ainsi, comme le précise ce directeur des risques opérationnels, EC-11, novembre 2012 : *« Le risque opérationnel pose un problème de périmètre, on est souvent en face d'une montagne tant le sujet est large. La maturité du secteur financier est faible sur ce sujet par rapport aux autres risques. Ce risque est plus dur à modéliser, on est obligé de le subir pour s'en rendre compte et collecter des données. Il est impossible à gérer sans réseau avec juste une équipe isolée, on doit donc faire remonter à tous la difficulté d'appréhension du risque, aux actuaires, aux financiers, et en faire un sujet intelligible ».*

-L'intéressement des collaborateurs à la problématique du risque opérationnel, une réalisation du Risk Manager

Au-delà de la problématisation du sujet, l'intéressement des acteurs à l'enjeu 'risque opérationnel' implique différents leviers que nos entretiens nous permettent de résumer.

<u>Intéresser et associer les différents acteurs à la problématique du risque opérationnel : un enjeu du Risk Manager</u>

Il existe en effet des leviers sur lesquels le Risk Manager peut s'appuyer pour intéresser les différents acteurs à la problématique du risque opérationnel :

-des leviers associés à la gouvernance d'entreprise : *« Il faut un sponsorship fort pour que cela marche est que le Risk Manager joue pleinement son rôle, sans l'appui des dirigeants, des membres de Comex on aura peu de poids et aucune réelle prise de conscience des collaborateurs sur les risques opérationnels »* constate ce directeur des risques, EC-15, novembre 2012. Ce que confirme ce directeur d'audit interne, EC-27, janvier 2013 : *« Le bon*

levier réside dans la gouvernance, pouvoir dire qui fait quoi sur le risque opérationnel, donner une visibilité et des informations, le Risk Manager a un rôle évident et essentiel sur ce point ».

-des leviers communicationnels comme le précise les différentes personnes interviewées :

« On adapte notre discours aux interlocuteurs, la plus-value du Risk Manager c'est de pouvoir être compris et entendu par tous en fonction de ses problèmes respectifs. Pour des dirigeants on se concentre sur les scénarios des risques opérationnels extrêmes, qui empêcheraient la réalisation de la stratégie, pour des managers on évoque le coût du risque opérationnel et le problème des budgets, pour des exécutants on aborde cela sous l'angle de la qualité ou du pilotage de l'activité » précise ce Risk Manager, EC-20, décembre 2012.

« Souvent les commerciaux sont très loin de ces préoccupations sur les risques, c'est mal compris et même mal perçu car leur difficulté première est de réussir à avoir de nouveaux clients. Il faut donc leur faire comprendre que notre démarche est complémentaire, qu'elle permet de garder les clients en portefeuille » exprime cette directrice des risques opérationnels, EC-51, avril 2013

-L'enrôlement des acteurs par le Risk Manager au sein d'une filière risque opérationnel:

Au-delà de ces leviers, nos entretiens nous permettent de mettre en exergue le rôle important joué par le Risk Manager comme acteur permettant de fédérer les différentes fonctions métiers et supports de l'organisation au travers de l'enjeu commun « risque opérationnel ». Par l'enrôlement autour de cet enjeu normatif, alors traduit comme un enjeu de gestion, le Risk Manager contribue à répondre à la fois à l'enjeu réglementaire ainsi qu'à un sujet d'effectivité. Les leviers communicationnels précités sont alors mobilisés aux fins de cet enrôlement et se matérialisent notamment sur plusieurs points :

-clarifier les attendus du régulateur face au risque opérationnel,

-préciser les besoins de la gouvernance concernant les différents acteurs sur ce même sujet,

-déterminer les actions à mettre en œuvre par chacun (rôles et responsabilités) sur leurs périmètres respectifs.

« Pour appréhender le risque opérationnel, il faut avoir une clé d'entrée, quelqu'un qui connait le système de contrôle et les procédures, qui peut guider l'action face à la confusion et éviter de se perdre, qui peut travailler en équipe élargie et sait apprécier jusqu'à quel niveau un risque est acceptable ou la sécurisation est supportable. Les Risk Managers s'inscrivent bien dans ce compromis difficile » commente un directeur de l'organisation, EC-24, janvier 2013.

« Le Risk Manager a le mérite de répondre à un problème clair sur le risque : l'attente d'un guichet unique pour gérer ce qui concerne tout le monde. Il faut savoir aller derrière les organigrammes, trouver les pôles d'expertise en interne sur un sujet très technique, entre connaissances fonctionnelles et maîtrise de chaque métier. C'est très difficile de constituer une bonne équipe sur le sujet. Le Risk Manager a aussi ce rôle de développer un pôle de compétence transverse sur la question des risques » confirme ce directeur d'audit interne, EC-13, novembre 2012.

« Pour inclure des collaborateurs parfois réticents, il faut au Risk Manager une vraie logique de conseil, la capacité à fournir des éléments aidant les collaborateurs à prendre conscience des risques. Cela ne se limite pas à faire une liste de recommandations inapplicables, il faut tenir le stylo, du moins au début. On commence toujours par expliquer qu'on est en interface, et non là pour descendre ou sanctionner un collaborateur » explicite cette directrice des risques opérationnels, EC-39, février 2013.

-La mobilisation des acteurs de la filière par le Risk Manager:

Au-delà de l'enrôlement, la phase suivante consiste clairement pour le Risk Manager à mobiliser de manière durable les acteurs de la filière risques opérationnels (référents risques, contributeurs risques).

Cette mobilisation consiste en plusieurs actions :

-recueillir les expertises lorsque celles-ci font défaut,

-collecter les remontées en matière de risques (identification, évaluation, priorisation mais aussi consolidation au travers des outils de cartographies des risques et de base de collectes des indicents et des pertes) ;

-s'assurer que chaque acteur de la filière risques opérationnels aient pris la mesure de son rôle au travers de la formalisation et de l'application de plans d'actions de maîtrise des risques (mises en place des moyens de protections, préventions, transferts de risques).

-faire en sorte d'être informé par chaque acteur de la réussite de la démarche de gestion des risques voire d'être alerté suffisamment tôt en cas de difficultés persistantes dans les solutions de traitement apportées face à un risque opérationnel donné.

-pouvoir s'adapter aux attentes et sollicitations de chaque acteur de la filière risques opérationnels.

« Un Risk manager a avant tout un réseau, pas une démarche type, il faut se méfier 'des y'a qu'à, faut qu'on', le vrai enjeu c'est de parler des sujets aux bonnes personnes comme les fonctions commerciales et les métiers, les collaborateurs des centres de gestions, des back offices » résume ce directeur des risques opérationnels, EC-25, janvier 2013.

Ce Risk Manager (EC-17 décembre 2012) nous commente ainsi : *« Le sujet du Risk Management est simple : rassembler suffisamment de relais pour avoir les connaissances permettant d'agir vite face à un risque survenu ou à venir. Cela passe par des relais officiels mais aussi et parfois surtout par des interlocuteurs avec qui échanger de manière informelle et qui se sentiront concernés ».*

Outre les résultats relatifs à la structuration des contrôles, nous constatons donc le rôle essentiel d'acteur réseau joué par le Risk Manager au centre d'un processus d'interactions qu'est la filière risques opérationnels.

2.3. Résultats émergents relatifs aux contrôles interactifs

Dans la continuité des travaux de Simons (1995), nos résultats issus des entretiens font émerger le rôle de contrôle interactif que rempli la fonction de gestion des risques opérationnels.

Cet apport se situe à plusieurs niveaux. En premier lieu dans l'intégration des fonctions de contrôle qualité et de contrôle de gestion pour ce qui est de la contribution de la gestion des risques opérationnels au management de la performance de l'entreprise (réduction des dysfonctionnements, réduction des surcoûts associés aux évènements de risques opérationnels).

En second lieu, ces résultats relatifs au contrôle interactif situent la gestion des risques opérationnels en interaction avec d'autres contrôles organisationnels centrés sur l'approche normative (le contrôle de conformité et le contrôle interne, respectivement centrés sur le respect des règles internes ou externes et sur le respect des procédures internes).

2.3.1. Les interactions entre gestion des risques opérationnels et fonctions de contrôles de la performance

Nos interlocuteurs rencontrés lors des entretiens insistent sur l'importance de développer les interactions en ce qui concerne la contribution de la fonction gestion des risques opérationnels en lien avec le contrôle de gestion et le contrôle qualité.

-Lien avec le contrôle de gestion. Les interactions entre ces deux fonctions concernent ainsi, pour nos différents interlocuteurs:

-l'analyse et le traitement du coût du risque opérationnel, trop souvent sous-estimé comptablement. Pour plusieurs interlocuteurs rencontrés, le risque opérationnel est par nature un coût caché[68] dans l'organisation. Il est insuffisamment compris et souvent mal évalué alors même que son coût peut être réel (coût d'erreurs de traitement de l'information, coûts des fraudes, coûts des pannes informatiques, coût des dispositifs de contrôles et des actions curatives à mettre en œuvre face à un risque opérationnel donné).

-la collecte des incidents et des pertes peut servir à mieux estimer les charges réelles au sein de l'entreprise, dans une logique d'interactions centrée sur l'outil de gestion (De La Villarmois, Stéphan, 2005).

-le contrôle de gestion est également une fonction historiquement impliquée dans l'analyse des dysfonctionnements et des incidents au sein de l'organisation. Aussi sa contribution à l'analyse des incidents opérationnels semble évidente pour plusieurs interlocuteurs, même si ces derniers évoquent des organisations encore peu matures sur les rapprochements gestion des risques opérationnels / contrôle de gestion,

[68] Au sens de coûts difficilement visible comptablement, cela concerne les pertes et coûts des incidents « risques opérationnels » tels que les fraudes, les interruptions SI, les erreurs de traitement d'opérations engendrant des surcoûts etc.

-le rapprochement entre contrôle de gestion et gestion des risques opérationnels est également un moyen de contribuer à automatiser et à industrialiser la collecte des incidents opérationnels, en pratique souvent très éparses et très variables d'une entité à l'autre quant aux données remontées (problème de fiabilité des données qualitatives et quantitatives remontées aux directions des risques opérationnels).

« Le lien avec le contrôle de gestion ? Cela nous aiderait mais on le fait peu car on a peur de l'usine à gaz. C'est cette peur qui nous a conduit à mettre en place des reporting fastidieux et à avoir un reporting aussi chronophage pour répondre aux exigences réglementaires » nous indique ce directeur des risques, EC-11, novembre 2012.

« Il y a une complémentarité évidente avec le contrôle de gestion, cela permet d'enrichir le processus d'identification et d'évaluation des risques, de savoir si l'on investit ou non dans les 'bons risques', cela montre aussi que le Risk Manager n'est pas seul face aux métiers » remarque ce directeur des risques, EC-14, novembre 2012.

« L'apport du contrôle de gestion dans les risques opérationnel se voit à deux titres : la fiabilité de l'information, la qualité des données et la capacité à agréger des données pour les rendre parlantes. Cela peut aider le Risk Management » admet ce consultant en risque opérationnel, EC-23, janvier 2013.

« Le lien avec le contrôle de gestion est d'autant plus fort que cela peut permettre de révéler un coût difficilement visible comptablement…. On est en quelque sorte sur du coût caché mais ce n'est jamais abordé sous cet angle par manque de temps » précise ce consultant expert risque, EC-2, juillet 2012.

-Lien avec le contrôle qualité : le lien entre gestion des risques opérationnels et contrôle de qualité, bien que semblant évident, ressort de nos entretiens comme ayant un vrai intérêt mais étant encore insuffisamment développé aujourd'hui au sein des filières risques.

L'apport d'un lien renforcé entre gestion des risques opérationnels et contrôle qualité semble pertinent pour plusieurs raisons, selon nos interlocuteurs :

-le contrôle qualité et la gestion des risques opérationnels impliquent le recours aux mêmes méthodes (le modèle PDCA et l'approche de type « roue du risque »[69] étant des approches similaires pour plusieurs interlocuteurs),

-la notion de dysfonctionnement en qualité renvoi clairement à la notion d'incident, transposée en gestion des risques opérationnels,

-l'approche processus souvent développée en contrôle qualité, est également très présente en gestion des risques opérationnels (pilotage par les processus et pilotage par les risques étant souvent imbriqués),

-historiquement, la gestion de la qualité, bien que très différente d'un établissement financier à un autre, est antérieure à l'approche par les risques opérationnels. Cependant, on constate que plusieurs des risques opérationnels présents dans les catégories baloises sont en fait des non-qualités comme le font remarquer plusieurs de nos interlocuteurs lors des entretiens confirmatoires.

Comme l'évoque ce consultant expert risque, EC-23, janvier 2013, *« On a un lien fort entre la qualité et le Risk Management car on retrouve dans ces deux fonctions la notion de 'client interne' mais aussi 'externe' et il y a dans les deux cas une vision de type 'conseil' à fournir, on est à chaque fois dans l'amélioration continue. Ces fonctions poursuivent le même objectif, l'une (risques) est plus interne et l'autre (qualité) plus tournée vers le client ».*

« Le lien entre qualité et risque opérationnel est évident : il s'agit de s'intéresser à tout ce qui peut polluer le bon fonctionnement du service au client, cela concerne les fraudes, la délivrance des moyens de paiement, faire le parallèle entre risque et qualité c'est incontournable si l'on veut parler des vrais sujets » nous informe ce directeur des risques, EC-15, novembre 2012.

Outre ces interactions entre contrôle des risques et contrôle de gestion / contrôle qualité, nos entretiens font également ressortir un enjeu de rapprochement avec d'autres types de contrôles, davantage organisationnels.

[69] Démarche itérative inspiré de la Roue de Deming et comprenant quatre phases que sont, successivement : l'identification des risques, l'évaluation-priorisation des risques, le traitement-réduction des risques et enfin une phase de suivi des risques (plans d'audit et de contrôle).

2.3.2. Les interactions entre gestion des risques opérationnels et les fonctions de contrôles organisationnels de la firme

Ces rapprochements sont à envisager en premier lieu entre l'audit interne et la gestion des risques opérationnels

-Le lien avec l'audit interne : Nos interlocuteurs, lors des entretiens, insistent sur l'apport de la gestion des risques opérationnels vis-à-vis de l'audit interne et inversement.

En premier lieu, la gestion des risques opérationnels, en établissant une cartographie des risques et une collecte des incidents et des pertes permet à l'audit interne de construire un plan d'audit davantage centré sur la réalité des risques de l'organisation. L'audit interne, en ayant recours à ces éléments (parmi d'autres), est ainsi mieux à même de prendre en compte les zones de vulnérabilités de l'organisation et les zones pour lesquelles des menaces potentielles peuvent l'affecter (capacités de fraudeurs à impacter l'entreprise, possibilité d'intrusion de hackers dans le système d'information, vulnérabilité de l'entreprise en cas de catastrophe naturelle etc.).

Inversement, la gestion des risques opérationnels peut également s'appuyer sur les rapports d'audit interne, pointant des dysfonctionnements internes à l'organisation, pour mener des actions plus poussées d'identification des risques opérationnels. En fonction des alertes remontées par l'audit interne, la direction des risques opérationnels pourra renforcer ses analyses ainsi que les mesures de traitement et de suivi des risques à mettre en œuvre.

« Cela parait évident aujourd'hui que l'audit interne se serve du Risk Management pour construire son propre plan d'audit, mais cela n'a pas toujours été ainsi et beaucoup d'entreprises ne fonctionnent pas encore comme cela » nous exprime de directeur d'audit interne, EC-13, novembre 2012.

-Le lien avec le contrôle interne et le contrôle de conformité : Outre le rapprochement avec l'audit interne, le lien fort existant entre gestion des risques opérationnels et le contrôle interne ou encore le contrôle de conformité est à souligner.

La fonction de gestion des risques opérationnels peut ainsi s'appuyer sur la fonction de conformité pour anticiper des risques opérationnels découlant de non conformités réglementaires notamment (et ainsi éviter un risque de sanction par exemple). Egalement, le

Risk Manager en charge des risques opérationnels pourra s'appuyer sur le responsable de la conformité pour les actions de veille juridique ou technique permettant d'anticiper des non-conformités en cours de matérialisation ou à venir.

Le lien avec le contrôle interne est également très fort comme nous l'indiquent nos interlocuteurs. Ainsi, le contrôle interne constitue l'un des acteurs contribuant à la remontée des incidents et des pertes opérationnelles. Dans le cadre de son plan de contrôle, il réalise une revue des processus et des procédures et est ainsi à même, avec un appui méthodologique adapté de la part du Risk Manager, d'identifier les risques opérationnels dans le cadre de ses contrôles.

Egalement, lorsque des risques opérationnels sont identifiés par le Risk Management comme étant à traiter en priorité, le contrôle interne constitue l'un des relais de la fonction de gestion des risques permettant de s'assurer de la réduction du risque ou du traitement de ses causes racines. Le contrôle interne constitue ainsi l'un des dispositifs de maîtrise des risques sur lesquels s'appui le Risk Management.
Les liens sont alors les suivants dans une démarche « cible » : le Risk Management s'appuie sur les dispositifs de contrôle pour s'assurer qu'à chaque contrôle correspond bien un enjeu de risque associé.
L'audit interne s'appuie sur la démarche de cartographie des risques pour identifier et évaluer la pertinence, l'efficacité et l'effectivité des contrôles en place.

Pour cette contrôleuse bancaire, EC-54, mai 2013 *« il est difficile d'envisager la conformité, le contrôle interne ou le risque de manière indépendante, c'est pour cela que regrouper le contrôle permanent et le risque opérationnel a du sens. Cela évite également que chacun se décharge du sujet, mais il faut un acteur pour piloter le tout et porter les sujets, on reboucle avec le Risk Management ».*

2.3.3. La gestion des risques opérationnels, entre gouvernance et chaine de valeur

Outre ces interactions multiples avec les acteurs de la filière risques opérationnels, qu'il s'agisse des fonctions métiers, supports, ou de contrôle, le positionnement interactionniste de la fonction de gestion des risques opérationnels se situe également entre gouvernance et activités de la chaine de valeur, comme nous l'avons évoqué lors des études de cas.

Ce double rattachement s'entrevoit donc en approche Top Down de la gouvernance d'entreprise (Conseil d'Administration et Direction Générale) vers la fonction de gestion des risques. A ce titre, la fonction de gestion des risques opérationnels applique la politique de maîtrise des risques opérationnels (qu'elle propose à la Direction Générale pour approbation) en ce qui concerne le profil de risque de l'entreprise (soit son seuil d'acceptation du risque et son seuil de tolérance au risque). La politique définit alors les limites à ne pas dépasser, les risques opérationnels acceptables et ceux à éviter en priorité.

Dans une approche Bottom Up également, les interactions de la fonction de gestion des risques opérationnels sont à envisager avec l'ensemble des fonctions de la chaine de valeur de l'entreprise, comme nous l'avons évoqué (fonctions supports et métiers).

Cette approche Bottom Up, dans les remontées d'informations faites à la direction des risques opérationnels, permet à la fonction de gestion des risques de s'assurer que les seuils d'acceptation et de tolérance aux risques sont respectés.

Comme l'exprime ce Risk Manager (EC-22, janvier 2013*) « La gouvernance nous fait confiance quant à la déclinaison de la politique risques opérationnels, nous sommes leur cellule d'alerte, de mise en garde, quant une activité s'emballe, qu'on est plus dans de la croissance effrénée que dans du réel développement. »*
« L'intérêt de notre fonction c'est que la direction générale nous fait confiance, nous écoute et sollicite notre avis avant le lancement d'un projet, sans cet appui de la gouvernance, notre fonction ne serait que du réglementaire, c'est notre principal levier » précise également ce directeur des risques opérationnels (EC-32, février 2013).

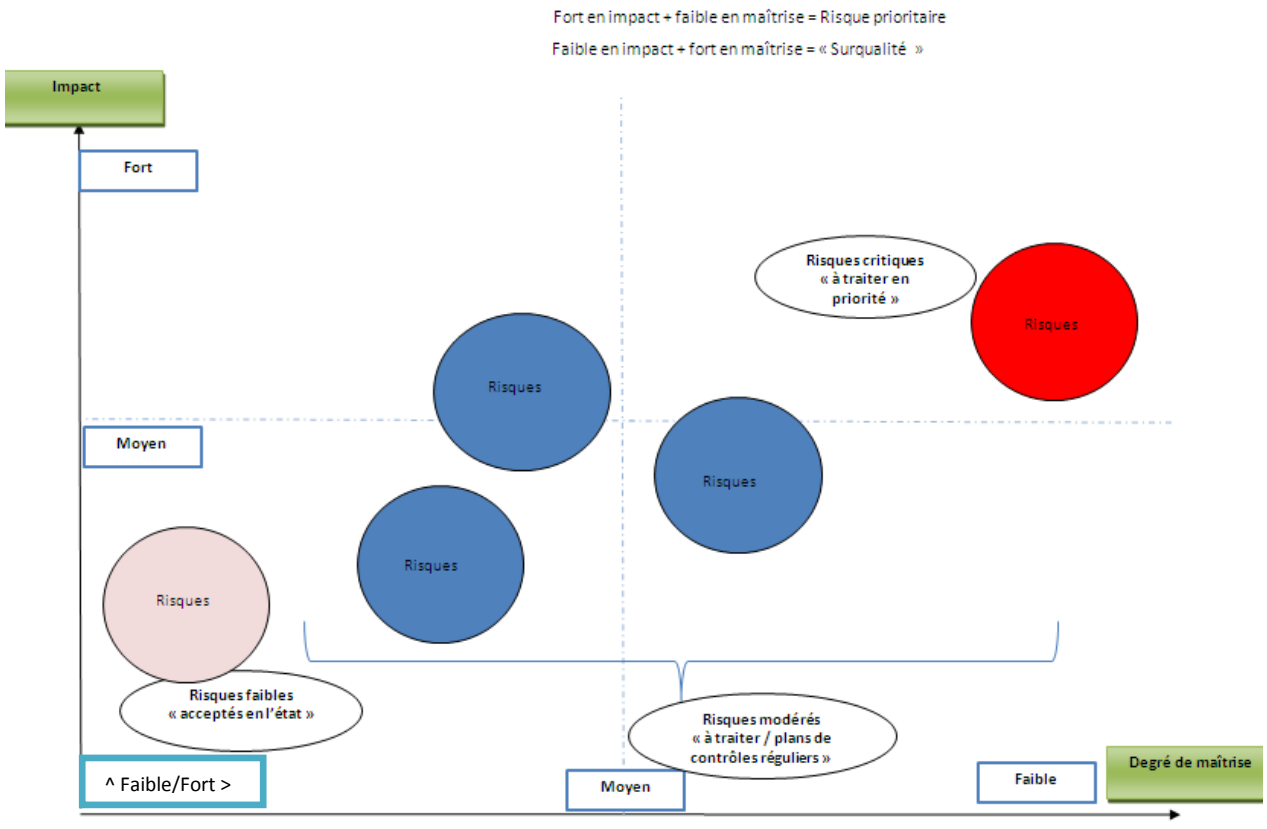
L'appui de la gouvernance ressort en effet de la majorité des entretiens comme le principal levier donnant une impulsion à la démarche de gestion des risques opérationnels. Toutefois, cet appui, bien qu'essentiel pour dépasser le simple cadre de la normativité, n'est en soi pas suffisant.

Pour plusieurs Risk Manager et directeur des risques, l'approche Bottom Up semble tout aussi importante. Pour ces derniers, le simple fait d'avoir l'appui de la gouvernance peut très bien ne pas suffire si le Risk Manager n'est pas entendu dans l'entreprise. La transposition de la politique de maîtrise des risques opérationnels au travers d'action concrètes et dans le cadre

d'une vigilance partagée n'est formalisée que si le Risk Manager bénéficie d'une certaine reconnaissance au sein de l'organisation et d'une visibilité vis-à-vis des différentes parties prenantes de l'organisation. Comme l'évoque ce directeur des risques (EC-15, novembre 2012) *« L'erreur souvent commise est que l'on se contente, au Risk Management, d'échanger avec le Top Management, il ne faut pas s'arrêter à ce niveau car autrement la redescente d'informations ne se fait pas et, pire, vous êtes alors perçu comme une fonction institutionnelle de plus car les métiers n'ont pas compris votre rôle de sécurisation de l'activité ».*

Le schéma ci-après résume ce rôle interactionniste de la fonction de gestion des risques des opérationnels dans une double logique Top Down et Bottom Up.
L'approche Top Down se situe au niveau de la priorisation des risques « à éviter », à traiter en priorité.
L'approche Bottom Up se situe quant à elle au niveau des risques modérés, à traiter dans le cadre des plans de contrôles réguliers.

Figure 41. Approche interactionniste de la fonction gestion des risques – déclinaison de la politique de maîtrise des risques opérationnels



En résumé, le rôle de contrôle interactif de la fonction de gestion des risques opérationnels se situe à trois niveaux :
-dans l'interaction de type Top Down avec la gouvernance d'entreprise, pour les risques critiques,
-dans le rapprochement transverse avec les différents types de contrôles, pour les risques modérés,
-dans les interactions fortes avec les fonctions métiers et supports de la chaine de valeur de l'entreprise, pour les risques modérés,.

Ces interactions situent bien, pour reprendre Simons (1995), la gestion des risques opérationnels entre les valeurs de l'entreprise et les risques à éviter (politiques de maîtrise des risques approuvée par la gouvernance), les incertitudes stratégiques (constatées par les parties prenantes de la chaine de valeur et remontées à la direction des risques) et les différentes variables influant sur la performance de l'entreprise (pour lesquelles la fonction de gestion des risques s'appui sur les différents contrôles de conformité, de gestion, internes etc.).

Conclusion du chapitre résultats - traduction, structuration, interactions comme leviers de l'effectivité du contrôle

Les résultats de notre recherche, au travers des deux cas d'étude menés en recherche-action ainsi que des entretiens confirmatoires réalisés s'orientent vers la nécessité de clairement prendre en compte les difficultés pratiques posées par la norme de contrôle du risque opérationnel.

En premier lieu, nous constatons au regard de ces résultats que la notion de risque opérationnel est trop extensive et confuse en pratique pour faire l'objet d'un management effectif et d'une collecte homogène au sein d'une organisation sans facteur d'incitation.

En second lieu, nos résultats abondent dans le sens du rôle essentiel joué par la fonction de gestion des risques opérationnels, fonction encore récente, en vue de coordonner les différents acteurs de la filière risques. Cette fonction a ainsi pour rôle de coordonner les différents propriétaires de risques (les entités opérationnelles et supports au sein de l'organisation, ce sur leurs périmètres respectifs de responsabilité). Toutefois, il découle de nos résultats que la fonction de gestion des risques opérationnels, incarnée par le Risk Manager, contribue également à interagir avec les différents contrôles de l'organisation autour de cette notion frontière qu'est le risque opérationnel.

Enfin, il ressort de nos résultats que le Risk Manager joue un rôle quant à l'effectivité des dispositifs de contrôle du risque opérationnel en assurant une fonction d'acteur-réseau sur cette thématique ainsi qu'une traduction de la notion de risque opérationnel telle qu'elle découle de la réglementation prudentielle. Ce rôle d'acteur-réseau permet ainsi au Risk Manager de contribuer à structurer les différents contrôles préexistants au sein des établissements financiers au travers de cette exigence de gestion du risque opérationnel.

Chapitre 6 - Discussion, perspectives théoriques et managériales : une contribution sous l'angle gestionnaire aux théories du risque

« En l'absence de prise solide sur un dispositif qu'une série d'expériences porte à traiter comme dangereux, il reste trois attitudes possibles : l'indifférence, la confiance ou la relance permanente de la critique »

Chateauraynaud F., Torny D.

Introduction

« A travers la catastrophe, c'est la continuité de la vie quotidienne qui est menacée et, partant, la confiance dans les dispositifs chargés de garantir cette continuité » nous disent Chateauraynaud et Torny (1999).

En transposition de notre objet étude et dans le prolongement des approches structurationniste et de type acteur-réseau, nous situons clairement la fonction de gestion des risques opérationnels comme un élément central, chargé de garantir la confiance dans l'organisation face aux différents évènements de risques opérationnels. Cette fonction contribue à la structuration des contrôles et à la fédération des acteurs de l'organisation autour de l'enjeu « risque opérationnel ». Elle est sensée interpréter et transposer la norme de contrôle en vue de dépasser l'aspect normatif lui étant inhérent en un enjeu gestionnaire parlant pour les parties prenantes de l'organisation.

Les résultats obtenus contribuent en particulier aux théories qualitatives du contrôle de gestion. Au plan pratique, ils déplacent le rôle du contrôle des risques de l'identification et de la mesure technique du risque vers un contrôle davantage tourné vers la médiation. Néanmoins ces recherches appellent des travaux complémentaires pour les approfondir et les valider sur une plus large échelle.

Ce chapitre vise à apporter un éclairage complémentaire sur les résultats produits, à les interroger au regard des éléments de littérature en réponse à des préoccupations managériales. Nous abordons également les limites propres à notre étude ainsi que les perspectives futures qui en découlent. Cette recherche étant considérée comme un point de départ au regard de la

nécessité de généraliser nos constats (voire de les contredire) dans des contextes empiriques ou différents (autres types d'établissements financiers telles que les mutuelles d'assurance ou courtiers ; autres secteurs d'activités que le secteur des services financiers ; autres contextes tels que les contextes de survenance de risques opérationnels en gestion de crise etc.) ou via des grilles de lecture distinctes (théorie de l'erreur humaine, théorie institutionnelle etc.).

1. Comparaison inter-cas : un rapprochement entre études de cas et témoignages d'experts

Ce premier paragraphe vise à détailler la comparaison inter-cas de notre recherche, soit les résultats comparatifs issus de nos études de cas ainsi que de nos entretiens.

1.1. Synthèse des cas relatifs aux enjeux de structuration

Nos deux études de cas font ressortir un premier constat : le risque opérationnel est un sujet difficile à comprendre et souvent confus en tant que notion (confusion avec des notions telles que les menaces externes, les vulnérabilités internes, les évènements redoutés etc.) et en tant que dispositif de gestion (délimitation du champ d'analyse, du périmètre et des acteurs concernés en termes de rôle et de responsabilité). Si ces derniers sont capables de discernement et de maîtrise dans leur domaine de compétence métier, l'objet *« risque opérationnel »* est appréhendé comme un enjeu encore récent, issu du monde réglementaire et prudentiel et pour lequel un besoin de *« bonnes pratiques »* se fait ressentir. Pour les différents responsables de département et d'entité rencontrés lors des études de cas, une attente forte de lignes directrices se faisait ressentir. Cette attente de précision et de restitution d'avis d'experts est même perçue comme la plus-value première d'une direction des risques opérationnels : fournir les enjeux de compréhension sur ce que le législateur et le régulateur[70] attendent, ce qu'il faut *« faire remonter »* comme éléments et informations, si les dispositifs de contrôle mis en place couvrent bien le périmètre attendu.

La conscience de la nécessité de faire ce travail dans l'organisation est souvent présente pour les managers, au-delà du simple aspect réglementaire, mais la question première est de savoir à quoi il est fait référence lorsque l'on aborde le risque opérationnel. Les managers et

[70] Autorité de Contrôle Prudentiel et de Résolution notamment, mais aussi la diffusion des lignes directrices du comité de Bâle en banque et de l'EIOPA (European Insurance and Occupational Pensions Authority) en assurance.

opérationnels savent que l'on cherche à éviter des pertes. Sur la mise en œuvre des méthodes et outils dédiés, la présentation de « cas types » et des retours d'expérience permet de concrétiser les attentes de cet enjeu abstrait. Ainsi, dans les études de cas, les observations participantes et non participantes révèlent la difficulté de saisir l'objet complexe risque opérationnel. Cette difficulté est en fait double et s'entrevoit par le caractère dématérialisé des activités de services financiers : les procédures sont largement informatisées et les différentes activités des centres de gestion pour la majorité décentralisées.

Tableau 31. Modernité et causes de risque opérationnel

Mécanismes de la modernité	**Modernité des services financiers et facteurs de risque opérationnel**
Mécanismes de délocalisation	Multiplicité des acteurs en charge des risques, Diversité géographique des centres de gestion et de distribution des services financiers, Management centralisé et activités opérationnelles décentralisées
Dématérialisation des échanges	Procédures informatisées, Rationalisation et industrialisation des activités de services financiers, Majorité de contrôle à distance et 'sur dossier'

De tels constats se retrouvent également dans nos entretiens confirmatoires, lesquels insistent cependant davantage sur le caractère de confusion propre à la notion de risque opérationnel, par définition trop extensive et nécessitant une interprétation des parties prenantes de l'organisation.

1.2. Synthèse des cas relatifs au rôle du Risk Manager, acteur -réseau

La gestion des risques, fédérer les nombreux acteurs du contrôle : Nos différentes études de cas, bien qu'appelant des recherches complémentaires, nous permettent d'insister sur le rôle clé de l'approche par les risques et des acteurs qui l'initient comme un moyen d'interactions et d'échanges en vue de contribuer au changement dans l'entreprise. Ces approches en termes de pilotage par les risques dans nos différents cas de recherche-action nous amène à considérer l'importance des échanges formels et informels afin que la thématique du risque ne soit pas qu'un enjeu de reporting réglementaire ou prudentielle. Il

s'agit bien d'un élément visant à améliorer de manière continue la performance au sein des établissements financiers. Le tableau comparatif ci-après résume ainsi les constats réalisés. Nous avons souhaité prendre des études de cas où le curseur 'risque' était d'une importance variable selon les périmètres étudiés. On constate ainsi que plus l'enjeu 'risque' est prioritaire dans nos études de cas, plus l'approche retenue est interactive. Un tel résultat est bien entendu intuitif, mais un élément complémentaire à prendre est que plus cette approche de contrôle par interaction est développée, plus le pilotage par les risques est un moyen d'inciter au changement des pratiques et des comportements sur des activités à risque. La thématique du risque est un sujet souvent perçu comme complexe lors de nos études de cas mais ayant le mérite que chaque acteur en ait sa propre compréhension. Renforcer les échanges sur ce sujet permet donc de passer d'une approche où le risque est un enjeu de gestion 'administrative' à un vrai sujet d'amélioration continue au même titre que la recherche de performance, la maîtrise de la qualité ou encore la maîtrise des processus.

Tableau 32. Comparatif inter-cas

Etude de cas	**Objectif 'risque'**	**Approche retenue**	**Limites et apports**
Risk Management	Prioritaire (objectif à part entière de la fonction)	Approche interactive insistant sur les échanges réguliers, conseils méthodologiques et techniques nombreux	Permet une meilleure sensibilisation et une compréhension forte de l'enjeu 'risque'/ est parfois perçu comme un simple enjeu de reporting réglementaire
Contrôle interne	Important mais secondaire (après le respect des processus)	Contrôle des dysfonctionnements et logiques de recommandations avec suivi de mise en œuvre	Permet une sensibilisation accrue sur le lien entre maîtrise des processus et maîtrise des risques / Les contrôles sont parfois jugés administratifs et 'de conformité'

Entretiens confirmatoires	Prioritaire (mais sources de nombreuses difficultés dans la manière de gérer, en pratique, le risque opérationnel, a fortiori en l'absence de « recommandations »)	Le manque de visibilité sur la manière de gérer le risque opérationnel rend la démarche souvent insuffisamment effective et s'éloigne ainsi de la vision « intégrée et globale » de la gestion des risques	La notion de risque opérationnel reste, même après plusieurs années un sujet exploratoire pour lequel une connaissance commune fait défaut

2. Les contributions théoriques et managériales des résultats

Ce paragraphe a pour objectif de mettre en lumière les apports théoriques et managériaux de notre étude. Ces apports se situent dans la transposition en sciences de gestion des théories socio-organisationnelles, nous permettant de souligner les conditions de rigueur propre au dépassement de la normativité en contrôle des risques. Les apports sur le plan managérial concernent la manière d'appréhender les enjeux de responsabilisation en contrôle des risques opérationnels, objectif attendu de l'effectivité de la démarche de contrôle précitée.

2.1. Contributions de la recherche sur le plan théorique

D'un point de vue théorique, la thématique du risque a été reprise dans la littérature managériale comme un moyen d'intégrer le rapport à l'autre. Certains auteurs insistent sur son caractère englobant et le fait que chaque acteur ait une compréhension propre de l'enjeu risque. Le risque est potentiellement partout, il est *« la mesure de l'action »* comme l'évoque Beck (1986). Il constitue un *« objet frontière »*[71] car il s'agit d'un enjeu commun de gestion sur lequel chacun peut agir sur son périmètre propre sous réserve qu'une traduction soit opérée par des acteurs dédiés à cette fonction. Cette réflexion est d'actualité sur ce que certains qualifient de *« Total Risk Management »* (Méric et al., 2009). Cette recherche se situe clairement dans le prolongement des travaux fondateurs sur le contrôle interactif (Simons, 1995). Elle complète également les recherches récentes sur le contrôle explicitant la variable

[71] Au sens de Star S.L., notion empreinte à l'anthropologie et à la sociologie, désignant des espaces de communication inter-groupe. Il s'agit en l'espèce de termes pouvant être désignés par des groupes distincts de manière similaire sans renvoyer nécessairement à une même compréhension. Le risque correspond typiquement à ce type de problématique et appelle en ce sens des recherches plus développées en épistémologie (Pesqueux, 2011 ; Larkèche, 2011).

risque comme un enjeu organisationnel à part entière où il s'agit de passer du dénombrement du risque à la prise de conscience du caractère mobilisant et fédérateur du risque (Mikes, 2011). A fortiori dans un monde post-crise, le risque opérationnel est identifié comme une catégorie vaste mais de plus en plus prioritaire pour les établissements financiers (Jebrin, Abu-Salma, 2012 ; Jednak, Jednak, 2013).

Cette étude exploratoire s'inscrit en premier lieu dans le prolongement des travaux de Beck (1986) et Giddens (1994) en ce qui concerne la théorie de la structuration, envisagée dans notre étude sous l'angle socio-organisationnel. En contribuant aux maintiens des différents garde-fous de la confiance moderne, la fonction de gestion des risques opérationnels joue un rôle de structuration des différents contrôles organisationnels.

En complément, et dans la lignée des travaux théoriques de Callon et Latour (1981), concernant la sociologie de la traduction, nous analysons le positionnement du Risk Manager comme celui d'un acteur-réseau, coordonnant et animant la filière « risques opérationnels » en tant que réseau structuré d'interactions.

Ces caractères de structuration et d'acteur-réseau qualifiant la fonction de gestion des risques opérationnels dans notre recherche, la positionne également comme une fonction de contrôle interactif au sens de Simons (1995).

L'étude de nos résultats montre également des liens émergents dans la pratique avec les théories d'inspiration socio-économiques (Savall, Zardet, 1987, 2010). Ces liens concernent notamment le rôle que peut jouer la fonction de gestion des risques opérationnels dans l'identification de certains surcoûts non-identifiés comptablement par l'organisation. Ces surcoûts peuvent ainsi s'analyser comme des coûts cachés voire des sources de performances cachées. Si l'on reprend en effet les travaux de Savall et Zardet (1987), les risques opérationnels peuvent ainsi faire figure de coûts cachés (en l'absence de dispositif de contrôle dédiés, de système de mesure voire d'une dénomination adaptée). Ces éléments constituent en soi une perspective de recherche future qu'il convient d'approfondir. Si nos entretiens confirmatoires montrent l'importance d'investiguer cet axe de recherche, une étude plus poussée d'un tel rapprochement reste à initier.

Egalement, le rapprochement avec les théories du sensemaking (Weick, 1995) semble un terrain d'investigation future. Nos entretiens confirmatoires nous alerte ainsi sur la nécessite de renforcer le sens donné aux différents contrôles préexistants dans l'organisation. Nous avons pris le parti d'aborder le rôle de la fonction de gestion des risques en tant que fonction d'animation et de coordination face à un enjeu normatif manquant d'effectivité. Les travaux relatifs à la perte de sens dans le contrôle constitueraient également un axe de positionnement théorique à développer (Jafari et al., 2011 ; Jednak, Jednak, 2013).

Enfin, nous démontrons que l'étude des risques opérationnels dans le domaine des services financiers implique d'une part de ne pas concentrer uniquement l'attention des managers sur les indicateurs purement financiers mais aussi de ne pas réduire cet objet de recherche à un enjeu purement normatif de reporting sur les risques, de formalisation de contrôles ou de quantification de coûts en fonds propres. Nous nous inscrivons ainsi dans le prolongement des apports récents en contrôle organisationnel, et plus spécifiquement des travaux de Mikes (2009, 2011), Kaplan et Mikes (2012) mais également de Power (2005, 2009).

Ce prolongement théorique se situe à plusieurs niveaux :
-dans l'étude critique des dispositifs de contrôle et de gestion des risques au sein des organisations du secteur financier. Nos résultats permettent d'insister sur le fait de développer une réelle culture du risque via l'animation et la coordination d'un dispositif effectif. L'étude de l'effectivité des dispositifs de contrôle, telle qu'elle ressort de nos résultats, est en soi l'un des facteurs les plus significatifs de la notion de culture du risque, restant complexe à définir car par principe diffuse et contingente à chaque individu.

-dans la nécessité de penser de nouvelles formes de contrôle, davantage axées sur les vulnérabilités ou les menaces entourant l'organisation que sur le formalisme des procédures et du reporting comme finalité première.

-dans le caractère fortement interprétatif des normes de contrôle. Les dispositifs de régulation prudentielle s'apparentent aujourd'hui encore à des formes d'auto-contrôle (Maijoor, 2000 ; Spira, Page, 2003 ; Mainelli, Yeandle, 2006). Cet auto-contrôle, pour critiquable qu'il soit, et malgré l'appui des autorités de régulation du secteur financier, semble demeurer la solution la plus adaptée en matière de risques opérationnels. Cette catégorie de risque est par nature spécifique à chaque organisation dans ses modes de survenance (le risque informatique

dépend bien de l'architecture organisationnelle d'une société, le risque de fraude de sa vulnérabilité interne, le risque d'erreur de traitement de l'information des défaillances de son personnel et de ses procédures internes etc.). Aussi, et à la différence des risques financiers ou de crédit (ayant des effets de contagions), hormis les cas de risques opérationnels extrêmes, le risque opérationnel, eu égard à son caractère spécifique, valide la thèse de l'auto-contrôle.

Cette thèse de l'auto-contrôle doit cependant être validée sous plusieurs conditions de rigueur sur le plan théorique :

-la norme de contrôle[72] des risques opérationnels doit faire l'objet d'une traduction par la fonction de gestion des risques opérationnels en vue de sa transposition dans l'organisation,

-le dispositif de contrôle des risques opérationnels est par nature diffus et réparti entre les différents contrôles de l'entreprise (contrôle de gestion, contrôle qualité, contrôle de conformité, contrôle et audit interne, contrôle des opérationnels). Ce caractère parcellaire du contrôle est lié à la multiplicité des catégories de risques opérationnels. Aussi, une seconde condition de rigueur consiste à structurer les différents contrôles autour de l'enjeu risque opérationnel. Cette structuration est possible à la condition de disposer d'une fonction dédiée à la gestion des risques opérationnels. Cette fonction contribue à animer et coordonner la filière de gestion des risques opérationnels.

-Au-delà de la traduction de la norme et de la structuration-animation de son dispositif de contrôle, voulues par la réglementation, une troisième condition de rigueur permettant de passer de la normativité à l'effectivité se situe dans le rôle interactionniste de la fonction de gestion des risques opérationnels. Cette approche, en dualité (Top Down et Bottom Up), rend ainsi effectif la démarche de gestion des risques à la condition que ladite fonction réalise son rôle d'animation de la gouvernance vers les différentes fonctions de l'entreprise et de ces fonctions vers la remontée faite à la gouvernance d'entreprise quant aux différents risques opérationnels. Sans cette dernière condition de rigueur, une filière de gestion des risques, aussi structurée soit-elle, manquera d'effectivité car ne remplissant pas pleinement son rôle (donner une visibilité à chacun sur ses risques et traduire cette visibilité dans des actions de traitement du risque avéré et/ou de vigilance quant au risque potentiel).

[72] Citée dans le premier chapitre au travers des dispositifs prudentiels Bâle II et Solvabilité II notamment.

- **Structuration des contrôles du risque opérationnel**

Nos études de cas et les entretiens confirmatoires mettent en avant l'effort nécessaire de structuration des contrôles en vue d'aller vers une gestion effective du risque opérationnel.

Tableau 33. « Fonctions de contrôle » : objectifs et rôles convergents 'risque opérationnel'

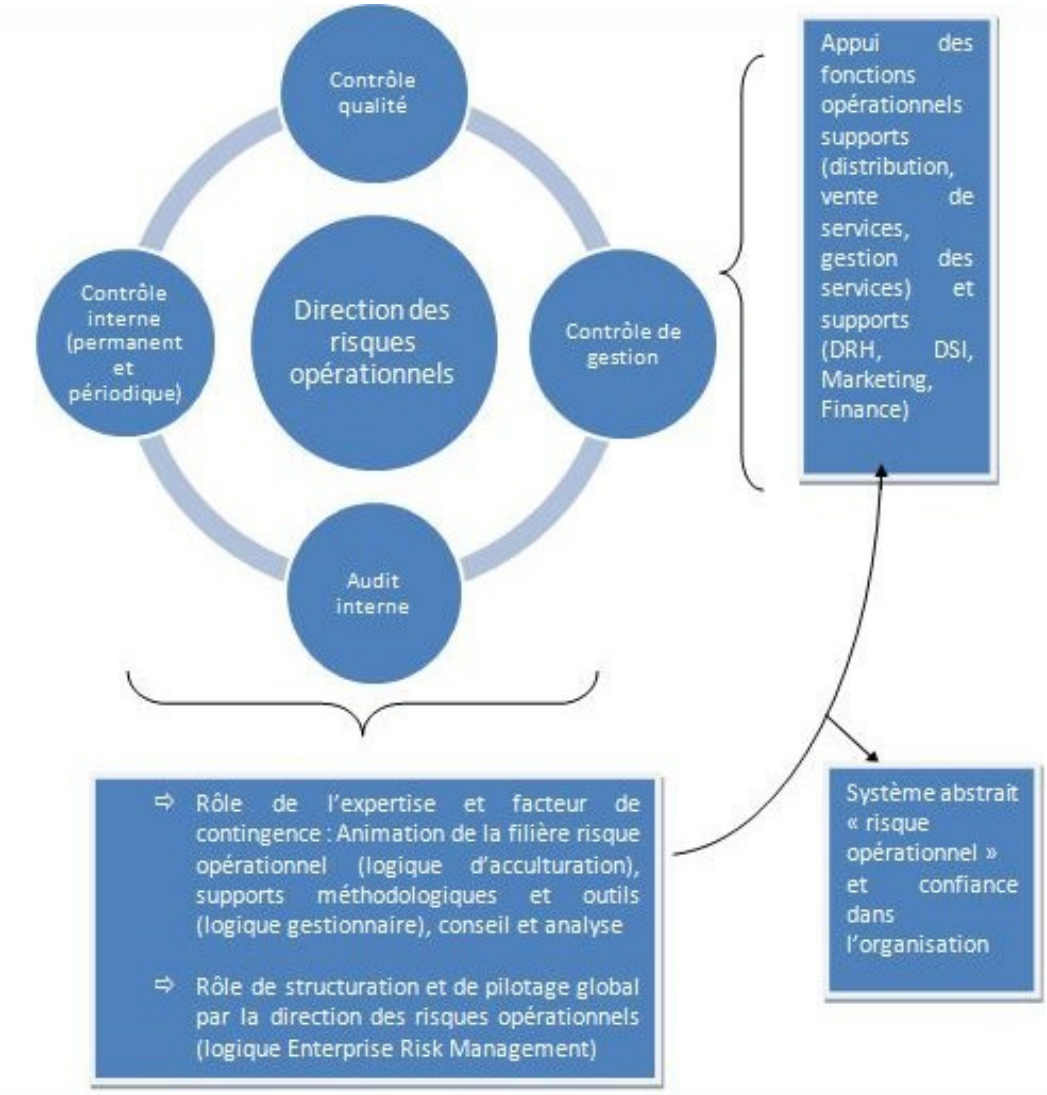
Fonctions	Objectifs de la fonction	Rôle risque opérationnel
Direction des risques opérationnels	Objectif global de maîtrise et de gouvernance du risque opérationnel.	Diffusion de la vision globale risque opérationnel, application et mise en œuvre de la politique de maîtrise des risques opérationnels, conseils méthodologiques et outils, analyses macro et micro sur des enjeux prioritaires de risques opérationnels, animation des correspondants risques opérationnels (reportings et déploiement des plans d'actions de traitement et réduction du risque etc.).
Contrôle interne (périodique et permanent)	Maîtrise et bonne application des processus.	Contribution à l'analyse et à la maîtrise des risques opérationnels par ligne métier (dans les fonctions opérationnels et supports de la chaine de valeur).
Contrôle de conformité	Conformité des pratiques commerciales aux lois et règlements (dont respect du devoir d'information et de conseil des clients).	Maîtrise du risque opérationnel sur les axes : juridique, respect de la réglementation sur les pratiques commerciales (devoir d'information et de conseil), veille juridique sur les enjeux de risques opérationnels
Contrôle de gestion	Analyse des données comptables et financières et maîtrise de la performance financière.	Intégration du facteur risque opérationnel dans les analyses de performance *(enjeu encore émergent)*.
Contrôle qualité	Maîtrise et amélioration continue des procédures (interne) et de la qualité de service (externe) délivrée aux clients.	Maîtrise du risque d'image et de réputation, prise en compte de l'impact des non-qualités et dysfonctionnement dans les analyses de vulnérabilités, analyses de causalité risque opérationnel *(enjeu encore émergent.*
Audit interne / Inspection Générale	Pertinence et efficacité du système de contrôle interne, analyse (croissante) des enjeux de maîtrise des risques.	Rôle d'appui dans le pilotage stratégique des risques, relais des sujets d'attention risque opérationnel auprès de la gouvernance : organes exécutifs, délibérants, comité d'audit, comité risque *(enjeu encore émergent)*.

Cette convergence d'objectifs vis-à-vis du risque opérationnel nous permet de résumer une approche organisationnelle en cours de développement au sein des établissements du secteur financier mais pour laquelle les établissements manquent encore de visibilité en termes d'interaction et précisément sur cette convergence d'objectifs observée lors de notre étude.

Cette approche organisationnelle est le fait des « filières risque opérationnels » exigées dans la réglementation prudentielle (notamment le règlement CRBF 97-02 mais aussi l'exigence de structuration du Risk Management dans le cadre du pilier II de la directive Solvabilité II en assurance.

Une telle approche est en partie transposée en pratique en banque et en cours de transposition en assurance, mais l'on remarque une structuration par étape, empreinte de variabilité. L'effectivité et l'efficacité du dispositif globale de gestion des risques dépendent de l'harmonisation de la vision et des pratiques orientées « risques » entre ces différentes fonctions.
Nous résumons ainsi un schéma fonctionnel de cette notion encore récente de « filière risque opérationnel ». L'effectivité de cette filière passe par la compréhension globale de ce besoin de structuration et son rôle de contribution à la confiance dans l'organisation.

Figure 42. Schéma fonctionnel de la structuration de l'expertise risque opérationnel



2.2. Contribution de la recherche sur le plan managérial

Sur le plan managérial, notre étude insiste sur le dépassement des éléments de reporting sur le risque, qui bien qu'importants, ne constituent que des moyens (de répondre aux enjeux réglementaires et prudentiels) au service de l'objectif d'amélioration de la gouvernance et de la performance de l'entreprise. Si certains des résultats semblent intuitifs, les échanges réalisés dans les études de cas montrent que bien souvent la thématique du risque opérationnel est réduite dans les établissements financiers au sujet de la conformité aux différents corpus de normes et à la réglementation macro-prudentielle. Dans les différents cas médiatiques, la gestion des risques et le contrôle interne sont souvent pointés du doigt comme étant défaillants. Ces dispositifs étaient pourtant bien réels mais manquaient d'effectivité au sens qu'ils étaient avant tout des contrôles de conformité et parfois de sanction. Notre apport est

d'insister sur le rôle de contrôle 'médiateur' voire 'formateur' des fonctions risques et contrôle interne.

- **Le contrôle des risques, ses écueils et voies d'amélioration**

Nos résultats font apparaitre des constats relatifs au rôle du contrôle des risques opérationnels comme facteur de responsabilisation.

-L'industrialisation des contrôles : l'écueil de la « technè »[73]

Un point récurrent abordé lors des entretiens concerne l'industrialisation des contrôles mis en place par les établissements bancaires depuis une dizaine d'années ainsi que par les sociétés d'assurance plus récemment. Ces contrôles ont été développés pour répondre aux normes citées dans notre partie théorique.

Nos entretiens exploratoires comme confirmatoires révèlent que l'on s'interroge aujourd'hui sur la pertinence des contrôles développés depuis le début des années 2000, de leur dimension globalisante et de leur vocation à s'étendre à toute l'organisation. Le coût du contrôle et ses externalités négatives (au sens de conséquences non voulues par les managers et décideurs) sont mis en avant mais il ressort principalement une critique portant sur le sens même des contrôles. Les différents responsables déplorent les limites de ces contrôles, souvent industrialisés : contrôles permanents de premier niveau réalisés par les opérationnels mais également les contrôles périodiques de second niveau et les audits internes (troisième niveau).

Les critiques sur le sens des contrôles sont d'ordre technique et méthodologique et induisent des résultats de contrôle souvent peu probants ou critiqués : seuils de déclenchement des contrôles peu pertinents au regard des risques, récurrence des fréquences de contrôles et des périmètres contrôlés, gestion du risque parfois uniquement par les outils et induisant un manque de communication et d'adhésion (fiche d'analyse de risque, cartographie des risques).

De telles problématiques sont clairement prises en compte mais il est difficile d'inverser une telle tendance comme l'illustrent les retours d'expérience ci-après :

Contrôleur autorité de régulation, EC-45, mars 2013, *« On s'est battu pendant des années pour que le contrôle et la gestion du risque cela ne soit pas que la cartographie ou les rapports internes, mais aujourd'hui les gens se cachent derrière les outils pour répondre aux exigences réglementaires. »*

[73] Au sens d'Hans Jonas (1979) : la « production » d'un savoir socialement organisé.

Directrice du contrôle interne et des risques opérationnels, EC-21, Décembre 2012, *« Sur le risque opérationnel, ce qui compte ce n'est pas tellement les outils ou le fait d'avoir bien tout renseigné, on estime que l'on a fait notre travail quand on sait qu'un projet lancé est sous contrôle ou que sur un périmètre on a enrayé les pertes. »*

Responsable du contrôle interne, EC-10, octobre 2012, *« Quand on est une petite structure, on est vite dépassé par l'importance des reporting réglementaires, cela peut devenir invivable et c'est souvent perçu comme quelque chose de bureaucratique, il y a un formalisme tel qu'on a l'impression de faire de la paperasse plus que du contrôle. »*

Consultant expert risque opérationnel, EC-30, février 2013, *« Pour les recommandations de l'audit et de l'inspection générale, c'est comme pour l'ACPR : l'égarement c'est de refaire sans cesse des recommandations. Depuis 2009, il n'y a aucune avancée sur les vrais sujets. On pense souvent que l'outil est génial, on pense que l'outil va « gérer le risque », or le risque et sa gestion c'est juste de l'humain ; on est dans l'illusion des outils. »*

-La stockholmisation[74] des contrôles : le mal de notre temps à dépasser

Pour plusieurs responsables de contrôles et de risques interviewés, les dispositifs normatifs relatifs au risque opérationnel, bien qu'ayant le mérite de laisser une marge d'autonomie posent une difficulté principale relative à leur interprétation. La notion de risque opérationnel est jugée comme extensive et comme donnant des lignes directrices générales sans toutefois préciser de mode opératoire sur les contrôles à mettre en place. Certains responsables ayant répondu de manière critique au sens des normes précisent notamment que la réponse « conformiste » au contrôle est à la fois le fait de normes très générales mais aussi très nombreuses, parfois contradictoires (conflits de normes). Le principal frein dans l'application des normes est également le fait de devoir être en veille constante sans pouvoir développer un recul suffisamment rapide sur l'interprétation et la lecture opérative de la norme.

[74] Expression reprise de l'un des entretiens avec un directeur contrôles et conformité et jugée très évocatrice par une vingtaine d'autres directeurs risques et contrôles interviewés. L'expression évoque l'idée que les contrôles sont davantage mis en place pour répondre aux attentes du régulateur que pour maîtriser les risques réels de la banque. Cette prise de position se fonde sur l'idée d'une décorrélation entre les attentes du régulateur, davantage axées sur la conformité des établissements financiers, et les soucis pratiques des directeurs risques et contrôles, cherchant à envisager les zones de risques au-delà des aspects de conformité normative.

Directeur conformité, EC-12, novembre 2012, *« Pendant longtemps, on a été dans l'interprétation de lois discutables sur la lecture que l'on en fait. Comme le régulateur représente l'autorité reconnue, même si on a notre propre interprétation on aura tendance à suivre celle du régulateur car on cherche à 'bien faire' d'emblée pour éviter d'avoir à réorganiser le contrôle. »*

Directeur Contrôle interne, EC-27, janvier 2013, *« Les risques opérationnels sont arrivés avant la mise en place des contrôles, on a voulu tout faire rapidement puis on a empilé des contrôles pour répondre aux demandes des différentes autorités, pour chercher à prouver que là où l'on était en risque, on mettait des garde-fous. »*

Consultant expert risque opérationnel, EC-23-janvier 2013, *« A force qu'il y ait de nouvelles normes, de nombreux groupes de travail, des études, des décisions nombreuses et contradictoires, des aléas dans la lecture des textes, on est noyé sous les normes donc on finit par dire au régulateur 'vous avez raison' alors qu'on ne devrait pas dire oui à tout mais rechercher notre propre lecture du sujet pour s'adapter à notre contexte. »*

Directrice des risques opérationnels, EC-19, Décembre 2012, *« Notre interprétation de la norme aurait du sens mais quand on est noyé sous les nombreuses analyses d'impacts, il est difficile de prendre le temps nécessaire pour prouver au régulateur notre bonne foi sur l'ensemble des sujets. »*

Outre ces constats, ce directeur de l'organisation, EC-24, janvier 2013, résume ainsi un tel sujet : *« Le législateur colle de plus en plus à la norme sans se poser la question de son application. Quand on a une nouvelle norme, on peut soit envisager des contrôles complémentaires, soit tenter de trouver l'occasion de réorganiser le contrôle, de répondre au problème des risques avant de chercher à tout encadrer par des procédures mal comprises ».*

-Le rôle des fonctions dédiées au contrôle des risques : guider les « risk owner » vers la responsabilisation

Afin de lever une difficulté inhérente à la logique d'auto-contrôle, soit des informations sur le risque fournies par les opérationnels et managers (il s'agit donc de déclaratif, pouvant induire

des biais), il incombe aux différents responsables des risques et contrôle de prodiguer les conseils et grilles de lecture sur les attentes réglementaires mais aussi des instances de gouvernance en matière de risque. Pour les différents Risk Managers et contrôleurs interviewés (tableau 3), leur rôle n'est pas fondé sur la sanction et sur l'approche réglementaire, un tel argument n'intervient qu'in fine. Les analyses en termes de discours nous montrent alors que ces responsables dédiés s'apparentent eux-mêmes à des « consultants internes » ou à des « organisateurs ». Le rôle d'animation (dans le cas des Risk Managers) et de conseil en matière de conduite du changement (dans le cas de nombreux contrôleurs) est mis en avant comme un rôle émergent qu'ils cherchent à développer. Le pouvoir de sanction intervient en cas de non adhésion à la démarche de contrôle et de gestion des risques.

Directeur des risques opérationnels, EC-11, Novembre 2012, *« Le régulateur est comme nous, dans une logique d'apprentissage sur ces sujets, ils construisent une philosophie, ils recherchent un équilibre entre l'intérêt de l'entreprise et la protection de la clientèle. On pense qu'ils sont en phase d'observations en grande partie. »*

Contrôleur autorité de régulation, EC-52, mai 2013, *« Notre souhait est avant tout que les méthodologies soient simples, claires, robustes, qu'il y ait un cercle vertueux. Il faut éviter les dispositifs compliqués et éloignés des préoccupations des opérationnels car ils chercheront à se débarrasser des contrôles le plus vite possible. »*

Directeur des risques opérationnels, EC-41, mars 2013, *« Les outils on s'en sert mais notre rôle c'est vraiment de faire de l'animation : nous ne sommes pas un grand groupe mais c'est un travail conséquent, il faut se parler fréquemment, on est obligé de faire en sorte d'être prévenu sur des nouveaux produits, sur des zones de risques, sur des fraudes qui repartent à la hausse, il faut être présent et avoir une vraie attention à l'égard des métiers. »*

Risk Manager-responsable du contrôle de gestion risques opérationnels, EC-20, Décembre 2012, *« Aujourd'hui nous n'avons pas de pertes mais cela ne veut pas dire qu'il n'y en aura pas demain : on doit donc guider nos opérationnels et leurs managers pour qu'ils fassent remonter leurs inquiétudes, on fait de l'ingénierie sociale en quelque sorte. »*

Directeur contrôle interne, EC-28, janvier 2013, *« On est avant tout dans une approche d'efficience : le métier accepte de nous suivre car on lui a expliqué pourquoi on contrôle,*

comment on le fait. On leur fait un retour fréquent et une analyse pour les aider à être vigilants. L'essentiel est que l'on soit cohérent : quand il n'y a pas d'enjeux on arrête le contrôle pour se focaliser sur les vrais risques. »

-Le « guidage » par les principes et l'autonomie de la volonté et de la responsabilité

Les démarches efficaces de mise en application des normes impliquent pour les responsables risques et les contrôleurs de réaliser une traduction des attentes et un maillage des nombreux points d'attention et de reporting sur le risque opérationnel. Cette traduction et ce « tri » étant réalisés, l'approche d'animation de filière risque (mettre en œuvre la politique de risque de l'entreprise) se fait alors en recherchant l'adhésion à la démarche de gestion des risques. La responsabilisation des acteurs est avant tout recherchée. Cette responsabilisation passe par l'autonomie, on entend ici autonomie au sens de mise en responsabilité des opérationnels chargés de fournir des informations sur le risque (les contributeurs ou correspondants risques opérationnels dans les différentes fonctions opérationnelles ou supports) ou encore des collaborateurs contrôlés. En matière de reporting « déclaratif », la responsabilisation suppose l'adhésion, cette dimension du contrôle est alors clairement qualitative car fondée sur le discours et sur la diffusion de bonnes pratiques, de conseils d'amélioration ainsi que de méthodologies et outils suffisants (dont la manière d'employer ces outils à bon escient). Il ressort de nos entretiens que le rapport à la norme est rarement évoqué (excepté par exemple le cas des reportings réglementaires tels que les états récurrents COREP[75]).

Directeur des risques opérationnels et conformité, EC-25, janvier 2013, *« On cherche à sortir de la logique du 'on a bien rempli les documents, on a bien fait remplir', notre but c'est que les métiers soient responsables et vigilants pour éviter le danger de la routine. »*

Risk Manager, EC-17, Décembre 2012, *« Ce qui compte pour être reconnu et que l'on fasse appelle à vous, c'est le pragmatisme. Quand on sait dire 'je m'écarte de la règle et des blocages pour faire avancer le projet' on gagne à être reconnu. Cela ne veut pas dire que l'on lâche du leste sur tout. Je continue à être intransigeant sur les risques importants, quand c'est potentiellement grave. Mais je ne mets un veto 'temporaire' que quand c'est nécessaire, c'est apprécié, on fait appel à moi pour des projets par conséquent. »*

[75] Déclaration réglementaire relative aux ratios de solvabilité des établissements de crédit.

Contrôleuse interne, Ec-18, Décembre 2012, *« On a peu de moyens donc on est obligé d'aller à l'essentiel, on s'assure que les contrôles et l'identification des risques soient faits de manière homogène. On s'appuie beaucoup sur les opérationnels alors il faut leur laisser une marge de manœuvre tout en s'assurant qu'ils ont bien compris ce que l'on attend et qu'ils en voient l'intérêt pour eux-mêmes, pas seulement pour faire du reporting. »*

Directeur contrôle interne, EC-34, février 2013, *« La plus-value du contrôle c'est de pouvoir investir sur les priorités, de ne pas mettre tous les risques au même niveau. On doit être factuel mais aussi proposer des solutions aux opérationnels, analyser le bon niveau de contrôle à fournir et admettre quand le travail fait est suffisant. De cette manière ils se responsabilisent eux-mêmes car ils ne nous voient pas comme des apporteurs de contraintes mais de solutions. »*

-Responsabilité et anticipation : une approche culturelle sur un « mode mineur »

In fine, on retrouve dans nos résultats la thématique de l'obligation à l'avenir dans la mesure où le rôle central du Risk Manager et des contrôleurs interne consiste en la diffusion d'une culture du risque opérationnel (envisagée comme une culture de la responsabilisation sur les sources de risques liées à l'activité de chaque opérationnel et manager). Cette culture du risque opérationnel n'est en pratique pas exprès, elle émerge dès lors que les différents métiers[76] ont intégré le risque dans leur activité courante, non comme une priorité, ce qui paralyserait l'action, mais comme un facteur parmi d'autres à prendre en compte dans la conduite de l'activité quotidienne. Si le résultat opérationnel (objectifs de vente, de chiffre d'affaires, de résultat d'exploitation et de résultat financier) reste une priorité de l'action, sur un mode « majeur », le facteur risque est envisagé sur un mode « mineur » comme un paramètre pouvant nuire à l'atteinte des objectifs opérationnels. La culture de la prévention face au « risque métier » qu'est le risque opérationnel s'acquiert dès lors qu'elle est associée à l'atteinte des objectifs de chaque partie prenante.

[76] Desks de trading, département d'activité de crédit, départements de souscription, de gestion et d'indemnisation en assurance, fonctions supports telles que la Direction RH, la Direction SI, la direction du Marketing, gestion des réseaux de distribution, la direction financière, la direction technique etc.

Directeur des risques opérationnels, EC-11, novembre 2012, *« On ne cherche pas à faire du normatif, notre activité de gestion du risque c'est avant tout de s'assurer que les métiers gardent ce paramètre en tête et pensent à nous solliciter s'ils ont un doute ou besoin d'une aide dans l'analyse de risque. »*
Risk Manager, EC-22, janvier 2013, *« Identifier les risques opérationnels, c'est beaucoup de formation à la prévention, on considère que l'on répond à l'esprit de la réglementation si les opérationnels font attention aux risques dont ils sont propriétaires. »*
Risk Manager, EC-50, avril 2013, *« Quand les managers passent d'une logique où les risques ne sont pas leur problème à une vision où ils souhaitent notre avis et notre appuie pour lancer un projet et le pérenniser, on mesure le chemin parcouru. »*

Directeur du contrôle interne, EC-21, décembre 2012, *« Le risque devient un sujet de prévention quand les managers et les directeurs voient l'impact de ce facteur sur leur résultat brut d'exploitation. On parle de culture du risque quand il se demande combien de chiffre d'affaires il faut réaliser pour compenser les pertes risques opérationnels. »*

- **Existe-t-il une demande d'effectivité du contrôle des risques opérationnels ?**

Les entretiens réalisés avec les membres de l'autorité de contrôle des secteurs banque et assurance nous fournissent également une compréhension quant à une réelle demande d'effectivité du contrôle des risques. Cette demande passe notamment par :

-des dispositifs de contrôles réellement mis en place et non limités à des procédures, afin de prendre en compte la réalité extensive du risque opérationnel,

-des dispositifs de contrôle et de maîtrise des risques transparents et, bien que perfectibles, permettant d'avoir une réelle vision de l'exposition au risque de l'entreprise et de ses zones de progression,

-se doter d'une réelle gouvernance du dispositif de contrôle des risques en vue de faciliter la diffusion d'une lecture commune et des règles de maîtrise des risques à appliquer, cette gouvernance comprenant une communication sur les risques.

Ce que confirment les verbatim suivants extraits de nos résultats :

« On préfère voir des cas où tout reste encore à faire que des entreprises où en apparence tout est bien et dont on découvre ensuite des risques. Il faut bien quatre à cinq ans pour avoir un dispositif mature » explique cette contrôleuse assurance, EC-46, mars 2013.

« Notre souci est que les contrôles soient réalisés et que ce qui est fait soit documenté. C'est bien de nous dire que tout est fait mais si il n'y en a aucune preuve comment voir les améliorations ou comment savoir si les contrôles en interne sont aussi poussés qu'on nous le prétend ... Cela nous est déjà arrivé de voir des process mis en place mais dont l'application n'était pas faite, c'était théorique. On le faisait pour être conforme » expose cette contrôleuse des assurances, EC-46, mars 2013.

« Il faut passer d'une culture du contrôle à une culture du risque, c'est long, progressif et parfois cela n'aboutit pas. Beaucoup de contrôles sont réalisés dans les établissements, mais le travail de centralisation est long et il y a des problèmes de redondances entre les contrôles réalisés » invoque ce contrôleur des assurances (risques et contrats), EC-45, mars 2013.

« Avoir une pluralité de contrôle cela n'est pas gênant en soi, mais il faut que cela donne lieu à une véritable communication sur le risque, sinon cela ne sert à rien » nous informe ce contrôleur bancaire, EC-55, mai 2013. Des propos complétés par cette contrôleuse bancaire, EC-52, mai 2013 : *« Dans la réglementation prudentielle, notamment le 97-02 il y a une marge d'interprétation, on peut en avoir des compréhensions différentes d'un établissement à l'autre, d'une direction à l'autre et même pour nous d'un contrôleur à l'autre. C'est à double tranchant : s'il est plus facile d'avoir une réglementation qu'on interprète, le risque est de passer à côté de l'essentiel. Le traitement du risque est alors différencié selon la lecture du risque que l'on peut avoir. Il faut un organe central qui fait une traduction, décrit la lecture à avoir des règles et leur interprétation, cela facilitera une lecture commune et partagée. »*

« Il ne faut pas limiter le risque opérationnel au risque client et au LAB/LAF/LAT[77]*, mais ces segments du risque opérationnel sont parfois sous-estimés. La démarche de base consiste à*

[77] Respectivement : lutte anti-blanchiment (LAB, parfois appelée LCB pour lutte contre le blanchiment), LAF pour lutte anti-fraude (recouvrant les fraudes internes et externes pouvant avoir comme source ou comme issue le blanchiment de capitaux et comprenant par extension la fraude fiscale), et LAT pour la lutte anti-terrorisme (comprenant généralement les mesures de gel des avoirs prises à l'encontre de terroristes ayant fait l'objet de condamnations sur les plans national et européen).

regarder ce que l'on vend et ensuite à voir les règlements applicables, les contrats vendus, les risques sur ces contrats », indique cette contrôleuse bancaire, EC-54, mai 2013.

« Un dispositif permanent : qu'est ce que ça signifie ? La frontière entre le périodique et le permanent n'est pas toujours tranchée, il faudrait des interactions plus fortes entre les deux mais sans limiter le dispositif à cela », EC-45, mars 2013.
Un contrôle effectif doit avoir du sens et ne pas se limiter à une approche minimaliste consistant à répondre uniquement aux exigences réglementaires ou aux demandes de l'autorité de tutelle. La recherche de sens dans le contrôle est donc une préoccupation partagée par les acteurs en charge du contrôle au sein de l'autorité de tutelle des secteurs banque et assurance.

« Un contrôle doit être intelligent et avoir du sens. On retrouve cet enjeu à la fois en contrôle interne mais aussi en conformité. On a un corpus de normes enrichit régulièrement avec des empilements de règles que les banquiers et les assureurs ont du mal à suivre. Mais ce n'est pas pour cela qu'un travail a minima doit être fait. » indique cette contrôleuse bancaire, EC-52, mai 2013.

- **La structuration du contrôle, une dimension du tryptique d'effectivité des contrôles orientée « confiance »**

Nos études de cas ainsi que les entretiens réalisés contribuent à conforter l'idée selon laquelle le contrôle et la gestion des risques contribuent à la notion de confiance dans l'organisation en structurant l'enjeu du risque opérationnel comme système abstrait et pour lequel les différents garde-fous de la notion de confiance sont assurés.

Toutefois, notre recherche met également en avant la nécessité d'un contrôle structuré dans l'organisation, écueil étudié lors de nos entretiens confirmatoires dans une dizaine de structure bancaires et une dizaine de sociétés d'assurance. *« Le risque opérationnel…on a beaucoup tourné autour du pot avec cela : les fiches risques clés, les nombreux reporting. Mais après tout le temps passé sur le sujet, dire si on a avancé sur le sujet est un vrai débat »* résume ce directeur des risques opérationnels (EC-32, février 2013).

Nos études de cas viennent étayer ce constat : il est possible de dépasser *« l'illusion du contrôle »* par la recherche d'interaction entre les contrôles, chaque type de contrôle contribuant à sa manière à la recherche de maîtrise du risque. « *Un contributeur peut faire à*

la fois du contrôle permanent, du risque opérationnel, de la cartographie et de la conformité. Le contrôle c'est parfois du 'multi-tasking' » explique ce responsable d'audit interne. Les entretiens réalisés auprès de responsables risques et contrôle confirment les finalités diverses de ces contrôles et la convergence d'objectifs sur l'enjeu risque opérationnel. *« Il y a une vraie attente de guichet unique car quand on est métier, on ne comprend pas tout. Sur les SI, sur la conformité, sur les risques opérationnels, sur le PCA il y a une confusion. Même les métiers dédiés entre eux ne comprennent pas tout, sur la correspondance entre conformité et contrôle interne par exemple. Sans parler des liens entre contrôle de gestion et les autres contrôles… »* commente ce Risk Manager (EC-22, janvier 2013).

La diversité des acteurs concernés tant dans nos études de cas que dans nos entretiens tend à mettre en avant certains enjeux actuels (lien entre contrôle interne, conformité et risque opérationnel) mais aussi les enjeux émergents de structuration en matière de Risk Management Opérationnel :

-Le lien entre **contrôle de gestion et risque opérationnel** est le suivant : le contrôle de gestion contribue aux outils de détection des risques opérationnels et nourrit ainsi le dispositif du risk management (alimentation des informations sur les indicateurs clés de risque). Le contrôle de gestion est une « sonde » fournissant des indicateurs avancés. Il n'est aujourd'hui pas essentiel dans les dispositifs risque opérationnel mais joue un rôle croissant de vigie et d'alerte pour les directions des risques opérationnels.

-Il y a un **lien entre risque opérationnel et qualité** dans certains cas : en matière de prestation de services, dans les systèmes d'information, il s'agit d'enjeux de qualité imbriqués à la thématique du risque opérationnel. Dans ces différents cas, la gestion du risque opérationnel est souvent faite de manière tacite dans la recherche de réponse aux problématiques de qualité vis-à-vis des clients. On retrouve également en qualité des indicateurs prédictifs[78] de risque opérationnel (notamment dans la recherche de fiabilité).

-Le lien entre gestion des **risques opérationnels et audit interne** a été observé et s'analyse comme une extension du rôle de l'audit interne traditionnellement positionné sur l'évaluation

[78] Notamment l'analyse d'écart entre la qualité produite et la qualité réalisée (sur une période de référence et entre période).

de la pertinence et de l'efficacité du dispositif de contrôle interne. Cette fonction est indépendante mais néanmoins proche de la gouvernance, ce qui tend à confirmer certaines recherches sur un domaine peu répandu à ce jour (Colbert, Alderman, 1995 ; Spira, Page, 2003). Ce rôle se fait notamment sur des points d'attention clés remontés aux organes de gouvernance par les rapports adressés au comité d'audit notamment. (Hillison et al., 1999).

Ces objectifs vis-à-vis du risque opérationnel nous permettent de résumer une approche organisationnelle en cours de développement au sein des établissements du secteur financier mais pour laquelle les établissements manquent encore de visibilité en termes d'interaction et précisément sur cette convergence d'objectifs observée lors de notre étude. Cette approche organisationnelle est le fait des *« filières risque opérationnels »* exigées dans la réglementation prudentielle (notamment le règlement CRBF 97-02 mais aussi l'exigence de structuration du Risk Management dans le cadre du pilier II de la directive en cours d'élaboration Solvabilité II). En répondant à ces objectifs de filière risque opérationnel, le Risk Management contribue à la structuration des garde-fous de la confiance évoqué et par la-même à améliorer progressivement la maîtrise du risque opérationnel. L'effectivité du dispositif global de gestion des risques dépend de l'harmonisation de la vision et des pratiques orientées « risques » des différentes fonctions ainsi que de la compréhension de la gouvernance du rôle joué par le Risk Management comme un système interactif d'aide à la décision. L'effectivité de cette filière passe par la compréhension globale de ce besoin de structuration et son rôle de contribution à la confiance dans l'organisation, rôle assumé par la direction des risques opérationnels dans son travail d'animation.

Notre recherche se situe dans le prolongement des travaux sur le contrôle interne et le Risk Management (Simons, 1995 ; Mikes, 2011). Ainsi, certaines recherches démontrent que les conditions d'effectivité du contrôle des risques sont notamment l'institutionnalisation du contrôle mais aussi le fait de mettre en œuvre un management actif (Cappelletti, 2006 ; 2009). Nous nous inscrivons dans cette perspective en précisant une composante essentielle qui est la recherche de structuration par la réponse aux garde-fous de la confiance moderne. L'institutionnalisation du contrôle est une première étape vers la recherche d'un contrôle des risques effectif (Spira, Page, 2003 ; Hakenes, 2004). Si le management actif est également une condition essentielle pour la réussite d'une démarche de contrôle, notre recherche tend à affirmer que ce management actif passe par le rôle d'influence et d'incitation à la démarche de gestion des risques que permettent les directions des risques opérationnels (Bon-Michel,

Dufour, 2013). Comme le relève Simons (1995, p.34), il est nécessaire de pouvoir développer un contrôle interactif, de diffuser les valeurs de l'entreprise mais aussi de développer un diagnostic efficace et une bonne visibilité des seuils de risque déterminés par l'entreprise. C'est à ces différents objectifs que contribuent les directions des risques opérationnels en termes de structuration des contrôles, cette structuration étant la condition d'un rôle d'influence permettant ce management actif. En permettant cette confiance dans le système abstrait *« risque opérationnel »,* cette fonction transverse contribue à une meilleure compréhension et au développement de l'entreprise (par son rôle de sauvegarde de la valeur).

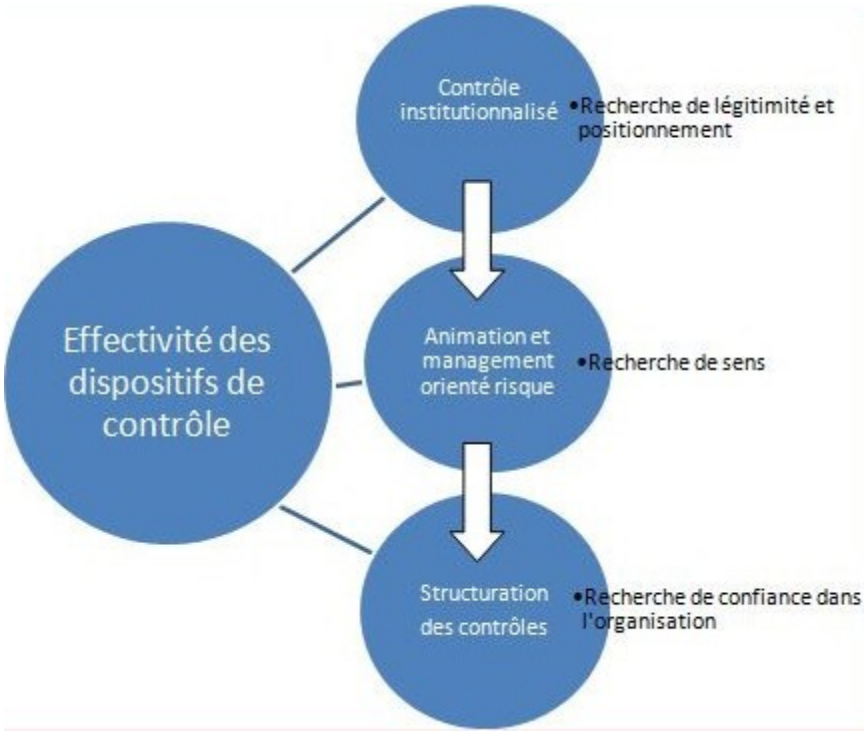
C'est alors dans cette optique associant institutionnalisation, structuration et management actif que l'organisation du contrôle des risques[79] peut s'inscrire dans la recherche de compréhension de l'organisation (une structuration du contrôle face aux zones de risque de l'organisation) et de développement interne de celle-ci dans une logique de performance durable (maîtrise du risque lié à l'activité et pérennisation des différentes lignes de business).

-L'institutionnalisation permet alors la légitimité du positionnement et une facilité de déploiement dans l'organisation.

-La structuration du contrôle permet de cerner l'objet complexe et abstrait risque opérationnel.
-Le management actif permet d'orienter le contrôle ainsi structuré pour que ce dernier soit parlant, porteur de sens et intégrant la vision risque pour les opérationnels et les managers.
Ces trois composantes tendent à expliciter l'objectif d'effectivité visant à transcender l'illusion du contrôle évoquée précédemment.

[79]Nous envisageons cette organisation en tant que filière risque opérationnel, soit la filière intégrée comprenant le Risk Management Opérationnel mais aussi l'ensemble des contrôles dédiés ou associés à l'enjeu risque opérationnel.

Figure 43.Tryptique d'effectivité des dispositifs de contrôle



- **Un besoin partagé de formalisations de bonnes pratiques en matière de risque opérationnel**

Notre recherche, outre les éléments précités, nous orientent également vers une préoccupation managériale forte, laquelle consiste en une demande récurrente des praticiens du contrôle des risques, pour la formalisation de bonnes pratiques (guidelines) en matière de gestion des risques opérationnels. La quasi-totalité de nos entretiens auprès d'acteurs en charge du contrôle des risques opérationnels fait ressortir une demande : « avez-vous des éléments à nous communiquer concernant des bonnes pratiques ou la manière dont procèdent les autres sociétés pour gérer leurs risques opérationnels ? ». Les phases de discussions-échanges contradictoires dans nos entretiens ont quasi-systématiquement été l'occasion de faire se livrer à ce type d'échanges. Les verbatim ci-après illustre ces demandes :

« Il faudrait plus de recommandations, des vrais guidelines, mais on a mis en place cette réglementation et réfléchi après à son application. Il faut aujourd'hui faire le travail inverse pour que cela reste applicable » confirme ce directeur des risques opérationnels (EC-14, novrembre 2012).

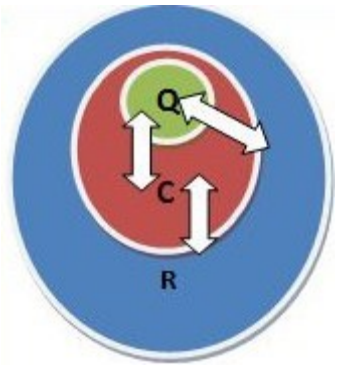
« Ce n'est pas à l'ACPR de traiter les causes racines. On est là pour contrôler que chacun a mis en place sa maîtrise des risques. On n'intervient encore a posteriori, en cas d'urgence. On déplore que beaucoup d'assureurs fassent le minimum en attendant d'en savoir plus sur Solvabilité II » explique ce contrôleur de l'autorité de contrôle (EC-46, mars 2013).

- **Vers un modèle pragmatique d'interactions structurées pour cerner le risque opérationnel ?**

Nos entretiens et les études de cas réalisés font ressortir les liens étroits existants entre fonction de gestion des risques, fonction de contrôle et fonction qualité. Nous proposons, à la lumière des enjeux pratiques et des interactions fortes constatées un « modèle » organisationnel d'interactions entre ce tryptique (Darsa, Dufour, 2014).
Il est essentiel de faire interagir les différentes dimensions relatives au risque. Faire interagir contrôle, qualité et maîtrise des risques est encore l'un des meilleurs moyens de créer du sens dans la démarche globale de gestion des risques. Si l'on essaye de représenter la cohérence et les interactions entre ces trois fonctions critiques, nous serions amenés à illustrer notre propos de la manière suivante :

Q :
Dispositifs Qualité
Actions centrées Clients
Satisfaction / Amélioration continue des processus
C :
Dispositifs de contrôle interne
Actions centrées Entreprise
Contrôle permanent, périodique, de conformité
R :
Dispositifs de maîtrise des risques
Actions centrées sur l'entreprise et son environnement
Pérennisation de l'organisation, quel que soit le spectre considéré
Les trois dispositifs interagissent en permanence entre eux, à l'appui d'objectifs et d'indicateurs de mesure de performance spécifiques. Leur vocation est diverse, mais l'indicateur d'alignement collectif de chacun des dispositifs demeure le même sur l'échelle temporelle éloignée de l'entreprise : la pérennisation de l'organisation.

Figure 44. Modèle QCR



Les démarches qualité, contrôle et risque s'avèrent par nature de puissants vecteurs de fédération des équipes et de différenciation des organisations. La fédération des équipes autour d'indicateurs d'alignement communs tels la pérennité de l'entreprise, la recherche permanente de la satisfaction client et le contrôle des opérations menées, quelles qu'elles soient s'inscrit ainsi à la création de Valeur de l'entreprise dans son ensemble, et contribue à donner du sens aux équipes. Les méthodes de conception, de mise en œuvre, de déploiement et de pilotage des enjeux qualité, de contrôle interne et de maitrise des risques contribuent enfin à devenir de véritables clés de différenciation affirmées pour l'entreprise.
Face aux risques, à la qualité ou à l'exigence de contrôle interne, les entreprises se positionnent, se définissent, se distinguent et, à l'issue se différencient positivement ou négativement vis-à-vis de leurs clients internes ou externes, de leurs tiers de confiance, de leurs réseaux relationnels, sociaux humains etc. De fait, les démarches qualité, de contrôle interne et de maîtrise des risques contribuent grandement à cette démarche essentielle de différenciation, à partir du moment où ces dernières sont mûrement réfléchies et affirmées, au-delà des pratiques superficielles et des effets d'annonce, trop souvent rencontrées dans les faits.

Différenciation et fédération des équipes autour d'un objectif commun, à l'appui de réflexions et d'actions construites relatives à la maîtrise de la qualité, du contrôle et des risques constituent sans nul doute de puissants vecteurs à rechercher au sein de chaque organisation.

- **Normativité, créativité, opérativité : les leviers du contrôle du risque ?**

L'analyse de nos études de cas et des entretiens réalisés vise à montrer que le rôle du Risk Manager en tant qu'acteur-réseau au centre de la politique de risque opérationnel suppose d'aller de la normativité à l'opérativité par la créativité des visions et des méthodes.
Notre recherche montre que l'un des leviers essentiels de réussite d'une politique de risque opérationnel est alors le levier communicationnel visant à créer de la connaissance sur la base de l'information en passant du dénombrement du risque à son discernement. Ce levier communicationnel prend fondement source à la fois la nécessité d'un chiffrage comme appui et d'éléments plus qualitatifs comme des scénarios et pédagogie du contrôle développé dans une logique relationnelle.

Cet axe de nos résultats met également en avant le rôle récurrent de traduction de la norme, de la réglementation prudentielle mais aussi des exigences du régulateur pour les managers opérationnels des établissements bancaires et d'assurances. Cette traduction de la norme passe également par l'animation des enjeux de gestion que suppose le risque opérationnel. Les entretiens tendent à confirmer les études de cas sur les points suivants : un besoin croissant de « conseil » et « d'accompagnement » du Risk Manager (direction des risques opérationnels) vers les opérationnels et managers (fonctions opérationnels comme supports). Ce besoin s'exprime au travers du rôle émergent « d'organisateur » auquel doit répondre le Risk Manager en charge des risques opérationnels par pôle d'activité dédié.

-Le rôle de la créativité face aux risques opérationnels, rompre avec les routines du contrôle : Cette approche plus « créative » en contrôle des risques est perçue comme un moyen d'éviter de déresponsabiliser les collaborateurs face à un contrôle routinier qui ne répond pas effectivement aux attentes d'assurance sur la bonne maîtrise du risque. Etre créatif concernant le contrôle des risques nécessite de développer des contrôles non systématiques, évitant que les opérationnels puissent les contourner facilement car ils ne les connaissent que trop bien. Il s'agit bien de l'un des écueils essentiels relevés dans les scandales qui ont affectés certains établissements financiers.

-Qu'est ce que la créativité en contrôle et gestion des risques opérationnels : La créativité peut consister à faire varier les seuils de contrôle, sans aller jusqu'à contrôler une opération financière au premier euro. En effet, des opérations dont les seuils dépassent la dizaine de

milliers d'euros ne sont pas toujours pertinents pour saisir des fraudes en cascade sur de faibles montants. La formation et l'information des contrôleurs et des personnels contrôlés, même s'il s'agit de bon sens, font encore défaut dans des dispositifs qui ont été rapidement industrialisés pour répondre aux exigences normatives. Quand les formations existent, elles répondent là encore à des enjeux principalement de respect de la norme plus que d'une recherche de diffusion de connaissance dans un objectif de faciliter la gestion du risque par les opérationnels : formation trop généraliste, e-learning standards par exemple. Cela représente un coût à prendre en compte, mais l'industrialisation des contrôles constitue elle-même un coût important dont il conviendrait de s'interroger sur l'efficacité et la rentabilité dans un rapport coût/bénéfice des contrôles. Superposer les contrôles génèrent une impression de lourdeur pour les opérationnels. Il est temps de réfléchir à une plus grande complémentarité des contrôles de premier, de second et de troisième niveau, notamment entre contrôles périodiques et permanents (Mitra, 2009).

La réussite du contrôle des risques consiste à se faire reconnaitre, à devenir indispensable. Cela se fait dans la durée et passe par l'expertise et la reconnaissance en interne. Il est alors possible de passer du cercle vicieux associant la gestion des risques à une autre forme de contrôle au cercle vertueux qui consiste à ce que les collaborateurs voient la politique de risque comme un élément essentiel de leur travail.

-Créativité dans le design du contrôle : Notre étude permet aussi de constater que si la culture du « contrôle à la tâche souffre de nombreuses limites », il faudrait davantage aller vers un contrôle de second niveau sur la base d'indicateurs. « *Le problème du contrôle qui répond uniquement à la demande du régulateur, c'est que l'on ne régule plus rien même si l'on contrôle bien »* nous précise ce responsable risques opérationnels. Il s'agit en effet d'être outillé par un reporting et une décision efficace (indicateurs clés de risque, outils de data mining, outil de cartographie efficace et de réalisation de scénario avec probabilités conditionnelles), mais cet outillage n'a d'utilité qu'en support d'une vision « supra » du rôle du contrôle des risques. Lequel apparait non seulement comme un système d'alerte dans l'organisation mais également comme un moyen de conseiller les opérationnels dans une démarche d'amélioration continue (Drott-Sjoberg, 1991).

-Repenser le contrôle en pensant les contrôles de manière intégrée: Notre recherche nous amène enfin à nous interroger sur le manque récurrent d'interactions entre des fonctions

comme le contrôle de gestion et les dispositifs de contrôle interne. Il ressort de notre étude et de certains des entretiens réalisés que si ces interactions font défaut et sont sources de confusions multiples, c'est à la fois en raison d'un éclatement des dispositifs de contrôle dans l'organisation mais aussi d'un manque de maturité des différents contrôles sur les sujets de risque. Ainsi, de nombreux directeurs nous confient que si cela reste en pratique difficile, les opérationnels seraient réellement en attente d'un « guichet unique »[80] en matière de contrôle, auquel adresser ses différents reportings et avec lequel échanger. Si les contrôles restent distincts, le rôle du Risk Manager des directions risques opérationnels peut être de faire le lien entre ces différentes sources d'informations internes. La créativité alors évoquée peut aussi être envisagée à ce stade des interactions entre contrôles interne, contrôle qualité, contrôle de gestion etc., source latente de création de valeur organisationnelle et supposant un « toilettage » régulier du contrôle interne (Cappelletti, 2006 ; Cappelletti, 2009b), à la lumière de l'enrichissement mutuel des constats, méthodes et démarches. Cela constitue en soi une perspective de recherche future.

- **« Vendre le risque » dans l'organisation, un enjeu de contrôle budgétaire et de responsabilisation des acteurs.**

La recherche menée met en avant comme levier la présence de responsabilisation face au risque opérationnel. S'il ressort de l'étude que le risque opérationnel est un risque principalement subi, l'un des axes de réflexion récurrent concerne l'intégration de la variable risque opérationnel dans le processus de contrôle budgétaire et d'information à disposition des décideurs (notamment dans le lancement de nouvelles activités, produits ou lors de réorganisations internes).

Nous remarquons également que la responsabilisation passe par la logique de compréhension de l'enjeu 'risque opérationnel' (de la notion, de ses implications pour l'organisation mais également du rôle joué par les contrôles de leur cohérence, de leur pertinence et aussi de leur efficacité).

-Formaliser le principe de responsabilité, une difficulté ?

[80] Au sens de disposer au sein des établissements financiers d'un acteur ou d'une fonction capable de centraliser les problématiques méthodologiques, techniques et réglementaires relatives au risque opérationnel et à sa prise en charge.

La transposition pratique d'un tel principe est en soi un objet d'étude à part entière. Notre étude montre qu'il n'est pas nécessaire « d'institutionnaliser » le principe de responsabilité, ce qui reviendrait à l'intégrer en tant que procédure ou document de référence et à chercher à normaliser ce qui est de l'ordre du contingent au facteur humain. Ce principe s'envisage a contrario comme la grille de lecture des dispositifs prudentiels en place.

Nos entretiens nous éclairent sur ce sujet : la responsabilisation des acteurs peut-être « institutionnalisée » en intégrant les pertes « risques opérationnels » comme un critère d'atteinte des objectifs impactant les bonus des managers et opérationnels. Toutefois, outre les aversions internes que de tels axes impliquent (dans plusieurs structures, cette approche était développée), cela ne permet pas complètement de résoudre les non-dits et dissimulation des risques dans l'organisation (surtout les risques les plus importants) : cette logique de responsabilisation devient alors une logique de « remise en cause » du travail accompli par le manager.

La diffusion de ce principe passe donc par les échanges et les interactions entre « les animateurs » des filières risques et contrôle, elle comprend une part d'informel mais peut-être déclinée dans les politiques de maîtrise des risques comme un axe prioritaire (Power, 2009 ; Mikes, 2008b ; 2011).

-S'assurer de la conformité des normes et de l'opérativité du principe de responsabilité.

Notre recommandation en terme managérial se situe davantage dans une perspective « humaniste » du contrôle (Burlaud et al., 2004) : chercher à contrôler tout en suscitant l'adhésion. Cette vision du contrôle est en pratique liée à la norme mais la norme n'est pas la finalité du contrôle. On se situe dans la vision du contrôle au sens de maîtrise de l'activité et des conséquences sur celle-ci.

La diffusion de ce principe de responsabilité s'appuie alors :
-sur le rôle d'animateur du Risk Manager et des contrôleurs internes dont les missions sont complémentaires pour à la fois sensibiliser sur les enjeux globaux de risques (l'un des rôles du Risk Management) et sur les spécificités de chaque métier en termes de risques opérationnels (l'un des rôles du contrôle interne). Cette approche collaborative entre Risk

Management et contrôle interne semble évidente mais sa mise en œuvre empirique reste encore une difficulté souvent exposée lors de nos entretiens. Or, si les directions des risques sont souvent encore sous-dimensionnées en termes d'effectifs, ces dernières ont tout intérêt à s'appuyer sur les réseaux de contrôle interne (permanent et périodique) en vue de contribuer à la diffusion de leur vision. Cela suppose un premier travail de présence et d'animation du Risk Management envers le contrôle interne. Ce qui constitue en soi une perspective d'évolution du contrôle interne qui, bien que déjà prise en compte depuis le début des années 2000, reste encore à ce jour très variable dans les secteurs banque et assurance. Le rôle du contrôle interne dans l'identification des risques, notamment opérationnels, est encore souvent à préciser et à formaliser (Hanssen, 2005 ; Pelzer, 2009). Nous prolongeons l'idée que si l'efficacité du contrôle interne dépend de l'institutionnalisation de cette fonction (Cappelletti, 2006), son objectif en termes de réduction des risques doit également être davantage mis en avant comme l'un des axes privilégiés de contrôle. Il s'agit en effet de l'un des objectifs sous-jacents à la démarche de conformité aux procédures internes : remédier à l'illusion du contrôle implique donc de dépasser la recherche de conformité pour étudier les zones de « mise en risque ».

-sur la recherche d'une organisation répondant aux normes comme l'un des objectifs des dispositifs de contrôle et de management du risque mais ces approches ne sont en pratique pas toujours porteuses de sens pour les opérationnels. Le travail de formation et de sensibilisation du Risk Management et du contrôle consiste à traduire cet enjeu puis à le transposer en lien avec les difficultés des opérationnels. Une telle approche vise à se centrer sur les risques prioritaires et à ne pas chercher à faire remonter toutes les informations dans les bases de collecte des pertes ou dans les cartographies (ce qui induit des confusions et une surcharge informationnelle).

S'assurer de la conformité aux normes passe par l'opérativité de ce principe de responsabilité, ce qui suppose d'intégrer dans la pédagogie du Risk Management le caractère « situé » de l'agir des opérationnels, tout en intégrant le rapport au risque. Ce rapport au risque n'est en pratique que rarement une priorité de l'action (on ne gère pas en permanence le risque, mais il reste une nécessité de la pensée (on envisage les zones de risque dans l'activité quotidienne).

-Transposer la norme et garder son sens.

L'environnement réglementaire ou normatif peut accompagner, faciliter ou renforcer les démarches de gestion des risques à initier. Mais il ne sera pas suffisant s'il se limite à une vision parcellaire, réglementaire ou contrainte de l'enjeu à considérer. Le risque de la routinisation et de la bureaucratisation du contrôle est un paramètre d'attention majeur dans une période où l'on cherche à la fois à rendre des comptes sur les risques de l'entreprise et à répondre de manière adaptée aux normes. Le contrôle basé sur l'environnement réglementaire peut être un point d'appui mais ne sera déterminant que pour des périmètres très limités (contraintes EHS[81], réglementation financière particulière). La sensibilisation à l'enjeu passe de manière déterminante non pas, par le règlementaire ou le prudentiel, ce qui constitue un point d'aboutissement parmi d'autres, mais par la compréhension (par les managers et les opérationnels comme par la gouvernance de l'entreprise) du sens et de la valeur produites par les démarches de gestion des risques en entreprise.

La transposition des normes par les fonctions dédiées au contrôle et à la gestion des risques est en soi un travail complexe, elle implique pour lesdites fonctions :
-une vision globale de l'organisation,
-une vision claire de l'enjeu réglementaire et des phénomènes d'incitations lui étant inhérents,
-des compétences multiples des Risk Managers dans des champs variés (communication et « ingénierie pédagogique », expertise métiers, vision des impacts financiers et organisationnels, la capacité à s'appuyer et à composer avec les autres fonctions du contrôle tels que le contrôle interne, l'audit interne, le contrôle de conformité, la direction juridique, le contrôle de gestion, le contrôle qualité etc.).

Enfin, un point n'apparait pas dans cette recherche : la responsabilisation démarre au niveau de la gouvernance (logique Top Down). Un tel constat est récurrent mais souffre d'une limite clairement identifiée : le risque opérationnel peut-être piloté globalement « en central » en tant que transmission d'une vision globale (la politique de maîtrise des risques opérationnels). Toutefois, la gestion de ce risque et sa réelle prévention a clairement lieu auprès des métiers et par des échanges fréquents. La gestion des risques opérationnels n'est pas seulement le fait

[81] Contraintes en matière de respect des règles environnementales et des règles de sécurité et d'hygiène sur le lieu de travail.

d'outils encore récents et parfois mal compris, qui bien souvent sont un moyen de se déresponsabiliser par un reporting formaliste.

3. Limites de l'étude : une démarche incrémentale et d'amélioration continue de notre protocole de recherche.

Ce paragraphe vise à détailler les différentes limites que nous avons pu identifier dans le cadre de la présente recherche doctorale. Si ces limites sont clairement identifiées, c'est pour mieux souligner le caractère incrémentale de notre recherche et la perspective d'amélioration continue qui la caractérise, tant sur le plan de la rigueur scientifique que de la validité scientifique des données mobilisées, s'agissant d'une recherche qualitative.

3.1. Limites théoriques de l'étude

Sur le plan théorique, nous pouvons considérer les limites de notre recherche. La recherche doctorale impliquant par nature de se centrer sur un objet de recherche suffisamment précis, nous ne prétendons pas ici avoir répertorié l'ensemble des travaux relatifs à la gestion des risques. De même, les grilles de lecture théoriques mobilisées sont également le fait d'un parti pris eu égard aux données collectées, d'où l'écho fait à une épistémologie de type constructiviste dans notre chapitre méthodologique. Ce choix s'inscrit dans une recherche de cohérence entre des grilles de lecture d'inspiration sociologique (théorie de la structuration, théorie de l'acteur-réseau, théorie du contrôle interactif) et des méthodologies de collecte et d'analyse des résultats issues du même domaine académique (recherche-action, méthode des entretiens). Qu'il s'agisse de notre approche théorique ou de notre étude du réel, nous avons transposé ces méthodologies en sciences de gestion. Cela comporte des biais d'analyse de données clairement identifiés, mais répond également à la préoccupation d'étudier le contrôle des risques sous un angle différent des recherches usuelles en Risk Management, notamment anglo-saxonne, se centrant sur une étude principalement quantitative des phénomènes de contrôle des risques. De telles études, aussi valident qu'elles soient, n'ont pas permis de fournir des solutions suffisamment robustes face aux critiques vives du Risk Management post-crise (Mikes Power, 2009 ; Mikes, 2008a, 2011 ; Kaplan, Mikes, 2012).

Un tel parti pris, bien que clairement assumé, implique de reconnaitre que d'autres grilles de lecture sembleraient également adaptées pour étudier les phénomènes de contrôle

organisationnel. Nous pensons notamment aux théories du sensemaking (Weick, 1995) que nous avons évoqué préalablement. L'action sans la traduction induit parfois la perte de sens.
D'autres approches sembleraient adaptées, au titre desquelles figurent les travaux relatifs au contrôle formel/informel, aux enjeux de rationalité limitée appliquée au contrôle organisationnel, aux rapprochements entre éthique et contrôle, aux champs théoriques relatifs au management de la valeur ou encore à l'étude des coalitions inter-groupes.

Nos limites théoriques résident, outre le choix des grilles de lectures, dans l'approche retenue pour envisager l'étude des enjeux normatifs relatifs au contrôle des risques opérationnels.
Certains auteurs (Huebner, 2010 ; Kulpa, Magdon, 2012) envisagent le risque opérationnel sous un angle principalement quantitatif. Pour ces derniers, les enjeux organisationnels relatifs au risque opérationnel (traiter les causes racines des risques opérationnels) ne peuvent être traités avec un degré de satisfaction suffisant, s'agissant de risques subis. Aussi, il importe de développer une approche quantitative permettant d'optimiser le coût du risque opérationnel en termes de fonds propres. Une telle démarche, en dépit de son intérêt, semble davantage porter sur l'étude réactive des risques et suppose un historique de données importants. Il s'agit en outre d'une perspective différente, davantage technique que gestionnaire en termes de démarches de recherche.

3.2. Limites méthodologiques de l'étude

La limite de notre recherche peut être également d'ordre méthodologique. Cette recherche impliquerait des études de cas plus nombreuses et dans des structures plus diversifiées (sociétés de gestion d'actif notamment) en développant les approches qualimétriques en vue d'étayer certains constats complémentaires. Comme nous l'avons évoqué dans notre chapitre méthodologique, la présente recherche, du fait qu'elle soit de nature qualitative, implique des limites intrinsèques mais aussi extrinsèques.
Des limites intrinsèques en premier lieu, car le recours à des outils qualitatifs de recherche est par nature limité et comporte des biais de collecte de données (le recours à la méthodologie de type recherche-action ou aux entretiens semi-structurés). Bien que nos études de cas soient de longue durée et que le nombre d'entretiens confirmatoires réalisés soit significatif, nous considérons cette recherche comme un point de départ plus qu'un aboutissement. En effet, et comme le soulignent Lindsay (2012) ou encore Cassell et al.(2006), la recherche en sciences de gestion, et notamment en comptabilité-contrôle-audit, implique le recours à des

méthodologies diversifiées pour mieux comprendre la réalité du fonctionnement des organisations et également mieux apporter à la création de connaissance. Si la recherche qualitative est en soi limitée, le recours à des méthodologies quantitatives ne peut se suffire à lui-même dans l'étude des phénomènes organisationnels. Le choix entre méthodologies qualitatives et quantitatives dépend donc de la nature de l'objet de recherche, de la problématique posée et de son adaptation au terrain envisagé. (David, 2004 ; Jönsson, Lukka, 2005 ; Lawrence Neuman, 2011). Les débats relatifs à ces enjeux méthodologiques ne sont pas récents et restent pour certains controversés. Nous abondons toutefois dans le sens d'un positionnement pragmatique de la recherche visant une adéquation entre accès au terrain, contraintes de disponibilité des données (a fortiori dans le secteur financier) et contraintes de généralisation des connaissances produites. Aussi, le recours aux méthodologies de type recherche-action, en comprenant des critères de rigueur scientifique, nous semble un compromis entre nécessité d'émancipation par rapport au terrain de recherche, employabilité des données et connaissances produites (McKernan, 1991 ; Drummond, Themessl-Huber, 2007 ; Johansson, Lindhult, 2008).

Des limites extrinsèques en second lieu, car la sélection des cas d'études ou des entretiens réalisés est par définition contingente de notre capacité d'accès au réel. Egalement, nous attirons l'attention sur le fait qu'une limite de nos cas d'études est relative à notre durée de présence en entreprise. Bien que s'agissant de période respectivement de un an et de six mois pour les cas C1 (société d'assurance) et C2 (établissement bancaire), des périodes plus prolongées auraient pu nous permettre de développer les constats réalisés. Certains échanges réalisés lors de nos entretiens confirmatoires auprès de directeurs risques nous ont permis d'évoquer le processus de mise en place de la démarche de gestion des risques opérationnels, de sa création ex nihilo à sa montée en puissance jusqu'à maturité. Ces directeurs ayant menés le projet de mise en place de politiques de maîtrise des risques opérationnels de bout-en-bout nous ont conduit à identifier qu'il fallait en moyenne a minima trois à quatre ans pour créer une filière risques opérationnels et l'amener à maturité. Nos études de cas ont davantage porté sur sa création (questionnements sur le déploiement chez C1 et redéploiement chez C2) que sur son maintien sur le long-terme. Des études longitudinales de plus longue durée nous permettraient donc de développer nos résultats.

En outre, la nature non-finalisée des résultats recueillis caractérise notre recherche. Les politiques de maîtrise des risques et la notion même de contrôle des risques dans le secteur

financier est fortement contingente des normes de contrôle en place et des interprétations faites par les entreprises étudiées.
Au-delà de ces limites, nous pouvons cependant souligner deux points :

- La plupart des recherches relatives au contrôle organisationnel des risques, ainsi qu'au risque opérationnel, sont de nature qualitative. Ces constats sont confirmés par différents auteurs en ce qui concerne notamment l'étude des phénomènes socio-organisationnels tels que les enjeux de structuration des contrôles (Harvey, 1990 ; Husser, 2010).

- Egalement, ces recherches insistent sur le caractère non finalisé d'un tel environnement, qui suppose, pour être réellement cerné, d'avoir recours à des méthodes variées, non uniquement quantitatives, et à des panels distincts dans l'espace et dans le temps. Une telle approche dépasse donc le simple cadre d'une recherche doctorale en s'inscrivant dans la durée. Les auteurs de référence ayant traité du risque opérationnel insistent clairement sur l'importance d'étudier le risque opérationnel dans le cadre de programmes de longue durée et ce dans différents contextes régionaux/nationaux mais aussi sectoriels (Hoffman, 2002 ; Knechel, 2007 ; Power, 2005, 2009 ; Mikes, 2011, 2012).

3.3. Limites managériales de l'étude

A la lumière des résultats exposés précédemment, notre analyse fait émerger plusieurs constats complémentaires. Notre étude contribue à étayer les travaux de recherche dans une logique socio-organisationnelle sur le passage de l'auto-contrôle à une logique de contrôle interactif et apprenant à laquelle contribue le Risk Management (Spira, Page, 2003 ; Hakenes, 2004). Cette culture du risque opérationnel que nous décrivons présente comme spécificité que le risque opérationnel est un risque subi et non un risque faisant l'objet d'un choix, d'une analyse d'opportunité, à la différence d'autres risques comme le risque de marché ou de crédit (qui font l'objet d'arbitrages avec la fixation d'une limite d'acceptation du risque). Par conséquent, l'enjeu de prévention et de responsabilisation se fait par l'intégration des effets négatifs liés à l'activité de l'entreprise dans le business model, non pas dans une logique assurantielle de provisionnement et d'allocation de fonds propres, mais dans une logique a

minima réactive (pour la fraude externe par exemple) et a fortiori préventive car visant à pérenniser l'activité.

Cependant, la limite de notre recherche tient probablement à la nécessité d'approfondissement du sujet abordé, sur le plan managérial. Cette dernière constitue un point de départ et il est complexe de résumer les multiples fronts de traductions et d'interactions auxquels doivent faire face les contrôleurs internes et Risk Managers. Ces sujets sont parfois techniques et constituent en soi un champ d'approfondissement (la fraude financière par exemple) mais aussi politiques (lien entre audit interne et Risk Management, entre fonctions risques et régulateur, entre fonctions risques et métiers, zones de conflits et de collaborativité pouvant constituer des biais en tant que tels).

-des facteurs de contingence difficiles à exclure en pratique : le secteur bancaire est en soi particulier quant au sujet des risques opérationnels car les activités de banque de financement et d'investissement ou les activités de moyens de paiement sont des vecteurs de risques opérationnels spécifiques. De même, les nouvelles activités gérées par les établissements financiers (banques en ligne, filiale de téléphonie-mobile) sont également des sources de risques opérationnels à part entière, éloignées des préoccupations usuelles des contrôleurs des risques. Autre illustration : l'identification de la fraude (interne ou externe) constitue en soi un réel programme de recherche appliqué. Les coûts associés aux évènements de risques opérationnels que sont les fraudes représentent des montants importants (tant en banque qu'en assurance). Ces montants, aujourd'hui envisagés de manière forfaitaire dans le cadre des formules standards et des modèles internes, appellent des études plus poussées. Il est ainsi difficile, au-delà même des méthodes robustes de quantification du risque, d'envisager les schémas de fraudes en salle de marché, de fraude aux moyens de paiement, de fraudes à l'assurance santé ou à l'assurance vie ou de biens.

Notre recherche est limitée sur le plan managérial en cela qu'elle n'apporte qu'une bribe de réponse sur ces problématiques, d'où sa dimension exploratoire. Nous situons cependant ces éléments comme des sujets de recherche complémentaire à initier. La recherche-action semble là-encore particulièrement adaptée car de telles recherches se fondent nécessairement sur l'expérience de terrain du chercheur, enraciné dans la pratique, en gardant toutefois un recul sur les méthodes de collecte de données utilisées (guide d'entretien, matrice d'analyse de contenu etc.).

-une variabilité des fonctions et dispositifs nécessaires mais rendant difficile la structuration des contrôles : nous constatons en effet l'une des limites de nos résultats qui est celle relative aux fonctions et dispositifs étudiés. Les normes de contrôle, bien que détaillant les fonctions à mettre en place dans les établissements financiers en vue de contrôler les risques opérationnels, insistent peu sur la configuration optimale à adopter. A titre d'exemple : est-il plus pertinent de cumuler fonction risque et fonction de conformité, fonction qualité et fonction de contrôle interne, fonction contrôle interne et fonction risque ? De telles configurations sont très diverses d'une entreprise à l'autre. Nos entretiens nous ont ainsi permis de constater, bien au-delà des cas d'études réalisés, que les configurations observées en recherche-action, aussi pertinente qu'elle semblait a priori, n'était pas nécessairement les plus adaptées. Il s'agit ainsi d'une limite managériale de notre recherche autant que d'une perspective de questionnement future : quelles sont les configurations optimales en termes de regroupement des fonctions clés de contrôle imposées par la réglementation prudentielle en banque et en assurance ?

-une approche par le capital humain : Nous avons également identifié une autre limite de l'étude sur le plan managérial. Nous insistons sur le rôle du Risk Manager en tant qu'acteur réseau au centre du processus d'interactions entre fonctions de contrôle, fonctions supports et fonctions opérationnels. Toutefois, en pratique, recruter des acteur-réseaux reste une gageure. Les compétences du Risk Manager (sur le plan technique mais aussi sur le plan relationnel et en termes de diversité d'expérience) constituent un véritable facteur de contingence que nous n'avons, dans le cadre de cette recherche, pas suffisamment mis en exergue. Aussi, une limite à traiter dans le cadre de recherche future concerne les compétences mais aussi les facteurs de crédibilité d'un Risk Manager, ayant un impact sur la réussite ou non du déploiement d'un dispositif de contrôle des risques.

4. Perspectives de recherches futures en contrôle des risques

Le paragraphe ci-après détaille les différentes perspectives de recherches futures visant à dépasser les travaux exposés dans cette recherche doctorale, constituant un point de départ de nos recherches sur le risque opérationnel et les normes de contrôle des risques.

4.1. Perspectives de recherches relatives au risque opérationnel

Concernant nos perspectives de recherches futures, l'objet de recherche « risque opérationnel » constitue un réel enjeu. La diversité même de cette notion de risque, la frontière entre le risque opérationnel et les autres catégories de risques, la perspective gestionnaire entourant cette notion constituent en soi des axes privilégiés encore peu étudiés.
Les aspects relatifs au risque opérationnel sont encore peu détaillés sur certains aspects théoriques et appliqués. Comme nous l'avons indiqué tout au long de cette thèse, si ce sujet fait l'objet de politiques dédiées dans le secteur financier, d'autres recherches peuvent s'inscrire dans cette continuité en management et contrôle. Nous pensons notamment aux axes suivants :

-Le rôle des acteurs et de leur perception du risque opérationnel, le rôle des incitations à gérer le risque. Ces aspects revêtent une dimension psychologique forte en matière de risque, étudiée par certains auteurs dans le monde anglo-saxon ainsi qu'en France dans le cadre du colloque francophone sur le risque (Oriane) ainsi que dans le cadre des travaux menés par l'Institut Psychanalyse & Management notamment.

-L'étude du risque opérationnel dans d'autres types d'entreprises du secteur financier ainsi que dans d'autres secteurs d'activités constitue également un axe de recherche essentiel pour comprendre cet objet complexe et vaste et ainsi distinguer le contingent du générique en la matière. A cet égard, et en prolongement de cette thèse, nous avons ainsi initié une recherche-action au sein du secteur mutualiste français en vue d'étudier la prise en compte de ce type de risque dans un autre contexte organisationnel. Ce contexte mutualiste étant marqué par d'autres axes opérationnels que la recherche de performance et comprenant des valeurs éthiques fortes ainsi qu'un poids plus important de la gouvernance (formalisée au travers de plusieurs commissions et comités). Ces caractéristiques ne sont pas sans conséquence en matière de maîtrise du risque opérationnel. Également, l'étude des risques opérationnels dans

les sociétés de gestion d'actifs ou les intermédiaires financiers peut constituer une voie d'étude du risque opérationnel. Ces entreprises sont en effet marquées par des risques opérationnels s'envisageant principalement au travers de la conformité normative et du respect des engagements vis-à-vis de leurs clients (respect des mandats de gestion, respect de la réglementation en matière de conformité, exigence croissante en matière de réglementation sur l'intermédiation financière en banque, gestion d'actifs et en assurance). Les sociétés de gestion privée (capital-investissement, gestion de fortune) sont également concernées par la problématique essentielle du risque opérationnel, envisagée principalement sous l'angle de la protection de la clientèle. Nous pensons également aux établissements financiers pratiquant la réassurance, pour lesquels le risque opérationnel se caractérise par une approche par fréquence faible et par coût élevé en cas de survenance tels que nous l'ont évoqués certains des interlocuteurs lors de nos entretiens. Des travaux sont donc à initier en compléments des recherches initiés par certains auteurs français sur ce sujet. Sans pouvoir parler « d'école française » relative aux recherches sur le risque opérationnel, on constate que plusieurs auteurs ont entendu détailler cette thématique comme axe d'étude à développer (Bessire, 1998 ; Journé, 2009 ; Cappelletti, 2009 ; Bon-Michel, 2011, Jardat, 2011).

-L'étude sectorielle du risque opérationnel, en tant qu'axe de recherche sous sa perspective gestionnaire, peut également s'entrevoir concernant les entreprises du secteur industriel. Dans ce secteur, le risque opérationnel est principalement envisagé sous les angles normatifs ou techniques (les « cyndiniques ») afin de circonscrire les risques principalement de types sécurité des biens et des personnes ou encore les risques liés à la continuité et à la reprise d'activité critiques pour lesquelles il existe une exigence de haute fiabilité (PCA-PRA-PSI)[82].

-L'objet d'étude relatif au contrôle des risques opérationnels compte encore peu de recherches en gestion sur la manière d'aborder pour les décideurs et les opérationnels certaines catégories de risques opérationnels. Aussi, des perspectives de recherche pertinentes concernent le contrôle des risques RH. Ces risques opérationnels, souvent les plus critiques pour les entreprises, sont encore peu étudiés (Ferrary, 2009 ; Mikes, 2011). Certains de ces risques (turn-over, risques psycho-sociaux) font déjà l'objet d'études nombreuses. Cependant ces derniers sont davantage envisagés dans une logique psychosociale. Toutefois, ce périmètre de

[82] Plan de continuité d'activité (PCA), Plan de reprise d'activité PRA), PSI (Plan de secours informatique). Ces risques constituent des risques opérationnels et se caractérisent principalement par une rupture dans le maintien en condition opérationnel de l'entreprise et l'exploitation courante de son activité ; pouvant engendrer un impact financier, image ou même des risques de pertes humaines dans les cas de survenance les plus graves.

risques opérationnels reste à étudier concernant notamment les risques RH liés à la compétence, à la maîtrise des coûts salariaux, aux risques sur l'administration du personnel, au risque homme clé etc. Ces risques peuvent davantage être envisagé dans le rapprochement entre contrôle des risques et contrôle de gestion socio-économique (Cappelletti, 2012) : cartographie des risques RH, indicateurs de risques RH, plans d'actions dédiés. Sur cette thématique, dans le prolongement de cette recherche doctorale un programme de recherche envisageant le risque RH sous l'angle du risque opérationnel a été initié en partenariat avec une association professionnelle reconnue en management des risques. Elle se matérialise via une participation active à la Commission Risques RH (et la réalisation d'une enquête qualitative auprès de directeurs des risques et directeurs RH).

-Enfin, l'étude des risques opérationnels en sciences de gestion s'entrevoit également comme perspective de recherche future concernant les risques de fraudes internes ou externes (fraudes aux moyens de paiement, fraudes à l'assurance fraude aux prestations santé, fraude au Président et dirigeant d'entreprise, dispositif de gestion en matière de Lutte Anti-Blanchiment et Financement du Terrorisme).

Les perspectives de recherches relatives au risque opérationnel sont donc riches et variées et constituent en soi un programme de recherche futur sur un objet de recherche encore émergent.

4.2. Perspectives de recherches relatives au contrôle interactif

Dans la lignée des travaux menés par Simons (1995) ou encore Kaplan et al. (2009), un axe de recherche futur consiste à approfondir les liens entre les différents modes de contrôle dans l'organisation et entre les différents niveaux de contrôle dans les établissements financiers.
Il s'agit notamment d'étudier comment le contrôle interne et la fonction de vérification de la conformité travaillent de manière coordonnée. Ces approfondissements peuvent également concerner les interactions fortes entre contrôle qualité et contrôle des risques. Cela s'envisage à la fois de manière positive (enrichissement mutuelle des méthodes et des démarches) et dans une logique négative (conflits et redondances entre les fonctions dès lors que ces activités sont séparées) de relation entre les différentes fonctions de contrôles organisationnels (Mikes, 2008b ; Galloppo, Rogora, 2011 ; Darsa, Dufour, 2014).

-On peut encore mentionner la nécessité de développer des études plus poussées concernant les liens entre contrôle de gestion et contrôle des risques, notamment sous l'angle de l'étude qualimétrique de la performance (méthode des scénarios, étude du coût du risque non modélisable, liens entre Key Risk Indicators/Key Performance Indicators, lien entre collectes des pertes et des incidents et optimisation des provisions pour risques et charges, calculs des coûts-performances cachés et formalisation du risque en tant que source de coûts cachés). Les interactions entre contrôle de gestion et contrôle des risques semblent donc très fortes. Ce sujet dépasse en soi le cadre de notre recherche doctorale mais constitue un réel potentiel de recherche sur l'enrichissement des travaux de ces fonctions transverses par nature.

-Egalement, au titre de ces perspectives de recherche en lien avec les théories du contrôle interactif, on peut mentionner l'étude des systèmes frontières (Simons, 1995). Le risque opérationnel étant par nature un « risque frontière » (Chelly, 2012). En effet, une multitude de cas de risques opérationnels font intervenir différents types d'acteurs et différentes fonctions de contrôle. Ces éléments, exposés notamment dans nos chapitres résultats et discussions appellent des compléments en vue d'envisager le potentiel de validité académique de la notion de risque frontière. La situer comme objet d'étude du contrôle interactif semble à cet égard un axe théorique privilégié.

-Enfin, nous pouvons envisager une perspective de recherche dans la lignée des travaux réalisés sur la distinction entre contrôle formel et informel. Un tel sujet, préoccupation croissante dans les congrès académiques en comptabilité-contrôle-audit (AFC, Iseor notamment), montre l'intérêt croissant accordé aux mécanismes de contrôle organisationnels. Envisager le contrôle des risques sous cet angle, comme perspective en dualité entre contrôle formel et informel, permettrait d'insister sur une dimension essentiel en gestion des risques (risques pouvant faire l'objet de reporting, risque devant être communiqué effectivement), que nous avons abordé brièvement dans le cadre de cette recherche. Une illustration forte d'un tel sujet concerne notamment les interactions formels et informelles entre les tenants de l'auto-contrôle dans les établissements financiers et les acteurs en charge du contrôle de conformité (internes et externes via l'autorité de contrôle du secteur financier).

4.3. Perspectives de recherches relatives aux normes de contrôle

Outre ces premiers axes de recherches futures, un autre axe privilégié nous semble directement en lien avec notre problématique de recherche. Dans la lignée des travaux en sciences de gestion sur le rôle des normes, notre étude au sein du secteur financier sur le rôle de norme de contrôle appellerait également des développements.

Nous pensons plus particulièrement à l'enrichissement des champs théoriques, initiés notamment par Bessire (1995) et développés par Savall et Zardet (2005b) concernant le concept de tétranormalisation. Un tel champ de recherche semble particulièrement intéressant car s'inscrivant dans une préoccupation forte et d'actualité : le rôle croissant des normes dans les économies et le management des organisations. Dans cette optique, des travaux récents insistent sur la nécessité pour les organisations de développer une « ingénierie normative » dont l'objet est de renforcer leur capacité à intégrer de nouvelles normes et à s'adapter aux contraintes de ces dernières. Cette agilité normative s'entrevoit au travers notamment du concept de tétranomalisation (Bessire et al., 2010) que nous avons cité préalablement. Des compléments, notamment au travers de recherches sectorielles, présentent un réel intérêt en sciences de gestion en matière d'analyse critique du rôle des normes et d'analyse gestionnaire de la manière de les transposer au sein des organisations. Cette « agilité normative » constituerait en soi un véritable axe de compétitivité voire un avantage concurrentiel selon qu'une entité soit plus apte qu'une autre à intégrer de nouveaux dispositifs normatifs. Il s'agirait donc d'étudier en contrôle le rôle de l'ingénierie normative (joué notamment par les fonctions de veille et de pilotage de la conformité) prenant en compte différente graduation : approche de formalisation, approche d'auto-contrôle, approche du contrôle sous tutelle.

-En lien direct avec cet axe, nous pouvons également mettre en avant le rôle des fonctions de contrôle comme aide à la décision de la gouvernance d'entreprise sur les arbitrages à réaliser quant à l'intégration des normes. Cela concerne notamment l'arbitrage entre les normes devant faire l'objet d'une intégration à minima (dispositif formel uniquement) et les normes ayant vocation à être envisagées via une intégration renforcée (dispositif effective avec suivi important). Un tel parallèle existe notamment en Lutte Anti-blanchiment entre les dispositifs de vigilance allégés, modérés et renforcés (compte tenu de l'exposition au risque) ainsi qu'en audit interne dans la graduation des actions à mettre en place (suivi périodique d'un risque, suivi régulier, suivi continu etc.).

-Enfin, l'étude critique du rôle des normes appelle également des recherches complémentaires concernant notamment les référentiels de contrôle à l'international. Nous pensons ici à des études ciblées sur le rôle des normes d'audit interne, désormais plus que jamais structurante dans la fonction d'audit, le rôle des référentiels de type COSO (2013) en ce qui concerne le contrôle interne et la fonction de gestion des risques.

4.4. Perspectives de recherches concernant les politiques de maîtrise des risques

Une autre série de perspectives de recherches, dans le prolongement de notre étude doctorale, concerne les recherches dédiées aux politiques de maîtrise des risques. Au-delà des aspects organisationnels cités dans la présente recherche doctorale, nous pouvons également mentionner les perspectives potentielles de recherches concernant les interactions entre corpus normatifs internes et externes (chartes, référentiels, politiques, règlement intérieur). L'impact en matière d'aide à la décision de tels corpus normatifs est en soi un objet d'étude corollaire à notre objet de recherche (Hubbard, 2009).

L'étude complémentaire des politiques de maîtrise des risques peut encore s'envisager sous un angle psychosocial : comment créer un climat propre à la diffusion d'une culture du risque au sein d'une organisation ? Quelles sont les barrières psychologiques à prendre en compte pour faire adhérer ou non un acteur à la démarche de gestion des risques ? L'expérience nourrit-elle la propension des acteurs à s'intéresser au sujet des risques en entreprise ?... .

Les perspectives de recherches en contrôle des risques sont donc nombreuses. Elles impliquent de mobiliser des terrains et des grilles théoriques variées, ce qui constitue en soi un véritable programme de recherche postdoctoral.

Conclusion du chapitre discussions - La gestion des risques opérationnels, un contrôle de médiation

Les normes traitant du risque opérationnel ont le mérite de donner une impulsion quant à la nécessité de se préoccuper de l'enjeu majeur que constitue le risque opérationnel. Toutefois, il semble qu'un tel enjeu, pour être pris en compte, passe par la diffusion de principes effectifs, dépassant le simple cadre normatif se traduisant par la mise en place de contrôles « conformistes ». La responsabilisation ouvre la voie à l'anticipation là où la recherche de conformité sans regard critique est un moyen de se défausser quant aux véritables enjeux du contrôle. La responsabilité est donc dans notre perspective le point de divergence entre un contrôle illusoire tel qu'il fut critiqué ces dernières années par de nombreux chercheurs et praticiens et un contrôle effectif et efficace, à savoir dans notre étude un contrôle suscitant un intérêt pour les collaborateurs des établissements bancaires et des sociétés d'assurances. La particularité de ce principe de responsabilité est sa dimension « obligation à l'avenir » : rendre des comptes non seulement pour les risques subis dans le passé mais aussi pour ceux pouvant survenir dans le futur. Sans responsabilisation, on ne rend compte que des pertes survenues en estimant être en conformité à la norme dès lors que les contrôles sont réalisés. Cette approche est donc à dépasser pour intégrer le lien entre les préoccupations opérationnelles des collaborateurs et les perspectives de « mise en risque » à venir.

In fine, la diffusion du principe de responsabilité est le fait de certains acteurs clairement identifiés (les Risk Managers, directeurs des risques, contrôleurs internes, auditeurs internes etc.) mais son application est l'affaire de tous dans l'organisation.

Conclusions générales de la thèse - De la normativité à l'effectivité, dépasser l'illusion du contrôle

Notre recherche sur la gestion du risque opérationnel s'inscrit dans un courant dans lequel l'accent est mis sur la nécessité de repenser le contrôle des risques dans un monde post-crise de 2007-2008. Depuis cette crise, de nombreux établissements financiers ont fait l'objet de cas de pertes associées au risque opérationnel. Ces cas médiatiques mettent en avant les défauts de la gestion des risques. Si la notion de risque opérationnel, pour technique qu'elle soit, n'est pas évoquée lors de ces différentes affaires médiatiques (fraudes affectant les banques d'investissement ou les banques privées, expositions non maîtrisée à des cyber-attaques, affaires de corruption etc.), on constate cependant que le caractère médiatique du risque est croissant ces dernières années. Les récentes crises financières ont contribué à une prise de conscience dans l'opinion publique de la fragilité des établissements financiers. Cette fragilité fait cependant toujours débat, qu'il s'agisse des risques financiers (de marché ou de crédit) mais aussi des risques opérationnels extrêmes (de type fraude de trader tels que les cas médiatiques de « rogue trading »).

Notre premier chapitre a entendu insister sur la diversité des risques auxquels peuvent faire face les établissements financiers en insistant sur le rôle particulier joué par le risque opérationnel, notion vaste et englobante parfois assimilée à une catégorie que l'on pourrait qualifier « d'autres risques » (ce qui n'est pas du risque de marché, du risque de crédit en banque ou encore du risque de souscription en assurance).

Le second chapitre de cette recherche souligne le fait que les différentes instances de régulation se sont emparées, principalement au début du XXIème siècle, de cette problématique pour l'institutionnaliser en tant qu'enjeu prudentiel sur lequel les établissements financiers devaient concentrer leur attention. La problématique du risque opérationnel, de par sa récurrence, son coût croissant et du fait du poids croissant du financier dans la vie quotidienne, doit, dans la perception des instances de régulation, constituer un enjeu de gestion pour les dirigeants des établissements financiers. Cet enjeu de gestion, pourtant préexistant, alors institutionnalisé, correspond ainsi à une contrainte normative de contrôle pour les établissements financiers.

Le troisième chapitre de notre étude démontre ainsi face à cet enjeu, qu'il existe dans les différents courants de recherche une « théorie de la gestion des risques » en cours de formalisation. En nous fondant initialement sur la théorie du risque du début du XXème siècle, nous constatons que le développement d'activités à risques ainsi que la progression des connaissances en sciences de gestion conduit progressivement à l'avènement d'un corpus théorique spécifique à la gestion des risques tout au long du XXème siècle. De manière plus précise encore, le début du XXIème siècle correspond, dans le prolongement de cette tendance, à la formalisation d'un cadre de recherche émergent relatif au risque opérationnel. C'est dans cette tendance que nous nous inscrivons en insistant sur le fait qu'il existe un nombre croissant d'études relatives aux risques opérationnels et que cet objet de recherche, de par la diversité des réalités qu'il recouvre, de par la complexité des problématiques qu'il soulève et du fait de son caractère englobant, correspond à un programme de recherche encore à initier.

Le quatrième chapitre de notre étude entend apporter des précisions quant à notre positionnement épistémologique, d'inspiration constructiviste. Ce positionnement, en phase avec nos cadres théoriques (structurationniste plus particulièrement) privilégie la compréhension des éléments de terrain comme constitutifs de sources de validation de savoirs théoriques. Cette approche de la recherche, formalisée par le recours aux méthodologies de type recherche-action fondée sur la pratique et sur l'étude, de manière située, des réalités socio-organisationnelles, nous semblent plus particulièrement adaptée au regard de l'objet émergent de recherche que constitue la norme de contrôle relative aux risques opérationnels.
Le recours à des entretiens confirmatoires nous semblaient également indispensable pour dépasser le caractère contingent de nos études de cas.

Le cinquième chapitre de la thèse, exposant nos différents résultats, nous permet d'insister sur l'importance des enjeux de traduction de la norme de contrôle relative au risque opérationnel ainsi que sur le caractère essentiel de la fonction de gestion des risques opérationnels dans l'animation d'une filière effective dédiée à la maîtrise de cette catégorie de risque. Nos résultats soulignent les difficultés pratiques posées par le contrôle du risque opérationnel. Ces difficultés se caractérisent par la compréhension des attentes des instances de régulation quant à une définition du risque opérationnel qualifiée d'extensive voire de confuse. Il s'agit également de déterminer l'approche organisationnelle la plus à même de cerner cet objet frontière. Enfin, nous constatons qu'un tel enjeu normatif fait l'objet d'un défaut

d'appropriation du fait de son caractère technique et normatif, l'assimilant à une approche « bureaucratique » du contrôle. Face à ces difficultés, l'apport de la fonction de gestion des risques opérationnels (à laquelle nous étions rattachés en recherche-action en tant que contrôleur interne puis Risk Manager) est de contribuer à expliciter cette notion ainsi que les attentes de régulation y étant afférentes, à coordonner les efforts des différentes fonctions de l'organisation sur ce sujet ainsi qu'à établir un lien entre les politiques de maîtrise des risques approuvées par la gouvernance et le rôle de chaque acteur concernant ces risques.

Le dernier chapitre de notre étude tend à insister sur les apports de notre recherche quant à la notion de risque opérationnel. Nous précisons ainsi les conditions de rigueur permettant de faire évoluer le contrôle des risques opérationnels de la normativité vers l'effectivité. Également, nous insistons, dans une logique propre à la formalisation de débats contradictoires dépassant le cadre de cette étude, sur le rôle clé du Risk Manager dans le fait de guider les différents « propriétaires de risques » vers la responsabilisation. Ce chapitre insiste encore sur l'importance de « vendre le risque » au sein des établissements financiers ainsi que sur le rôle essentiel des interactions entre les différents types de contrôles organisationnels de la firme, en soulignant le fait que ces rapprochements restent émergents dans les études théoriques en sciences de gestion. Notre étude présentent des limites méthodologiques, théoriques et managériales, nous sommes conscients des marges de progression existantes en termes de cadre d'analyse ainsi que de généralisation des connaissances produites. Nous précisons enfin que l'objet de recherche relatif au contrôle des risques, et notamment aux risques opérationnels, constitue en soi un axe de recherche riche en perspectives tant sur le plan managérial que concernant les aspects théoriques qu'il recouvre.

La validation de notre corps d'hypothèses, en réponse à notre question centrale de recherche, (détaillée en annexe 1) se situe principalement au regard de l'étude des politiques de maîtrise des risques, du rôle des normes de contrôle ainsi que de l'objet d'étude « risques opérationnel ». Les hypothèses consistant à étudier les interactions entre coûts cachés et risque opérationnel voire encore risque opérationnel et valeur de l'entreprise n'étant que partiellement validée au regard de notre étude qualitative. La validation de nos hypothèses de recherches nous amène à interroger la pertinence de la recherche conduite.

Le cadre théorique auquel nous avons eu recours lors de cette étude doctorale était centré sur les problématiques organisationnelles ainsi que sur la littérature dédiée à la gestion des risques. Nous l'avons resitué dans une perspective socio-organisationnelle en ayant recours

successivement à la théorie de la structuration et à sociologie de la traduction en tant que grilles de lecture premières. Dans une moindre mesure, la théorie du contrôle interactif et les cadre théoriques émergents en contrôle organisationnel de la firme nous semblaient adaptés pour décrire et analyser une réalité empirique.

Egalement, le recours aux méthodologies de recherche-action nous a semblé particulièrement adapté pour comprendre cette réalité encore émergente que constitue la formalisation des politiques de maîtrise des risques opérationnels, en réponse aux normes de contrôles dédiées. Le recours à la recherche-action, par l'ancrage dans la pratique et l'immersion que cette méthodologie permettait, a eu un réel apport pour la réalisation d'observations participantes et non participantes. Le nombre d'études de cas réalisées étant par nature limité (dans le temps notamment), une phase de distanciation dans l'analyse des résultats ainsi qu'une confrontation à des résultats confirmatoires, via une enquête par entretiens, semblaient également nécessaires pour répondre à notre question de recherche. Le recours à ces méthodologies qualitatives, bien qu'appelant des limites, semble cependant adapté pour un objet de recherche encore exploratoire, et sur une thématique à la fois technique et encore empreinte de subjectivité (du fait du caractère parcellaire et peu homogène des données collectées en matière de risques opérationnels).

Enfin, la pertinence de nos résultats peut s'envisager au regard de la confrontation avec la pratique. D'une part, nous avons confrontés les résultats de nos études de cas aux responsables des entreprises d'accueil. Ces résultats ont fait l'objet de débats contradictoires et d'une validation quant à la pertinence des problématiques soulevées, parlantes pour les praticiens et répondant à de réelles difficultés empiriques. D'autre part, ces résultats, complétés par les apports de nos entretiens, ont été confrontés aux différentes personnes interviewées. De manière incrémentale, et du fait de la situation théorique rencontrés lors de la réalisation des entretiens, nous avons constaté la récurrence des problématiques soulevées par nos différentes hypothèses, ce sur les différentes entreprises étudiées (lors des cas et des entretiens). Ces échanges contradictoires en phase de distanciation confirment également le caractère adapté des solutions proposées quant aux enjeux de traduction de la norme relative aux risques opérationnels, à la structuration des contrôles ainsi qu'à l'importance des enjeux d'animation et de coordination.

L'apport de notre recherche ne se situe pas dans le fait de démontrer que les différents établissements financiers, qu'il s'agisse d'établissements bancaires ou de sociétés d'assurance, sont vulnérables face aux risques opérationnels. Nous insistons davantage sur le

fait que la régulation prudentielle, et en particulier concernant le risque opérationnel, comprend des limites pratiques liées à un défaut d'appropriation des acteurs des établissements financiers. Ce défaut d'appropriation s'explique par le caractère normatif et technique de la notion même de risque opérationnel, comme le montrent les différents entretiens réalisés.

Notre recherche complète certaines études récentes (Spira, Page, 2003 ; Power, 2005, 2009 ; Cappelletti, 2009 ; Maurer, Lamarque, 2009 ; Mikes, 2009, 2011 ; Kaplan, Mikes, 2012) en insistant sur la dimension interaction des acteurs en charge du contrôle des risques au sein des établissements financiers. C'est à cette condition de bon sens mais difficile à mettre en œuvre en pratique que répond l'enjeu de gestion des risques : initier le changement des pratiques instituées en prenant en compte la variable risque comme sujet de bonne gestion.

Cette recherche contribue à démontrer que l'enjeu de structuration est indispensable pour dépasser la nécessaire institutionnalisation du contrôle et permettre un management actif du risque. Cet enjeu de structuration contribue à consolider la confiance en interne dans l'organisation ainsi qu'à l'égard des tiers par le renforcement des garde-fous de la confiance moderne. Il s'agit d'un sujet d'actualité à l'heure où les organismes des secteurs bancaire et assurantiel mettent en avant une importante communication sur leurs dispositifs d'identification, de quantification mais aussi de réduction des risques. Cette communication sur le risque (le pilier III de la réglementation baloise et le pilier III de celle à venir Solvabilité II) est un enjeu de recherche à part entière car permettant de comparer la logique esthétique liée à la gestion des risques à la réalité d'une structuration du contrôle de l'organisation. La structuration du contrôle s'analyse encore à la lumière des grilles de lecture établissant le lien entre structure et comportement. Il s'agit donc d'une perspective de recherche future dans le prolongement notamment de la théorie socio-économique des organisations en tant que sujet de compréhension de l'environnement interne face au risque.

En conclusion de cette recherche, nous insistons sur l'importance de considérer les problématiques de risques en entreprise sous l'angle gestionnaire et organisationnel plus que technique et réglementaire (Méric et al., 2009). Un tel positionnement permet ainsi d'envisager les problématiques notamment normatives en tant qu'enjeux d'effectivité et préoccupation pratique pour les établissements financiers. A défaut, les critiques fortes de notre temps relativement aux limites du Risk Management modernes, risque fort de valider les

approches selon lesquelles nous nous situons davantage dans une « illusion du contrôle » que dans une réalité de l'action. Les travaux de ces dernières années pointent successivement l'illusion du contrôle (Maijoor, 2000), l'hypocrisie normative (Cappelletti, 2010), le développement puis l'implosion du contrôle (Jobst, 2007 ; Power, 2009, Jednak, Jednak, 2013). Bien que constituant un point de départ, cette recherche, en insistant sur les problématiques d'effectivité du contrôle visant à dépasser les aspects normatifs, constitue une première étape dans la formalisation d'un cadre de pensée permettant d'éviter « l'illusion du contrôle ».

Références bibliographiques

Articles et ouvrages

AEBI V., SABATO, G., SCHMID, M. Risk management, corporate governance, and bank performance in the financial crisis, *Journal of Banking & Finance*, 36 (12),, 2012, pp.3213–3226.

AI J., BROCKETT P.L., COOPER W.W., GOLDEN L.L., Enterprise Risk Management through Strategic Allocation of Capital, *The Journal of Risk and Insurance*, Vol. 00, No. 0, 2011, pp.1-27

ALEMANNO A., DEN BUTTER F., NIJSEN A., TORRITI J., *Better Business Regulation in a Risk Society*, Springer, 2013.

AGLIETTA M. BERREBI L., *Désordres dans le capitalisme mondial,* Odile Jacob, Paris, 2007.

AGLIETTA M. *La crise : Pourquoi en est-on arrivé là ?* Comment en sortir ? Ed. Michalon, Paris, 2008.

AKRICH M. Comment décrire les objets techniques, *Techniques et Culture,* 9, p.49-64, 1987.

AKRICH M. CALLON M. LATOUR B., *Sociologie de la traduction : Textes fondateurs*, Presses de l'Ecole des Mines, 2006.

ALCOUFFE S., BERLAND N., LEVANT Y., Actor-networks and the diffusion of management accounting innovations: A comparative study, *Management Accounting Research*, 19 (1), 2008, pp. 1–17.

ALTAMURA J., BEATTY A., How does internal control regulation affect financial reporting?, *Journal of Accounting and Economics*, Vol.49, 2010, pp..58-74.

AMALBERTI R. *La conduite des systèmes à risques,* Paris, Presses Universitaires de France, 1996.

AMRI P., APANARD P. ANGKINAND, CLAS W. International comparisons of bank regulation, liberalization, and banking crises, *Journal of Financial Economic Policy*, Vol. 3 (4), 2011.

ANDERSEN L. B., HAGER, D., MABERG S., NAESS, M. B., TUNGLAND, M. The financial crisis in an operational risk management context—A review of causes and influencing factors, *Reliability Engineering & System Safety*, Vol.105, 2011, pp 3–12.

ANGERS M., *Initiation pratique à la méthodologie des sciences humaines*, CEC Editions, 1996.

APGAR D., *Risk Intelligence, Learning to manage what we don't know,* Harvard Business School Press, Boston, 2006.

APPERE, G. Gestion des risques et information endogène. *Revue Française de Gestion*, 162, 2006, pp. 63-76.

ARENA M., ARNABOLDI M., AZZONE G., 2010, The organizational dynamics of Enterprise Risk Management, *Accounting, Organizations and Society,* 35, 2010, pp.659–675.

ARGYRIS C., PUTNAM R., MCLAIN SMITH D., *Action Science,* San Fransisco, Jossey-Bass, 1985.

AVENIR M.J., (1992), Recherche-action et épistémologies constructivistes, modélisation systémique et organisations socio-économiques complexes : quelques « boucles étranges » fécondes, *Revue Internationale de Systémique*, 6 (4), pp.403-420.

ARMATTE M., *Crise financière: modèle du risque et risque de modèle,* Mouvements, 58, 2009, p.160-176.

ARNOLD V., BENFORD T., CANADA J., SUTTON S.G., The role of strategic enterprise risk management and organizational flexibility in easing new regulatory compliance*, International Journal of Accounting Information Systems,* Vol.12, 2011, pp.171–188.

BACHELARD G., *Le nouvel esprit scientifique,* PUF, 1934.

BAKER R.C., Action Research and Social Engagement, *Proceedings of the American Accounting Association Annual Meeting*, August, Chicago, 2007.

BALDWIN R., CACE M., *Understanding Regulation: Theory, Strategy and Practice*, Oxford University Press, 1999.

BARBIER R., *La Recherche-Action*, Ed.Anthropos, 1996.

BEASLY M.S., CLUNE R., HERMANSON D.R., Enterprise Risk Management: An Empirical Analysis of Factors Associated with the Extent of Implementation, *Journal of Accounting and Public Policy,* 24, 2005, pp.521–531.

BECK G., KROPP C., Infrastructures of risk: a mapping approach towards controversies on risks, *Journal of Risk Research*, 14 (1), 2011, pp.1–16

BECK U. (1986), *La société du risque, sur la voie d'une autre modernité*, Flammarion, Paris.

BECK U., GIDDENS A., LASH S., Living in the Post-Traditional Society. In *Reflexive Modernization*, Cambridge: Polity Press, 1994.

BECK U. *World Risk Society*. Polity Press, London, 1999.

BERNSTEIN P.L., *Against the Gods, the Remarkable Story of Risk.* Wiley, New York, 1998.

BECKER G., *Human capital, a Theoretical and Empirical Analysis*, Columbia University Press, 1964.

BERETTA S., BOZZOLAN S., A framework for the analysis of firm risk communication, The *International Journal of Accounting,* Vol. 39, 2004, pp.265– 288.

BERNOTH K., PICK A., Forecasting the fragility of the banking and insurance sectors, *Journal of Banking & Finance,* 35, 2011, pp.807–818.

BESSIRE D., *Régulation et systèmes de planification-contrôle,* Economica, 1995.

BESSIRE D., Logiques d'entreprise et design du contrôle de gestion : une comparaison entre le commerce de détail intégré et la banque commerciale », *Finance Contrôle Stratégie*, 1 (4), 1998, pp.5-37.

BESSIRE D., CAPPELLETTI L., PIGE B., Normes : Origines et Conséquences des Crises, Economica, Paris, 2010.

BETBEZE J-P., Les leçons de la crise financière, *Études*, (412), 2010, pp. 331-341

BIRD F. B., *The muted conscience: Moral silence and the practice of ethics in business*, Greenwood Publishing Group, 2002.

BIRD F., WATERS J.A. The Moral Muteness of Managers. *California Management Review*, 32, 73, 1989.

BOATRIGHT J.R., Risk Management and the Responsible Corporation: How Sweeping the Invisible hand?, *Business and Society Review*, 116 (1), 2011, pp. 145-170.

BODUR Z., Operational Risk and Operational Risk related Banking Scandals/ large Incidents, *Maliye Finans Yazilari,* 26, 2012, pp.61-82.

BOJE, D.M., Organizational Storytelling: the Struggles of Pre-modern and Postmodern Organizational Learning Discourses, *Management Learning,* 25 (3), 1994, pp.433-461.

BOJE, D.M., *Narrative methods for organizational & communication research*, Sage publications, 2001.

BONIN H., *La banque et les banquiers en France,* Larousse, 1992.

BON-MICHEL B., *Identification du risque opérationnel et apprentissage organisationnel, Etude d'un établissement de crédit, le Groupe Société Générale*, Thèse de doctorat, Cnam, 2010.

BON-MICHEL B. La cartographie des risques : de la rationalisation du futur à l'apprentissage du risque, *Management et Avenir*, 8 (48), 2011, pp.326-341.

BON-MICHEL B., DUFOUR N. *La gestion des risques opérationnels : normativité, créativité, opérativité. Le cas du secteur financier*. Actes du 3ème Congrès Transatlantique de Comptabilité, Contrôle, Audit, Contrôle de Gestion et Gestion des coûts, ISEOR, 2013.

BORRAZ O., *Les politiques du risque*, Les Presses Science-Po, Paris, 2008.

BOWER J.L., LONARD H.B., PAINE L.S., Global capitalism at Risk, What are you doing about it?, *Harvard Business Review,* September, 2011, pp. 105-112.

BRAITHWAITE S., The Need of a Corporate Strategy on Risk Management and Risk Transfer, *European Management Journal*, 7(4), 1989, pp.467-482.

BRAMMERTZ W., Risk and Regulation, *Journal of Financial Regulation and Compliance*, 18 (1), pp.46-55.

BRENDER A., PISANI F., *Les déséquilibres financiers internationaux*, Repères, Paris, 2007.

BRICKER R., BOROKHOVICH K., SIMKINS B., The impact of accounting research of finance, *Critical Perspectives on Accounting*, 2003, 14, pp.417–438

BRIERS M., CHUA W.F., The role of actor-networks and boundary objects in management accounting change: a filed study of an implementation of activity based costing, *Accounting, organizations and Society*, 26, 2001, pp.237-269.

BRUNSSON N., JACOBSSON B., *A World of Standards,* Oxford University Press, 2005.

BRYMAN A., BELL E., *Business Research Methods,* Oxford University Press, 2011.

BUCKHAM D., WAHL J., ROSE S., (*Executive's guide to Solvency II*, Wiley Business Services, 2010.

BUEHLER K., FREEMAN A., HULME R., The New Arsenal of Risk Management, *Harvard Business Review,* 2008a, pp. 93-100.

BUEHLER K., FREEMAN A., HULME R., Owning the wright risks, *Harvard Business Review,* 2008b.

BUGALLA J., KALLMAN J., LINDO S., NARVAEZ K., The new model of governance and risk management for financial institutions, *Journal of Risk Management in Financial Institutions,* 5 (2), 2012, pp.181–193.

BURLAUD A., CHATELAIN-PONROY S., MIGNON S., TELLER R., WALLISER E., (2004), *Contrôle de gestion*, Vuibert.

BURNABY P., HASS S., Ten Steps to enterprise-wide risk management, *Corporate Governance*, Vol.9 (5), 2009, pp.539-550.

BUSCO C., Giddens' structuration theory and its implications for management accounting research, *Journal of Management and Governance*, 13 (3), 2009, pp.249-260.

CALLON M., LATOUR B., Unscrewing the Big Leviathan : How Actors Macrostructure Reality and How Sociologists Help Them To Do So, in, *Advances in Social Theory and Methodology : Toward an Integration of Micro-and Macro-Sociologies,* Boston, Routledge and Kegan, 1981, p. 277-303.

CALLON M., *La science en action,* Ed. La Découverte, 1995.

CALLON M., Sociologie de l'acteur-réseau, in N.Smelser et P.Baltes, (dir.) *International Encyclopedia of the Social and Behavioral Sciences*, Oxford, 2001.

CALLON M., LASCOUMES P., BARTHE Y., *Agir dans un monde incertain, essai sur la démocratie technique,* Paris, Seuil, 2002.

CAPPELLETTI L., Vers une institutionnalisation de la fonction contrôle interne ?, *Comptabilité – Contrôle – Audit,* 12, 2006, pp.27-43.

CAPPELLETTI L., DELATTRE M., NOGUERA F., Introducing the First Management Control System in Independent Professions: A Qualimetric Inquiry, *Tamara Journal of Critical Organization Inquiry*, 6 (6.3, 6.4), 2007, pp. 23-42.

CAPPELLETTI L., *Un contre effet de la crise : l'hypocrisie normative*, Cahier de recherche Tétranormalisation. Coordonné par D. Bessire et Y. Dupuy, 2009a, pp.12- 13.

CAPPELLETTI L., Performing an Internal Control Function to Sustain SOX 404 and Improve Risk Management: Evidence from Europe, *Management Accounting Quaterly,* 10, 2009b, pp.17-27.

CAPPELLETTI L., *La recherche-intervention: quels usages en contrôle de gestion* ? Communication pour le Congrès de l'AFC, Nice, 2010.

CAPPELLETTI L., Baker R., Measuring and developing human capital through a pragmatic action research: a French case study, *Action Research,* 8 (2), 2010, pp. 211-232.

CAPPELLETTI L., *Le contrôle de gestion de l'immatériel, une nouvelle approche du capital humain*, Dunod, 2012.

CASSELL C., SYMON G., Taking qualitative methods in organization and management research seriously, *Qualitative Research in Organizations and Management: An International Journa*l, 1 (1), 2006, pp.4-12.

CASSELL C., SYMON G., BUEHRING A., JOHNSON P., (2006) The role and status of qualitative methods in management research: an empirical account, *Management Decision*, Vol. 44 Iss: 2, p.290-303.

CASTELLS M., *La société en réseaux*, *l'ère de l'information*, Paris, Fayard, 2001.

CECH R., Measuring causal influences in operational risk, *Journal of Operational Risk*, 4 (3), 2009, pp.59-76.

CHATEAURAYNAUD F., TORNY D., *Les sombres précurseurs, une sociologie pragmatique de l'alerte et du risque,* Editions EHESS, 1999.

CHAUVEY J-N., Hypocrisie, déraison : les nouveaux leviers du contrôle ?, *Comptabilité Contrôle Audit*, 16 (1), 2010, pp.33-51.

CHANDRA A., CALDERON T.G., Information intensity, control deficiency risk, and materiality, *Managerial Auditing Journal*, 24 (3), 2009, pp. 220-232.

CHARBONNEAU S., *La gestion de l'impossible, la protection contre les risques techniques majeurs*, Economica, 1992.

CHENHALL, R., Management control systems design with in its organizational context: Findings from contingency-based research and directions for the future. *Accounting, Organizations and Society*, Vol.28, n°2-3, 2003, pp.127-168.

CHERNOBAI A., JORION P., YU F., The Determinants of Operational Risk in U.S. Financial Institutions, *Journal of Financial and Quantitative Analysis*, 46 (6) 2011, pp. 1683–1725

CHICK V., Entretien, in Snowdon et al., *La pensée économique moderne*, Ediscience International, 1997.

CHITAKORNKIJSIL P., Enterprise Risk Management, *The International Journal of Organizational Innovation*, 2010, pp.309-337.

CHONG Y.Y., How to achieve realistic Risk Management, *Balance Sheet*, 11(4), 2003, pp. 44 – 64 (extract from handling Investment Risk).

CHONG Y.Y., Corporate governance: Risk management starts at the top, *Balance Sheet*, Vol. 12 (5), 2004, pp.42 – 47

CINGOLANI P., Le risque, entre sentiment public et vice-privé, *Mouvements,* 2(14), 2001, pp.55-60.

CLARKE, C., VARMA, S. (1999). Strategic Risk Management: the new competitive Edge. *Long Range Planning,* 32, p. 414–24.

COAD F.A., HERBERT I.P. (2009), Back to the future: New potential for structuration theory in management accounting research?, *Management Accounting Research*, 20, pp.177-192.

COHEN E., *Penser la crise,* Fayard, 2010.

COLBERT J.L., ALDERMAN C.W., A risk-driven approach to the internal audit, *Managerial Auditing Journal*, 10 (2) 1995, pp.38-44

COLQUITT L., HOYT E.R., LEE R.B., Integrated Risk Management and the Role of the Risk Manager, *Risk Management and Insurance Review,* 2 (3) 1999, pp.43-61.

CORDEL F., *Gestion des risques et contrôle interne. De la conformité à l'analyse décisionnelle*. Vuibert, 2013.

CORNFORD A., Revising Basel II: the impact of the Financial Crises, *Finance & Bien Commun,* 34-35, 2009, pp. 60-78.

COUILBAUT F., ELIASHBERG C., *Les grands principes de l'assurance*, L'Argus Editions, 2009.

CUNLIFFE A.L., LUHMAN J.T., BOJE D.M., Narrative temporality: Implications for organizational research, *Organization Studies,* 25 (2), 2004, pp.261-286.

CRAWFORD M., STEIN W., Auditing Risk Management: Fine in Theory but who can do it in Practice?, *International Journal of Auditing*, 6, 2002, pp.119-131.

CROZIER M. FRIEDBERG E. *L'acteur et le système*, Paris, Seuil, 1977.

CROTTY M., *The Foundations of Social Research : Meaning and Perspective in the Research Process,* Sage Publications, 1998.

CVILIKAS A., The Structure of Decisions for banking Risk Managements's Economic Efficiency Assessment, *Economics and Management*, 15, 2010, pp.893-899.

DARSA J-D., *La gestion des risques en entreprise : Identifier, comprendre, maîtriser*, Le Mans, Gereso, 2011

DARSA J-D., DUFOUR N., *Le coût du risque, un enjeu majeur pour l'entreprise*, Editions Gereso, 2014.

DAVID R., *Intervention methodologies in management research*, Track: Collaborative management, Research approach, 1999.

DAVID A., *La recherche intervention, un cadre général pour les sciences de gestion ?,* IXème Conférence Internationale de Management Stratégique Montpellier, 24 au 26 mai 2000.

DAVID R., Etudes de cas et généralisation scientifique en sciences de gestion, *Revue Sciences de Gestion*, Vol.39, 2003, pp.139-166.

DAVID R., *Les connaissances en science de gestion : devons-nous choisir entre scientificité et actionnabilité ? Traversée des frontières entre méthodes de recherche qualitatives et quantitatives.* Acte du colloque AOM –IAE de Lyon, 2004, pp.845-870.

DANIELSSON J., JORGENSEN B.J., DE VRIES C.G., Incentives for effective risk management, *Journal of Banking & Finance* 26, 2002, pp.1407-1425

DE COUSSERGUES S., BOURDEAUX G., *Gestion de la Banque : du diagnostic à la stratégie*, Dunod, 2010.

DEDU V., NECHIF R., Banking Risk Management in the Light of Basel II, *Theoretical and Applied Economics*, 2(543), 2010, pp. 111-122

DE LA VILLARMOIS O., STEPHAN O., Quand l'outil de diagnostic devient interactif, *l'Expansion Management Review,* 119, 2005, pp.60-65.

DE LAGARDE O., *L'invention du contrôle des risques dans les organismes d'assurance,* Thèse de doctorat, Université Paris-Dauphine, 2010.

DE LOACH, J., *Enterprise-wide Risk Management: Strategies for Linking Risk and Opportunities*. London: Financial Times/Prentice Hall, 2000.

DEMIDENKO E., MCNUTT P., The ethics of enterprise risk management as a key component of corporate governance, *International Journal of Social Economics,* 37 (10), 2010, pp.802-815.

DEMORTAIN D., *Scientists and Regulation of Risk. Standardising Control*, Edward Elgar Publishing Ltd, 2011.

DENZIN N.K., LINCOLN Y.S., Sage Handbook of Qualitative Research, Sage Publications, 2011.

DE ZWAAN L., STEWART J., SUBRAMANIAM, N., Internal audit involvement in enterprise risk management, *Managerial Auditing Journal*, 26 (7), 2011, pp.586 - 604

DI MAGGIO P.J., POWELL W., Le néo-institutionnalisme dans l'analyse des organisations. *Politix,* 10 (40), 1997, pp. 113-154.

DRUCKER-GODARD C., EHLINGER S., GRENIER C., Validité et fiabilité de la recherche, in THIETART R-A., *Méthodes de recherche en management*, Dunod, 2007.

DRUMMOND, J.S., THEMESSL-HUBER, M., The cyclical process of action research. The contribution of Gille Deleuze. *Action Research*, 5(4), 2007, pp.430-448.

DOBLER M., Incentives for risk reporting - A discretionary disclosure and cheap talk approach, *The International Journal of Accounting* 43, 2008, pp.184–206

DOHERTY, N.A., *Integrated Risk Management: Techniques and strategies for reducing risk.* McGraw-Hill, New York, 2000.

DON VANGEL, At the brink of regulatory convergence, *Journal of Investment Compliance*, 5 (4), 2004, p. 72-75

DOUGLAS M., WILDAVSKY A., *Risk and culture. An Essay on the Selection of Technological and Environmental Dangers*, University of California, Press, London, 1983.

DREYFUSS M-L., *Les grands principes de Solvabilité II*, Editions l'Argus de l'Assurance, 2012.

DROTT-SJOBERG B-M., Risk: How you See it, react and Communicate, *European Management Journal*, 9 (1), 1991, pp.88-97.

DRUCKER, P., *Management Tasks, Responsibilities and Practices,* 1973.

DUCROCQ C. et al., Les compétences du contrôleur de gestion : des besoins autant humains que techniques, *Revue Management & Avenir*, 55 (5), 2012, pp. 36-57.

DUFOUR N., La financiarisation est-elle un vecteur majeur d'avènement d'une « société du risque » ?, *Revue Management & Avenir,* 48 (8), 2011, pp.258-271.

DUFOUR N., TENEAU G., *Gestion des risques opérationnels et structuration du contrôle : un enjeu de recherche et développement pour le secteur financier*, Actes du 11ème colloque francophone sur le risque (Oriane), 2013.

DUMONTIER P., DUPRE D., MARTIN C., *Gestion et contrôle des risques bancaires, l'apport des IFRS et de Bâle II*, Revue banque Editions, 2008.

ECCLES R., Newquist S.C., Schatz R., Reputation and its Risks, *Harvard Business Review*, February 2007, pp.104-114.

EDOUARD S., Vers une gestion globale des risques : place des systèmes d'information et de l'organisation, in Lemettre J-F., *Risque, information et organisation*, L'Harmattan, 2008.

EDWARDS J., WOLFE S., A compliance competence partnership approach model, *Journal of Financial Regulation and Compliance,* 14 (2), 2006, pp.140-150.

EISENHARDT K.M., Organizational and Economic Approaches, *Management Science*, 31 (2), 1985, pp. 134-149.

EISENHARDT K.M., BOURGEOIS L.J., Politics of Strategic Decision Making in High Velocity Environments: Toward a Mid-Range Theory, *Academy of Management Journal*, 31, 1988, pp.737-770.

ELIAS N., *La société des individus*, Paris, Fayard, 1991.

ENGLUND H., GERDIN J., Structuration theory and mediating concepts: Pitfalls and implications for management accounting research, *Critical Perspectives on Accounting,* 19, 2008, pp.1122-1134.

ENGLUND H., GERDIN J., BURNS J., 25 Years of Giddens in accounting research: Achievements, limitations and the future, *Accounting, Organizations and Society*, 36, 2011, pp.494-513.

EVANOFF D.D.., WALL L.D., (2002), Measures of the riskiness of banking organizations: Subordinated debt yields, risk-based capital, and examination ratings, *Journal of Banking & Finance*, 26, 989–1009.

EWALD F., *L'Etat providence*, Grasset, 1986.

EWALD F., Norms, Discipline and the Law, in Post R., *Law and the Order of Culture*, University of California Press, p.138-161, 1990.

EWALD F. *Insurance and risk*, in G.Burchell, C.Gordon, P.Miller, *The Foucault Effect: Studies in Governmentality*, Londres, pp.197-210, 1991.

EWALD F., *La naissance du risque social*, Risques, 81-82, 2010, pp.157-175, mars-juin.

EWALD F., THOUROT P., *Gestion de l'entreprise d'assurance,* Dunod, 2013.

FADZIL F.H., HARON H., JANTAN M., Internal auditing practices and internal control system, *Managerial Auditing Journal*, 20 (8), 2005 pp. 844 - 866

FIORDISELY F., MARQUES-IBANEZ D., MOLYNEUX P., Efficiency and risk in European banking, *Journal of Banking & Finance,* 35, 2011, pp.1315-1326.

FEHLE, F. TSYPLAKOV, S., Dynamic Risk Management: Theory and Evidence. *Journal of Financial Economics* 78, 2005, 3-47.

FERGUSON N., *L'irrésistible ascension de l'argent* (trad. The ascent of money), Editions Saint-Simon, 2009.

FERNÁNDEZ-LAVIADA A., Internal audit function role in operational risk management, *Journal of Financial Regulation and Compliance*, 15 (2), 2007, pp.143-155

FERRARY, M., Les ressources humaines à risque dans le secteur bancaire. Une application de la gestion des risques opérationnels. *Gestion 2000*, 2009, pp. 85-102.

FOOT F., Operational risk management for financial institutions, *Journal of Financial Regulation and Compliance*, 10 (4), 2002, pp. 313 – 316

FOX J., Risk management from a banking compliance officer's viewpoint, *Journal of Financial Regulation and Compliance*, 7 (1), 1999, pp.27-30.

FRANCIS S., The most insidious operational risk: lack of effective information sharing, *Journal of Operational Risk*, 6 (1), 2011, pp55-68.

FROOT, K. A., STEIN, J. C., Risk management, capital budgeting, and capital structure policy for financial institutions: An integrated approach. *Journal of Financial Economics,* 47(1), 1998, pp.55-82.

FROST C., ALLEN D., PORTER J., BLOODWORTH P., *Operational Risk and Resilience: Understanding and Minimising Operational Risk to Secure Shareholder Value*, Ed. Butterworth-Heinemann, 2000.

FROUD J., The Private Finance initiative: risk, uncertainty and the state, *Accounting, Organizations & Society*, 28, 2003, pp. 567-589.

FRASER, I., HENRY, W., Embedding risk management: structures and approaches, *Managerial Auditing Journal*, 22 (4), 2007, pp. 392-409.

FRIGO M.L., ANDERSON R.J., Strategic Risk Management: A Foundation for Improving Enterprise Risk Management and Governance, *The Journal of Corporate Accounting & Finance,* 2011, pp.81-88.

GADIOUX S-E., Qu'est-ce qu'une banque responsable ? Repères théoriques, pratiques et perspectives, *Management & Avenir,* 38, 2010, pp. 33-51.

GALLAGHER, R.B., Risk Management: New Phase of Cost Control. *Harvard Business Review,* 1956.

GALBRAITH J.K., *Le temps des incertitudes,* Gallimard, 1977.

GALLOPPO G., ROGORA A., What has worked in Operational Risk?, *Global Journal of Business Research*, 5 (3), pp.1-17, 2011.

GALLOWAY D., FUNSTON R., The challenges of enterprise risk management, *Balance Sheet*, 8 (6), pp.22-25, 2000.

GARDENER E., A balance sheet approach to bank risk management, *European Management Journal*, 2 (1), 1983, pp.84-93.

GAVER J.J., PATERSON J.S., Do insurers manipulate reserves to mask solvency problems? *Journal of Accounting & Economics*, 37, 2004, pp.393-416.

GIBBONS M., LIMOGES C., NOWOTWY H., SCHWARTZMAN S., SCOTT P., TROW M., *The new production of Knowledge*, Sage Publications, 1994.

GIDDENS A., *Central Problem of Social Theory,* London, MacMillan, 1979.

GIDDENS A., *La constitution de la société, éléments de la théorie de la structuration*, PUF, 1984.

GIDDENS A., *Les conséquences de la modernité,* Editions l'Harmattan, 1994.

GILBERT C. LASCOUMES P., Les politiques du risque en Europe, *Revue internationale de politique comparée*, (10), 2003, pp.151-160.

GILLET R., HÜBNER G., PLUNUS S., Operational risk and reputation in the financial industry*, Journal of Banking & Finance,* 34, 2010, pp. 224-235.

GIROD-SEVILLE M., PERRET V., Fondement Epistémologique de la Recherche, in Thiétart R.A., *Méthode de Recherche en Management*, 2ème Ed. Dunod, 2003, pp. 13-33.

GIROTRA K., NETESSINE S., How to Build Risk into your Business Model, *Harvard Business Review*, 2011, pp.100-105.

GODARD O., HENRY C., LAGADEC P., MICHEL-KERJAN E., *Traité des nouveaux risques*, Folio, 2002.

GORDON, L.A., LOEB, M.P., TSENG, C-Y., Enterprise Risk Management and Firm Performance: A Contingency Perspective, *Journal of Accounting and Public Policy.* 28, 2009, pp. 301-327.

GORDON-HART S., Basel Two: the risk to the global consensus, *Balance Sheet,* 12 (1), 2004, pp. 22-26.

GOURIEROUX C., *Statistique de l'assurance*, Economica, 1999.

GRAFTON J., LILLIS A.M., MAHAMA H., Mixed methods research in accounting, *Qualitative Research in Accounting & Management*, 8 (1), 2011, pp.5-21.

GRANDAZZi G., in *Dictionnaire des risques*, 2ème édition, Armand Colin, 2007.

GRAY D. E., *Doing research in the real world*. Sage Publications. London. Thousand Oaks, 2004.

GREIMAS A-J., COURTES J., *Sémiotique. Dictionnaire raisonné de la théorie du langage*, Hachette, Paris, 1979.

GUEGAN D., HASSANI B.K., Operational risk: A Basel II step before Basel III, *Journal of Risk Management in Financial Institution*s, 6 (1) 2013, pp.37-53.

GUILLON B., Pour une approche globale du risque. *Responsabilité & environnement (Annales des Mines)*, 77, 2009, p. 7-8.

GUILHOU, X., LAGADEC, P., *La fin du risque zéro*. Editions d'Organisation, Paris, 2002.

GUSTAVSEN B., Theory and Practice: the Mediating Discourse, in Reason P., Bradbury H., *Handbook of Action Research*, Sage Publications, 2001.

HAKENES H., Banks as delegated risk managers, *Journal of Banking & Finance,* 28, 2004, pp.2399–2426.

HAMMOND M., Behaviour-based Risk Management systems: Reducing costs by changing attitudes*, Balance Sheet*, 10 (4), 2002, pp. 26-28.

HANLON G., Knowledge, Risk and Beck: Misconceptions of Expertise and Risk, *Critical Perspectives on Accounting,* 21, 2010, pp.211–220.

HANSSEN J., Corporate Culture and Operational Risk Management, *Bank Accounting & Finance, 2005,* pp.35-38.

HAOUAT ASLI M., Risque opérationnel bancaire, le point sur la réglementation prudentielle, *Revue Management & Avenir*, Volume n°48, 2011, p.15.

HARVEY D., *The Condition of Post-modernity,* Oxford, 1990.

HAYEK F., *Droit, législation et liberté*, PUF Paris, 1980.

HERRING R., Implementing Basel II: Is the Game Worth the Candle?, *Financial Markets, Institutions & Instruments,* 14 (5), 2005, pp.268-287.

HOFFMAN D.G., *Managing Operational Risk, 20 Firmwide Best Practice Strategies,* Wiley & Sons, 2002.

HOFSTEDE G., NEUIJEN B., DAVAL OHAYV D., SANDERS G., Measuring Organizational Cultures: A Qualitative and Quantitative Study Across Twenty Cases, *Administrative Science Quarterly*, 35, (2), 1990, pp. 286-316

HOLLINGSWORTH C., Risk Management in the Post-SOX Era, *International Journal of Auditing*, 16 (1), 2012, pp. 35-53.

HOQUE Z., COVALESKI M.A., GOONERATNE T.N., Theoretical triangulation and pluralism in research methods in organizational and accounting research, *Accounting, Auditing & Accountability Journal*, 26 (7), 2013.

HORA M., KLASSEN R.D., Learning from other's misfortune: Factors influencing Knowledge acquisition to reduce operational risk, *Journal of Operations Management*, 31, 2013, pp.52-61.

HOUSTON, D.B., Risk theory. *Journal of Insurance,* 27, 1960, pp. 77-82.

HUBBARD D.W., *The Failure of Risk Management, Why it's broken and how to fix it*, Wiley & Sons, 2009.

HUBER G.P., VAN DE VEN A.H., *Longitudinal Field Research Methods, Studying Process of Organizational Change,* Sage Publications, 1995..

HUBER C., SCHEYTT T., The dispositif of risk management: Reconstructing risk management after the financial crisis, *Management Accounting Research*, 24 (2), 2013, pp.88-99.

HULL J.C., *Risk Management and Financial Institutions,* Pearson, Prentice Hall, 2007.

HUNT, S.B., *The Timid Corporation: why Business is Terrified of Taking Risk*. John Wiley, London, 2003.

HUSSER J., La théorie de la structuration : quel éclairage pour le contrôle des organisations ?, *Vie & sciences économiques*, 183-184 (1), 2010, pp.33-55.

HUTTER B., *Risk and Regulation,* Oxford University Press, 2000.

JAFARI M., CHADEGANI A., BIGLARI V., Effective Risk Management and Company's Performance: Investment in Innovations and Intellectual Capital using Behavioral and Practical Approach, *International Research Journal of Finance and Economics* Issue, 80 p. 75-83, 2011.

JEBRIN A.H., ABU-SALMA A.J., Conceptual Knowledge Approach to Operational Risk Management (A Case Study), *Intemational Joumal of Business and Management* 7 (2), 2012, 2,p.289-302.

JEDNAK D., JEDNAK J. Operational Risk Management in Financial Institutions, *Journal for Theory and Practice Management*, 66, 2013, pp.71-80

JEMISON D.B., Risk and the Relationship among Strategy, Organizational Processes, and Performance, *Management Science*, 33 (9), 1987, pp.1087-1101.

JIANG W., RUPLEY K.H., WU J., 2010, Internal control deficiencies and the issuance of going concern opinions, Research in Accounting Regulation 22 (2010) 40–46

JICK D.T. Mixing qualitative and quantitative methods: triangulation in action, *Administrative Science Quarterly*, 24, 1979, pp.602-611.

JOBST A., The sting is still in the tail but the poison depends on the dose, *Journal of Operational Risk*, 2 (2), 2007, pp.3-59.

JOGULU U.D., PANSIRI J., Mixed methods: a research design for management doctoral dissertations, *Management Research Review*, 34 (6), 2011, pp.687-701.

JOHANSSON, A.D., LINDHULT, E. Emancipation or workability? Critical versus pragmatic scientific orientation in action research. *Action Research*, 6(1), 2008, pp.95-115.

JONAS H., *Pour une éthique du futur*, Payot-Rivages, 1998.

JÖNSSON S., LUKKA K., *Doing interventionist research in management accounting,* Gothenburg Research, Institute-report, 6, 2005.

JOURNE B., La fiabilité et la résilience comme dimensions de la performance organisationnelle, *M@n@gement*, Vol. 12, 2009, pp.224-229.

JOUSSE G., *Traité de riscologie,* Imestra Editions, 2009.

JUSTESEN L., MOURITSEN J., Effects of actor-network theory in accounting research, *Accounting, Auditing & Accountability Journal*, 24 (2), 2011, pp. 161-193.

KAHNEMAN, D., TVERSKY, A., Prospect theory: An analysis of decisions under risk. *Econometrica,* 47, 1979, pp. 262-291.

KAPLAN R.S., Innovation Action Research: Creating new management theory and practices, *Journal of Management Accounting Research,* Vol.10, 1998, pp.89-113.

KAPLAN R.S., MIKES A., Managing Risk: A New Framework, June, *Harvard Business Review*, 2012, pp.49-60.

KAPLAN R.S., MIKES A., SIMONS R., TUFANO P., HOFMANN M., Managing Risk in the New World, *Harvard Business Review*, 2009, pp.69-75.

KAVCIC K., BERTONCELJ A., Strategic orientation of organizations: risk management perspectives, *Kybernetes,* 39 (5), 2010, pp.735-749.

KEKÄLE T., Construction and triangulation: weaponry for attempts to create and test theory, *Management Decision*, 39 (7), 2001, p.556 - 563

KNECHEL, W. R. The business risk audit: Origins, obstacles and opportunities. *Accounting, Organizations and Society.* 32, 2007, pp.383-408.

KEMMIS S., MCTAGGART R., Participatory Action Research, in Denzin, Lincoln, *The Sage Handbook of Qualitative Research,* Sage Publications, 2005.

KERVERN G-Y., *Eléments fondamentaux des cyndiniques,* Economica, 1995.

KESSLER D., Les noces du risque et de la politique, *Le Débat*, n°109, 2000, pp.55-72.

KIM Y., PARK M.S., Market uncertainty and disclosure of internal control deficiencies under the Sarbanes–Oxley Act, *J. Account. Public Policy*, 28, 2009, pp.419-445.

KIPPENBERGER T., Internal audit and governance, the shift from control to risk, *The Antidote*, 4 (3), 1999, pp.6-7.

KLEIN, A., Corporate culture: its value as a resource for competitive advantage. *Journal of Business Strategy,* 32 (2), 2011, pp. 21-28.

KNIGHT F., *Risk, Uncertainty and Profit,* New York, Augustus, M.Kelley, 1921.

KRAUJALIS S., KARPAVICIENE E., CVILIKAS A., The Specifics of Operational Risk Assessment Methodology Recommended by Basel II, *Engineering Economics*, 48 (3), 2006, pp. 7-17.

KULPA X., MAGDON A., Operational Risk management in a Bank, Internal Auditing and Risk Management, 28 (4), 2012, pp.35-50.

KUMAR R., *Research methodology, a step-by-step guide for beginners*, Sage Publications, 2005.

KVALE S., *Interviews: an introduction to qualitative research interviewing*. Thousand Oaks, Sage Publications, 1996.

LALLE B. Production de la connaissance et de l'action en sciences de gestion. Le statut expérimenté de « chercheur-acteur », *Revue française de gestion*, 158 (1), 2004, pp. 45-65.

LAFFORT E., *Appropriation croisée : vers une diminution du risque de fraude. Application au contrôle des opérateurs de finance de marché*, Université de Pau, mai 2013.

LAMARQUE, E., La banque sait-elle encore gérer le risque ?, *Revue Française de Gestion*, 198-199, 2009, pp. 193-207.

LARKECHE S. *Epistémologie du risque*, l'Harmattan, 2011.

LASCOUMES P., La précaution comme anticipation des risques industriels, in *Conquête de la sécurité, gestion des risques,* l'Harmattan, 1991.

LAUFER R., *L'entreprise face aux risques majeurs : à propos de l'incertitude des normes sociales,* logiques sociales, l'Harmattan, 1993.

LAWRENCE NEUMAN W., *Social Research Methods, qualitative and quantitative approaches*, Pearson, 2011.

LI X., WU Z., Corporate risk management and investment decisions, *The Journal of Risk Finance*, 10 (2), 2009, pp. 155-168.

LINDBERG D.,SEIFART D., Enterprise Risk Management (ERM) Can Assist Insurers in Complying with the Dodd-Frank Act, *Journal of Insurance Regulation*, 2011, pp.319-337.

LEBRATY J-F., Améliorer la prise des décisions risquées : comment transformer une équipe d'experts en une équipe experte ?, in *Méthodes et thématiques pour la gestion des risques*, (dir. B.Guillon), colloque Oriane, l'Harmattan, 2008, pp.48-64.

LEE T.W., *Using qualitative Methods in Organizational Research,* Sage Publications, 1999.

LEE B., HUMPHREY C., More than a numbers game: qualitative research in accounting, *Management Decision*, 44 (2), 2006, pp.180-197.

LEEDY A., ORMROD J.E., *Practical research: Planning and Design,* Pearson, 2005.

LE MOIGNE J.L., Epistémologies constructivistes et sciences de l'organisation, p.81-140, in Martinet A.C., *Epistémologies et sciences de gestion*, Economica, 1990.

LEWIN K., *Action Research and minority problems, Resolving social conflicts,* p.201-216, Harper & Row, 1946.

LEWINS A., SILVER C., *Using software in qualitative research: a step-by-step Guide,* Thousand Oak, CA Sage, 2007.

LIEBENBERG, A.P., HOYT, R.E. The Determinants of Enterprise Risk Management: Evidence from the Appointment of Chief Risk Officers. *Risk Management and Insurance Review,* 6 (1), 2003, p. 37-52.

LIEDTKE P.M. (2005), L'assurance et son rôle prépondérant dans les économies modernes, *Revue Risques* n°63.

LINDSAY R.M., We must overcome the controversial relationship between management accounting research and practice: A commentary on Ken Merchant's 'Making Management accounting research more useful', *Pacific Accounting Review*, 24 (3), 2012, pp. 357-375.

LINSLEY P.M., SHRIVES P.J., Mary Douglas, risk and accounting failures, *Critical Perspectives on Accounting,* 20, 2009, pp.492–508

LIU M., *Fondements et pratiques de la recherche-action*, l'Harmattan, 1997.

LUHMANN, N., *Risk : a Sociological Theory*, Berlin, Eds Walter de Gruyter, 1993.

MAIJOOR S., The Internal Control Explosion, *International Journal of Auditing*, 4, 2000, pp.101-109.

MAINELLI M., YEANDLE M., Best execution compliance: new techniques for managing compliance risk, *The Journal of Risk Finance*, 7 (3),, 2006, pp. 301 – 312.

MARCH J.C., OLSEN J.P. The New Institutionalism: Organizational Factors in Political Life, *American Political Science Review*, 78, 1984.

MARTINET A.C., Pesqueux Y., *Epistémologie des sciences de gestion*, Vuibert, Fnege, 2013.

MARTUCCELLI D., *Sociologie de la modernité,* Folio Essais, 1999.

MAURER F., LAMARQUE E., Le risque opérationnel bancaire. Dispositif d'évaluation et système de pilotage, *Revue Française de Gestion*, 191, 2009, pp.93-108

MCGREW J.F., BILOTTA J.G., The effectiveness of risk management: measuring what didn't happen, *Management Decision*, 38 (4), 2000, pp. 293-301.

MCKERNAN, J., *Curriculum Action Research. A Handbook of Methods and Resources for the Reflexive Practitioner*. London: Kogan Page, 1991.

MCSHANE M.K., Nair A., Rustambekov E., Does Enterprise Risk Management Increase Firm Value?, *Journal of Accounting, Auditing & Finance*, 26(4), 2011, pp.641–658

MEHR, R.I., HEDGES, B.A. *Risk Management in the Business Enterprise*. Homewood, 1963.

MERIC J., PESQUEUX Y., SOLE A., *La société du risque, analyse et critique*, Economica, 2009.

MERIC J., SFEZ F. La créativité d'experts comme risque opérationnel : contournements et détournements de la régulation bancaire, *Revue Management & Avenir,* Vol.48, 2011, pp.29-47.

MERTON R.C., Financial innovation and the management and regulation of financial institutions, *Journal of Banking & Finance,* 19 (1995), pp.461-481.

MIKES A., Convictions, Conventions and the Operational Risk Maze-The Cases of Three Financial Services Institutions. *International Journal of Risk Assessment and Management,* 7 (8), 2007, pp.1027-1056.

MIKES A., *Accounting, Risk Management and the Aftermath of a Control Debacle,* 2008a.

MIKES A. Chief Risk Officers at Crunch Time: Compliance Champions or Business Partners?, *Journal of Risk Management in Financial Institutions,* Vol.2, n°. 1 (November-December 2008), 2008b.

MIKES A., Risk management and Calculative Culture, *Management Accounting Research*, 20, 2009, pp.18–40.

MIKES A., From counting risk to making risk count: Boundary-work in risk management, *Accounting, Organizations and Society*, 36, 2011, pp.226–245.

MILES M.B. Qualitative Data as an Attractive Nuisance: The Problem of Analysis, *Administrative Science Quarterly*, 24 (4), 1979, *Qualitative Methodology* (Dec., 1979), pp. 590-601.

MILES M.B., HUBERMAN A.M, *Analysing qualitative data: a source book for new methods*, Beverly Hills, CA, Sage, trad. franc. : Analyse des données qualitative, Bruxelles, De Boeck, 2003, 1984.

MILLER, K. D., Organizational risk after modernism, *Organization Studies*, 30 (2-3), 2009, pp.157-180.

MINSKY H. (2008), *Stabilizing an Unstable Economy*, McGraw-Hill Professional.

MINTZBERG H., An Emerging Strategy of Direct Research, *Administration Science Quarterly*, 24, 1979, pp.580-589.

MIRON D., PETCU M., SOBOLEVSCHI D, Applicative Approach to Risk Management, *Review of International Comparative Management,* 12 (5), 2011, pp.883-892.

MITRA S., Pervasiveness, severity, and remediation of internal control material weaknesses under SOX Section 404 and audit fees, *Review of Accounting and Finance*, 8 (4), 2009.

MITRA S., HOSSAIN M., Corporate governance attributes and remediation of internal control material weaknesses reported under SOX Section 404, *Review of Accounting and Finance,* 10 (1), 2011, pp. 5-29.

MOE T., *Interests, Institutions, and Positive Theory: the Politics of the NLRB,* Studies in American Political Development, Yale University Press, 1987.

MOERMAN L.C., VAN DER LAAN S., Risky business: Socializing asbestos risk and the hybridization of accounting, *Critical Perspectives on Accounting,* 2, 2012, pp. 107– 116

MOUREAU N., RIVAUD-DANSET D., L'incertitude dans les théories économiques, Editions La Découverte 2004.

MUERMANN A., OKTEM U. The Near-Miss Management of Operational Risk, *Journal of Risk Finance*, 2002, pp.25-36.

MUNIER B., L'ingénierie du risque, *Risques,* n°44/ Décembre 2000.

MURPHY M.E., Assuring responsible risk management in banking: the corporate governance dimension, *Delaware Journal of Corporate Law*, 36, 2011, pp.121-163

MORLAYE F., *Risk management et Assurance*, Economica, Paris, 2006.

MORTON J.C., The development of a compliance culture, *Journal of Investment Compliance,* 6 (4), 2005, pp. 59-66.

NEEF D., Managing Corporate Risk through Better Knowledge Management, *The Learning Organization*, 12 (2), 2005, pp.112-124.

NEUENDORF K.A., *The Content Analysis Guidebook,* Thousand Oaks, Sage, 2002.

NICHOLSON G., KIEL G., KIEL-CHISHOLM S., The Contribution of Social Norms to the Global Financial Crisis: A Systemic Actor Focused Model and Proposal for Regulatory Change, *Corporate Governance: An International Review*, 19(5), 2011, pp.471-488.

NIESTAT, E., PA Consulting Group. *Financial Times, Business Report, Risk Management,* 2005.

NOOTEBOOM B., BERGER H., NOORDERHAVEN N.G., Effects of Trust and Governance on Relational Risk, *The Academy of Management Journal*, 40 (2), Special Research Forum on Alliances and Networks, 1997, pp. 308-338

NOUY D. Le champ du risque opérationnel dans Bâle II, *Revue d'économie financière*, n°84, 2006, p.11.

NOY E., ELLIS S., Corporate Risk Strategy: Does it Vary across Business Activity?, *European Management Journal,* 21 (1), 2003, pp.119-128.

OGIEN D., *Comptabilité et audit bancaires,* Dunod, 2008.

OJO M., *Financial regulation and risk management: adressing risk challenges in a changing financial environment*, Munich Personal RePEc Archive, 2006.

OJO M., Risk management by the Basel Committee: Evaluating progress made from the 1988 Basel Accord to recent developments, *Journal of Financial Regulation and Compliance,* 18 (4), 2010, pp. 305 – 315.

ORLEAN A., *Le pouvoir de la finance*, Odile Jacob, Paris, 1999.

ORLEAN A., *De l'euphorie à la panique* : *penser la crise financière*, Collection CEPREMAP-n°16, Editions Rue d'Ulm, Paris, 2009.

ORLEAN A., *Le pouvoir de la finance,* Odile Jacob, 2010.

OSPITAL D. Le risque opérationnel ou l'opportunité unique pour les banques de s'approprier une véritable culture du risque, *Revue d'Economie Financière,* n°84, juin 2006.

OUCHI W.G., The Relationships between Organizational Structure and Organizational Control, *Administrative Science Quarterly,* 22, 1977, pp.95-113.

PAILLE P., MUCCHIELLI A., *L'analyse qualitative en sciences humaines et sociales,* Armand Colin, 2012.

PARKER L.D., Qualitative management accounting research: Assessing deliverables and relevance, *Critical Perspectives on Accounting*, 23, 2012, pp.54-70.

PARSONS T., Suggestions for a sociological approach to the theory of organizations, *Administrative Science Quarterly*, 1, 1956, pp.63-85.

PATHAK J., Risk management, internal controls and organizational vulnerabilities, *Managerial Auditing Journal*, 20 (6), 2005, pp.569-577.

PATTON M.Q., *Qualitative Research and Evaluation Methods*, Sage Publications, Newbury, 2002.

PAUL J., Between-method Triangulation in organizational Diagnosis, *International Journal of Organizational Analysis*, 4 (2), 1996, pp.135-153.

PELZER P., The displaced world of risk: risk management as alienated risk(perception)?, *Society and Business Review*, 4 (1), 2009, pp.26-36.

PERETTI-WATEL, P. *Sociologie du risque*. Armand Colin, Paris, 2000.

PESQUEUX Y., Pour une épistémologie du risque, *Management & Avenir,* 43 (3), pp.460-475.

PEYREFITTE A., *La société de confiance*, Odile Jacob, Paris, 1995.

PFEFFER J., SALANCIK G.R., *The External Control of Organizations. A Resource Dependence Perspective,* Stanford Business Classics, 1978.

PIGE B. (2001), *Audit et contrôle interne*, Ed. EMS.

PIPAN T., CZARNIAWSKA B., How to construct an actor-network: Management accounting from idea to practice, *Critical Perspectives on Accounting,* 21, 2010, pp.243-251.

PHILIPPAS D.T., SIRIOPOULOS C., Influence of financial innovation to the validation of operational risk, *Managerial Finance*, 35 (11), 2009, pp. 940 – 947.

PLIHON D., COUPPEY-SOUBEYRAN J., SAÏDANE D., *Les banques, acteurs de la globalization financière*, La Documentation française, Paris, 2006.

POPPER K., *La logique de la découverte scientifique*, Payot, Paris, 1973.

POWELL W., DI MAGGIO P.J., *The New Institutionalism in Organizational Analysis*, the University of Chicago Press, 1991.

POWER, M., *The Audit Implosion: Regulating Risk from the Inside*, ICAEW, London, 1999.

POWER M., The invention of operational risk, *Review of International Political Economy*, 12 (4), 2005, pp. 577-599.

POWER, M., *Organized uncertainty: Designing a world of risk management*. Oxford: Oxford University Press, 2007.

POWER M., The Risk Management of Nothing, *Accounting, Organizations and Society,* 34 2009, pp.849–855.

PRADIER P-C., Le concept de risque: encore la politique et l'épistémologie, *Risques*, n°67, Septembre 2006, pp. 76-80.

PRICE J.L., *Organizational Effectiveness: an Inventory of Propositions*, Homewood, 1968.

PYLE D., On the Theory of Financial Intermediation, *Journal of Finance*, n°26, juin 1971.

RAIMBAULT C-A., BARR A*., Les risques émergents, un pilotage stratégique*, Economica, 2010.

REASON P., BRADBURY H., *Handbook of action research,* London, Sage, 2001.

RENAUD A., Les configurations de contrôle interactif dans le domaine environnemental, *Comptabilité Contrôle Audit,* 19 (2), 2013, pp.101-132.

RESWELER J-P., *La recherche-action, que sais-je ?,* PUF, 1995.

REVET S., Penser les catastrophes : de la vulnérabilité à la société du risque, in *La culture du risque en question*, Ed.La Dispute, 2013.

RICHARDSON J.G. The certainty of uncertainty: risk management revisited, *Foresight,* 12 (4), 2010, pp.47-64.

RÖTHELI T.F., (2010) Causes of the financial crisis: Risk misperception, policy mistakes, and banks'bounded rationality, *The Journal of Socio-Economics*, 39, 2010, pp.119-126.

SAEIDI P., SOFIAN S., RASID S.Z., SAEID S.P., The Role of Chief Risk Officer in Adoption and Implementation of Enterprise Risk Management-A Literature Review, *International Research Journal of Finance and Economics*, 2012, pp.118-123.

SAMPATH V., The need for greater focus on nontraditional risks: The case of Northern Rock, *Journal of Risk Management in Financial Institutions*, 2 (3), 2009, pp.301-305.

SARENS G., DE BEELDE I., Internal auditors' perception about their role in risk management: A comparison between US and Belgian companies, *Managerial Auditing Journal,* 21 (1), 2006, pp. 63-80.

SARDI A., *Pratique de la comptabilité bancaire*, Afges, 2012.

SARENS G., CHRISTOPHER J., (2010), The association between corporate governance guidelines and risk management and internal control practices: Evidence from a comparative study, *Managerial Auditing Journal*, 25 (4), 2010, pp. 288-308.

SAVALL H., ZARDET V., *Recherche qualimétrique, approche qualimétrique : observer l'objet complexe*, Economica, 2004.

SAVALL H., ZARDET V., *Le management socio-économique*, Economica, 2005a.

SAVALL H., ZARDET V., *Tétranormalisation, défis et dynamiques*, Economica, 2005b.

SAVALL H., ZARDET V., *Maîtriser les coûts et les Performances Cachés,* Economica, 2010.

SERAN-LUU T., *Système de contrôle et de pilotage pour une entreprise organisée essentiellement en équipes à distance : le cas de deux BSI bancaires*, Thèse de doctorat, Université de Montpellier, 2012.

SCIALOM L., *Economie bancaire*, La Découverte, Paris, 2004.

SCIMIA D., Mitigating the Cost of Organizational Behavioral Risk, *Employee Relations Law Journal*, 36 (2), 2010, pp.48-58.

SCHÖN D.A., *The Reflective Practitioner: How Professionals Think in Action*, Basic Books Ed, 1983.

SHAPIRO B., MATSON D. (2008), Strategies of resistance to internal control regulation, *Accounting, Organizations and Society,* Vol. 33, p.199-228.

SHEEHAN N.T., A risk-based approach to strategy execution, *Journal of Business Strategy*, 31 (5), 2010, pp.25-37.

SHILLER R., *Exubérance irrationnelle*, Valor Editions, Hendaye, 2000.

SHILLER R., *The New Financial Order: Risk in the Twenty-First Century*, Princeton University Press, 2003.

SHORTRIDGE R.T., SMITH P.A., Understanding the changes in accounting thought, *Research in Accounting Regulation*, 21, 2009, pp.11-18.

SIMISTER T., Risk Management, the need to set standards, *Balance Sheet,* Vol.8, n°4, p.9-10, 2000.

SIMONS R., *Levers of control, how managers use innovative controls systems to drive strategic renewal*, Harvard Business School, Boston, 1995.

SIMONS R., *Performance Measurement & Control Systems for Implementing Strategy.* Prentice Hall, 2000.

SINGH, J.V. Performance, Slack, and Risk Taking in Organizational Decision Making. *The Academy of Management Journal*, 29 (3), 1986, pp. 562-585.

SITKIN S.B., BIES R.J., The Legalistic Organization: Definitions, Dimensions and Dilemmas, *Organization Science*, 4 (3), 1993, pp.345-351.

SITKIN, S.B., WEINGART, L.R., Determinants of Risky Decision-Making Behavior: A Test of the Mediating Role of Risk Perceptions and Propensity. *The Academy of Management Journal*, 38 (6), 1995, pp. 1573-1592.

SHEEHAN N.T., Making risk pay: the board's role, *Journal of Business Strategy,* 30 (1), 2009, pp.33-39.

SORMANI P., IN LERESCHE J-P., BENNINGHOFF M., GRETTAZ VON ROTEN F., MERZ M., *La fabrique des sciences, des institutions aux pratiques*, Presses polytechniques universitaires romandes, 2006.

SPIRA L., PAGE, M., Risk Management: The Reinvention of Internal Control and the Changing Role of Internal Audit. *Accounting, Auditing and Accountability Journal* 16 (4), 2003, pp.640-661.

STEEN J., (2010), Actor-network theory and the dilemma of the resource concept in strategic management, *Scandinavian Journal of Management,* 26, 2010, pp.324-331.

STEINER P., Philosophie, technologie et cognition: état des lieux et perspectives. Introduction au dossier, *Intellectica*, 53-54 (1-2), 2010, pp.7-40.

STRAUSS A.L., *Qualitative Analysis For Social Scientists,* Cambridge University Press, 1987.

STULZ, R., Ways Companies Mismanage Risk. *Harvard Business Review*, March, 2009, pp. 86-94.

STURM P., Operational and reputational risk in the European banking industry: The market reaction to operational risk events, *Journal of Economic Behavior & Organization,* 85, 2013, pp.191– 206.

SUBRAMANIAM N., MCMANUS L., ZHANG J., Corporate governance, firm characteristics and risk management committee formation in Australian companies, *Managerial Auditing Journal,* 24 (4), 2009, pp.316-339.

SUTTON, G., Extended-enterprise systems' impact on enterprise risk management, *Journal of Enterprise Information Management*, 19 (1), 2006, pp.97-114.

SYLLA, R., Financial systems, risk management, and entrepreneurship: historical perspectives, *Japan and the World Economy*, 15 (4), 2003, pp. 447-458.

SZPIRGLAS M., Gestion des risques et quiproquos, *Revue française de gestion*, 161, 2006, pp.67-88.

TALEB, N.N., GOLDSTEIN, D.G., SPITZNAGEL, M.W., The Six Mistakes Executives make in Risk Management. *Harvard Business Review*, p. 78-81, 2009.

TANI T., Interactive control in target cost management, *Management Accounting Research*, 6 (4), 1995, pp.399-414.

TAYLOR-GOOBY P.F., Sociological approaches to risk: strong in analysis but weak in policy influence in recent UK developments, *Journal of Risk Research*, 11 (7), 2008, pp. 863-876.

TER BOGT H., VAN HELDEN J., The practical relevance of management accounting research and the role of qualitative methods there in: The debate continues, *Qualitative Research in Accounting & Management,* 9 (3), 2012, pp.265 - 273

THIERY-DUBUISSON S., Approche par les risques : les auditeurs peuvent-ils innover ?, *Comptabilité Contrôle Audit*, 2003, pp.249-268.

THIETART, R. A., *Méthodes de recherche en management,* Paris, Dunod, 2003.

TORBERT W.R., The distinctive developmental action inquiry asks, *Management Learning*, 30 (2), 1999, pp.186-206.

TRAN H.C., *Entre idées et projets d'innovation : approche sociocognitive & perspective stratégique*, Thèse de doctorat Université Paris-Est, Val-de-Marne, 2008.

TRELEAVEN L., The Turn to Action and the Linguistic Turn: Towards an Integrated Methodology, in Reason, Bradbury, *Handbook of Action Research*, Sage Publications, 2001.

TORRE-ENCISO M.I., BARROS M.H., Operational Risk Management for Insurers, *International Business Research,* 6 (1), 2013, pp.1-11.

VAN DE VEN, A.H., JOHNSON, P.E. Knowledge for Theory and Practice. *The Academy of Management Review* 31(4), 2006, pp.802-821.

VAN MAANEN J., Reclaiming Qualitative Methods for Organizational Research: A Preface, *Administrative Science Quarterly*, 24 (4), Qualitative Methodology, Dec., 1979, pp. 520-526.

VAUGHAN, E., VAUGHAN, T., *Essentials of Insurance: A Risk Management Perspective*. Wiley & Sons, 1995.

VERBANO C., VENTURINI K., Development Paths of Risk Management: Approaches, Methods and Fields of Application, *Journal of Risk Research* 14 (5), 2011, pp.519-550.

VERET, C., MEKOUAR, R., *Fonction : Risk Manager*, Dunod, Paris, 2005.

VOLLMER H., Management accounting as normal social science, *Accounting, Organizations and Society,* 34, 2009, pp.141–150.

VYAS M., SINGH S., Risk Management in Banking Sector, *Management Edge,* 4 (1), 2010, pp. 15-24.

WACHEUX F., *Méthodes qualitatives et recherche en gestion,* Economica, 1996.

WAHLSTRÖM G., Risk management versus operational action: Basel II in a Swedish context, *Management Accounting Research*, 20, 2009, pp.53–68.

WALTER F., *Catastrophes, une histoire culturelle XVI-XXIème siècle,* Seuil 380 p., 2008.

WANG T., HSU C., Board composition and operational risk events of financial institutions, *Journal of Banking & Finance,* 37, 2013, pp. 2042–2051

WEICK K.E., *Sensemaking in organizations,* Londres, Sage publications, 1995.

WEICK K.E., SUTCLIFFE K.M. OBSTFELD D., Organizing and the Process of Sensemaking, *Organization Science,* 16 (4), 2005, pp. 409-421.

WHITE D., Application of systems thinking to risk management: a review of the literature, *Management Decision,* 33 (10), 1995, pp. 35-45.

WILLIAMSON O., *The Economic Institutions of Capitalism,* The Free Press, New York, 1985.

WILLIAMSON O. *The Firm as a Nexus of Treaties,* Sage Publications, Londres, 1990.

YAZID A.S., The influence of Chief Executive Officers' Traits on Financial Risk Management Perceptions: Evidence from Malaysia*, International Journal of Economics and Finance,* 4 (4), 2012, pp. 78-85.

YIN R., The Case Study Crisis: Some Answers, *Administration Science Quarterly*, 26, 1981, pp.58-65.

YIN R.K., Discovering the future of case study method in evaluation research. *Evaluation Practice,* 15, 1994, pp.283-290.

YIN R.K., *Applications of case study research,* Sage Publications, 2012.

ZADJENWEBER D., *Economie des extrêmes, Krachs, catastrophes et inégalités,* Champs essais, 2009.

ZEGHAL, D., EBONDO, E., Management des risques de l'entreprise: Ne prenez pas le risque de ne pas le faire. *La Revue des Sciences de Gestion*, 237-238, 2009, pp.17-26.

Rapports et documentations professionnelles de référence

COMITE DE BALE, *Gestion du risque opérationnel,* (Septembre 1998).

COMITÉ DE BÂLE, *Sound Practices for the Management and Supervision of Operational Risk*, (Décembre 2001).

COMITÉ DE BÂLE, *Sound Practices for the Management and Supervision of Operational Risk,* (Juillet 2002).

COMITE DE BALE, *Vue d'ensemble du nouvel accord de Bâle sur les fonds propres*, Banque des Règlements Internationaux, 2003a.

COMITE DE BALE, *Saines pratiques pour la gestion et la surveillance du risque opérationne*l, Banque des Règlements Internationaux (Février 2003), 2003b.

COMITE DE BALE, *Operational risk tranfer across financial sectors,* (Août 2003), 2003c.

COMITE DE BALE, *Outsourcing in Financial Services,* (Février 2005), 2005a.

COMITE DE BALE, *High-level principles for business continuity,* (Décembre 2005), 2005b.

COMITE DE BALE, *Enhancing corporate governance for banking organizations,* (Février 2006).

COMITÉ DE BÂLE, *Enhancements to the Basel II framework* (juillet 2009).

COMITÉ DE BÂLE, (*Recognising the risk-mitigating impact of insurance in operational risk modeling.* (Octobre 2010).

COMITÉ DE BÂLE, *Principles for the Sound Management of Operational Risk* (Juin 2011), 2011a.

COMITÉ DE BÂLE, *Operational Risk- Supervisory Guidelines for the Advanced Measurement Approaches,* (Juin 2011), 2011b.

COMITE DE BALE, *Principes aux fins de l'agrégation des données sur les risques et de la notification des risques* (janvier 2013).

Règlement n° 97-02 du 21 février 1997 relatif au contrôle interne des établissements de crédit et des entreprises d'investissement, modifié par les règlements n° 2001-01 du 26 juin 2001 et n°2004-02 du 15 janvier 2004 et par les arrêtés du 31 mars 2005, du 17 juin 2005, du 20 février 2007, du 2 juillet 2007, du 11 septembre 2008, du 14 janvier 2009, du 29 octobre 2009 et du 3 novembre 2009. Banque de France.

EIOPA (2013), *Orientations relatives à l'évaluation prospective des risques propres (basée sur les principes de l'ORSA).*

Glossaire

ACPR (Autorité de Contrôle Prudentiel et de Résolution) : Née en janvier 2010 de la fusion de l'ACAM et de la Commission bancaire, elle est le superviseur pour le marché français des organismes financiers

Acteur réseau : acteur d'une organisation au centre d'un processus d'interactions avec une multiplicité d'autres acteurs, coordonnant des activités dans le cadre d'un processus formel ou non d'interactions.

Acteurs : Ceux jouant un rôle important dans le système par l'intermédiaire des variables caractérisant leurs projets et plus ou moins contrôlées par ces derniers.

Aléa : *alea*, coup de dé, chance. Evènement dont on ne peut connaitre à l'avance la survenance et le moment de celle-ci de même que ses conséquences.

Anticipation : Accomplir une action en avance. Penser en avance : « *Regarder l'avenir le transforme »* (Gaston Berger).

Appétence au risque : Niveau de risques que l'organisme est prêt à prendre dans le cadre de ses objectifs stratégiques, pouvant inclure des marges de tolérance / Lien entre la stratégie et la gestion quotidienne des risques. Exemple : ne pas descendre en dessous de 150% de couverture de l'exigence de capital

Approche « *bottom up* » (approche « ascendante ») : Inventaire des risques à partir de la description des processus opérationnels et supports principalement. L'intérêt de cette méthode par rapport à l'approche descendante relève de la précision des risques identifiés, notamment pour ceux de type « opérationnel », en termes d'occurrence et d'impacts sur la réalisation quotidienne des activités, grâce à différents outils (entretiens, base incidents,…).

Approche « *top down* » (approche « descendante ») : Recensement des risques par les équipes de direction, à partir d'une vision d'ensemble de l'organisation, de ses objectifs, de ses activités. Cette vision est complémentaire par rapport à l'approche ascendante, car elle permet par entretiens d'obtenir une liste des risques majeurs de l'organisation et d'assurer un relai pour diffuser ensuite une culture de la gestion du risque à tous les niveaux de l'organisation.

Audit interne : Fonction de contrôle réalisant un audit des processus de l'entreprise, en se basant généralement sur la cartographie des risques de l'entité. La fonction d'audit interne est une fonction indépendante devant fournir à la gouvernance de l'entreprise un degré d'assurance raisonnable sur la maîtrise de ses activités (internes ou externalisées).

Aversion au risque : La cause du rejet du risque pour est que le supplément de bien-être dû à une action risquée est inférieur à son gain pour l'individu. (Bernoulli, 1738). L'utilité

marginale des gains est décroissante avec la richesse acquise. Voir sur ce point la théorie de l'espérance d'utilité (Von Neumann et Morgenstern, 1944-Savage, 1954).

Base de collecte des incidents et des pertes : Il s'agit d'un outil de gestion des risques dans lequel les incidents (significatifs ou non) sont renseignés par les collaborateurs de l'entreprise dans le cadre des filières risques (ce rôle est généralement assumé par les référents risques). En cas de survenance d'un évènement, le référent doit renseigner dans l'outil le type de risque auquel l'évènement se rattache, le descriptif de l'évènement (enchainement de type cause / conséquence), le coût avéré ou potentiel, la nature d'impact (financier, image, humain) et le cas échéant les mesures déjà prises pour pallier les conséquences dommageables de l'évènement. La base incident donne une vision détaillée des risques et sert à renseigner la cartographie des risques.

Cartographie des risques : Outil dans lequel les fonctions des risques et les différentes entités métiers et supports renseignent les risques identifiés potentiels ou avérés (issus de la base incidents lorsqu'ils sont avérés). La cartographie des risques visent à identifier les risques de l'entreprise sur la base d'un référentiel de risque (catégories de risques).

Continuité d'activité : La continuité d'activité (ou le maintien d'une entité en condition opérationnelle) est fréquemment abordée via la Plan de Continuité d'Activité (détaillant les cas de crises auxquels l'entreprise peut faire face et engendrant une interruption d'activité ainsi que les moyens associés pour maintenir l'entreprise en continuité d'activité). On distingue généralement le plan de continuité d'activité (PCA) du plan de reprise d'activité (PRA) et du plan de secours informatique (PSI). Les problématiques de PCA sont envisagées par la réglementation en banque et assurance sous l'angle des risques opérationnels.

Contrôle de conformité : Fonction de contrôle en charge de vérifier la conformité des processus et procédures internes aux lois et règlements, mais également aux la conformité des pratiques internes aux procédures, charte, code de déontologie de l'entreprise etc. La fonction de contrôle de conformité occupe généralement un rôle ad hoc de veille juridique et réglementaire et de consolidation des différentes veilles techniques dans l'entreprise (veilles faites par les différentes fonctions métiers et supports).

Contrôle de gestion : Fonction de contrôle au sein de l'organisation, généralement rattachée à la direction financière voire à la direction générale, et ayant pour objectif de piloter la performance de l'entreprise par le recours à des indicateurs de performance adossé à des objectifs définis en lien avec la stratégie opérationnelle de l'entreprise.

Contrôle interactif : Type de contrôle où les différentes parties prenantes au contrôle participent à la réalisation des contrôles et à la consolidation des reporting y étant associés. Généralement, les contrôleurs travaillent en interaction forte avec les entités contrôlés, notamment dans la réalisation des plans d'actions correctrices.

Contrôle interne périodique : Type de contrôle au sein des établissements bancaires et d'assurance, généralement assumé par la fonction d'audit interne. Il s'agit de contrôler périodiquement (ponctuellement ou de manière périodique dans le cas d'un plan d'audit) une entité, un processus, une activité de l'organisation (aussi parfois appelé contrôle de troisième niveau)

Contrôle interne permanent : Type de contrôle réalisé par des entités avec récurrence dans le cadre d'un plan de contrôle généralement annuel (on parle également de contrôle de premier niveau et de second niveau, respectivement pour les contrôles réalisés par les entités opérationnels et pour ceux réalisés par la fonction de contrôle interne).

Coût d'opportunité (face au risque) : Il s'agit du rapport entre le fait d'investir ou non pour se couvrir face à un risque donné. Cela correspond à la question : est-il plus judicieux d'investir dans des moyens de protections/préventions face au risque ou de ne rien faire ? (Eu égard à la faible probabilité de survenance d'un risque). Pour certains risques, les plus graves, la question de l'occurrence ne se pose cependant pas en ces termes : l'entreprise cherchera à tout prix à éviter ce risque.

Crise : La notion de crise correspond au cas dans lequel un évènement de risque est survenu et affecte une organisation, la situation de crise est par définition urgente et appelle une réponse rapide du management de l'entreprise. A défaut d'autres risques peuvent survenir (effet d'escalade).

Criticité : Vraisemblance du risque, intensité plus ou moins grande du risque. (Produit de la probabilité par l'impact du risque (aussi appelée espérance).

Danger : Un danger se définit par la menace qu'il engendre pour un individu ou une organisation. Le danger remet en cause la pérennité d'une organisation, l'intégrité d'un individu. Le danger peut encore se définir comme *« tout phénomène, situation ou évènement potentiel dus à un ou plusieurs évènements déclencheurs susceptible de menacer une cible »*.

Destin : *destinare,* fixer.

Erreur de traitement et de saisi de l'information : Il s'agit de l'une des catégories de risques opérationnels telle que définie dans la réglementation baloise. Elle correspond à la catégorie la plus fréquente de risque opérationnel (mais aussi la moins coûteuse le plus souvent). Il peut s'agir d'erreurs dans le contrat, d'erreur dans la tarification d'un produit financier, d'erreur de saisie d'un montant d'un trader lors d'un ordre de vente ou d'achat, d'erreur de saisie d'un gestionnaire, d'un comptable etc. Ces erreurs constituent un risque par les coûts agrégés qu'elles impliquent pour l'entreprise. Elles ne sont généralement prises en compte que si elle dépasse un certain montant (plusieurs milliers d'euros dans les grandes entreprises).

Evènement : *evinere,* advenir, avoir lieu. *« Etre abstrait dont la seule caractéristique est de se produire ou de ne pas se produire »* (E.Borel).

Eventualité : *eventus,* évènement, résultat.

.

Filière risque : la filière risque correspond à l'ensemble des acteurs impliqué directement dans le processus de gestion des risques de l'entreprise. Elle comprend généralement les équipes centrales travaillant à temps plein sur la gestion des risques, les référents risques chargés du reporting et du suivi des risques par départements / entités, et des contributeurs risques étant des opérationnels et collaborateurs des fonctions supports. Ces contributeurs reportent directement aux référents risques sur les risques incidents qu'ils ont pu identifier dans leurs périmètres respectifs. La filière risque est généralement coordonnée/animée par le Risk Manager ou par les contrôleurs des risques.

Fonctions clés : Capacité administrative à accomplir des tâches, selon une liberté d'organisation laissée aux organismes d'assurance (service, direction, comité, équipe,…). Selon la directive cadre Solvabilité 2, il s'agit des fonctions de conformité, d'actuariat, de gestion des risques et d'audit interne. Les fonctions sont susceptibles d'être externalisées, pas les systèmes.

Fraude externe : Il s'agit des actes de malveillance volontaires réalisés par des personnes externes à une organisation, ayant pour but de nuit à la réputation de celle-ci ou de profiter indument de ses actifs. Les fraudes externes peuvent être l'objet de tiers (prestataires, fournisseurs, clients, autres tiers). Exemples : fraude d'un professionnel de santé à l'encontre d'une mutuelle, fraude d'un client à l'encontre de sa banque, fraude d'un hacker sur la banque en ligne d'un établissement de crédit.

Fraude interne : Il s'agit des actes de malveillance volontaires réalisés par un ou plusieurs collaborateurs d'une entreprise. Exemple : fraude d'un trader à l'encontre de sa banque de rattachement, fraude aux moyens de paiement d'un guichetier dans une agence bancaire, fraude d'un gestionnaire de contrats d'assurance se payant pour son propre compte de manière indue des prestations d'indemnisations.

Gestion globale des risques / Risk Management (ERM) : La gestion globale des risques est généralement définie comme un processus transversale de création de valeur visant à maîtrise les risques de l'entreprise. Certains travaux récents l'identifient davantage comme un moyen de sauvegarder la valeur de l'entreprise en réduisant les différentes vulnérabilités internes et en se préparant à faire face à d'éventuelles menaces externes. La gestion globale des risques vise à recenser et à anticiper les multiples risques auxquels peut faire face une organisation.

Hasard : Pour Antoine-Augustin Cournot, *(Essai sur les fondements)* le hasard consiste en la rencontre d'au minimum deux séries de phénomènes de causes et d'effets mutuellement indépendants concourant à produire un phénomène ou un évènement dont la raison ne se trouve pas dans la série elle-même.

Impact : Capacité maximum de destruction possible. Ensemble des conséquences d'un risque (financier, image, humain).

Incident : Un incident lié à un risque opérationnel peut se traduire par une perte financière principale à laquelle seront associées des pertes connexes qu'il sera aussi nécessaire d'identifier.

Incertitude : A la différence du risque, l'incertitude concerne les évènements dont la survenance n'est pas probabilisable. On parlera d'incertitude radicale lorsqu'il est impossible d'établir la liste des évènements possibles liés à un aléa. En situation d'incertitude on ne sait ni où, ni quand un évènement se produira. C'est l'exemple même de l'inondation centenaire. On sait qu'elle arrivera, mais l'on ne peut dire où et quand.

Indicateur d'appétence : Un indicateur permet de mesurer de façon objective un phénomène étudié. Un indicateur d'appétence consiste à mesurer le niveau de risque que l'entreprise souhaite prendre.

Indisponibilité SI : L'indisponibilité du système d'information constitue pour les établissements financiers, fortement basé sur l'informatique pour toute activité, un risque opérationnel essentiel à prendre en compte. Une indisponibilité prolongée peut avoir un réel impact financier (perte de client, surcoût, indemnisations etc.), des indisponibilités partielles sont peu impactantes sauf en cas de récurrence (journalière, survenance pendant les heures de fonctionnement des centres de relation client par exemple).

Invariant : Phénomène supposé permanent jusqu'à l'horizon étudié. (Exemple : caractéristique climatique

Irréversibilité : Décision prise, évènements, tels que l'on ne peut plus faire marche arrière.

Maîtrise : Evaluation des moyens mis en œuvre pour le traitement d'un risque.

Menace : Du latin *minacia, minae,* se définit comme l'acte ou le propos démontrant une volonté de faire du mal.

Opportunité : Transformation d'un risque en évènement positif.

Organisation : Ensemble de moyens (humains, techniques, financiers…) regroupés au sein d'une même structure où circule l'information en vue de répondre à des besoins et attentes spécifiques.

Passivité : Qui subit le changement.

Politique de maîtrise des risques opérationnels : La politique de maîtrise des risques d'une organisation définit les risques acceptés par l'entreprise et les risques non acceptés par cette dernière. Pour les risques acceptés elle pose des limites à ne pas franchir (quantitatives et/ou qualitatives). Pour les risques non acceptés elle définit les moyens à mettre en œuvre pour réduire/éviter/transférer ainsi que les rôles et responsabilités au sein de l'organisation en vue de répondre à un risque donné. La politique de maîtrise des risques clarifie généralement le profil de risque de l'entreprise (niveau d'acceptation du risque et niveau de tolérance au risque).

Politique de maîtrise des risques : Au sein des établissements financiers, en plus des politiques dédiées aux risques financiers, on distingue fréquemment des politiques dédiées à la maîtrise des risques opérationnels. Ces politiques remplissent le même rôle qu'une politique de maîtrise des risques, en distinguant toutefois les moyens, acteurs, rôles et responsabilités selon les catégories de risques opérationnels.

Préactivite : Qui se prépare au changement prévisible, par la prévention.

Prévision : Estimation assorti d'un degré de confiance.

Priorisation des risques : Il s'agit de l'arbitrage opéré par une organisation face à ses principaux risques. En présence de moyens limités, une entreprise se concentre sur ses risques majeurs. Après identification et évaluation des conséquences d'un risque, l'entreprise définit les risques à piloter en priorité.

Proactivité : Qui agit pour provoquer les changements souhaités.

Probabilité : La probabilité d'un évènement est le rapport du nombre d'évènements favorables sur le nombre d'évènements possibles. (Jérôme Cardan, *Livre sur les jeux de chance.*) Du latin *probabilis* : digne d'approbation. La probabilité d'occurrence est la capacité d'un risque à survenir.

Procédure : Une procédure est un descriptif d'un ensemble d'action à réaliser sur une activité donné, comprenant la répartition des rôles et des acteurs concernés. La procédure répond à la question du (qui fait quoi ? Où ? Quand ?). Les procédures sont généralement rattachées à des processus et peuvent également se décliner de manière plus granulaire via des modes opératoires (la question du comment faire ?).

Processus : Succession d'activités interconnectées qui utilisent des ressources (hommes, matériel, …) pour transformer des éléments d'entrée en éléments de sortie, avec en résultat attendu un produit ou un service. Un processus présuppose une valeur ajoutée, un caractère récurrent (par opposition au projet) et transversal**.**

Profil de risque : Le profil de risque consiste à mesurer le niveau d'exposition au risque de l'organisme par branche, par classe de risque ou encore, par structure. Le profil de risque doit

permettre une mesure de l'exposition aux risques de l'organisme à un niveau agrégé et à un niveau détaillé.

Prospective : Anticipation pour éclairer l'action. *Indiscipline intellectuelle* (P.Massé).

Réactivité : Qui attend la survenance d'un évènement pour agir.

Résilience : Art de rebondir pour un individu ou une organisation suite à un évènement traumatisant/ aux conséquences dommageables.

Responsabilité : La responsabilité correspond au fait de rendre des comptes pour un acteur donné sur des actions ou faits ayant eu lieu sur son périmètre de responsabilité.

Risque : De l'italien *risco, « est un danger, un inconvénient, un sinistre éventuel plus ou moins probable auquel on est exposé »* (source : Le Petit Larousse)
Le risque est donc l'ensemble des évènements possibles et leurs probabilités associées. Le risque n'est pas toujours probabilisable. Toutefois, la faculté de probabiliser fait la différence entre risque et incertitude pour Frank Knight *(Risk, Uncertainty and Profit*, 1921*)* : Une situation de choix en avenir incertain est une situation de risque lorsqu'il est possible d'associer à chaque stratégie une distribution de probabilités de résultats. Evènements à l'arrivée aléatoire susceptibles de causer un dommage aux personnes ou aux biens.

Risques opérationnels : Le risque de perte résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs.
Il s'agit des risques le plus souvent internes à l'organisation ou en lien avec celle-ci tels que la fraude interne ou externe, l'indisponibilité du SI, les erreurs de traitement et de saisie de l'information, les failles dans la sécurité informatique ou dans le dispositif de sécurité-sûreté des biens et des personnes.

Roue du risque : La roue du risque consiste en une approche itérative (inspirée du modèle PDCA) se déclinant en quatre phases que sont l'identification des risques, l'évaluation des risques, le traitement puis le suivi des risques.

Système : Ensemble d'éléments connectés, en interaction, participant à une même finalité.
Tolérance au risque :

Vraisemblable : D'origine évidente.

Annexes

Annexe 1-Validation des hypothèses au travers des résultats de recherche

Hypothèse non validée □
Hypothèse partiellement validée ◪
Hypothèse entièrement validée ■

Code hypothèse	Hypothèses descriptives	Hypothèses explicatives	Hypothèses prescriptives	Chapitres correspondant
H1	■ Les processus d'institutionnalisation et de tétra normalisation permettent une marge de manœuvre réglementaire	■ Même dans les secteurs réglementés tels que les secteurs bancaire ou assurantiel, l'inflation normative contribue à créer des confusions voire des conflits de normes de telle sorte qu'il existe une marge non négligeable d'interprétation de la réglementation prudentielle.	■ Il existe certains acteurs clés (Risk Manager notamment) dans l'organisation dont le rôle est de permettre une lecture et une traduction commune de la réglementation prudentielle 'risque opérationnel'. Ce rôle doit être un rôle d'influence et non de coercition.	Chapitres 2, 3, 4, 5
H2	■ Les risques opérationnels sont des risques subis, diffus et mal compris. Ils sont sources de défiance dans l'organisation.	■ Leurs normes de contrôle et de gestion sont sources de confusions, ils se gèrent par la négative, par la recherche des dysfonctionnements et des sources de défiance.	■ Le passage du négatif au positif dans la gestion des risques opérationnel suppose un management actif par des acteurs clés dédiés. Ces derniers permettent de renforcer la confiance dans	Chapitres 2, 5, 6

			l'organisation.	
H3	◪ La création de valeur associée à la gestion du risque opérationnel se situe dans la réponse à ces dysfonctionnements.	◪ La création de valeur dans le cas du risque opérationnel est davantage une « sauvegarde de la valeur » qu'une création nette de valeur.	□ L'analyse de la valeur concernant les démarches de gestion du risque opérationnel doit à la fois reposer sur des approches qualitatives (valeur organisationnelle) et quantitatives (économie de fonds propres et maîtrise des coûts)	Chapitre 6
H4	◪ Les risques opérationnels sont principalement des coûts et performances cachés pour les institutions financières	◪ Les coûts-performances cachés 'risques opérationnels' sont une catégorie issues de difficultés de dénombrement (quantitatif) mais aussi de discernement dans l'organisation (qualitatif).	◪ La gestion du risque opérationnel doit s'inscrire dans le passage d'une démarche conformiste à une logique d'intelligence du risque (démarche cohérente et apprenante).	Chapitres 5, 6
H5	■ Les politiques de maîtrise des risques opérationnels se structurent autour de plusieurs fonctions et dispositifs dédiés en totalité ou partiellement dont les attributions divergent mais pour lesquels il existe un objectif commun 'risque opérationnel'.	■ L'effectivité d'une politique de maîtrise des risques opérationnels est liée à la capacité des acteurs à comprendre et à se mobiliser autour de l'enjeu 'risque opérationnel' tout en tenant compte de leur lecture spécifique de cet enjeu.	■ Les politiques de maîtrise des risques opérationnels nécessitent une approche intégrée et un management actif des différentes fonctions de contrôle (Audit, Contrôle Interne, Conformité, Risk Management…) pour être effectives.	Chapitre 3, 5, 6

Annexe 2-Evènements de risque opérationnel, extraits de la base de données ORX

Tableau a. Pertes liées au risque opérationnel, classement des montants de pertes moyennes par ligne d'activité

Type d'activité	Perte moyenne par évènement de risque opérationnel majeur	Rang
Corporate Finance	1 865 106 €	1
Trading and Sales	810 031 €	2
Asset Management	720 984 €	3
Commercial Banking	454 252 €	4
Private Banking	343 414 €	5
Retail Brokerage	299 649 €	6
Agency Services	235 366 €	7
Clearing	219 855 €	8
Retail Banking	210 558 €	9

Source: 2012 ORX Report on Operational Risk Loss Data

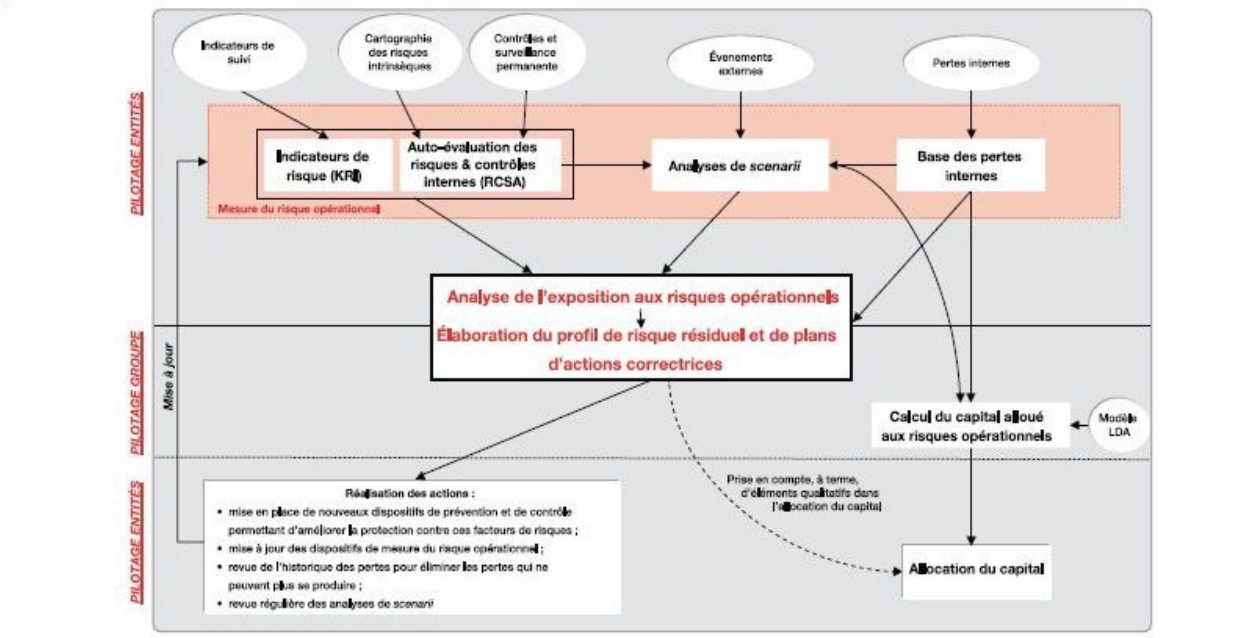
Tableau b. Pertes liées au risque opérationnel, classement des montants de pertes pour 100 euros de revenu brut par activité.

Type d'activité	Perte brute liée au risque opérationnel pour 100 euros de revenus bruts	Rang
Trading and Sales	3,04 €	1
Private Banking	2,24 €	2
Asset Management	2,03 €	3
Retail Brokerage	1,88 €	4
Corporate Finance	1,74 €	5
Agency Services	1,67 €	6
Retail Banking	1,31 €	7
Commercial Banking	1,24 €	8
Clearing	0,65 €	9

Source: 2012 ORX Report on Operational Risk Loss Data

Annexe 3-Exemples de dispositifs de contrôles relatifs aux risques opérationnels

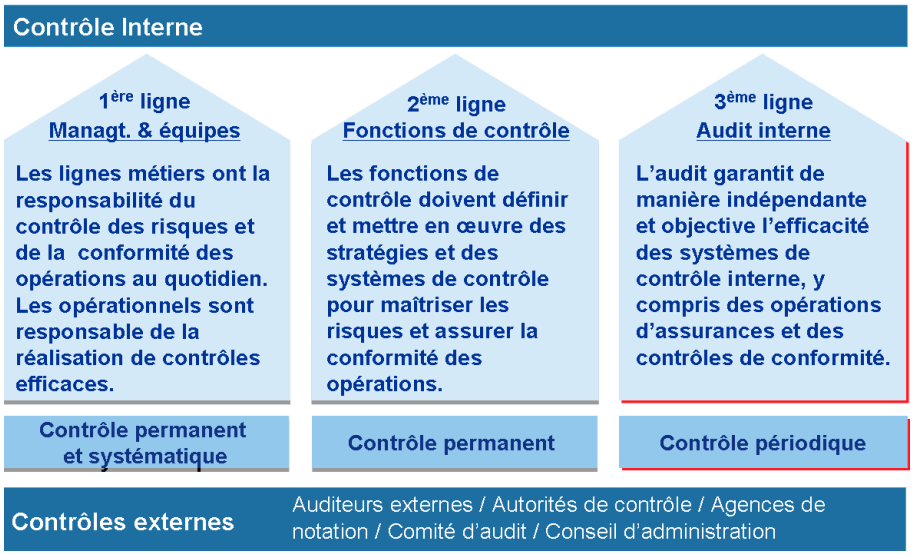
-Exemple en banque de détail, le cas de Société Générale (extrait du document de référence 2013)



La classification par Société Générale des risques opérationnels en huit catégories d'événements et quarante-neuf sous-catégories mutuellement exclusives est la pierre angulaire de sa modélisation des risques. Elle garantit la cohérence d'ensemble du dispositif et permet de réaliser des analyses transversales.

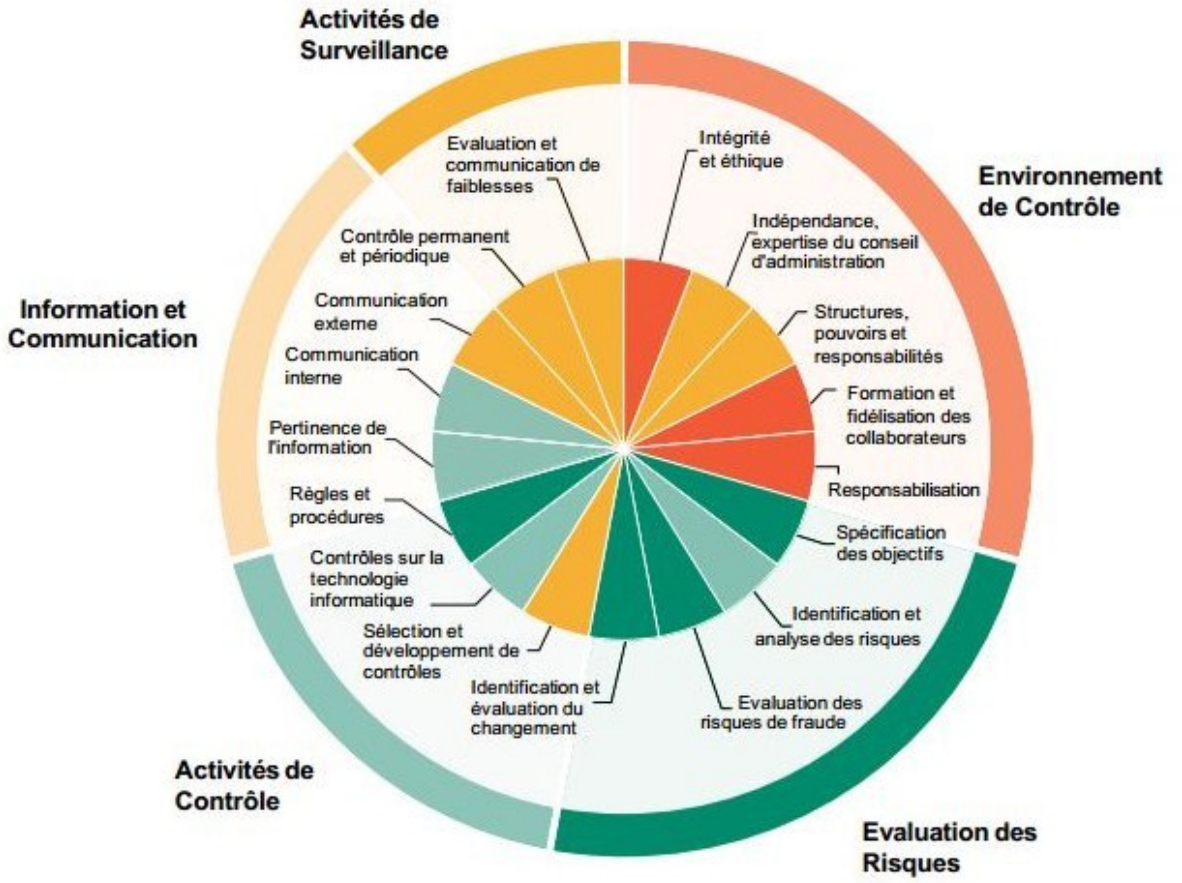
Litiges commerciaux	Fraude et autres activités criminelles
Litiges avec les autorités	Activités non autorisées sur les marchés (*Rogue trading*)
Erreurs de tarification (« *pricing* ») ou d'évaluation du risque	Perte de moyens d'exploitation
Erreurs d'exécution	Défaillance des systèmes d'information

-Exemple en assurance, le cas d'Axa (Extrait du document de référence 2011 et de documentation collaborateur)



Annexe 4 - « Coso 2013 »

Extrait du référentiel Coso 2013-PWC.



Annexe 5 - Exemples de risques opérationnels-Comité de Bâle, 2003, p.2.

Fraude interne *:* par exemple, informations inexactes sur les positions, vol commis par un employé et délit d'initié d'un employé opérant pour son propre compte.

Fraude externe *:* par exemple, hold-up, faux en écriture, chèques de cavalerie et dommages dus au piratage informatique.

Pratiques en matière d'emploi et sécurité sur le lieu de travail *:* par exemple, demandes d'indemnisation de travailleurs, violation des règles de santé et de sécurité des employés, activités syndicales, plaintes pour discrimination et responsabilité civile en général.

Pratiques concernant les clients, les produits et l'activité commerciale *:* par exemple, violation de l'obligation fiduciaire, utilisation frauduleuse d'informations confidentielles sur la clientèle, opérations boursières malhonnêtes pour le compte de la banque, blanchiment d'argent et vente de produits non autorisés.

Dommages aux biens physiques *:* par exemple, actes de terrorisme, vandalisme, séismes, incendies et inondations.

Interruption d'activité et pannes de systèmes *:* par exemple, pannes de matériel et de logiciel informatiques, problèmes de télécommunications et pannes d'électricité.

Exécution des opérations, livraisons et processus *:* par exemple, erreur d'enregistrement des données, défaillances dans la gestion des sûretés, lacunes dans la documentation juridique, erreur d'accès aux comptes de la clientèle et défaillances des fournisseurs ou conflits avec eux.

Annexe 6 – Principes de gestion du risque opérationnel, Comité de Bâle, 2003, p.3-4.

Élaboration d'un environnement adéquat pour la gestion du risque

Principe 1 – Le conseil d'administration devrait considérer les principaux aspects du risque opérationnel de la banque comme une catégorie distincte de risque à gérer, et il devrait approuver et réexaminer périodiquement le dispositif de gestion de ce risque. Ce dispositif devrait fournir une définition du risque opérationnel valable pour la banque tout entière et poser les principes servant à identifier, évaluer, suivre et maîtriser/atténuer ce risque.

Principe 2 – Le conseil d'administration devrait garantir que le dispositif de gestion du risque opérationnel de la banque est soumis à un audit interne efficace et complet, effectué par un personnel fonctionnellement indépendant, doté d'une formation appropriée et compétent. La fonction d'audit interne ne devrait pas être directement responsable de la gestion du risque opérationnel.

Principe 3 – La direction générale devrait avoir pour mission de mettre en œuvre le dispositif de gestion du risque opérationnel approuvé par le conseil d'administration. Ce dispositif devrait être appliqué de façon cohérente dans l'ensemble de l'organisation bancaire, et les membres du personnel, à tous les niveaux, devraient bien comprendre leurs responsabilités dans la gestion du risque opérationnel. La direction générale devrait aussi être chargée d'élaborer des politiques, processus et procédures de gestion du risque opérationnel pour tous les produits, activités, processus et systèmes importants.

Gestion du risque : identification, évaluation, suivi et maîtrise/atténuation du risque

Principe 4 – Les banques devraient identifier et évaluer le risque opérationnel inhérent à tous les produits, activités, processus et systèmes importants. Elles devraient aussi, avant de lancer ou d'exploiter des produits, activités, processus et systèmes nouveaux, soumettre à une procédure adéquate d'évaluation le risque opérationnel qui leur est inhérent.

Principe 5 – Les banques devraient mettre en œuvre un processus de suivi régulier des profils de risque opérationnel et des expositions importantes à des pertes. Les informations utiles à une gestion dynamique du risque opérationnel devraient être régulièrement communiquées à la direction générale et au conseil d'administration.

Principe 6 – Les banques devraient adopter des politiques, processus et procédures pour maîtriser et/ou atténuer les sources importantes de risque opérationnel. Elles devraient réexaminer périodiquement leurs stratégies de limitation et de maîtrise du risque et ajuster leur profil de risque opérationnel en conséquence par l'utilisation de stratégies appropriées, compte tenu de leur appétit pour le risque et de leur profil de risque globaux.

Principe 7 – Les banques devraient mettre en place des plans de secours et de continuité d'exploitation pour garantir un fonctionnement sans interruption et limiter les pertes en cas de perturbation grave de l'activité.

Rôle des superviseurs

Principe 8 – Les autorités de contrôle bancaire devraient exiger que toutes les banques, quelle que soit leur taille, aient mis en place un dispositif efficace pour identifier, évaluer, suivre et maîtriser/atténuer les risques opérationnels importants, dans le cadre d'une approche globale de la gestion du risque.

Principe 9 – Les superviseurs devraient procéder régulièrement, de manière directe ou indirecte, à une évaluation indépendante des politiques, procédures et pratiques des banques en matière de risque opérationnel. Les superviseurs devraient veiller à ce qu'il existe des mécanismes appropriés leur permettant de se tenir informés de l'évolution dans les banques.

Rôle de la communication financière

Principe 10 – La communication financière des banques devrait être suffisamment étoffée pour permettre aux intervenants du marché d'évaluer leur méthodologie de gestion du risque opérationnel.

Annexe 7 -Correspondance des enjeux de tétranormalisation et des catégories de risque opérationnel

(adaptation d'après Savall & Zardet, 2005b)

Risque opérationnel			**Tétranormalisation**	
Catégories de risque opérationnel de niveau 1	**niveau 2**		**niveau 2**	**Problèmes liés à la tétranormalisation niveau 1**
Clients, produits et pratiques commerciales	-Conformité (lois, règlements, normes) -Défaut de production -Service conseil -Pratiques commerciales incorrectes		-Public / privé (idéologie et choix politiques) -Normes IFRS -Dilemmes entre normé et non normé	Production et prolifération de normes
Dommages aux actifs corporels	-Catastrophes et autres sinistres		-Normes de conformité -Normes émanant des instituts, agences de notation	Prolifération de standards organisationnels et de normes de marché
Dysfonctionnement de l'activité des systèmes	-Sécurité des systèmes		-Concentration des firmes -Contradiction des normes, politiques, économiques, techniques	Conflits/concurrence de normes
Exécution, livraison et gestion des processus	-Admission et documentation clientèle -Contreparties commerciales -Fournisseurs -Saisi, exécution et livraison des transactions -Surveillance et notification financière		-Territorialité -Conflits de normes publiques / privées	Conflits de hiérarchisation des normes
Fraude externe	-Vol et fraude		-Escroqueries -Influence politique -Respect de la propriété intellectuelle -Corruption -Pratiques de fraude	Fraude
Fraude interne	-Activité non autorisée		-Sûreté -Droit du travail -Audit comptable -Pratiques réglementaires et légales -Applications du droit social	Enjeux d'application de la norme
Pratiques en matière d'emploi et sécurité sur le lieu de travail	-Egalité et discrimination -Relations de travail -Sécurité du lieu de travail		-Taxes, fiscalité -Applications des sanctions et amendes -Ressources disponibles	Sanctions financières et pénales

Annexe 8 – Détails des entretiens confirmatoires réalisés

Entretiens	Code entretien	Renseignements personnels	Entreprise	Durée de l'entretien	Date de réalisation
Consultant sénior	EC-1	55 ans, femme, expérimentée	Cabinet de conseil spécialisé gouvernance des risques	1 heure	Juillet 2012
Consultant sénior	EC-2	48 ans, homme, expérimenté	Cabinet de conseil en Risk Management	1 heure	Juillet 2012
Directeur d'audit interne	EC-3	45 ans, Homme, expérimenté	Institut de prévoyance	1 heure	Septembre 2012
Directeur des risques	EC-4	56 ans, Homme, expérimenté	Société d'assurance généraliste	1 heure 10 minutes	Septembre 2012
Directeur d'audit interne	EC-5	40 ans, Femme, expérimentée	Mutuelle d'assurance	1 heure	Septembre 2012
Consultant senior, associé cabinet	EC-6	48 ans, Homme, expérimenté	Cabinet de conseil en contrôle et risque	2 heures	Septembre 2012
Directeur des risques	EC-7	57 ans, Homme, expérimenté	Société de réassurance	1 heure	Septembre 2012
Consultant expert risque	EC-8	53 ans, Homme, expérimenté	Consultant indépendant	1 heure 15 minutes	Octobre 2012
Responsable risques opérationnels: cartographie et scoring	EC-9	40 ans, Homme, expérimenté	Banque de détail	1 heure	Octobre 2012
Responsable du contrôle interne	EC-10	52 ans, Homme, confirmé	Banque de détail	1 heure 15 minutes	Octobre 2012
Directeur des risques opérationnels	EC-11	35 ans, Homme, confirmé	Société d'assurance de dimension internationale	1 heure	Novembre 2012
Directeur de la conformité	EC-12	58 ans, Homme, expérimenté	Banque de détail	1 heure	Novembre 2012
Directeur d'audit interne	EC-13	46 ans, Homme, confirmé	Société d'assurance généraliste	1 heure	Novembre 2012
Directeur des risques	EC-14	53 ans, Homme, expérimenté	Société d'assurance généraliste	1 heure	Novembre 2012
Directeur des risques	EC-15	55 ans, Homme, confirmé	Filiale bancaire, société	1 heure 30 minutes	Novembre 2012

			d'assurance		
Responsable Veille et réglementation prudentielle risque opérationnel	EC-16	40 ans, Homme, confirmé	Banque de détail	1 heure 30 minutes	Décembre 2012
Risk Manager, en charge des risques psychosociaux	EC-17	44 ans, Homme, confirmé	Banque de détail	1 heure	Décembre 2012
Contrôleur interne, en charge de l'approche gestion des risques	EC-18	43 ans, Femme, confirmée	Société d'assurance généraliste	1 heure 20 minutes	Décembre 2012
Directrice des risques opérationnels	EC-19	46 ans, Femme, expérimentée	Banque de détail	1 heure	Décembre 2012
Risk Manager, responsable du contrôle de gestion risques opérationnels	EC-20	36 ans, Homme, confirmé	Banque de détail	1 heure	Décembre 2012
Responsable du contrôle interne et des risques opérationnels	EC-21	48 ans, Femme, expérimentée	Société d'assurance généraliste	1 heure 15 minutes	Décembre 2012
Risk Manager, réseau de distribution, banque de détail	EC-22	46 ans, Homme, confirmé	Banque de détail	1 heure 30 minutes	Janvier 2013
Consultant sénior	EC-23	47 ans, Homme, expérimenté	Cabinet de conseil spécialisé en gestion des risques	2 heures	Janvier 2013
Directeur de l'organisation	EC-24	60 ans, Homme, expérimenté	Banque de détail	1 heure 15 minutes	Janvier 2013
Directeur des risques opérationnels et conformité	EC-25	54 ans, Homme, expérimenté	Banque de dimension internationale	1 heure	Janvier 2013
Directeur de la sécurité financière	EC-26	52 ans, Homme, expérimenté	Banque de détail	1 heure	Janvier 2013
Directeur	EC-27	49 ans, Homme,	Société	1 heure	Janvier

d'audit interne		confirmé	d'assurance régionale		2013
Directeur du contrôle interne	EC-28	44 ans, Homme, confirmé	Société d'assurance régionale	1 heure	Janvier 2013
Responsable plan de continuité des activités	EC-29	41 ans, Homme, confirmé	Société d'assurance régionale	1 heure 10 minutes	Janvier 2013
Consultant sénior	EC-30	51 ans, Homme, expérimenté	Consultant indépendant	1 heure	Février 2013
Directeur d'audit interne	EC-31	42 ans, Homme, confirmé	Société d'assurance internationale	1 heure	Février 2013
Directeur des risques opérationnels	EC-32	47 ans, Homme, expérimenté	Banque d'investissement	1 heure	Février 2013
Directeur d'audit interne	EC-33	35 ans, Homme, confirmé	Banque d'investissement	1 heure 15 minutes	Janvier 2013
Directeur du contrôle interne	EC-34	34 ans, Homme, confirmé	Société d'assurance internationale	2 heures	Février 2013
Consultant risque informatique	EC-35	33 ans, Homme, confirmé	Banque de dimension internationale	1 heure 30 minutes	Février 2013
Risk Manager	EC-36	48 ans, Homme, expérimenté	Consultant indépendant	1 heure	Février 2013
Directeur des risques opérationnels	EC-37	49 ans, Femme, expérimentée	Banque de détail	1 heure 30 minutes	Février 2013
Responsable du contrôle interne	EC-38	47 ans, Femme, expérimentée	Mutuelle d'assurance	1 heure 30 minutes	Février 2013
Directeur des risques opérationnels	EC-39	51 ans, Femme, expérimentée	Banque de détail régionale	2 heures	Février 2013
Directeur des risques	EC-40	45 ans, Homme, confirmé	Mutuelle d'assurance	1 heure	Mars 2013
Directeur des risques opérationnels	EC-41	45 ans, Homme, confirmé	Société d'assurance	1 heure	Mars 2013
Directeur du contrôle interne	EC-42	46 ans, Femme, confirmée	Société d'assurance généraliste	1 heure	Mars 2013
Directeur de l'audit interne	EC-43	52 ans, Femme, expérimentée	Banque de détail	1 heure 30 minutes	Mars 2013
Analyste risques	EC-44	32 ans, Homme, confirmé	Autorité de tutelle, régulateur	1 heure	Mars 2013
Contrôleur	EC-45	40 ans, Homme,	Autorité de	1 heure	Mars 2013

contrats et risques		confirmé	tutelle, régulateur		
Contrôleur des assurances	EC-46	30 ans, Femme, novice	Autorité de tutelle, régulateur	1 heure	Mars 2013
Responsable contrôle juridique et conformité	EC-47	52 ans, Femme, expérimentée	Autorité de tutelle, régulateur	1 heure	Mars 2013
Directeur des risques opérationnels	EC-48	48 ans, Homme, expérimenté	Banque d'investissement	1 heure	Avril 2013
Responsable du contrôle interne, périmètre informatique	EC-49	37 ans, Homme, confirmé	Banque de détail	1 heure	Avril 2013
Risk Manager	EC-50	44 ans, Homme, confirmé	Banque de détail	1 heure	Avril 2013
Directeur des risques opérationnels	EC-51	38 ans, Femme, confirmée	Banque de détail internationale	1 heure	Avril 2013
Contrôleur bancaire	EC-52	51 ans, Femme, confirmée	Autorité de tutelle, régulateur	1 heure	Mai 2013
Contrôleur bancaire	EC-53	27 ans, Femme, novice	Autorité de tutelle, régulateur	1 heure	Mai 2013
Contrôleur bancaire	EC-54	37 ans, Femme, confirmée	Autorité de tutelle, régulateur	1 heure	Mai 2013
Contrôleur bancaire	EC-55	25 ans, Homme, novice	Autorité de tutelle, régulateur	1 heure	Mai 2013

Total : 63 heures 25 minutes

Annexe 9-1 Exemple de référentiel de risques opérationnels, Société d'assurance C1

Catégorie de risque (niveau 1)	Sous catégorie de risque (niveau 2)	Code Evénement de Risque	Evénement de risque générique (niveau 3)
Fraude interne Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'enfreintes à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne	Activité non autorisée	FI1	Dissimulation volontaire de position
		FI2	Transactions intentionnellement non notifiées
		FI3	Abus de pouvoir, activité intentionnelle non autorisée
	Vol et fraude (interne)	FI4	Autres fraudes internes
		FI5	Vol / détournement de fonds
		FI6	Vol / détournement de biens
		FI7	Contrefaçon de documents
		FI8	Usurpation de compte / d'identité
		FI9	Fausses déclarations intentionnelles
		FI10	Fraude fiscale / évasion délibérée
		FI11	Non-respect des règles en matière d'opérations financières personnelles / délits d'initiés
		FI12	Non respect des règles déontologiques relatives aux cadeaux et aux invitations (reçus et donnés)
	Sécurité des systèmes (fraude interne)	FI13	Malveillance informatique (virus, destruction de fichiers, piratages...)
		FI14	Vol et divulgation de données
Fraude externe Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'enfreintes à la législation ou aux règles par une tierce partie	Vol et fraude (externe)	FE1	Fausses déclarations intentionnelles
		FE2	Contrefaçon de documents
		FE3	Vol
		FE4	Autres fraudes externes
		FE5	Usurpation de compte / d'identité
	Sécurité des systèmes (fraude externe)	FE6	Malveillance informatique (virus, destruction de fichiers, piratages...)
		FE7	Vol et divulgation de données
Pratiques en matière d'emploi et sécurité sur le lieu de travail Pertes resultant d'actes incompatibles au regard de la loi en matière d'emploi, de législation relative à la santé ou à la sécurité , du paiement d'indemnités ou de discrimination sociale	Sécurité du lieu de travail	PE1	Non respect des règles de santé et de sécurité sur le lieu de travail => accidents du travail/maladies professionnelles
		PE2	Responsabilité civile => accidents de tiers (clients, partenaires, fournisseurs, autres…)
	Relations de travail	PE3	Grève, contestation syndicale
		PE4	Litiges avec les employés / indemnisation du personnel
	Egalité et discrimination	PE5	Comportement impropre : discrimination / harcèlement
	Gestion des ressources humaines	PE6	Recrutements inadaptés
		PE7	Formation inadaptée
		PE8	Gestion des emplois et des compétences inadaptée
		PE9	Politique salariale inadaptée
		PE10	Inadaptation de la politique de rémunération variable et d'évaluation annuelle des collaborateurs
		PE11	Turnover excessif
		PE12	Départ/absence d'une ressource clé
		PE13	Non respect des dispositions relatives à la protection de la vie privée des collaborateurs
		PE14	Non respect de la réglementation sociale (code du travail, conventions collectives...)
		PE15	Autres problèmes liés à la gestion des ressources humaines
Clients / Tiers, produits et pratiques commerciales Pertes resultant d'un acte non intentionnel ou d'une négligence dans l'exercice d'une obligation professionnelle face au client (incluant les exigences en matière fiduciaire et de conformité) ou pertes résultant de la nature ou de la conception d'un produit.	Conformité, diffusion d'informations et devoir fiduciaire	C1	Non respect de la réglementation applicable à l'acte commercial (ex : DDAC, MIFID...)
		C2	Non respect des règles relatives aux informations privilégiées et au secret professionnel
		C3	Non respect des dispositions relatives à la protection des données personnelles des clients (ex:CNIL)
		C4	Utilisation abusive d'informations confidentielles
		C5	Pratiques de ventes agressives
	Pratiques commerciales / de place incorrectes	C6	Infraction à la législation sur la concurrence
		C7	Défaut d'agrément réglementaire
		C8	Non respect des réglementations relatives au blanchiment et aux obligations s'y rapportant (TRACFIN)
		C9	Non respect des règles de fonctionnement des marchés financiers (déclarations en matière d'opérations suspectes, principe de l'intégrité du marché)
		C10	Non respect des règles de " meilleure exécution " des ordres
		C11	Non respect des règles liées à la " ségrégation des avoirs des clients "
		C12	Conflits d'intérêts entre deux ou plusieurs clients concernés par une même opération
		C13	Non respect de l'égalité de traitement des clients
		C14	Non respect du principe de primauté de l'intérêt du client
		C15	Non respect des dispositifs de " muraille de Chine " et non application des procédures
		C16	Franchissement de seuil et seuils de détention non déclarés
	Défauts dans les produits	C17	Mauvaise implémentation des modèles (modules de tarification, pricers, ...)
		C18	Non respect de la politique de tarification
		C19	Non conformité des produits
		C20	Non respect de la procédure de validation des nouveaux produits et nouvelles activités
		C21	Non respect des procédures relatives aux opérations complexes et sensibles
	Risques juridiques	C22	Contractualisation insuffisante (clauses protégeant insuffisamment l'entreprise)
		C23	Risques juridiques et de mise en cause

Dommages aux actifs corporels **Pertes résultant de la perte ou du dommage sur un actif corporel à la suite d'une catastrophe naturelle ou d'un autre sinistre**	**Catastrophes et autres sinistres**	DAC1	Catastrophes naturelles et industrielles
		DAC2	Autres dommages causés aux actifs corporels
		DAC3	Destruction malveillante de biens / vandalisme
		DAC4	Litiges liés aux immeubles et infrastructure
		DAC5	Autres causes liées à l'indisponibilité des immeubles et infrastructures
Dysfonctionnements de l'activité et des systèmes **Pertes résultant d'interruptions de l'activité ou de dysfonctionnement des systèmes**	**Systèmes**	DAS1	Perte ou altération irrémédiable de données informatiques (accidentelle)
		DAS2	Erreurs de développement
		DAS3	Atteinte involontaire à la sécurité logique
		DAS4	Inadéquation de ressources informatiques
		DAS5	Panne système, insuffisance, indisponibilité passagère de ressources informatiques
		DAS6	Autres causes d'origine technologiques (à préciser)
		DAS7	Défaillance ou indisponibilité d'une ressource (énergie, télécommunication, transport)
Exécution, livraison et gestion des processus **Pertes résultant d'un problème dans le traitement d'une transaction ou dans la gestion des processus ou pertes subies avec les contreparties commerciales et les fournisseurs**	**Saisie, exécution et suivi des transactions**	E1	Erreurs dans la saisie, le suivi ou le chargement des données
		E2	Non respect ou mauvaise interprétation des procédures
		E3	Déficiences dans l'organisation et les procédures internes de traitement ou de contrôle
		E4	Problèmes dus à l'inadéquation des systèmes d'information aux activités et produits
		E5	Mauvaise gestion des référentiels
		E6	Erreur de manipulation ou de paramétrage d'un modèle / système
		E7	Erreur d'affectation comptable (compte, entité…)
		E8	Défaut de preuve (archivage, traçabilité) / piste d'audit (SOX)
		E9	Problèmes de communication
		E10	Non respect des délais et/ou des obligations envers les clients et/ou les fournisseurs
		E11	Insuffisance de surveillance des comptes et/ou des opérations
		E12	Défaillance dans le traitement des réclamations
		E13	Autres causes liées aux traitements et procédures (à préciser)
	Communication externe	E14	Inexactitude d'informations communiquées à l'extérieur (occasionnant des pertes)
		E15	Manquement à une obligation déclarative (comptable ou réglementaire)
	Documents contractuels clients	E16	Documents contractuels imprécis, inadéquats ou manquants
		E17	Défaillance dans la collecte et la conservation des dossiers et des documents relatifs aux clients
	Gestion des comptes clients	E18	Non sécurisation des accès aux comptes clients
		E19	Données erronnées communiquées aux clients
	Fournisseurs	E20	Mauvaise exécution des prestations
		E21	Absence de dispositions contractuelles encadrant les obligations et les engagements pris en matière de performance par les sous-traitants
		E22	Litiges avec les fournisseurs

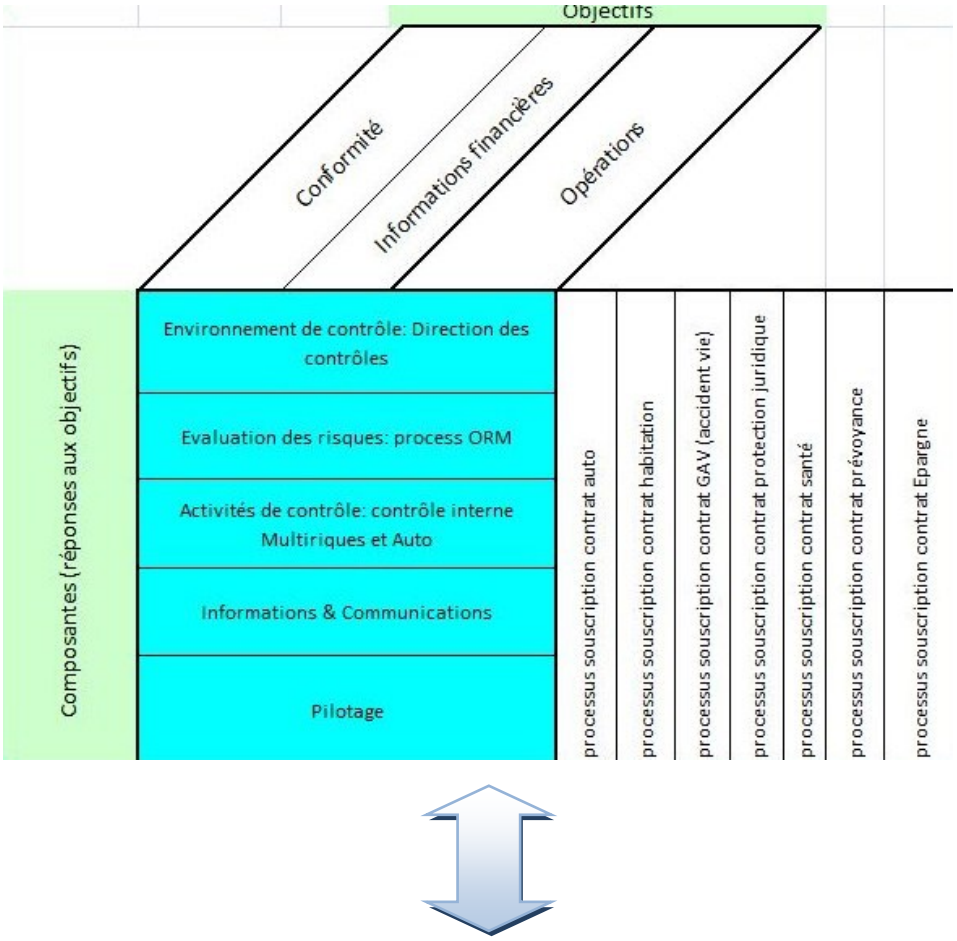
Annexe 9-2 Matrice d'évaluation des risques de la société d'assurance C1 – Exemple relatif à la fraude à l'assurance (fraude interne / externe)

		Vulnérabilité		Fréquence		Sévérité	Contrôle	
Typologie des risques	Evènement de risque	Vulnérabilité (O/N)	Incidents avérés (O/N)	Estimation de la fréquence de survenance moyenne (rating 1 à 5)	Evolution attendue de la fréquence estimée en N+1 (O/N)	Estimation de la sévérité moyenne (rating 1 à 5)	Niveau de contrôle (1 à 4)	Plan d'action initié (O/N)
Fraude externe	Fausses déclarations intentionnelles							
	Contrefaçon de documents							
	Vol							
	Autres fraudes externes							
	Usurpation de compte / d'identité							
	Malveillance informatique (virus, destruction de							
	Vol et divulgation de données							
Fraude interne	Dissimulation volontaire de position							
	Transactions intentionnellement non notifiées							
	Abus de pouvoir, activité intentionnelle non							
	Autres fraudes internes							
	Vol / détournement de fonds							
	Vol / détournement de biens							
	Contrefaçon de documents							
	Usurpation de compte / d'identité							
	Fausses déclarations intentionnelles							
	Fraude fiscale / évasion délibérée							
	Non respect des règles en matière d'opérations							
	Non respect des règles déontologiques relatives							
	Malveillance informatique (virus, destruction de							
	Vol et divulgation de données							

Exemple relatif au respect des obligations en matière de pratiques commerciales

		Vulnérabilité		Fréquence		Sévérité	Contrôle	
Typologie des risques	Evènement de risque	Vulnérabilité (O/N)	Incidents avérés (O/N)	Estimation de la fréquence de survenance moyenne (rating 1 à 5)	Evolution attendue de la fréquence estimée en N+1 (O/N)	Estimation de la sévérité moyenne (rating 1 à 5)	Niveau de contrôle (1 à 4)	Plan d'action initié (O/N)
Exécution, Livraison et gestion des processus	Erreurs dans la saisie, le suivi ou le chargement	OUI	NON	Very Low	NON	Very Low	Good	NON
	Non respect ou mauvaise interprétation des	OUI	NON	Very Low	NON	Very Low	Good	NON
	Déficiences dans l'organisation et les	NON						
	Problèmes dus à l'inadéquation des systèmes							
	Mauvaise gestion des référentiels							
	Erreur de manipulation ou de paramétrage d'un							
	Erreur d'affectation comptable (compte, entité…)							
	Défaut de preuve (archivage, traçabilité) / piste	OUI	NON	Very Low	NON	Low	Good	NON
	Problèmes de communication							
	Non respect des délais et/ou des obligations	NON						
	Insuffisance de surveillance des comptes et/ou							
	Défaillance dans le traitement des réclamations							
	Autres causes liées aux traitements et							
	Inexactitude d'informations communiquées à							
	Manquement à une obligation déclarative							
	Documents contractuels imprécis, inadéquats ou							
	Défaillance dans la collecte et la conservation							
	Non sécurisation des accès aux comptes clients							
	Données erronnées communiquées aux clients							
	Mauvaise exécution des prestations							
	Absence de dispositions contractuelles							
	Litiges avec les fournisseurs							

Annexe 9-3 Plan de contrôle des risques opérationnels, vision COSO-Exemple Plan de contrôle Souscription des contrats d'assurance



Evaluation du risque, souscription du risque et Emission de la police	Absence d'enregistrement ou enregistrement incomplet des offres ou des polices.
	Non conformité de la police souscrite par l'intermédiaire aux décisions de souscription compagnie.
	Non conformité des polices et des protocoles aux lois et règlements en vigueur
	Non conformité des décisions des souscripteurs et/ou les gestionnaires compagnie aux guides ou instructions de souscription
	Tarification des risques incorrecte
	Emission de police incorrecte
	Estimation incorrecte des primes (garantie et évaluation des risques) / créances suite à une modification de la police (avenant ou renouvellement).

Annexe 10 - Exemple de politique de maîtrise des risques opérationnels, illustration avec la banque C2

Politique de Maîtrise des risques opérationnels

La gestion des risques opérationnels de la banque « C2 »[83] répond :

- Aux prescriptions réglementaires édictées notamment par le Règlement n° 97-02 modifié relatif au contrôle interne et par l'arrêté du 20 février 2007 relatif aux exigences de fonds propres, transposant en réglementation française les accords de Bâle II.
- Aux bonnes pratiques pour la gestion du risque opérationnel émises par le Comité de Bâle sur le contrôle bancaire actualisées en juin 2011
- A la charte de Management des risques du groupe auquel est affiliée la banque « C2 » dans la mesure où ces dispositions sont compatibles avec les obligations de la banque C2 comme établissement de crédit.

1-Organisation de la maîtrise des risques opérationnels

1.1. Le périmètre

Le risque opérationnel est inhérent à tous produits bancaires, activités, processus et systèmes. Sa prise en compte est un élément fondamental dans le dispositif de maîtrise des risques bancaires.

La gestion des risques :

- ⇨ est un processus, qui implique l'ensemble des acteurs de l'entreprise, depuis les organes de gouvernance jusqu'aux opérationnels,
- ⇨ couvre à la fois la notion de risques et d'opportunité (bénéfice),
- ⇨ contribue à l'atteinte des objectifs de la structure, et concerne l'ensemble des activités.

Le processus de maîtrise du risque opérationnel intervient à tous les niveaux de l'entreprise : élaboration de la stratégie, mise en œuvre des projets, activités de gestion, à la fois pour identifier les événements potentiels susceptibles d'en affecter l'organisation et pour gérer les risques dans les limites de la tolérance exprimée.

1.2. La filière risques au sein de la banque « C2 »

La maîtrise des risques repose sur l'organisation des responsabilités au sein de la banque. Les premiers acteurs sont les managers des différentes entités appuyés par une fonction interne de risk management et des fonctions d'expertises et de maîtrise du risque transversales.
La Direction des Risques de la banque s'assure du bon fonctionnement de l'ensemble, de la gestion de risques transverses et du niveau de risque pris à travers cette filière risques mise en œuvre conformément à l'obligation faite aux articles 11-8, 11-9 et 11-10 du CRBF 97-02.

[83] Le présent document a été anonymisé par respect de la confidentialité de l'étude de cas au sein de la banque C2, les éléments clés de la politique de maîtrise des risques restent toutefois non changés.

Les entités concernées au sein de la banque :

⇨ **Les responsables d'entité de la banque**

Les responsables d'entité sont en charge de l'atteinte des objectifs, de la gestion des moyens et de la maîtrise de leurs activités. Dans le cadre de cette mission, ils portent la culture risque de le la banque, la diffusent et la mettent en œuvre. Ils ont la responsabilité de l'identification, de l'analyse et du traitement de leurs risques et du choix d'organisation retenue pour les maîtriser.

Ils peuvent déléguer cette fonction de risk management.

⇨ **Les risk managers**

Une fonction de risk management est mise en place afin d'assister les responsables, ainsi que leurs équipes, dans le processus de prise de décision et de gestion des risques. Logée au sein de l'entité, elle doit être servie par une excellente maîtrise du métier, compréhension des enjeux et contraintes et un positionnement compatible avec une indépendance de vue et une proximité d'accès au responsable.

Les risk managers s'assurent de l'organisation, de la cohérence et de la pertinence des informations remontées portant sur l'identification et la gestion des risques, les plans d'actions et les dispositifs de maîtrise des risques associés, le suivi des incidents et la mesure des pertes, vers leur responsable et vers la Direction des Risques de la banque.

Ils dépendent hiérarchiquement du responsable de l'entité qui les nomment et fonctionnellement de la Direction des Risques qui valide leur désignation et assure leur formation et leur animation.

Les fonctions d'expertise et de maîtrise des risques

Un certain nombre d'entités au sein de l'organisation assurent pour le compte de la banque une double fonction sur un domaine particulier, en apportant à la fois leur expertise aux différents métiers et en en garantissant la bonne maîtrise pour la banque. Ils mettent en œuvre des dispositifs propres et adaptés à leur mission.

Elles identifient des risques, les décrivent, les cotent et les traitent pour le compte de la banque et accompagnent les différents métiers dans leurs travaux d'analyse et de prise de décision sur leurs propres risques.

Elles contribuent ainsi à la fois à une bonne prise de risques et à leur bonne gestion.

⇨ **Au sein de la Direction des Risques Opérationnels**

1. Le Responsable de la Sécurité des Systèmes d'Information (RSSI) définit les principes directeurs, le cadre de référence et l'organisation permettant d'instaurer un espace de confiance forte au sein des Systèmes d'Information de la banque « C2 » au travers de la Politique Générale de Sécurité des SI. Cette Politique de sécurité est déclinée notamment en :
   - une Politique d'accréditation aux Systèmes d'Information décrivant les principes directeurs permettant de garantir la maîtrise des droits d'accès aux SI de la banque ;
   - une Politique de Sécurité des Moyens de Paiement de la banque ;
   - une Charte de gestion de l'information sensible.

Il détermine le niveau de sécurité et les règles correspondants aux normes de la profession et au niveau souhaité par la gouvernance. Il valide la mise en œuvre des moyens et contrôle leur mise en application.

2. Les règles à respecter en matière de continuité des activités de la banque sont décrites au travers de la Note de Politique Générale des Plans de Continuité d'Activités, dont l'objectif est de fournir un cadre de référence en définissant l'organisation, les missions et les responsabilités en matière de PCA, ainsi que les principes et les règles à respecter au sein de la banque. Le Responsable Plans de

Continuité de l'Activité (RPCA) s'assure que la banque dispose bien de Plans de Continuité de l'Activité et pilote, si nécessaire, les tests à effectuer et les améliorations à apporter.

3. Le responsable de la Sécurité des Biens et des Personnes (RSPB) définit la politique générale de sécurité physique de la banque et veille à son application.

Il évalue également le niveau de sécurité physique et à ce titre établit les référentiels nécessaires à ses travaux, et notamment :

- un référentiel de ***structures***, recensant les sites concernés, leur rattachement et leurs différentes caractéristiques, et notamment celles de sûreté-sécurité.
- un référentiel *de* ***textes,*** recensant ceux de divers niveaux (législatif, réglementaire, professionnel, et leurs annexes -doctrine, jurisprudence,…-) applicables aux domaines de la sûreté et de la sécurité.

Sur ces bases, il définit des dispositifs de mesure du niveau de maîtrise de la sécurité physique par les différents acteurs impliqués dans le développement et l'exploitation des moyens (organisationnels et techniques) mis en œuvre pour réaliser l'activité.
Il assure enfin le reporting sur l'organisation et les moyens de suivi et de maîtrise des risques liés à la sécurité physique dans le périmètre concerné.

Afin de relayer l'action du RSPB dans les différentes entités, un correspondant sécurité placé sous l'autorité du directeur de tutelle de l'entité est désigné. Il assure l'animation et le pilotage de la sécurité au sein du périmètre couvert par sa direction en liaison avec le RSPB.

La Direction des Risques Opérationnels

La Direction des Risques Opérationnels est en charge de la mise en œuvre de la politique de maîtrise des risques sur le domaine des risques opérationnels.

A ce titre, elle définit l'organisation, les éléments de méthodologie et les outils permettant de :
- donner à la banque l'assurance raisonnable que la prise de décision s'effectue en connaissance de causes, avec une anticipation suffisante sur les risques pris ; et une organisation et des outils.
- donner au management une vision synthétique de ses risques et processus les plus sensibles afin de les gérer.

La Direction des Risques accompagne les entités dans le déploiement de leur propre dispositif de maîtrise des risques :

- Elle vise les Politiques de Maîtrise des Risques des filiales de la banque.
- Elle s'assure de la mise en place par l'entité d'une organisation de management des risques compatible avec les exigences de la banque, dont elle prendra en charge la formation et l'animation.
- Elle fait implémenter un dispositif global de reporting et d'alerte.
- Elle rend compte au Comité des Risques de la qualité du dispositif et des risques encourus par l'entité.

La Direction des Risques Opérationnels met en place une surveillance sur une base consolidée du groupe auquel appartient la banque « C2 », du bon fonctionnement du dispositif et du niveau de prise de risques à partir du suivi d'indicateurs et de la collecte des incidents et des pertes. Ces analyses et tableaux de bord sur l'évolution des risques sont produits à destination du Comité des Risques et du Comité d'Audit, rapportant respectivement à la gouvernance sur leurs domaines de responsabilités.

La Direction des Risques est dotée d'une équipe de Risks Managers Groupe, experts du management des risques dont les missions sont de contribuer :

- à la construction, la mise à jour et à la diffusion de la méthodologie d'analyse et de gestion des Risques Opérationnels,
- à la mise en place, à la formation et à l'animation de la filière,
- à l'alimentation de la cartographie des Risques Opérationnels de la banque,
- à la surveillance des risques par la réalisation d'analyses et de suivi de l'avancée des plans d'action,
- aux différents projets transverses de la banque, pour à la fois aider à identifier les risques liés, préconiser des mesures de maîtrise de ces risques, et contribuer ainsi à compléter, si nécessaire, la cartographie des risques,
- à l'élaboration, à l'aide des outils de gestion et systèmes disponibles, des tableaux de bord risques opérationnels destinés tant au comité risques qu'aux entités du groupe auquel appartient la banque « C2 ».

2. Les règles d'engagement

2.1. La prise de décision

Le but recherché est de s'assurer que les décisions prises dans les différentes entités placent la banque à un niveau de risque compatible avec ses choix stratégiques et que les différents moyens de maîtrise (prévention et détection de la survenance, réaction) soient prévus et mis en œuvre.

Il est de la responsabilité de chaque manager de s'assurer que les choix faits soient en adéquation avec les objectifs et la tolérance aux risques définis par la gouvernance de la banque « C2 » et son niveau de délégation.

La banque dispose d'une méthodologie pour mener et rédiger une analyse, basée sur les standards de la profession de maîtrise du risque et répondant aux exigences d'un établissement de crédit et de la banque en particulier. L'accent est mis sur l'anticipation par les métiers en matière de prises de risque, en intégrant dans les projets des analyses sur les différentes hypothèses envisageables avec entre autres l'identification des causes, une mesure des éventuelles conséquences et une description des éléments de maîtrise nécessaires. Cette description a priori s'applique de la même façon sur les processus existants.

Cette analyse doit permettre aux métiers d'identifier des événements de risques potentiels et de se tourner vers les entités dont l'expertise permettra d'affiner, en particulier les conséquences et définir les éléments de maîtrise de risque requis pour maîtriser la survenance et/ou le niveau d'impact. Le résultat de ces consultations, la connaissance des contraintes et objectifs s'imposant au métier sont nécessaires pour une prise de décision en « meilleure » connaissance de cause par le responsable de l'entité.

Une fois le risque identifié et décrit (activité, cause de défaillance, conséquences, potentiel ou avéré), le métier doit en évaluer la criticité à la fois à « dire d'expert » en se basant sur sa connaissance des sujet et sur une méthodologie fournie par la Direction des Risques. Cette cotation est faite en intégrant l'éventuel dispositif de maîtrise des risques, la banque ayant optée pour une mesure « nette » et la plus proche de la réalité. Cette exigence nécessite pour le métier d'avoir une bonne analyse des éléments de maîtrise des risques existants pour être en mesure de réagir en cas de suppression d'un de ces éléments ou de baisse de son efficacité.

La cartographie permet de consigner ces risques acceptés par la banque. La Direction des Risques prend à sa charge les actions de coordination sur des risques transverses et complexes.

2.2. La gestion du risque

Il est demandé, a minima, au métier de réviser son évaluation une fois par an pour tenir compte des évolutions internes et externes. Le niveau de criticité est suivi à partir d'indicateurs représentatifs (que ce soit en impact et/ou en occurrence). Ces indicateurs sont définis, décrit et alimentés par le métier.

Cette révision régulière doit permettre à chaque entité de traiter ses risques, c'est-à-dire de prendre des décisions de gestion. Le risque reste acceptable, soit en l'état, soit après des plans d'action visant à en réduire la criticité (soit en agissant sur la survenance et/ou sur le niveau des impacts), le supprimer (arrêt d'une activité…).

2.3. La mesure et la surveillance des Risques

La surveillance des risques se fait au travers des 7 grandes familles bâloises[84]
Au-delà de la réponse à l'exigence réglementaire, les travaux de la Direction des Risques Opérationnels visent à fournir à l'organe exécutif et, via le Comité d'audit, à l'organe délibérant, une vision synthétique du profil de risques opérationnels de La Banque Pola banque « C2 » et des conséquences notamment financières de leur matérialisation, dans une optique de management dynamique des risques et d'intégration de la maîtrise des risques opérationnels dans la gestion quotidienne.

Les risques identifiés par chaque entité doivent être décrits dans une cartographie permettant à la Direction des Risques de s'assurer de la réalité de la mise en œuvre du dispositif, de mener des analyses, d'alimenter ses échanges avec sa filière et de produire une vision consolidée au niveau du groupe auquel appartient la banque « C2 » , de leur criticité et des plans d'action en cours et prévus.
Cette analyse qualitative doit être complétée par une collecte des incidents et pertes (directes et indirectes) permettant, au travers de données quantitatives, de challenger le dispositif.
Les risques jugés significatifs sont remontés en comité des risques.

La Direction des Risques doit définir des indicateurs de suivi des risques opérationnels, validés par le Comité des Risques, permettant de mesurer le risque ou de vérifier que les règles de la politique de gestion des risques sont respectées. Des indicateurs d'alerte, également validés par le comité des risques, doivent venir compléter le dispositif.

L'*arrêté du 14 janvier 2009 modifiant le règlement n° 97-02 du CRBF,* précise que les systèmes d'analyse et de mesure des risques doivent prévoir les critères et seuils permettant d'identifier comme significatifs les incidents révélés par les procédures de contrôle interne, y compris lorsque ces incidents ne se sont pas encore matérialisés par des pertes. Le texte indique à l'article 17 *ter « Est réputée à cet effet significative toute fraude entraînant une perte ou un gain d'un montant brut dépassant 0,5% des fonds propres de base».* C'est le seuil que la banque[85] a retenu après consultation du Comité d'Audit.

[84] Fraude interne, Fraude externe, Pratiques en matière d'emploi et de sécurité sur le lieu de travail, Clients, produits et pratiques commerciales, Dommages aux actifs corporels, Interruption d'activité et dysfonctionnement des systèmes, Exécution, livraison et gestion des processus.
[85] Seuil de significativité arrêté par l'organe délibérant, conformément à l'article 38-1 du règlement n° 97-02.

Annexe 11 - Retranscriptions d'entretiens confirmatoires, exemples

Entretien EC14 du 20/11/12, Directeur du contrôle des risques – société d'assurance

Parcours de l'interviewé :
53 ans, Formation en finance, plus de 30 ans de carrière au sein de la société d'assurance, d'abord sur des activités comptables et financières puis sur des activités de management des opérations avant de prendre la direction des opérations et d'être ensuite responsable du contrôle interne. Après plusieurs années en tant que responsable contrôle, passage depuis plus de 5 ans au poste de directeur du contrôle des risques avec comme projet transverse la mise en œuvre des méthodologies de la société mère en matière de référentiel de risques et d'analyse des risques.

-Quelle compréhension des politiques de maîtrise des risques opérationnels (freins et leviers) ?

Le contrôle des risques cela inclus avant tout les processus opérationnels mais aussi l'enjeu normatif. Solvabilité II et les normes c'est une pression nécessaire pour que le contrôle interne voit le jour.
Le levier réglementaire est intéressant pour faire évoluer les structures. Sarbannes-Oxley cela a été un levier de progrès pour nous.
De la même manière, Solvabilité II c'est un moyen d'aller plus vite et d'avoir plus d'impact sur les responsables.
Cela a été l'occasion de développer des loss data base, nous l'avons mise en place en 2008. Aujourd'hui on est plus vers une phase de maturité.
Sans solvabilité II nous aurions eu plus de mal : cela nous a donné une visibilité vis-à-vis des dirigeants par rapport à avant. Il y a des comités Contrôle Interne où l'on parle des pertes opérationnelles au Top Management, on a désormais une véritable écoute.
On va encore plus loin, depuis 2012 on est dans un exercice de modélisation des risques. On décline notre modèle interne au niveau France. Avant cela, on était davantage dans la description de tendances assez générales au comité d'audit, au conseil d'administration etc. On est dans la réalisation de scénarios sur la base des pertes avec une évaluation de ces scénarios et un calcul du capital alloué au risque opérationnel. C'est un donc un sujet clé pour les dirigeants. On donne des informations aux dirigeants et on informe sur les besoins en capitaux propres.
Sans ce message réglementaire, sensibiliser les dirigeants des différentes entités aurait été plus dur.
Avec Sarbannes-Oxley cela n'était pas aussi abouti : il n'avait pas de cartographie des processus par rapport aux risques, donc pas de rapprochement entre les deux.
On a donc décrit les processus, les risques, les contrôles, les responsables processus, sous-processus et les responsables de contrôle. Au-delà on visait la fiabilisation des informations financières. Le risque opérationnel et la conformité y participent.
Avec le contrôle des risques opérationnels, on vise le même formalisme en allant plus loin. SOX cela a été un gros apport, même si on a été délisté du NYSE en 2009.

Risques opérationnels : quelles confusions en pratique sur la notion et entre les différentes fonctions qui en traitent ?

On a des outils dédiés au niveau informatique pour avoir une remontée de l'ensemble des directions et ce de manière structurée. Cela émane des correspondants des unités métiers. Sur le risque opérationnel c'est là où on leur fourni le plus de guidelines, pour les aider à remonter les pertes.
Cela s'est passé lentement au départ, il y avait beaucoup de craintes des opérationnels car on évoquait le sujet sensible des pertes dans leur domaine. Ils ne voulaient pas « être jugés » pour avoir participé à nos travaux car qui dit erreur dit sanction et cela implique un travail par-dessus d'amélioration en plus du travail supplémentaire de la remontée d'information. Avec cette vision, le contrôle cela reste limité…
Si un processus est défaillant, les opérationnels informent pour avoir de l'aide. On se rencontre pour faire en sorte d'agir au plus vite sur un dispositif qui ne fonctionne pas.

On renseigne chaque évènement puis son impact loss associé et son recovery (montant recouvré) pour voir l'impact net de chaque évènement.
Dès qu'un impact brut est supérieur à 10 000 € on l'enregistre. En dessous cela a peu de sens, c'est peu significatif. On se concentre sur les pertes opérationnelles qui nous semblent vraiment pertinentes pour ne pas être noyés.

-Le risque opérationnel est-il pour vous un risque subi / diffus ?
-Le risque opérationnel reste-t-il le « parent pauvre » par rapport aux autres risques (très liés au cœur d'activité) ?

Sur les outils informatiques, c'est le plus important, on cherche à avoir une photo trimestrielle des risques opérationnels. On arrête une date puis l'on structure notre vision. On fait des comparaisons dans le temps. On décrit l'explication des risques opérationnels puis de leur catégorie. Pour les catégories on s'est inspiré de Bâle II : 7 catégories de niveau 1 puis 20 catégories de niveau 2 puis bien davantage en niveau 3.

-Existe-t-il un besoin et manque de « guidelines », de bonnes pratiques quant aux normes de contrôle des risques opérationnels ?

Avec Solvabilité II on travaille sur une base de connaissance que l'on n'avait pas avant. En parallèle on est dans une démarche d'ERM avec la cartographie des risques : cela nous permet de challenger les correspondants. Quand on a une annonce de risque, on matche toujours avec le quantitatif pour voir si l'on a un trou dans la cartographie, ce qui peut arriver.
On cherche ensuite à mettre en place de vrais plans d'actions : quand a-t-on des pertes ? Pourquoi ? Sont-elles récurrentes ? Les nouveaux contrôles et la formation permettent-ils de les réduire ?

-Quels sont les principaux freins et leviers lors de la mise en œuvre des politiques de risques opérationnels ?
-Quelles sont les difficultés d'interprétations du risque opérationnel dans la réglementation ? Marges de manœuvre ?

On fait un arbitrage coût du risque / Valeur ajoutée du contrôle interne.
Il y a un réel coût d'opportunité : sans contrôle interne, que se passerait-il ? On fait une économie de fonds propres sensibles entre modèle interne et modèle standard mais il faut aussi voir ce que le contrôle permet d'arrêter : savoir où sont les risques, les failles, c'est tout aussi important. : il y a une valeur d'image, c'est rassurant (on a eu le trophée du contrôle interne début des années 2010) et puis il n'y a pas que les mathématiques car des risques sont très dur à mesurer.
Cette valeur d'image c'est aussi le fait d'éviter la sanction et ses conséquences allant au-delà. On réalise une double économie : à court et à moyen terme.
C'est donc une question de curseur pour justifier le contrôle : l'ensemble des contrôleurs a un coût mais il est bien souvent justifié.

-Le risque opérationnel est-il un enjeu de contrôle budgétaire et de gestion des coûts ?

On peut ici parler du lien Contrôle de gestion / contrôle interne : Le contrôle de gestion appartient au dispositif, il a un rôle dans l'élaboration des plans triennaux. Le risque opérationnel est clairement un coût que l'on ne devrait pas avoir, c'est un coût caché.
L'approche est cependant différente : le contrôle de gestion c'est principalement une approche économique. Le contrôle interne c'est une autre plus organisationnelle.

-Qu'est ce que la culture du risque opérationnel pour vous ?

Le risque opérationnel c'est du concret, la définition est peu complexe. C'est juste une question de sensibilisation.

Dès lors qu'on a une organisation avec une structure centrale puis des correspondants par unité cela devient plus facile. Nous avons des risk managers locaux qui chapote le contrôle permanent et diffusent la culture du risque. Pour que l'on ait la remontée d'informations nécessaires.
Le contrôle interne contribue à la définition de méthodologies puis à la présentation des exemples. Cela permet de concrétiser le sujet et d'être toujours en support pour quand il y a des questions des métiers.
Notre réseau est bien en place. On a des outils dédiés : Un outil « Open pages » pour centralise l'information essentielles et décentraliser l'information secondaire dans le réseau de correspondants. Le tout est de bien définir à quel niveau on arrête.
Le réseau comprend la direction des risques et pour chaque unité le contrôle permanent puis les correspondants risque.

-Qu'est ce que la responsabilité face au risque ? Quand a-t-elle lieu ? Sur quoi peut-on jouer pour la rendre effective face au risque?

Ce sujet s'envisage pour nous concernant la formation et remontée d'information ainsi que le rôle des réseaux compréhension, remontée d'information).

Il faut faire des efforts de formation. Pour les différents cas remontés il faut faire comprendre que cela doit être justifié et comment, pour ne pas être noyé de cas non pertinents.
On forme notamment sur les fiches de risque sous Excel, cela reprend les besoins en matière d'outils, de reporting, ce sont des documents simples mais il faut s'assurer que tout y est bien compris, notamment la terminologie et les informations à renseigner. Il faut être sûr que les correspondants ont bien compris. On a donc plusieurs niveaux de déclarants.
Les contrôleurs permanents regardent si les bons évènements de risque opérationnel ont été renseignés, si cela a bien été qualifié, si les catégories et les montants sont les bons.
Après cette première phase d'assessment, on a la direction des risques : elle regarde si la qualité de l'information est bonne et satisfaisante, s'il n'y a pas de doublons. Si l'on a une clarté suffisante. Puis elle valide pour que l'information soit définitivement dans la base.
Une fois par an on fait une revue complémentaire de la qualité avec les correspondants formé à la démarche risque opérationnel. On les fait décrire et qualifier. On prend des échantillons et s'assure que le sujet est bien maîtrisé.
Un compte-rendu régulier des contrôleurs permanents permet de s'assurer que tout va bien et que le sujet est bien maîtrisé.
Puis une veille en central assure l'homogénéité de l'information. Il faut voir si sur chaque unité métier les déclarants travaillent sur la même base et de la même manière. On doit pouvoir remonter la piste d'audit.
Par exemple : la direction juridique fait remonter des informations sur l'ensemble de ces dossiers contentieux, des recours etc. La direction distribution fait remonter des données sur la fraude. C'est aujourd'hui bien cadré et cohérent, mais cela a demandé du temps et de la formation.
Un contre exemple : quand on travaille avec des correspondants et qu'il n'y a pas d'informations remontées, peu de déclarations, on sait que ce n'est pas normal. Surtout sur des périmètres sensibles.
On bénéficie aussi de l'information groupe : une information d'ensemble émanant du siège sur les différentes filières. Cela permet de se comparer. De voir où il y a beaucoup de risque opérationnel et pourquoi, de voir s'il on est dans la moyenne ou s'il y a des efforts à faire.
On recherche la différence avec la France, ce que l'on a de bien, ce que l'on a pas et qu'il faudrait avoir en matière de dispositif, d'outils, de méthodologie.
Cela permet l'amélioration de la collecte régulièrement, et au-delà de rechercher l'exhaustivité dans le travail avec nos correspondants, de travailler plus en profondeur, car ce n'est pas un travail statique fait une fois. Notre action s'inscrit dans le temps…dans la durée même.
Se comparer grâce à des bases externes c'est limité, biaisé pour nous. Cela reste différent de la réalité de notre organisation et de son profil de risque.

-Créativité et design du contrôle ? Est-ce le vrai sujet pour cerner le risque opérationnel?

Cela concerne à la fois le déploiement de la filière et le choix des correspondants.
De 2008 à aujourd'hui un long chemin a été parcouru. La 1ère année a été celle de la chauffe, de la mise en mouvement de notre action.
Au bout de trois ans on arrive à avoir des remontées régulières, on en tire des enseignements. Sur la fraude interne on a par exemple un bon niveau de maturité.
L'une de nos difficultés au début était la méconnaissance du sujet :
-c'était du travail en plus
-on en voyait peu l'intérêt,
-il y avait la peur d'être jugé
-il y avait un problème de formalisation et de formation : si tout n'est pas bien défini précisément et bien expliqué, cela ne marche pas. C'est essentiel d'avoir des bons correspondants, de bons outils et un niveau de formation suffisant.

Les correspondants sont pris dans les contrôleurs permanents. Pour les choisir et décider des déclarants on définit les besoins au cas par cas avec les comités de direction locaux. Il ne faut pas prendre quelqu'un de trop bas dans la hiérarchie et dans l'organisation car autrement il n'aura pas l'information suffisante. Il faut avoir une vision de l'endroit où l'on est et une bonne compréhension de chaque environnement métier. Il faut bien décrire et retranscrire ce qu'est le risque opérationnel.
En plus de cela, on fournit donc une aide sur la description de ce qu'est un déclarant. Dans la partie RH : il y a une fiche de déclarant ORM, cela correspond à une activité clairement identifiée. Le responsable doit le savoir et le valoriser. Le déclarant doit avoir l'appui de la hiérarchie.
Dans la revue de qualité que l'on fait dans chaque secteur le contrôle permanent fait une note et diffuse les notes dans les directions. Une fois en place, cela permet une vraie remontée car les déclarants sont connus.
Une des limites que l'on a identifiées est que peu d'informations au niveau central reviennent aux déclarants.

-Qu'est ce qu'un contrôle interne cohérent face au risque?

Chaque trimestre des présentations sont faites au comité contrôle interne plus un comité risque opérationnel a lieu où l'on réunit l'ensemble des correspondants : on évoque les informations remontées, on fait des retours sur les évènements de collecte (vision consolidée). On réalise encore des points réguliers sur le rôle des contrôleurs dans chaque métier.

-Qu'est ce qu'un contrôle qui a du sens par rapport au risque opérationnel ?

Cela concerne différentes thématiques :
-la Sensibilisation
Pendant longtemps il y a eu la peur de la sanction. Au niveau de la DG on fait souvent le point sur le top 5 des principales pertes. L'objectif n'est pas de trouver des responsables ni de faire tomber des têtes.
L'axe responsabilité ce n'est pas évident en communication. C'est pour nous un axe à approfondir.
Cela concerne par exemple le lancement de nouveaux produits : fournir la bonne information, la documentation adéquate. On s'en aperçoit souvent trop tard de ce type de carence car on est focalisé sur le projet, parfois pas simple à faire aboutir alors on ne souhaite pas rajouter de la complexité à la complexité.
Dans tous les cas quand il y a un problème on ne cherche pas à faire ressortir un nom, mais on se concentre sur des dysfonctionnements, sur des pertes, comment on peut éviter que cela se reproduise en décrivant clairement les schémas de survenance et en les diffusant avec de la pédagogie.

-le lien qualité / contrôle des risques

Il y a un lien clair, les démarches sont proches. Dans les deux cas on parle de risque et de contrôle. Il s'agit dans les deux cas respectivement de l'objectif et du moyen.

-Le lien avec les autres fonctions
L'audit, la conformité, le risque ce sont des fonctions différentes.
Mon opinion sur le contrôle interne : historiquement on parlait d'audit. Puis on a commencé à faire du contrôle permanent (sans que cela soit vrai partout). Les contrôles clés étaient testés chaque année par les auditeurs (depuis SOX). On teste l'ensemble des contrôles clés. On voit où sont les zones de faiblesses de l'entreprise.

-Le lien Audit / Risk Management
Pour la direction des risques : nous sommes comme indépendants. Nous sommes habitués à faire des tests et des bilans sur nos sujets. Les CAC s'appuient beaucoup sur nos travaux et analyses donc on a un réel apport pour sécuriser l'entreprise. On permet un autre point de vue, crédible, complémentaire à l'audit interne, qui apporte elle aussi une expertise.
C'est important pour la direction des risques d'avoir un retour de l'audit interne, une information sur le plan d'audit et sur les déficiences de l'entreprise, cela oriente aussi le travail à fournir et inversement ils sont plus vigilants aux zones qu'ils savent être à risque lorsqu'ils construisent le plan d'audit.
Il y a un lien fort entre les fonctions sur les missions d'audit : on travaille dans les deux cas sur les zones de faiblesse. On est complémentaire parfois :
On échange sur les projets, les missions, on donne notre accord ou non sur tel projet.
L'audit interne cherche quant à elle à voir si le contrôle est efficace. Nous sommes des fonctions sœurs, travaillant en complétude. Avec des angles différents. Ce sont donc deux fonctions différentes mais très proches.
Tous les trimestres on fait un point avec les directeurs de mission, l'audit interne échange sur les résultats principaux de ses missions.

Tant que l'on n'avait pas une base de données fondée sur une solide expérience c'était dur de communiquer avec les responsables. Quand on gagne en profondeur, on voit ce que cela représente.
Quand on montre des chiffres on en voit concrètement l'intérêt. Sur la fraude de 2006 à 2007 c'était localisé dans une direction. On en parlait peu, Aucun dirigeant n'avait une vision claire et exhaustive. On ne pouvait pas résonner proactivement.
Aujourd'hui on fait des requêtes pour anticiper, des recoupements avec les bases de données, on peut anticiper les scénarios de fraudes et les profils de fraudeurs ; on ne se contente plus d'attendre qu'un risque éclate ou qu'il y ait une dénonciation sur certaines pratiques.
Plus on a une vision, plus le niveau de sensibilisation est fort. Quand on a une collecte de données, cela permet de sortir du flou. Cela facilité la sensibilisation du Top Management avec des chiffres.

Il y avait déjà un Risk Management par le passé, dans les nombreuses filiales (Italie, Allemagne, UK). Notre structure organisationnelle permet un benchmark entre les filiales. Ce n'était pas le cas avant. Aujourd'hui on a les mêmes référentiels, les mêmes outils (open page), cela permet de comparer les résultats suivant la même nomenclature. On voit mieux nos faiblesses et nos forces vis-à-vis des autres pays.
On n'a une indépendance limitée : le siège a la main sur le modèle interne et son paramétrage. Il nous donne un cadre général. Le vrai sujet est donc du côté du pilier 2 et pas tant du pilier 1.

-Contrôle des risques opérationnels et rapport à la réglementation prudentielle, rapport régulateur-entité.

L'ACP nous donne une interprétation sur Solvabilité II. Mais il s'agit de sa vision. Par exemple entre l'ACP et la BAFIN (Allemagne) l'approche est différente.
Les textes ont pris du temps à émerger à être clair. Cala a pu être intenable… Il y a de nombreux intervenants (EIOPA, Parlement, superviseur). Cela reste peu efficace au niveau européen.

L'objectif de l'ACP est à terme d'avoir quelque chose de plus transverse. C'est cependant difficile pour un groupe comme le notre.
L'idée serait d'avoir un superviseur européen facilitant les choses, cela éviterait les divergences d'approches car l'ACP n'est pas toujours claire.
Sur la modélisation du risque opérationnel, cela n'est pas nouveau en banque mais il n'y a pas de dispositif reconnu comme pertinent, de guideline, le régulateur est absent.
Il nous donne peu de conseil, est peu directif : assez de personne, suffisamment de travail et de temps sur la démarche ? On ne sait pas si on va dans le bon sens or on a les mêmes besoins que les banques et les autres assureurs sur la clarification de ce qui est à faire ou non.
Les échanges sur les risques opérationnels avec le régulateur : on est toujours sur une approche très théorique.
Cela manque de pragmatisme. On nous propose des « usines à gaz » là où l'on voudrait des conseils.
On manque donc de clarté sur l'exercice, sur les meilleures pratiques. On est loin d'être les premiers sur le sujet mais l'on se pose toujours les mêmes questions. Sur les principes de bases, tous les acteurs sont proches.
Exemple : les Scénarios
On a une vraie difficulté opérationnelle sur l'évaluation des scénarios. Sur la base des pertes et de la cartographie on tente de construire ces derniers. Puis on se livre à une évaluation, par des jugements d'experts. Il s'agit de probabilités subjectives. C'est difficilement opposable au superviseur.
Nos raisonnements tiennent la route mais le régulateur en a une vision très théorique.
C'est un vrai problème : comment bien évaluer un scénario car un modèle c'est mécanique (il est question de valeur moyenne, de pire cas…) On doit partir du concret sur la base de nos pertes car sur l'ensemble des sujets risque opérationnel on n'a pas assez d'experts pour assurer une vraie convergence. Ce type de méthode est parfois théorique…
Notre besoin c'est aussi de savoir quelle méthode est acceptable et laquelle ne l'est pas. Laquelle est bonne pour le superviseur.
Mais le cœur du problème reste cependant au-delà de la définition des scénarios, et de son évaluation. Solvabilité II c'est sensé « soulager » les équipes car on a une vraie assise mais cela suppose encore qu'on sache clairement comment s'y prendre.

Entretien EC-6, 19/09/2012, durée 2h30, Directeur d'un cabinet de conseil, expert risque opérationnel (banque et assurance), ex-directeur risque opérationnel banque.

Parcours, positionnement et expérience de l'interviewé sur la thématique risque opérationnel de l'interviewé

Parcours dans l'audit interne puis dans différents métiers du risque, avant de prendre la direction des risques opérationnels d'un groupe bancaire, aujourd'hui auteur de plusieurs publications sur le risque et directeur au sein d'un cabinet de conseil en gestion des risques.

Quelle compréhension des politiques de maîtrise des risques opérationnels (freins et leviers)

La sensibilisation passe par le fait d'envoyer aux opérationnels un message fort : Ce sont eux qui sont responsables des risques qu'ils engendrent. Dans leur activité, ils doivent se saisir du problème, éviter la logique du « ce n'est pas nous ». Quand on en arrive là, c'est que le message est mal passé.

Le risque opérationnel reste un sujet récent, cela date de 1998, avec le comité de Bâle. On a commencé à en parler vraiment à partir de 2001.
A cela s'ajoute le fait que le risque opérationnel est un sujet très vaste, qui couvre tous les domaines de la banque. Il est diffus et subis dans l'organisation. Ce risque est un risque frontière, il est dur à appréhender et à étiqueter. La prise de conscience et la communication sur ce risque sont difficiles.

En matière de risque opérationnel il y'aurait en fait 3 sujets :
-Les risques de fréquence : à la frontière avec la qualité, il s'agit du « petit risk management », le contrôle de 1er niveau s'en occupe, son coût est faible. Exemple : la monétique, on gère le 0,1% de fraude, par un traitement statistique et par des dispositifs de sécurité. C'est de la perte attendue (expected loss), on l'intègre dans le prix provisoire/an.

-Il y a ensuite les risques arrivant entre 2 et 20 fois par an, de grosses fraudes, plus lourdes à gérer. Ces risques extrêmes posent des problèmes de traitement.

-il y a aussi des risques de sévérité. Ceux qui font l'objet du PCA, que l'on gère par l'assurance, de la RC-pro, du dommage aux biens etc.

-Quelles sont les difficultés d'interprétations du risque opérationnel dans la réglementation ? Marges de manœuvre ?

On parle bien de risques opérationnels dans tous ces cas mais ce ne sont pas les mêmes sujets. Ils sont à géométrie variable. Au-delà des catégories baloises, il y a des catégories de risques opérationnels spécifiques pour chaque entreprise : entre une banque et son GIE le risque opérationnel n'est pas forcément le même. Exemple de risques majeurs : reconstituer un parc de cartes bancaires, gérer les skymers suite à cela etc. / une erreur de saisie de dossier, on renvoi le dossier au client car il y a une mauvaise tarification. Autre exemple : lorsque l'on passe un ordre d'achat au lieu de passer un ordre de vente, cela peut très rapidement nous coûter cher à nous (banque) et à notre client. Ce sont des risques complètement différents qui supposent une organisation différente.

La variabilité du risque opérationnel est le plus dur à comprendre. Peu d'organisations ont compris ce qu'est le risque opérationnel. Dans les banques, c'est surtout une logique de production d'information et de conformité réglementaire, de respect des exigences de fonds propres.

Pour beaucoup d'assureurs, on est plus dans une étape de présentation des avancées de la mise en œuvre des filières et des dispositifs et fonctions que d'un véritable management actif et effectif. On en est à ce stade sur les cartographies, sur la collecte des incidents etc. C'est une logique d'avancée des

projets en interne plus que de pilotage effectif du risque. Cela explique le désintérêt des directions générales pour le sujet.
En comité risque, peu sont dans une logique de gestion et de pilotage du risque. On se projette peu, on gère les projets sur le sujet.

Le risque opérationnel a en pratique un faible poids. Il y a les risques de chaque métier (ce que les métiers savent faire) et souvent c'est un risque subi.
Quand on calcul le poids relatif du risque opérationnel par rapport aux autres risques, cela donne l'impression que c'est un sous-sujet. Ce risque est mal évalué, sous-évalué. Dans les faits cela va bien au-delà.

Top Down:

Sur l'approche Top Down, il faut parler de risque extrême, on sensibilise plus par le top down que par le bottom up. Quand on descend dans les niveaux de granularité, cela fausse le sujet, le réduit à un sujet de faible intérêt pour les dirigeants.

Créativité et design du contrôle ? Est-ce le vrai sujet pour cerner le risque opérationnel?

Le problème est que l'on mélange tout sur le risque opérationnel. Il y a 3 discours à avoir pour les 3 types de risques opérationnels. On n'accordera alors pas le même temps et le même investissement selon les différents types de risques opérationnels :

-pour les grands risques : l'assurance, le PCA etc.
-pour les risques moyennement importants, on les présente aux comités etc.
-pour les risques de fréquences : on met en place un traitement statistique, des dispositifs de contrôle interne et une analyse du risque pour rebondir rapidement dans l'organisation.

Il ne faut pas tout mélanger car ces problèmes d'incompréhensions font que l'on accorde ou non de l'importance au sujet. Si l'on a bien saisi ce que c'est, on décidera de se couvrir contre. On mettra sur pied quelque chose de solide mais si cela semble obscur, cela risque d'être très différent quant aux budgets alloués…

-Le risque opérationnel est-il pour vous un risque subi / diffus ?

Le risque opérationnel, partant de là, c'est un problème de formation des acteurs et d'accompagnement du changement dans la filière.

C'est un sujet nouveau, donc quelque chose qui se vend en interne. C'est essentiel à comprendre car on est souvent sur de l'auto-déclaratif et de l'auto-évaluation par les métiers eux-mêmes.

Si l'enjeu est mal compris et mal perçu à tous les niveaux, cela ne marche pas. Il faut adapter son discours à la Direction Générale, au comité d'audit, aux opérationnels, sur quels sont les rôles et les responsabilités des différents acteurs. Il y a beaucoup d'adaptation de discours dans ce domaine.

Avec des outils de cartographie des risques opérationnels (type e-front), on a parfois plus de 8000 utilisateurs dans une grande banque. Il y a des membres du comité d'audit mais aussi des opérationnels sur des niveaux de détails très poussés. Ces différents profils ne sont pas prêts à entendre le même discours quand on les forme.

Pour le comité d'audit par exemple, il faut leur faire comprendre que l'on ne cherche pas à faire du reporting mais que le risk management est là comme un « poil à gratter ». Il doit bien comprendre son rôle par rapport à cela. Ce qu'il doit faire. Pour les risques retenus, il s'agit de comprendre s'il y a de

vrais dispositifs de maîtrise de risque. Si cela est réel et si c'est ensuite suffisant. Il faut pouvoir alerter si le dispositif perd de son efficacité ou si l'on risque de voir un problème trop tard.

Pour un opérationnel : le discours est davantage axé sur l'idée que le risk management peut aider dans la conduite de l'activité, que cela « soulage » et évite de se sentir seul sur des sujets posant problème. On donne un regard extérieur. On peut aider à faire remonter des problèmes ou documenter sur une activité à risque. On fait en sorte qu'un sujet à risque pour l'opérationnel compte réellement dans la hiérarchie : « il y a tant d'évènements, cela coûte tant, et voilà ce que l'on peut récupérer ».
Il faut leur faire comprendre que si l'on objective le risque, on peut être écouté. Si le collaborateur, l'opérationnel joue le jeu, alors on a suffisamment de matière.
C'est essentiel car une Direction Générale a besoin d'éléments pour prendre une décision. Elle doit voir de manière tangible de quoi il retourne pour décider si elle accepte le risque en l'état, l'auto-finance, ou choisit de le réduire. On est bien dans une logique d'aide à la prise de décision.

Il subsistera toujours des freins sur le risque opérationnel : même si l'on échange sur la base d'éléments réels, il ya un temps de latence entre la découverte des problèmes, la remontée, l'annonce et la décision de traitement prise. C'est un problème de déploiement lié à une difficulté de communication sur le sujet ; plus le fait de ne jamais être sûr de tout voir…

Contrôle des risques opérationnels et rapport à la réglementation prudentielle, rapport régulateur-entité

De plus, le régulateur n'offre pas toujours une compréhension claire du sujet, on se situe dans un carcan politique. Les comités risque opérationnel sont l'affaire de quelques experts en France. Il en va de même en assurance qu'en banque. Du point de vue de Bâle III il n'y a eu aucun apport quant au risque opérationnel. Si les subprimes ont pour origine un risque opérationnel, on octroya du crédit à des clients non solvables en le sachant pertinemment, la réglementation ne l'a pas vraiment pris en compte depuis.

Le schéma était le suivant : du risque opérationnel => un risque de crédit bancaire => de la titrisation puis du risque de marché puis une crise de défiance sur la solvabilité et les engagements de banques comme Dexia, Fortis, Lehman Brothers, ce qui donna une crise systémique.

Ce n'est pas un évènement, il y a toujours du risque opérationnel à un moment donné.
Bâle II nous fournit l'ensemble des textes sur le risque opérationnel.

Solvabilité II nous donne 20 lignes sur le sujet. Cela concerne la sous-traitance, le PCA etc. Mais le sujet des risques opérationnels en lui-même est très peu abordé. La méthode de calcul standard du risque opérationnel a en outre peu de sens, car complexe.
Pour le régulateur, Solvabilité II est peu voire mal compris. On a mal appréhendé cette réglementation et on a peu de recul sur le sujet. Surtout si l'on fait le lien avec les évolutions comptables, les IFRS, les évolutions de solvabilité II ajoutent en complexité.

Existe-t-il un besoin et manque de « guidelines », de bonnes pratiques quant aux normes de contrôle des risques opérationnels ?

En matière de risque opérationnel, le sponsoring est essentiel. Il est question d'une filière au sein d'une organisation. Sur l'ensemble des métiers, avec une vraie animation pour la remontée des échos. Il doit y avoir un « effet cheminée », une sensibilisation du conseil d'administration, de l'organe délibérant. Le comité d'audit doit aussi avoir en tête cette question, puis la direction générale, pour que cela ait un effet sur les opérationnels, le management et que les risques soient vraiment gérés.
Il faut créer une demande, émanant de la direction des risques, le principal interlocuteur en la matière. « Le risque opérationnel ne se gère pas dans une tour d'ivoire », c'est ce genre de message fort que tous doivent comprendre.

Pour la Direction générale, le traitement du risque opérationnel suscite peu d'enthousiasme sauf s'il y a déjà un problème. En France nous n'avons pas une culture de l'anticipation.

Par exemple le rogue trading a toujours existé. Souvent même après un problème le soufflet retombe rapidement. On pense que cela ne se reproduira plus. UBS ou ce qui se passe à Londres sur les taux interbancaire en sont de bons exemples.
Le côté business revient toujours au 1er plan. Face à des millions de commissions et de frais facturés, le risque de pertes sur 5-10 ans peut parfois peser faiblement. Il faut rester prêt à prendre des risques dans les faits.

Risques opérationnels : quelles confusions en pratique sur la notion et entre les différentes fonctions qui en traitent ?

Sur la cartographie on constate que beaucoup d'acteurs se sont lancés dans la cartographie. On a normé l'exercice et chercher à automatiser l'organisation du risque opérationnel, à faire le lien avec le contrôle, avec l'audit interne etc.

La problématique encore récente était de s'en occuper, la question qui se pose toujours c'est « par quoi commencer » ?
Sur ce sujet naissant, les big 4 sont beaucoup intervenus pour poser leur signature, on a cru qu'ils connaissaient mieux le sujet. Cela a représenté des budgets importants mais au final l'action a été peu pertinente dans la plupart des cas. Les méthodologies employées étaient trop complexes, cela a été une source de « décrédibilisation » pour les fonctions en charge du risque opérationnel auprès des directions et de la Direction Générale. Pour eux, c'en est parfois devenu un non sujet.
On s'est donc retrouvé avec un référentiel sur lequel pouvoir travailler est souvent peu clair, peu parlant, engendrant un déficit de contrôle, avec peu de clarté sur le risque.
Les méthodologies des cartographies n'étaient pas aisées à comprendre, dure à appréhender et encore plus à mettre en place.
Quand on est opérationnel, parler de « fréquence brute du risque » et faire le lien avec son business ce n'est pas simple. Alors en déduire que cela veut dire « j'ai 100 000 opérations, mon risque opérationnel peut arriver 100 000 fois si je ne fais rien et me coûter 1 million d'euro », c'est une autre étape à laquelle on n'est pas encore préparé le plus souvent.
Parler de « risque à piloter », de « transfert de risque », de « risques résiduels », c'est également loin d'être clair.
On retrouve toujours les mêmes méthodes, les mêmes outils et matrices, ce problème n'est pas isolé. Les problèmes d'évaluation du risque opérationnel sont donc très fréquents. Alors même si on peut ne jamais en avoir, le risque peut survenir en brut sans être géré. Il faut pouvoir faire comprendre, qu'en net (avec des éléments de maîtrise du risque), c'est un autre fonctionnement.

Sur le risque de sévérité, en pratique, ce dernier est rare et coûteux. On ne les voit pas. C'est ce genre de risque qui est vraiment inquiétant. Les risques très fréquents c'est une chose, mais quand on voit que des risques de sévérité sont « en jaune » dans une matrice, cela pose un vrai problème car on peut en déduire et présenter à sa direction que l'on n'a rien du point de vue de ces risques opérationnels là.
Le risque opérationnel c'est donc un problème à la fois d'identification et d'évaluation. On ne cadre pas ce risque dans de nombreuses organisations.

Un autre frein est qu'on a un vrai problème d'appropriation sur ce risque. La méthodologie, les référentiels, les approches sont peu claires. Cela décrédibilise une direction quand on a consacré un budget important, de nombreux jours/hommes, pour au final un rendu faible, des constats présentant peu d'intérêts. On en revient alors au réglementaire, on traite le risque opérationnel dans une logique du « on n'a pas le choix ».

-Le risque opérationnel est-il un enjeu de contrôle budgétaire et de gestion des coûts ?
-Qu'est ce que la culture du risque opérationnel pour vous ?

-On peut également penser au lien entre comptabilité et contrôle de gestion/ quel rôle par rapport au risque opérationnel ?
Ces fonctions sont importantes et devraient davantage jouer un rôle, mais en soi elles ne sont pas suffisantes. Dans un compte, il y a une fiche incident associée. On décide ou non de passer l'opération en fonction du message associé. Avec ce genre de disposition on ne capte qu'une part des choses : l'écriture comptable mais pas le coût d'opportunité ou le manque à gagner si l'on décide de bloquer l'opération. Pour les coûts cachés c'est assez limité : on ne voit pas les coûts d'opportunité, les manques à gagner avec un contrôle de gestion classique. C'est donc une réponse partielle au sujet.

Le risque opérationnel implique encore de bien définir s'il y a ou non un incident. Ce que l'on rencontre comme évènement et si l'on considère cet évènement uniquement. La comptabilité ce n'est donc pas suffisant pour des risques imbriqués, à la frontière de plusieurs problèmes.
Par exemple, une indisponibilité de système d'information. Quand on saisi l'évènement de risque, pour l'indicent cela fonctionne, mais pour son impact réel ?
La Direction des Systèmes d'Information (DSI) ne voit pas toujours tous les incidents transverses, et quand bien même, comment tous les référencer dans la base d'incident ? Même avec un référentiel, c'est en pratique trop variable pour avoir quelque chose de normé sur les différents niveaux de risques opérationnels.
Pour un évènement multi-impact, c'est un véritable écueil : on a plusieurs incidents, de natures variables, aux impacts parfois chiffrés, parfois non. Alors comment agréger cela ?

On tente donc d'avoir une logique causale le plus souvent : déterminer des effets en chaines, des arbres de défaillances, mais le problème est que les opérationnels ne savent pas toujours où s'arrêter, surtout pour le « hors entreprise » (qui fait partie du risque opérationnel). De grosses erreurs ont été faites dans la vente des dispositifs. C'est un vrai problème au niveau opérationnel mais surtout concernant les instances de gouvernance.

Quels sont les principaux freins et leviers lors de la mise en œuvre des politiques de risques opérationnels ? Qu'est ce qu'un contrôle interne cohérent face au risque?

Les vrais sujets sont les suivants : sponsoring, implication, communication, compréhension, sensibilisation.
Il s'agit de « vente » du risque opérationnel, du dispositif associé, par une équipe interne.

De grosses erreurs ont été faites dans la vente des dispositifs. C'est un vrai problème au niveau opérationnel mais surtout concernant les instances de gouvernance.
Il faut bien faire comprendre le rôle du contrôle interne, du risk management et leurs liens, car il y a beaucoup de confusion lorsque l'on créer et développe les fonctions. On crée des fonctions puis lorsqu'il y a un problème on rationalise. Ce genre d'approche explique que la prise de conscience est longue.

Une autre difficulté est qu'on gère trop souvent ce risque par la petite porte et non par la grande.

Pour les risques de GRH (prud'hommes etc.), les dommages aux biens et aux personnes, il en va de même.
Pour les erreurs sur l'exécution des processus ou encore les RPS, cela se complique très rapidement.

Il y a en pratique un défaut de conseil, on le gère trop souvent par le juridique alors qu'il faudrait en faire un sujet stratégique.
Si des sujets de risques opérationnels comme la fraude interne/fraude externe sont faciles à appréhender, les cyber-attaques, les documents frauduleux ou les complicités en interne sont des sujets bien perçus, on peut sensibiliser sur ces derniers.

Le risque opérationnel reste-t-il le « parent pauvre » par rapport aux autres risques (très liés au cœur d'activité) ?

Par rapport au risque opérationnel, on a besoin du droit, du levier réglementaire, pour crée la fonction, pour s'appuyer lors de la mise en place, mais cela ne doit pas se faire en se posant les questions clés plus tard. On résout le problème en mettant du contrôle, en recrutant des collaborateurs au lieu de tenter de comprendre les enjeux.
Le régulateur n'est pas non plus forcément très clair.
Bâle II date de 2004, à l'époque il était question de la transposition de la fonction de conformité. On transposa la conformité avant de le faire sur les textes relatifs au risque opérationnel. Le problème est que la conformité comporte des risques opérationnels lui étant inhérents. On a ensuite admis que la conformité était un risque opérationnel en tant que telle.

La vraie question est un problème organisationnel : la conformité est rattachée à la Direction Générale mais ce n'est pas la seule. La direction des risques, et notamment opérationnelle est rattachée à la Direction Générale dans de nombreuses organisations.
Mais il existe une confusion : le régulateur n'a pas toujours spécifié d'approche dédiée aux risques de non-conformité. La non-conformité constitue un risque opérationnel. Mais il existe des risques opérationnels plus larges liés à la conformité. Il faut donc prendre en compte le rôle des N+1 etc. quant au risque opérationnel, au sein même de la fonction conformité, en cas de défaut de celle-ci, qui seule ne peut pas tout voir. Le lien entre la fonction risque opérationnel et la fonction conformité est à prendre en compte.

Avec Solvabilité II, le sujet est le suivant, on a la fonction conformité, le dispositif de contrôle interne et en fin de compte un vrai problème de positionnement du contrôle interne.
Solvabilité II est à cet égard peu claire, on a un discours et un périmètre différent sur la conformité bancaire et celle en assurance. La simple transposition des textes n'a pas de sens, il aurait fallu s'adapter et être plus précis.
Les objectifs sont les mêmes, mais en pratique cela n'a rien à voir.
Il y a un vrai imbroglio. Ce problème d'organisation engendre une réelle perte de sens dans ce qui peut être fait.
Du coup on tente de rationaliser tout cela en mélangeant la conformité, le risque opérationnel, la qualité etc.
La confusion se résume comme cela : avec le tout ensemble, on gère le risque de fréquence et non le vrai risque opérationnel.

-Qu'est ce que la responsabilité face au risque ? Quand a-t-elle lieu ? Sur quoi peut-on jouer pour la rendre effective face au risque?
-Qu'est-ce qu'un contrôle interne cohérent ?

Les pistes de réflexions sont les suivantes :
-mettre en place des « cheminées de communication », il s'agit non seulement de mettre en place ces cheminées mais aussi d'entretenir le feu, le flux d'informations et de communication.
-c'est aussi une question de crédibilité de l'approche. Cela dépend de la maturité de l'entreprise. Exemple, au Crédit Mutuel CIC, avec ce qui est mis en place sur les réseaux bayésiens, c'est assez poussé mais cela ne convient pas à toutes les structures, surtout les plus récentes.
La complexité est dure à vendre, si l'on veut parler du risk management de demain, il faut s'y prendre autrement car de nombreux acteurs ont du mal à s'approprier ce sujet. Dans la plupart des cas on n'est pas entre ingénieurs, spécialistes du sujet, il faut faire avec différents profils dont le degré de compréhension n'est pas le même. Cela demande un vrai investissement.
Une approche complexe par réseau bayésien, cela consiste en un « détricottage » des chaines causales et une affectation aux bons endroits. Mais c'est dur à construire et à maîtriser. Si l'on a à la base un problème de culture et de compréhension du sujet, cela sera dur de dénouer les vrais risques avec ce type de réseau.

A cela s'ajoute un aspect de complexité de la méthode. Plus les collaborateurs s'y retrouvent, plus ils en comprennent l'utilité. Cela suppose aussi qu'ils aient un feedback sur les informations qu'ils transmettent.
Quand on demande des informations aux opérationnels sur leurs risques mais qu'ils n'ont jamais retrouvé d'informations pouvant leur resservir, ils n'en voient pas l'utilité et assimilent ça à du reporting. On peut aussi faire des choses complexes mais qui paraissent simples, il suffit de ne pas montrer la complexité, de traduire en quelque sorte ce qui est fait.
Par exemple les scénarios s'y prêtent bien. Quand on a peu d'information sur le risque, pas de maturité suffisante. On peut faire comprendre aux dirigeants comme aux opérationnels l'intérêt de la démarche pour leur faire parler de leurs risques.

Les risques opérationnels restent en grande partie des risques frontières, cela n'est pas assez pris en compte depuis 2004, où à la base on parlait de mesures transitoires. Il n'y a pas eu de réelles prises de conscience depuis (régulateur, organisations).
Les fonds propres sont un faux sujet au final. Il est plus important d'imposer aux établissements de faire une analyse approfondie. Les risques opérationnels sont largement sous-estimés, ils vont bien au-delà des 8-10 % provisionnés car ils sont à la base de nombreux autres sujets.
Le vrai problème est un sujet de communication. On a un problème pour comprendre et faire comprendre la réalité des enjeux. L'enjeu perçu se fait via le poids dans les fonds propres, ce qui fausse la donne.
Les risques opérationnels c'est aussi une question de motivation au travail (lien RH) : il faut recréer une dynamique. Il faut une vraie « conscientisation » du risque opérationnel. Du dynamisme, de la lisibilité. Le risque opérationnel ce n'est pas qu'un montant de fonds propres. Il faut faire du pilotage, mais le faire avec un réseau actif et faire vivre même après la mise en place de la filière.

Entretien EC-37, Directeur risque opérationnels-établissement bancaire, 1 heure 30, 27/02

Parcours, positionnement et expérience de l'interviewé sur la thématique risque opérationnel de l'interviewé

Parcours dans différentes fonctions opérationnelles, gestion d'actifs, gestion des opérations, avant d'initier une carrière dans différentes fonctions supports et de prendre la direction des risques opérationnels.

Le risque opérationnel est-il pour vous un risque subi / diffus ?

Historiquement les métiers de la banque ce sont le crédit, on pense aux pertes, alors on pense parfois aux risques opérationnels mais dans une certaine logique : « j'en souffre dans mon métier, les risques opérationnels c'est surtout par rapport au cadre réglementaire qu'on le fait » c'est ce genre de retour que l'on peut avoir.
C'est une matière récente, difficilement appréhendable, c'est un risque subi, une question de défaillance de l'entreprise sur laquelle on tente de se rattraper, quand on a une perte sur un compte, mais c'est déjà fini, le risque est survenu.
Les risques opérationnels, c'est très confus, c'est difficilement explicable même dans la banque. Même dans la banque de détail, le contrôle des risques opérationnels y est très déployé, les inspecteurs groupe comprennent tout mais cela reste dur sur le risque opérationnel.
Même au niveau des tops managers, il faut passer par des exemples pour que cela devienne plus clair.
Sur les RH, sur les SI, sur l'ensemble des points et catégories, peu de collaborateurs imaginent ce qu'est le risque opérationnel. Et c'est parfois mal perçu.
Pour les reportings états Corep, c'est très complexe pour en expliquer l'intérêt aux métiers. Et ils ont la vision à un instant T du sujet alors pour être en risk management proactif c'est une autre étape.
Sur les pertes c'est mal appréhendé, la matière « baloise » est peu parlante. Le pilotage par les processus est plus efficace, cela devient plus parlant sur les processus d'octroi de crédit par exemple. Il faut du temps : c'est un vrai combat pour qu'avec les responsables de processus, on diffuse la vision risque opérationnel. Nos responsables processus sont les CRO (contributeurs risques opérationnels). Ils vont nous aider à coter dans la cartographie des risques car ils connaissent mieux les processus. C'est cette logique que l'on essaye de mettre en place depuis 4 ans sur les deux réseaux *(Banque Populaire / Caisse d'Epargne).*

Quelle compréhension des politiques de maîtrise des risques opérationnels (freins et leviers) ? Le risque opérationnel reste-t-il le « parent pauvre » par rapport aux autres risques (très liés au cœur d'activité) ?

L'un des nos problèmes, cela concerne la hiérarchie, avec les directeurs. C'est très politique, ils sont responsables des risques mais ont une vision et un intérêt très variable sur le sujet. Sur la production sur la monétique ou sur les RH cela fonctionne bien mais sur le marketing c'est par exemple bien plus compliqué. C'est un problème car la défaillance sur la connaissance client est à la base de nombreux risques opérationnels.
Nous avons une organisation de la banque en filière, cela tue la vision globale sur les risques opérationnels : on regarde les risques mais ce n'est pas le problème.
Le problème c'est quand on est sur des processus non formalisés, ce qui arrive encore souvent. Il nous faut un « organisateur » avant tout sur les risques opérationnels. Nous sommes 25 dans le groupe sur la gestion de la filière, à se battre pour que le risque opérationnel ce ne soit pas qu'une vision ex post. Il faut voir la logique financière mais aussi la logique commerciale sur les moyens de paiement par exemple. =>c'est avoir la vision client avant tout. Pour beaucoup de métiers, aucun lien n'est fait avec les risques opérationnels et la pratique du métier. Le risque opérationnels dans les comités nouveaux produits c'est assimilé et réduit au risque image. Or le problème du risque opérationnel est qu'il est rapidement stratégique : c'est un paradoxe, lorsque c'est valorisé en interne cela devient stratégique et

on en parle plus car il y a des vétos ou alors cela reste un sujet technique pas pris en compte à sa juste valeur au regard des risques que l'on encourt vraiment.
Nous avons une présence et des relais dans les différents métiers et fonctions mais notre direction comprend des profils variés : l'audit, le marketing, les responsables risques op des différentes caisses. Un adjoint direction des risques de manière plus globale. Des profils MOA pour la partie outil et des anciens consultants risques opérationnels.
Notre quotidien nous pèse trop. On passe beaucoup de temps à chercher des chiffres et on fait des kilomètres de power point pour expliquer et justifier sans cesse. Cela devient dur d'avoir du recul et d'être en dehors de l'approche opérationnelle. Traiter des sujets de fond est difficile dans ce contexte et on a parfois l'impression que notre travail ne tient pas la route.
Nous sommes sur des postes qui demandent beaucoup d'abstractions, de schémas et de représentations. C'est l'un des postes qui demande le plus de vision de l'organisation. Il y a un vrai enjeu de capitalisation des connaissances et de maturité.
=>Sur les profils qui alimentent cette démarche, s'il y a une erreur de casting, ils partent vite.
Il y a un vrai sujet de crédibilité, comme nous sommes les parents pauvres, il faut être animé par autre chose que la recherche de reconnaissance. Par exemple, le contrôle n'est pas toujours valorisé, et n'a pas forcément les moyens nécessaires, cela peut démotiver et c'est un moyen de faire le tri.
On peut être bon sur son métier mais passer à côté des choses. Rien que sur le PCA, c'est dur de vendre le lien avec les risques opérationnels en interne.

Risques opérationnels : quelles confusions en pratique sur la notion et entre les différentes fonctions qui en traitent

- **Risque opérationnel et qualité :**

Il y a un lien entre risque opérationnel et qualité dans certains cas oui. En matière de prestation de service, en SI, on est tout de suite dans de la qualité. Sur les réclamations clients c'est évidemment complètement imbriqué. Dans ces cas là on fait souvent du risque opérationnel sans le savoir mais on peine à capter rapidement la problématique vis-à-vis des clients.
On retrouve quand même des indicateurs prédictifs de risque opérationnel : sur la fiabilité, tourné qualité. Il faudrait élargir cette logique aux autres métiers. Alors cela peut être efficace. Sur les SI, sur les prestataires quand on parle de risque, oui on fait de la qualité.
Cela n'est pas utilisé partout, sur le crédit par exemple, c'est topé autrement, sur la notation on part tout de suite sur du contentieux par exemple. C'est une autre logique de veille et de vigilance.

- **Lien entre risque opérationnel et GRH :**

Le fait d'être CRO n'est pas dans les fiches. Ce n'est pas dans les objectifs ni dans les fiches de poste et cela peut constituer un frein. C'est notre plus grosse difficulté. Pour que cela marche il faut officialiser les choses. Il faut challenger les métiers en termes d'objectifs et de moyens. C'est dur quand cela se chevauche entre leurs objectifs métiers et les enjeux risques opérationnels. Quand on agrège les sujets de contrôle permanent et les enjeux SI, qualité : le contrôle interne cela peut faire gagner du temps. C'est une vraie préoccupation aujourd'hui dans des banques où l'on cherche à réduire les effectifs, dans des modèles de cost killing où l'on réduit les coûts, où l'on se préoccupe avant tout des coefficients d'exploitation.
La fonction n'est pas non plus toujours valorisée en interne. C'est un problème de recrutement, de fidélisation des équipes sur le sujet.
A cela s'ajoute le fait que souvent personne ne comprend l'intérêt des bases d'incidents et des pertes, des cartographies. C'est un travail pharaonique et coûteux pour modéliser des choses or ce n'est pas modélisable. => Les scénarios, les situations extrêmes cela fait plaisir à certain, c'est un bel exercice intellectuel mais cela reste une vue de l'esprit car les cas de survenance extrême ne seront jamais celles auxquelles on s'attend.
La seule vertu de nos démarches, c'est l'insertion opérationnelle, avoir des exigences minimales, répondre aux standards mais comme cela reste non attractif il y a peu de sachants. Alors on passe par

des prestataires. Mais trouver du personnel qualifié c'est dur à trouver, Les gens ne sont pas attirés par la complexité. Les profils sur le marché sont rares, il faut avoir eu des expériences dans les autres métiers, cela ne s'invente pas : en finance, en banque de détail, en SI.

- **Liens entre les contrôles :**

Il y a une vraie attente de guichet unique car quand on est dans les fonctions « métiers », on ne comprend pas tout. Sur les SI, sur la conformité, sur les risques opérationnels, sur le PCA il y a une confusion. Même les métiers dédiés entre eux ne comprennent pas tout, sur la correspondance entre conformité et contrôle interne par exemple. Sans parler des liens entre contrôle de gestion et les autres contrôles…
L'idée c'est de décrire les dispositifs où chacun a une part de responsabilité, une tâche à accomplir. Un contributeur peut faire à la fois du contrôle permanent, du risque opérationnel et de la cartographie et de la conformité. Le contrôle c'est parfois du multi-tasking.
Dans un même métier, on peut décliner le contrôle sur différents niveaux, c'est un problème de parler de vision globale si les filières sont séparées (ce qui se comprend) mais si elles ne communiquent ni n'interagissent pas entre elles.

Qu'est ce que la culture du risque opérationnel pour vous ?

- **Dénombrent / discernement :**

Sur les bases de données d'incidents et de pertes on retrouve cette double difficulté constamment, aujourd'hui, l'objectif est de centraliser les choses et d'incrémenter les pertes. On est parfois frustré, en direction générale de voir que le travaille consiste pou beaucoup à engranger les pertes.
Il y a deux questions à se poser :
-on constate les pertes, mais qu'en fait-on ? Discerne-t-on vraiment les problèmes dans la cartographie, les cartographies (locales, des risques majeurs)
-Réaliser des projections futures, est-ce que cela aide ?
Mais les vraies questions à se poser sont : quelles stratégies sur les risques opérationnels ? On perd x millions d'euros par an. Si l'on perd 50 millions au titre du risque opérationnel mais que c'est sous-estimé de 10 millions d'euros cela fait x % de PNB, cela affecte dans quelle proportion notre RBE (résultat brut d'exploitation).
Le vrai sujet c'est de faire un plan d'action sur les filières, au niveau groupe a fortiori, même si cela peut sembler plus dur.
Le problème sur les SI par exemple, ce sont les normes et leurs détails, la documentation irriguent-elle l'ensemble des réseaux ? Et ce de manière efficace ? Nous n'avons pas les réponses pertinentes sur le sujet aujourd'hui, on ne voit pas clairement émerger des réponses.

- **Industrialisation :**

Cela a été notre cas. Mais le problème reste que fait-on ? Dès que l'on fait un plan d'action cela devient lourd, sur le juridique, sur les SI plus en termes d'objectifs…ainsi que comment mesurer l'efficacité de ces plans d'action en termes de réduction de x millions de charges ? Voilà très rapidement quelques-unes de nos difficultés.

Le risque opérationnel est-il un enjeu de contrôle budgétaire et de gestion des coûts ?

- **Coût et performances cachées :**

C'est vraiment le sujet, il faudrait faire un benchmark entre les banques à ce sujet. Aller au-delà de nos simples mesures : comment cela affecte notre PNB, combien il faut provisionner et combien de CA il faut faire pour rattraper nos pertes opérationnelles.

Il faut mesurer l'impact sur le RBE (Résultat Brut d'Exploitation) de ces coûts dissimulés de risque et apostropher un directeur, un président de caisse régionale sur la logique RBE : le risque opérationnel c'est x % du RBE et x % des dossiers de prêts : toute suite on mettrait les choses en perspectives.
On constate ex post mais on voit la déperdition et le nombre de contrats affectés, c'est une première base pour se comparer dans la durée et voir le chemin parcouru ou si l'on fait du surplace ? C'est un vrai enjeu dans nos contextes de gouvernance où l'on cherche à réduire les coefficients d'exploitation. Mais en pratique cela rencontre encore peu d'échos des directeurs. Si l'on vendrait le risque comme un coût caché cela aurait probablement un vrai écho.
Par exemple : pour le risque frontière du crédit : on ne prend pas la bonne garantie, on est défaillant, au lieu de se retourner contre son assurance, ne se retourne pas et passe en perte car l'on ne s'est pas couvert correctement.

- **Lien risque opérationnel / contrôle de gestion :**

C'est un sujet à la fois de pilotage et de contrôle de gestion. Le problème c'est d'avoir un bon contrôle de gestion. Car cela change en permanence, Et il faudrait pouvoir faire le lien entre ce contrôle de gestion et les logiques de plans et d'actions stratégiques.

- **Le vrai sujet est-il la maturité du contrôle de gestion ?**

Non car il y aura toujours la vision erreur humaine et défaillance qui est au centre du risque opérationnel. Cela ne peut pas être capté par la logique de contrôle de gestion. On ne remonte pas suffisamment la problématique des causes, la chaine causale doit être bonne et clairement explicitée, c'est une plus grande difficulté, plus englobante pour le risque opérationnel.

Qu'est ce que la responsabilité face au risque ? Quand a-t-elle lieu ? Sur quoi peut-on jouer pour la rendre effective face au risque?

L'un de nos problèmes c'est que le risque opérationnel et son contrôle, c'est encore vécu comme une sanction. Il faut le déclarer au titre de l'article 17 ter.
Le problème de la responsabilité, est parfois occulté car on avance l'argument du « coup de pas de chance » quand une perte importante survient. C'est pris comme un problème de management et de gestion là où cela devrait être pris comme un problème de processus. Cela implique forcément des sujets de responsabilité.

Existe-t-il un besoin et manque de « guidelines », de bonnes pratiques quant aux normes de contrôle des risques opérationnels ?

La vision globale est mal comprise, même au sein des directions des risques dont on manque souvent du recul (peut-être aussi du temps) nécessaire pour y réfléchir, la penser et voir en quoi elle concerne nos métiers. Il faut aussi prendre en compte le fait qu'on reste bien le parent pauvre : on est sous-dimensionné : nous sommes une équipe de 11 là où ils sont 50 pour les marchés et le crédit.
L'audit interne nous l'a dit, sa recommandation était : « il faut s'assurer que les risques opérationnels disposent des moyens suffisant pour assurer leur mission ».
Quand on gère les risques concernant 3500 collaborateurs avec un responsable risque à temps partiel sur le PCA en priorité et sur les autres risques opérationnels en plus, cela devient dur de bien avancer, alors la vision globale, c'est quelques chose de très lointain. =>c'est pour cela qu'il faudrait davantage s'appuyer sur le lien avec le contrôle permanent.
Sur le PCA on n'y arrive pas non plus, car les filières sont séparées. Le PCA est dans la conformité en centrale alors que c'est aussi du risque opérationnel. Le lien serait essentiel alors que chacun vit sa vie.
On a lancé une campagne pour intégrer le PCA dans les dispositifs risques opérationnels. Pourquoi ? Le PCA est un dispositif DMR, actionné quand il y a une crise et il obéit à des méthodes claires, à de tests et à une documentation précise. C'est un sujet de risque intégrant les aspects techniques, SI, humains. On a intégré le PCA dans le dispositif de cartographie des risques opérationnels. Dans la

partie maîtrise des risques et protection, mais cela n'a pas été compris à la base. Pour beaucoup ce n'était pas vu comme étant dans la logique risques opérationnel. C'est une logique administrative pour certains, on fait de la sécurité, si l'on a jamais eu d'accident on ne comprend pas.
Par exemple pour le pôle Asset Management, le PCA c'est quelque chose que l'on fait dans une logique bureaucratique, c'est géré par la norme car il faut bien le faire mais c'est très éloigné de leurs préoccupations. Une fois que l'on est dedans, on comprend la difficulté. Vivre le sujet de risque dans une vision obligatoire c'est une erreur car on ne voit pas le volet « entrainement » : ce n'est pas que du documentaire de faire du risque opérationnel en SI. Mais souvent si ce n'est pas du business il n'y a pas de réelle mise en œuvre.

- **Chiffrage**

Pour la logique « perte d'exploitation » associée au risque, on n'y arrive pas, on n'a jamais chiffré réellement certains risques. Quand on fait des tentatives on se rend bien compte que quand il n'y a pas de chiffrage on n'est pas entendu. Quand il y a des chiffres c'est le début des débats. Cela donne lieu à des critiques et à toutes les interprétations possibles en interne.
Quand on remonte les filières, par la chaine informatique, sur par exemple la chaine de crédit, on tombe déjà sur des chiffres en PNB, on y arrive presque. On a tenté d'instaurer des règles identiques par caisse, mais on a perdu beaucoup de temps sur cela.
Si l'on a la logique stratégique : dans le plan stratégique on dit ce que l'on doit avoir comme limite de perte opérationnel, le manque à gagner maximum et le réalisé…là cela devient efficace.
L'une des difficultés qui explique que cela est chronophage est qu'il faut faire soi-même ces chiffrages et analyses (alors que cela devrait venir des métiers) car comme cela les chiffres sont indiscutables.
Sur les problèmes de SI et sur la partie assurance, on peut avoir recours au contrôle de gestion mais ce sont les deux seuls cas où l'on y arrive. On pourrait le faire, on a tout en central : les sachants, les experts et les chiffres au niveau du groupe. Mais on n'y arrive pas, on a du mal à être rejoint dans cette démarche. Cela devient illusoire, jamais à un moment donné on utilise les données pour aider à piloter le risque ou à gérer une crise. On manque d'aider pour être valorisé : soit c'est une logique informationnelle, soit c'est une logique technique. On a par exemple eu un directeur qui a tout fait, a tout mis en œuvre mais qui a oublié le paramètre humain dans son PCA…
On a beau leur faire comprendre que c'est un mal nécessaire et montré à l'ACP que l'on a bien fait les démarches, cela reste un chantier dont on ne voit pas le bout.
On retrouve une vraie difficulté de consolidation et de restitution des analyses consolidées : on refait 10 fois les slides avant de les présenter en comité pour éviter le risque du « sur le risque opérationnel on présente ce qu'on veut ».
Souvent on affiche peu ses pertes quand on est dans les métiers. Il y a de la dissimulation mais personne pour faire ce genre de réflexion. Il n'y a que les missions sur place qui sont efficaces car le déclaratif reste un problème.
On est souvent aussi formaté dans la méthodologie dans les métiers mais ça n'empêche pas pour autant le manque de cohérence des contrôles plus le fait que les thèmes soient parfois imposés : on voir des recommandations quelque soient les faiblesses, les risques.
On manque encore trop de sujets concrets, de constats sur ce que l'on fait, pour certains le risque c'est uniquement une vision « restriction des moyens ».

- ⇨ Un vrai levier consiste à imposer/mettre en exergue un résultat qui ne soit pas bon : mais apparemment on est encore trop riche dans les banques car cela n'est pas une priorité si l'on perd quelques dizaines de millions sur plus de 6 milliards de résultat, on est loin des vrais soucis.

On a rien compris à la crise, on est confrontés rapidement aux problèmes mais on en reparlera encore dans des années car on est encore sur un matelas de sécurité confortable. Il y a un effet ciseau sur le PNB : réduction des résultats et hausse des coûts, les marges sont grignotées peu à peu.
Mais c'est un problème de pilotage, nos dirigeants ne pilotent pas. On est sur du court terme, sur des sujets de positionnement politique des managers qui changent souvent de place, or il faut plusieurs années pour faire bouger une banque sur des sujets et cela suppose un peu de stabilité.

Quelles sont les difficultés d'interprétations du risque opérationnel dans la réglementation ? Marges de manœuvre ?

On a empilé un ensemble de choses en matière de contrôle car l'on n'est pas à maturité sur les sujets. Le contrôle permanent a la vision la plus proche mais il est souvent mal positionné.
Pour les recommandations de l'audit et de l'IG, c'est comme pour l'ACP : l'égarement c'est de refaire sans cesse des recommandations. Depuis 2009 il n'y a aucune avancée sur les vrais sujets. On pense souvent que l'outil est génial, on pense que l'outil va « gérer le risque », or le risque et sa gestion c'est juste de l'humain ; On est dans l'illusion des outils.
Il faut aussi admettre que l'on nous fait souvent des recommandations théoriques, par exemple : « il nous faut une cartographie unique des risques » nous a demande le régulateur.
La vision normative est tronquée, elle est le fait de théoriciens. Nous ne somme pas dans une logique de gestion avec ces approches.

-Qu'est ce qu'un contrôle qui a du sens par rapport au risque opérationnel ?

Quand on a un risque dans la cartographie alors on lance un contrôle mais cela se fait entièrement dans cette logique de syndrome de stockholm.
Il y a une dichotomie : entre les dispositifs où il y a une inefficience globale : ils sont plus ou moins bien suivis. 50 % du contrôle permanent n'est pas efficient, pas pertinent. On est dans le « rêve » sur le contrôle : si l'on fait une cartographie « béton » sur les 10 premiers risques et que l'on y déploie de vrais contrôles qui permettent de constater les risques et les vraies défaillances avec suffisamment de garanties, alors cela a du sens. Il faut aller vers des contrôles sur les vraies zones de sensibilité.
Par exemple sur la fraude ou sur l'archivage, il faudrait partir des 10 risques majeurs. Et avoir 10-20 contrôles ciblés. La bonne solution pour réduire ces risques opérationnels est donc de se baser sur le contrôle permanent.
Nous avions un DG qui y voyait l'intérêt, mais cela a changé donc il faut tout refaire. Quand on en parle en local, ils nous confirment qu'ils s'y retrouvent, on peut dialoguer.

Qu'est ce qu'un contrôle interne cohérent face au risque?

L'un des problèmes est que nos collègues des crédits et marchés, ne sont pas toujours au courant des risques opérationnels. On reste sur des discussions de type « qu'est ce que le niveau 1 et le niveau 2 de contrôle ? »
La banque vivrait aussi mieux avec de vrais organisateurs, capables de communiquer et d'organiser le sujet.
On passe notre temps à communiquer sur des éléments consolidés, auprès des métiers et des dirigeants. Il y a plusieurs discours : un discours de traduction sur les états Corep, c'est classique. Il faut adapter le fond des analyses en général selon les différents niveaux de nos interlocuteurs. On se rend alors compte que beaucoup de dirigeants ne savent pas qu'ils perdent tant sur leurs périmètres.
En plus de cela, c'est souvent mal vécu, c'est assimilé à une faute, on renvoie la balle sur le voisin.
Il y a une vraie stratégie de communication, d'autant plus forte que l'on a la nécessité d'être très intégré dans la filière risque.
Même avec des experts pointus, sans la communication on n'avance pas. A une époque, nous centralisions les mails sur les sujets risques opérationnels, on ne faisait plus que ça. On n'était plus dans la politique de risque, on perdait le sens de l'action et la vision globale surtout.
Aujourd'hui, nous tentons d'avoir une journée par trimestre dédiée à l'animation de la filière avec des échanges. Cela reste épuisant car il faut beaucoup de pédagogie. Quand on voit la taille du groupe et sa jeunesse (2009) nous sommes noyés sous les nombreux évènements.
Quand on communique sur les risques opérationnels, on commence toujours par un préambule sur une note de 30 pages, qui rappelle aux dirigeants les éléments de contexte et le détail de l'analyse, qu'ils puissent s'approprier le sujet et se poser des questions en local car ils n'ont pas la même vision. On

doit faire attention à éviter la défiance possible en central des dirigeants face à ces sujets venant du « réglementaire » en premier lieu.
L'un des problèmes est quand même que l'on reste dans la critique du contenu et pas dans l'analytique. C'est un sujet de traduction, il nous faut donner toutes les clés d'analyse. Notre vision est alors de pouvoir travailler sur des notions de stocks, de flux, cerner le sujet par d'autres approches.

Créativité et design du contrôle ? Est-ce le vrai sujet pour cerner le risque opérationnel?

C'est complètement un sujet de créativité, quand on constate un risque, un contrôle pourrait très bien n'être que temporaire.
Il faut avoir une vision risque avant, la créativité est là dès lors qu'on a une maîtrise clair du sujet. On ira plus finement dans le détail, on cherchera sans cesse à affiner l'analyse et à être pertinent.
Il faut aussi avoir une revue régulière des contrôles : contrôler des choses différentes, mesurer le rôle des contrôles et la progression dans le parcours du contrôle dans le temps.
Cela reste flou pour l'audit et le contrôle interne : ils ne comprennent pas toujours cette logique. C'est un point important : le contrôle permanent est trop pris par son travail et l'audit n'a jamais une prise effective complète sur ces sujets.

Contrôle des risques opérationnels et rapport à la réglementation prudentielle, rapport régulateur-entité.

L'ACP a des guidelines, mais elle n'est pas sur les vrais sujets. Elle est à des années lumières de la réalité des choses. Elle est toujours sur des schémas qui ne sont pas adaptés à la banque et aux opérationnels. On manque de guidelines et on n'arrive pas à mettre en place les recommandations nombreuses que l'on a.

Il n'y a aucun groupe de travail sur le risque opérationnel sur la place. Il y en a eu mais cela n'est plus le cas. On est perdu et on manque de recul sur le sujet, mais on se précipite tous dans les méthodes avancées…
Le 97-02, l'article 17ter de mai 2009 sur les incidents significatifs : cela nous a fait du travail, l'ACP a été efficace chez nous mais elle n'a jamais saisi la balle pour nous demander telle ou telle chose qui nous aurait aidé à nous améliorer. On reste dans la logique administrative lourde.
A contrario, l'ACP nous surprend parfois, elle est allée voir les 70 établissements du groupe pour travailler sur l'ensemble de nos seuils de risque dans le cadre du 97-02. Elle a tout synthétisé, même sur le rapprochement entre les articles 42 et 43, cela a été un travail titanesque qui aurait pu être très utile. Mais cela n'a jamais resservi dans leurs recommandations alors qu'il y avait un à deux contrôleurs ACP à temps plein pendant plusieurs mois.
Par exemple pour la fraude on se doute qu'il y a un problème, tout le monde l'écrit et marque ses bonnes intentions mais le passage à l'acte est plus problématique. On s'attend à une augmentation de la fraude mais on reste passif. Sur les fraudes sur les virements on travaille dessus mais on s'épuise réellement pour les faire redescendre.
Il n'y a pas que le fait de constituer des chiffres, en soi c'est un moyen, mais il n'y a qu'un intérêt intellectuel pour le sujet qui peut faire bouger les choses. Sinon un tel ou un tel se cantonne à relever les compteurs avec l'aide de cabinets mais les sources du risque restent là et avec les changements de dirigeants il faut tout recommencer. Pour eux, le risque n'est pas toujours dans la réalité des préoccupations.
Il n'y a pas de culture du risque opérationnel, même sur la notion de risque en général. Les métiers sont dans d'autres logiques.
Il y a aussi le problème du positionnement des directions des risques. Le rattachement au président du directoire est obligatoire, si l'on dépend su secrétariat général c'est inutile.

Entretien EC-45 - Contrôleur des assurances, autorité de régulation, mars 2013

-Parcours, positionnement et expérience de l'interviewé sur la thématique risque opérationnel de l'interviewé

Parcours de juriste pendant 10 ans en tant qu'avocat puis en tant que juriste d'entreprise. Contrôleur des pratiques commerciales au sein de l'autorité de régulation du secteur financier.

-Le risque opérationnel est-il pour vous un risque subi / diffus ?
-Le risque opérationnel reste-t-il le « parent pauvre » par rapport aux autres risques (très liés au cœur d'activité) ?

Les collaborateurs ont encore peu de sensibilité au pilier II en assurance. Peut-être plus en banque, cela se ressent sur la thématique du risque opérationnel.
Le risque opérationnel on en parle encore trop peu aux opérationnels. Cela leur parle peu. C'est la preuve qu'on travaille encore en silo dans les établissements financiers. C'est même parfois une forme d'agression pour eux quand on évoque le sujet. Ils ne voient pas pourquoi on vient s'occuper de cela, où imagine qu'on les perçoit comme une source de risque.

Quelle compréhension des politiques de maîtrise des risques opérationnels (freins et leviers) ?

La cartographie des risques opérationnels : si cela n'est pas suivi des faits cela a peu d'intérêt, cela doit donner lieu à un vrai travail de suivi pour les directions. Il doit y avoir des démarches permettant de quantifier, de vraies méthodologies et une analyse détaillée : pour quantifier le risque juridique par exemple ce n'est pas évident.
On est tous d'accord qu'il faut des outils de pilotage, une vraie maîtrise des risques. Cela doit être fait par le métier, alors c'est satisfaisant. Mais souvent cela reste limité : on se cache derrière l'outil, or on s'est battu pour que la gestion des risques cela ne soit pas que les cartographies…
Dans certaines entreprises cela donne plus de 1000 risques avec l'ensemble des déclinaisons, et plus de 30 collaborateurs à temps plein sur le sujet. Quand tout cela a été lancé, il n'y a pas eu de remise en question, on a eu beaucoup recours à des prestataires extérieurs et résultat : on est dans un travail conformiste aujourd'hui…

Risques opérationnels : quelles confusions en pratique sur la notion et entre les différentes fonctions qui en traitent

Cela concerne plusieurs thématiques :
-Remontée incidents :
Le problème c'est de faire remonter des incidents. Mais il ne faut pas s'arrêter à cela : s'il n'y a rien au niveau du traitement… On n'imagine même pas ce qui peut se faire. Sur l'analyse et le traitement des problèmes les gens préfèrent ne pas avoir d'idée pour ne pas avoir de problème.
-Confusion
Par exemple le risque pénal : c'est un risque fort, et c'est typique dans les cartographies il y a des confusions régulières, on a beaucoup d'informations, une surcharge même…

Qu'est ce que la culture du risque opérationnel pour vous ?

Le risque opérationnel c'est de la sensibilisation et de la formation, plus que des outils coûteux, longs à mettre en œuvre. Donc le nombre d'acteurs importe moins.

L'animation de la filière risque opérationnel suppose d'avoir quelqu'un de haut niveau, qui a accès à tout le monde. Il faut quelqu'un avec un haut niveau de sensibilité au sujet, pas quelqu'un de lambda, c'est la même problématique pour la filière conformité et pour l'audit interne où le travail réalisé est parfois peu connu. Dans certaines entités (BNP, SG) ils sont nombreux, bons sur la technique et pointus, alors cela avance et progresse.

Expertise, vision globale :
Il y a beaucoup de difficultés à dépasser pour vraiment avancer dans les filières risques : éviter la réunionite, ne pas faire que de la présence et s'écouter parler, même quand on est bon. C'est souvent interminable et la filière n'avance pas.
Ce qui fait changer les entreprises : ce n'est pas tellement les pertes financières, mais surtout le risque d'image et de réputation associé à un risque opérationnel, il y a une vraie peur des entreprises à ce sujet. Cela permet d'avoir des investissements dans de bonnes équipes mais souvent après la catastrophe.
Parfois on positionne des gens qui n'y connaissent rien (un biologiste venu dans la finance comme responsable du contrôle) : tout est à refaire car ce n'est pas leur sujet même avec de la bonne volonté.
Syndrome de Stockholm :
On fait essentiellement du risk management pour le régulateur c'est certain, parfois on y est sensible pour autant, c'est la culture d'entreprise qui fait tout en la matière. Là où certains sont efficaces d'autres sont malhonnêtes. Ils se cachent derrière le doute et le fait qu'on cherche l'interprétation pour faire comprendre qu'ils n'ont rien à se reprocher.
Ils estiment qu'ils sont en responsabilité à partir du moment où ils ont réalisé un travail pour se couvrir, qu'il y a eu des contrôles.

Existe-t-il un besoin et manque de « guidelines », de bonnes pratiques quant aux normes de contrôle des risques opérationnels ?

Sur la mise en œuvre des dispositifs prudentiels, beaucoup veulent bien faire, mais ils sont dans l'attentisme quand il n'y a pas de contrainte réglementaire.
Ils sont à l'écoute le plus souvent, notamment de ce qu'il faut faire, des best practices venant des cabinets (BCG, Ernst & Young)
Des guidelines émanant de l'ACP serait attendu, cela pourrait avoir un intérêt, il y a eu un document émanant de l'ACAM à l'époque sur le contrôle interne, c'était un ovni, car l'ACAM n'a pas à se prononcer et elle ne l'a jamais fait sur le risque opérationnel. Elle précisait cependant que c'était peu engageant.

-Quelles sont les difficultés d'interprétations du risque opérationnel dans la réglementation ? Marges de manœuvre ? -Contrôle des risques opérationnels et rapport à la réglementation prudentielle, rapport régulateur-entité.

L'ACP est l'autorité de tutelle, elle n'a pas le droit de conseiller les entreprises. De plus les gens y ont peur de leur ombre, alors ils ne se mouillent pas, certains trouvent ça mesquin.
Quand en contrôle les collaborateurs nous demandent « on fait quoi ? ». On peut les aider une fois leurs choix faits mais on doit rester neutre avant tout. Il ne faut pas se mouiller, ce serait gênant après de réaliser des contrôles. Quand on a envie de bien faire mais que l'on n'a pas le droit de se mouiller, alors on ne prend pas position. Les différents collaborateurs attendent souvent une réponse même si parfois pour nous certaines questions sont évidentes. Après il y a des entreprises où les gens sont à l'écoute et celles où ils sont sur la défensive ou font de la résistance car développer ces démarches, c'est coûteux.
Tant que solvabilité II n'est pas clairement en vigueur, les entreprises avancent lentement.
Pour 97-02 en banque cela a bien progressé, heureusement qu'il y a eu cela, cela aide quand même.

L'ACP aide un minimum mais nous n'avons pas l'obligation de proposer une organisation ou un modèle organisationnel. Cela freine quand ce n'est pas une obligation. C'est quand même le principal levier face au risque, mais tant qu'il n'y a pas de risque de sanction c'est balbutiant.

-Qu'est ce qu'un contrôle qui a du sens par rapport au risque opérationnel ? -Qu'est ce qu'un contrôle interne cohérent face au risque?

Les démarches ont toujours du sens car il faut sensibiliser quoi qu'il arrive. Sans contrôle, on est dans l'impunité.
Même sans sanction, cela permet de faire évoluer les choses du tout au tout.
L'utilité du contrôle : dans des entreprises comme Swiss Life etc. c'est utile cela ouvre les yeux sur des dysfonctionnements jamais vu sans nous. Dans beaucoup de cas on retrouve ces similitudes (Allianz, CASA, CNP).
Il faut faire les choses de manière coopérative et quand c'est trop grave être cependant intraitable.
Le sentiment d'impunité sur le non ou peu réglementé est institutionnalisé. Cela pose problème quand on se demande juste si la boite est solvable, si le risque est provisionné. On ne peut pas laisser de côté les sujets où le client est lésé (sur les contrats en déshérence, quand le bénéficiaire est décédé sans jamais avoir touché l'argent des contrats d'assurance vie etc.).Il y a de l'impunité et de l'hypocrisie dans certaines pratiques commerciales. Pour certains les clients ne sont que des numéros.
Le tout dans le contrôle est de ne pas être broyé dans l'administratif, de faire juste ce qu'on demande.
Il y a aussi toujours le risque que les avancées réelles soient enterrées tôt ou tard. On en revient alors à une cartographie de façade. C'est autre chose que les cas où l'ensemble des contrôles sont pris au sérieux et qu'il y a une vraie approche conseil.
Sans faire peur à tout le monde, on peut être sympathique, confiant, sinon les opérationnels vont dissimuler des éléments.

Créativité et design du contrôle ? Est-ce le vrai sujet pour cerner le risque opérationnel?

-

-Qu'est ce que la responsabilité face au risque ? Quand a-t-elle lieu ? Sur quoi peut-on jouer pour la rendre effective face au risque

Parfois on pense que l'on est bon partout. On a en fait plus par peur pour sa crédibilité. On va sur des domaines connus en occultant les autres. On va tout le temps dans la même direction ou les mêmes services, en évitant soigneusement les endroits où l'on se doute qu'il y a le plus de risque, qu'il n y a pas de juriste ni de vrais économistes pour prendre du recul sur le sujet.
Le contrôle au final est « super encadré », la marge de manœuvre est faible, mais le fait de l'industrialisé est aussi positif : c'est mieux qu'un contrôle artisanal qui ne marche pas et qui serait peu clair. Cela peut être utile même si c'est rare sur certains contrôle (dans le juridique par exemple). C'est cependant une erreur de ne pas auditer les fonctions support. Pour les réseaux c'est souvent audité superficiellement car c'est complexe, et cela nécessite bien plus de contrôleurs, qui ne connaissent pas toujours la réglementation eux-mêmes.

Le risque opérationnel est-il un enjeu de contrôle budgétaire et de gestion des coûts ?

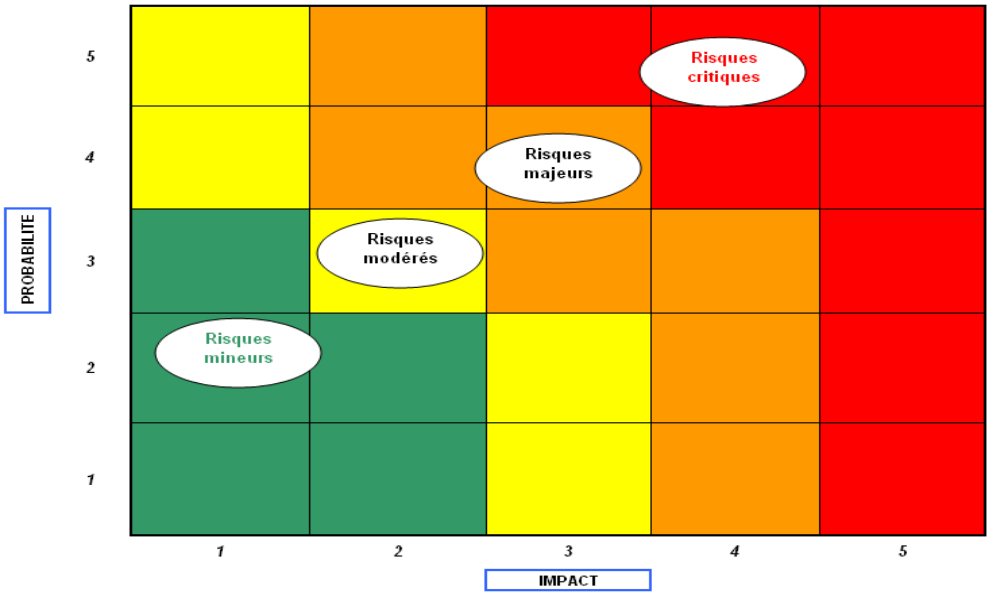
-

Annexe 12 – Outils et méthodes utilisées dans le déploiement des politiques de maîtrise des risques opérationnels

Afin d'identifier et de mesurer leurs risques, les assureurs et établissements bancaires ont recours à différents outils. Ce paragraphe présente les principaux outils utilisés par ces derniers (direction des risques). Nous présentons ci-après deux approches complémentaires d'un outil fréquemment utilisé pour la mesure du coût du risque et de son importance relative. La matrice de cotation des risques.

Les matrices de cotation des risques

Sous cette forme, la matrice de cotation du risque permet d'associer probabilité de survenance et niveau d'impact financier. Nous fournissons également des exemples récurrents dans les entreprises.
La représentation ci-après est une vision schématique permettant de positionner les risques par ordre de probabilité d'occurrence et de criticité (impact). La probabilité peut être exprimée en % ou en nombre d'occurrences dans une période de référence. L'impact peut recouvrer plusieurs ensembles : il peut s'agir de l'impact financier (coût faible / coût élevé), de l'impact médiatique (circonscrit / de grande ampleur), de l'impact en termes de priorité (tolérable / inacceptable), de confidentialité de l'enjeu (Usage restreint-interne / Confidentiel / Secret) etc.
On distingue ainsi les risques mineurs / modérés / majeurs / critiques, ces derniers correspondent aux situations suivantes :
-**risques mineurs** : il s'agit de risques très fréquents au faible coût financier pour l'entreprise.
Exemples : panne informatique de courte durée, erreur de saisie d'information et mauvaise facturation,
-**risques modérés :** ce type de risque également fréquent se caractérise déjà par une importance de son coût plus élevée,
Exemples : perte d'un client, panne informatique de plusieurs erreurs, grève d'une partie des salariés, recours d'un client mécontent,
-**risques majeurs** : des risques rares pouvant engendrer l'arrêt temporaire d'activité de l'entreprise ou remettre en cause sa solidité financière,
Exemples : incendie d'une partie des locaux, grève d'ampleur majeure empêchant de nombreux salariés de se rendre sur leur lieu de travail,
-**risques critiques** : des risques si fréquents ou si importants en termes d'impact matériel, humain ou financier qu'ils engendrent l'arrêt définitif d'activité pour l'entreprise,
Exemples : pertes financières récurrentes pour l'assureur, surendettement et défaut de liquidité engendrant la faillite de l'entreprise.



Survenance	Plusieurs fois par jour Ou Probabilité ≥ 50 %	Plusieurs fois par semaine Ou 25 % ≤ Probabilité < 50 %	Plusieurs fois par mois Ou 10 % ≤ Probabilité < 25 %	Plusieurs fois par an Ou 5% ≤ Probabilité < 10 %	Moins d'une fois par an Ou Probabilité < 5 %
Niveau	1 - Rare	2 - Faible	3 - Modérée	4 - Forte	5 - Très forte
Impact financier	≥ 0 € et < 10 000 €	≥ 10 000 € et < 1 millions d'€	≥ 1 millions d'€ et < 25 millions d'€	≥ 25 millions d'€ et < 100 millions d'€	≥ 100 millions d'€
Exemples	Dysfonctionnement de certaines applications informatiques, Article de presse au niveau local.	Interruption partielle des activités sur un site, Temps de traitement d'une opération simple augmenté de 50%, Article de presse au régional.	Dysfonctionnement majeur des applications informatiques, Article de presse ponctuel au niveau national.	Dommages matériels interrompant de manière partielle l'exploitation d'un site, Campagne de presse d'ampleur nationale.	Dommages matériels important (destruction/détérioration) d'un ou plusieurs sites, Campagne de presse et télévisée d'ampleur nationale.

La notion d'impact : il s'agit de l'ensemble des conséquences négatives associées à la survenance du risque, à savoir son coût financier, son coût humain, son coût en termes d'image et de réputation, le potentiel de désorganisation et de déstabilisation de l'entreprise. L'impact est élevé quand il dépasse de loin la capacité normale de l'entreprise à l'absorber ou qu'il implique pour cette dernière une compensation par réduction des coûts ou un programme de financement spécifique du risque.
La notion de probabilité : aussi appelé fréquence, il s'agit de la chance de survenir d'un risque dans un intervalle de temps donnée. Sur une année par exemple, combien de fois un risque de liquidité ou d'incendie pourra survenir. La probabilité est dite élevée lorsqu'un risque surviendra plusieurs dans une période de temps courte.

Le recours aux scénarios probabilistes

Issue des travaux de la Rand Corporation (1950's) ou encore de la Datar (1970's) et de la SEMA, la méthode des scénarios consiste en la description de plusieurs futurs possibles. Le scénario se définit comme un ensemble formé par la description d'une situation future et du cheminement des évènements qui permettent de passer de la situation origine à la situation future. Les scénarios sont construits grâce au recours à des méthodes d'experts (Delphi, matrices d'impacts croisés). La méthode des scénarios vise à déterminer quels sont les invariants (phénomènes supposés permanents jusqu'à l'horizon étudié), les tendances lourdes (mouvement affectant un phénomène sur longue période), les facteurs de changements (à peine perceptibles aujourd'hui, mais qui constitueront des tendances lourdes demain), les ruptures plus ou moins critiques, afin de décrire une situation future. On distingue alors les scénarios possibles, les scénarios réalisables, les scénarios souhaitables ou encore les scénarios tendanciels (correspondant à l'extrapolation de tendances), de référence (le plus probable), contrastés (extrapolation d'un thème volontairement extrême : une situation de crise liée à un risque majeur par exemple) ou encore d'anticipation.
La méthode des scénarios vise :
-à déceler quels sont les domaines à étudier en priorité (variables clés) par la mise en relation des variables caractérisant le système étudié.
-à déterminer à partir desdites variables clés dans l'organisation ou dans un secteur donné, quels sont les acteurs importants, leurs stratégies et les moyens en leur disposition pour résoudre une problématique, faire aboutir un projet…

-à décrire, par des scénarios, l'évolution du système étudié sur la base des évolutions les plus probables des variables clés ainsi que de jeux d'hypothèses sur les attitudes des acteurs.
« La méthode des scénarios est un outil clé pour représenter ce qui peut arriver à l'entreprise. Nous nous en servons pour sensibiliser le Top Management mais aussi les différents métiers. Il s'agit de faire parler plusieurs dirigeants de l'entreprise indépendamment sur les risques qui leur semblent importants puis de mettre en commun ces avis » nous confie un directeur des risques du secteur assurance.

La cartographie des risques où l'étude des futurs possibles

La réalisation d'une cartographie des risques est un processus de réflexion commun permettant de diagnostiquer les vulnérabilités de l'entreprise et de se représenter, pour chaque classe de risque, l'étendue des futurs possibles identifiés comme ayant un potentiel vraisemblable de survenance.
Établir une cartographie des risques répond à différents objectifs : répondre à l'obligation réglementaire de communiquer sur les risques (loi NRE, document de référence…), identifier et évaluer les risques liés à la non-conformité, réduire les risques opérationnels (sécurité, informatique…), élaborer le plan d'audit, identifier et piloter les couples risques/opportunités ou encore hiérarchiser les risques recensés et décider des mesures prioritaires (optimisation des ressources, définition du niveau raisonnable de prise de risque).
Au niveau de la méthodologie, la cartographie des risques peut être élaborée selon la double démarche Top-Down et Bottom-Up. On trouve ainsi des cartographies locales par périmètres (exemple : DRH, direction financière, direction commerciale) et une cartographie globale de l'entreprise. La cartographie des risques peut prendre différentes formes : permettre de classer les risques selon leur probabilité et leur impact (fréquence/ sévérité), selon leur nature (classe de risque), selon la part de chaque entité pour un risque (portefeuille de risques), mais également selon leur horizon (court, moyen, long terme).

Cartographie des risques par type d'activité, taux d'exposition au risque

	Fraude interne, externe	Risque de perte d'homme clé	Risque SI	Risque sur les processus (formalisation, implémentation, exécution)	Pertes opérationnelles
Activités Supports					
Finance, actuariat	74%	45 %	15%	40%	33%
Ressources Humaines	12%	18%	9%	12%	5%
Audit, organisation	21%	42%	63%	72%	7%
Activités opérationnelles					
Souscription	50%	20%	36%	72%	56%
Indemnisation	55%	11%	41%	11%	78%

Gestion-Services aux clients	10%	8%	40%	58%	23%

Cartographie des risques de type périmètrique :