Introduction

La notion de gestion des risques est loin d'être récente, elle remonte, en tant que sujet d'entreprise, aux années vingt avec l'avènement de travaux sur la manière de mieux contrôler l'organisation. Toutefois, il n'a vraiment été question de fonctions en lien avec la gestion des risques que dans les années cinquante-soixante avec l'avènement de chargés de gestion des assurances et des risques.

Le XXI^{e} siècle a véritablement consacré la fonction gestion des risques en tant qu'acteur clé de l'organisation. Les réglementations récentes sur la protection des données, la fraude, la corruption, le blanchiment d'argent ainsi que sur les risques prudentiels et financiers en ont fait une fonction voire un ensemble de fonctions dédiées au contrôle de l'organisation (contrôle interne, audit interne, risk management, conformité, sécurité financière, Hygiène-Sécurité-Environnement - HSE).

L'objet de cet ouvrage est de se centrer sur la fonction de gestion des risques (que nous appelons Fonction Risk Manager) en tant que fonction transverse à celles précitées. Le gestionnaire de risque (que nous appelons Risk Manager), proche de la direction générale, mais aussi des opérationnels et autres fonctions transverses (qualité, sécurité, projets, directions financière et comptable, direction commerciale, back-office, systèmes d'information, ressources humaines) est sûrement l'une des fonctions les plus transverses de l'entreprise.

Il paraît aujourd'hui difficile d'imaginer une organisation sans gestion des risques et enfin de compte il n'est souvent qu'une question de temps et de moyens avant qu'une direction générale ne se rende compte de la nécessité d'intégrer cette fonction.

Dans ce contexte transverse, le paradigme selon lequel la gestion des risques est l'affaire de tous est souvent repris. Cet ouvrage y souscrit et apporte sa contribution illustrée en insistant sur les savoir-faire techniques mais surtout relationnels que la fonction suppose. Il est essentiel à ce titre d'insister sur le rôle de la Fonction Risk Manager : rôle de fournisseur d'informations à la direction générale, rôle de coordinateur de ces informations, rôle d'assistance du management local, rôle d'alerte, de formateur, de sensibilisation, de pédagogie mais aussi de contrôle face aux risques internes et menaces externes que l'entreprise peut subir.

L'ouvrage insiste à la fois sur les notions fondamentales que les Risk Managers sont amenés à appréhender et contextualise la Fonction Risk Manager en revenant sur sa naissance dans les entreprises. Nous détaillons également l'activité des Risk Managers (que font les Risk Managers ? Quelles sont leurs relations avec la direction, les opérationnels et les autres fonctions ?), illustrons avec des exemples de terrain un ensemble de catégories de risques essentielles auxquelles ils sont confrontés dans leur activité et, sans prétendre à l'exhaustivité, les méthodes et outils clés qu'ils utilisent. Enfin, nous insistons sur sa place dans l'organisation tout en mettant en avant les compétences essentielles pour l'exercice de la fonction.

Par ses différents apports méthodologiques et pratiques, cet ouvrage vise à contribuer non seulement à la littérature importante sur la gestion des risques, mais aussi à apporter des clés de lecture sur l'actualité de la Fonction Risk Manager. De nombreuses questions y sont ainsi développées : la question de la diversité des risques à appréhender ; la question de ses relations avec ses commanditaires (direction générale, conseil d'administration, auditeurs externes et internes, directions métier) et de ses enjeux sous-jacents ; la problématique du (des) rôle(s) du Risk Manager (à quoi sert-il ?) et plus particulièrement de son rôle d'alerte et de communicant et du biais par lequel il l'exerce. Nous abordons également les enjeux relatifs à la formation et au suivi de carrière du Risk Manager.

Enfin, cet ouvrage envisage de manière longitudinale un ensemble de questionnements sur la Fonction Risk Manager en elle-même :

- La question de sa diversité.
- Jusqu'où faut-il aller entre une exigence forte de formalisme propre à cette fonction et l'enjeu essentiel de pragmatisme dans la déclinaison de plans d'action, d'outils, de préconisations ? Le Risk Manager est-

il davantage un poil à gratter/un empêcheur de tourner en rond ou un facilitateur dont le champ d'intervention est bien souvent plus tacite et progressif que par action rapide ?

- La question de la légitimité du Risk Manager pour asseoir son autorité. Quels leviers méthodologiques, organisationnels ou politiques dans l'organisation utiliser ? Doit-il être un expert technique ? Connaître l'entreprise ? Être un bon communicant ?

Le présent ouvrage apporte ainsi une contribution pragmatique faite de retours d'expérience mais aussi de synthèses de travaux académiques afin de cibler tant les professionnels de la gestion du risque que les étudiants désireux de se tourner vers les métiers de la filière risques.

Chapitre 1

Définition des notions mobilisées et contextualisation de la Fonction Risk Manager

Dans ce chapitre, nous présentons les notions mobilisées. Nous décrivons ensuite la naissance de la Fonction Risk Manager et cherchons à comprendre pourquoi, à un moment donné, les grandes entreprises françaises ont décidé de la mettre en place, montrons comment elle s'est constituée, a évolué jusqu'à aujourd'hui, identifions les acteurs de l'émergence et de l'évolution de la fonction. Nous interrogeons enfin la fonction en proposant une explication théorique de son émergence et en mettant en perspective ses évolutions futures.

Définition des notions mobilisées : risque, gestion des risques, Risk Manager

Le risque

Définition

La définition du risque fait l'objet d'un consensus : c'est « *un aléa dont la survenance prive un système d'une ressource et l'empêche*

d'atteindre ses objectifs » (Wibo, 2000). D'autres définitions peuvent être évoquées : « *Une situation dont l'occurrence est incertaine et dont la réalisation affecte les objectifs de l'entreprise qui le subit.* » (Barthélémy, 2000). « *Un danger, inconvénient plus ou moins probable auquel un individu, un acteur est exposé.* » (Larousse).

Une notion ancienne

La notion de risque est ancienne, ancrée dans la société et associée à une connotation de peur, de danger. Quand Beck (2001) affirme que notre monde est le premier à être confronté au risque suprême de la destruction de la vie sur la terre, de la fin de l'Humanité, Méric et al. (2009) rappellent que les Aztèques redoutaient le retour du Néant provoqué par l'arrêt de la course du soleil et ainsi l'ancrage du risque dans l'histoire de l'Humanité. Dans cet ouvrage, les auteurs rappellent que le mot français daterait du XVI^{e} siècle et que son étymologie serait liée à l'activité commerciale maritime (le risque que court une marchandise), avec comme postulat implicite, les conséquences néfastes de l'occurrence du risque. Laperche (2003) établit un lien entre le risque, expression du danger et la nécessité de le récompenser ou de le réduire.

La notion de risque n'est pas nouvelle dans les entreprises (Knight, 1921). Il est présent dans toute action, fait partie de l'univers des entrepreneurs (Schumpeter, 1926) ; il est inhérent à toute décision : « *Décider, c'est choisir, en univers incertain notamment, c'est prendre un risque en espérant que le choix s'avérera* a posteriori *judicieux.* » (Persais, 2003). Le risque est ainsi 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). 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.

Pour Beck (1986), le risque et son corollaire le coût du risque, sont à intégrer comme faisant partie des « effets induits latents » associés à toute activité économique. Ce coût du risque est à mettre en lien avec la notion de pari sur l'avenir. La prise de risque 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.

Dès 1921, Knight distingue le risque avéré (l'agent possède des informations concernant la probabilité de réalisation et les conséquences du risque potentiel (l'agent ne peut pas définir la liste des conséquences possibles d'un évènement ou ne peut pas déterminer de probabilité de réalisation des résultats identifiés comme dans l'assurance, avec la loi des grands nombres).

Pourtant, au début des années quatre-vingt-dix, la notion de risque reste floue : risque et danger, risque et incertitude (« *Aléa auquel on ne peut associer de probabilités objectives.* » Knight, 1921), sont souvent confondus. Malgré cela, il est devenu une variable centrale de la réflexion organisationnelle des entreprises. Le risque a-t-il changé ?

La gestion des risques

Définition

La gestion des risques est « *le processus appliqué tout au long d'un programme et qui regroupe des activités d'identification, d'estimation et de maîtrise des risques* » (Courtot, 1998). La démarche repose sur une phase d'analyse à partir de classes de risques (« *ensemble cohérent de risques quant à leur nature et aux responsabilités associées à leur management* ») par phase, cause, origine, fonctionnalités et par risques organisationnels et humains. Cela permet de distinguer les risques mineurs des risques majeurs, critiques et catastrophiques. La phase de maîtrise est l'« *ensemble des actions définies et conduites dans le but de réduire et de maintenir la gravité des risques à un seuil plus ou moins tolérable.* » Elle vise soit à lever, transférer ou atténuer le risque, soit à l'accepter sous sa forme résiduelle (part qui n'a pu être traitée après les contrôles et actions appropriées). Elle conduit à la mise en œuvre d'un suivi dans le but de maintenir ou d'améliorer la visibilité sur le risque et de s'assurer de l'application des plans d'action. Ce suivi, considéré comme un enjeu majeur, fait émerger la notion de culture du risque.

Une démarche en cinq étapes

Dans nos travaux (Aubry, 2005), nous avons décrit une démarche de gestion des risques divisée en cinq étapes, qu'il est important de rappeler. Elles seront détaillées dans la suite de l'ouvrage (chapitre 4).

Étape 1 - Élaboration d'une stratégie de définition des risques majeurs

L'entreprise commence par définir une stratégie de maîtrise des risques majeurs à partir de deux niveaux d'identification : les objectifs stratégiques ou les processus opérationnels de l'entreprise. Le deuxième niveau est privilégié par les entreprises souvent réticentes à « divulguer » leur stratégie ou par toutes celles qui se livrent à la « navigation à vue ». Il consiste pour la direction générale à visualiser régulièrement les grands risques majeurs permanents qui menacent la mission de l'entreprise, les quelques grands projets dont la dérive causerait un tort majeur à l'entreprise et les processus clés constituant *le business model* de l'entreprise.

Le *business model* de l'organisation est le premier dispositif utilisé par les entreprises. Il ne s'agit pas en soi d'un outil de gestion des risques mais c'est un prérequis permettant de procéder à leur analyse. Il présente les principaux processus de l'entreprise et met à sa disposition des éléments d'identification des risques à tous les niveaux.

Étape 2 - Identification des risques (passés, présents, émergents)

Deux méthodes sont possibles :

- La démarche descendante ou *top down* consiste à identifier et effectuer une première estimation des risques auprès des dirigeants (les membres du comité exécutif) et de leurs principaux responsables (directeurs métier-zone, directeurs fonctionnels, directeurs opérationnels, par exemple) puis à descendre vers les opérationnels.
- La démarche ascendante ou *bottom up* consiste à interroger les opérationnels les plus proches de l'activité puis les directeurs opérationnels ou fonctionnels.

L'identification des risques se fait par *interview via* des questionnaires, des ateliers, des entretiens individuels…) de chaque responsable stratégique et opérationnel et par l'utilisation de grilles (*best practices*). Les outils les plus libres (ateliers, entretiens individuels, *best practices*, comparaisons/*benchmarks*) sont privilégiés dans le cadre de la méthode *bottom up*. Ces outils sont par ailleurs l'occasion de faire travailler ensemble les membres du personnel et sont le point de départ de la diffusion d'une culture du risque au sein de l'entreprise.

Étape 3 - Évaluer, quantifier, prioriser ls risques et réalisation de cartographies de risques

Une fois les processus et les risques identifiés, l'entreprise élabore et met à jour une cartographie. Pour ce faire, elle évalue les risques en fonction de :

- L'impact (*gravity*) qu'ils pourraient avoir s'ils se matérialisaient. L'impact est la quantification de la perte engendrée par la réalisation du risque. Les niveaux d'impact changent selon les entreprises : échelle de 1 à 4 (faible, moyen/modéré, fort, très fort/catastrophique) ou de 1 à 9, par exemple. Les niveaux sont associés à des pertes financières engendrées (en euros, par exemple, ou en numéraire) ou des pertes d'exploitation (en journées de production).
- La probabilité de survenance appelée aussi l'occurrence (*probability*). La probabilité de survenance sont les « possibilités » de réalisation du risque. Les niveaux de probabilité sont variables selon les entreprises : échelle de 1 à 4 (rare, peu probable, possible, quasiment certain) ou de 1 à 9, par exemple. Les niveaux sont associés à une probabilité de réalisation (en pourcentage) et une fréquence (une fois par jour…). Le résultat de la combinaison, impact x probabilité, donne le poids du risque et donc son coût. Concrètement, la cartographie des risques prend la forme d'une matrice impact/probabilité. Elle est établie par branche, filiale, entité et au niveau global (*corporate*).

Elle donne une image synthétique des risques et de leur poids respectif. En effet, il semble essentiel compte tenu du contexte de chaque entreprise et son exposition aux risques, de tenir compte de l'importance relative de chaque risque. Ainsi, si le risque de conformité tend à avoir une importance majeure en banque, il est à relativiser dans d'autres secteurs d'activité tels que la grande distribution. Une cartographie permet de qualifier certains risques de stratégiques (probabilité faible/impact élevé) encore de transférables (probabilité moyenne/impact moyen), c'est-à-dire susceptibles d'être traités par l'assurance, donc externalisés tels que les risques d'incendies d'agences, de tempêtes, d'inondation ; d'autres risques sont appelés opérationnels (probabilité forte/impact faible), ces derniers regroupant tous les risques « mal connus » qui peuvent empêcher la réalisation des objectifs à court terme de l'entreprise et les risques récurrents dont les enjeux financiers sont importants tels que les risques clients, les risques liés au système d'information du type de facturation, les fraudes, la fiabilité du *reporting*…

Elle permet une hiérarchisation des risques analysés conduisant les dirigeants à se focaliser sur les risques majeurs (« *top ten* des risques » à gérer, par exemple) et sur les systèmes de contrôle interne adaptés.

Étape 4 - Identification des dispositifs de contrôle et définition de plans d'action

Une quatrième étape consiste à analyser les systèmes de contrôle interne : existe-t-il des dispositifs de contrôle ? De quels types sont-ils (procédures, chartes, formations, responsabilisation, assurances) ? Sont-ils efficaces, pertinents, fiables ?

La réponse à la deuxième série de questions se fait à partir de la mesure du risque résiduel : si le risque résiduel est trop élevé, cela signifie que le risque est sous-contrôlé ; s'il est faible, le risque est potentiellement sur-contrôlé. Dans les deux cas, les dispositifs de contrôle sont à revoir.

Les conclusions quant aux dispositifs de contrôle du risque permettent à l'entreprise de définir un ou des plans d'action (bénéfice/ressources à investir) destinés à améliorer la couverture des risques majeurs (action sur l'impact et/ou la probabilité). Ils sont mis en œuvre à travers trois types de dispositifs (Diard et Maurain, 2003) :

- Un dispositif d'ingénierie pour identifier les risques et repérer, à partir des items que l'entreprise a décidé d'analyser les bonnes pratiques de leur maîtrise.
- Un dispositif de déploiement pour mettre à disposition des opérationnels les bases d'une auto-évaluation de la maîtrise de leurs risques.
- Un dispositif d'audit pour évaluer sur le terrain impact et probabilité de survenance de chaque risque identifié dans le référentiel puis la pertinence et la fiabilité de la qualité des contrôles internes existants au regard des principes de contrôle de référence.

Les plans d'action sont diffusés *via* la responsabilisation et la mise en réseau. En face de chaque risque majeur est positionné un responsable chargé d'un plan d'action (également appelé le « propriétaire » du risque) : un réseau de responsabilités est ainsi mis en place. Pour chaque famille de risques, des experts sont choisis pour aider ces « propriétaires » de risque : un réseau de soutien est mis en place. Un comité de risques central chapeaute ces deux réseaux.

Ces outils donnent à la démarche de gestion des risques son caractère dynamique.

Étape 5 - Analyse, suivi, apprentissage des risques

Les actions font l'objet d'une analyse, d'un suivi et d'un apprentissage. L'analyse des résultats se fait en introduisant dans les tableaux de bord des indicateurs de suivi des actions mises en place et de mesure de maîtrise des risques mis sous contrôle. Les questions à renseigner sont le choix des indicateurs, leur fréquence, leur présentation et leur rattachement à un *processowner.*

Les résultats font ensuite l'objet d'une communication à la hiérarchie (conseil d'administration, direction générale, comité de direction, comités des risques, comité d'audit). La direction générale est informée de la qualité de la maîtrise des risques dans l'entreprise. Les enjeux de cette dernière étape sont la transparence vis-à-vis du management et des actionnaires - le climat de confiance - et la diffusion d'une culture du risque dans l'entreprise avec l'introduction d'une boucle d'apprentissage collectif.

L'analyse des résultats peut enfin donner lieu à la mise en place de retours d'expérience. Ils prennent la forme de mises à jour régulières du site de l'entreprise au fur et à mesure de la réalisation des plans d'action, d'échanges d'informations entre le terrain et les équipes de management *via* les bases de données ou encore de diffusion des meilleures pratiques accessibles à tous.

Ces outils donnent à la démarche de gestion des risques son caractère opérationnel.

Ces outils sont également nécessaires pour constituer une « mémoire du risque » en entreprise. L'un des objectifs d'une politique de maîtrise des risques consiste à fournir un degré de confiance suffisant sur la capacité de l'entreprise à anticiper ses risques. Cela vaut bien entendu pour les risques présents et futurs mais aussi, et cela peut être omis, pour des situations déjà rencontrées par les dirigeants, managers et opérationnels de l'organisation. L'enjeu n'est bien entendu pas d'enfermer la réflexion sur les risques au champ de ce qui est déjà connu, mais il consiste à ne pas occulter par principe ce qui fut traité et serait donc *a priori* « déjà sous contrôle », partant de l'idée préconçue que la foudre ne frapperait pas deux fois au même endroit.

« En comité des risques, on nous présente souvent ce qui ne va pas ou ce qui pourrait ne pas aller, mais on oublie souvent les situations dans lesquelles ces sujets avaient déjà été traités, débattus, résolus !… On

va même jusqu'à oublier que certains projets ont été mis en place suite à des incidents majeurs. »

« Bien avoir en tête des incidents passés permet de voir quand des équipes métiers relâchent l'attention. C'est quand on vous demande de retirer un moyen de maîtrise - des contrôles par exemple, jugés trop chronophages - au motif qu'on ne voit pas où est le risque, que les garde-fous sautent peu à peu. Il faut sans cesse réaffirmer les raisons ayant justifié de couvrir des incidents ou des risques, peut-être anciens, mais pouvant toujours menacer l'entreprise. »

Cependant, dans de nombreux cas, l'hypothèse d'un apprentissage organisationnel en matière de risque apparaît théorique.

Le manque de temps ne permet pas toujours de documenter suffisamment des incidents majeurs ou de capitaliser sur les retours d'expérience (lorsque ceux-ci sont réalisés) post-crise.

Le fait de penser que des incidents majeurs ne peuvent arriver qu'aux autres entreprises, qu'aux autres filiales dans un groupe, peut également amener l'entreprise à en oublier des situations à risques déjà connues. Cela vaut notamment pour des risques à faible probabilité voire à faible vraisemblance (risques terroristes, fraudes majeures, cas de fraude interne en bande organisée, cyberattaques d'ampleur majeure, etc.).

« Lors des revues des risques, on en arrive souvent à éluder tout ce qui s'inscrit dans un contexte spécifique pour ne retenir que le générique, cela vide de son sens l'exercice même de cartographie des risques. »

Peuvent enfin être évoqués le départ de « sachants », la mobilité en interne et notamment des équipes risques, audit et contrôle impliquant que la mémoire des incidents n'est pas conservée sur les fonctions dédiées, l'absence d'appropriation des historiques de pertes par les métiers, la non/sous-utilisation des bases incidents par des fonctions qui peuvent en avoir l'utilité (qualité, contrôle de gestion par exemple), la priorisation accordée aux objectifs opérationnels. La construction d'une mémoire du risque en entreprise est un long apprentissage s'inscrivant dans la constitution progressive d'une culture du risque dans l'organisation.

La mise en place des cinq étapes confère à la gestion des risques une approche globale qui la rapproche de l'*Enterprise-wide-Risk-Management* (ERM), modèle anglo-saxon d'une gestion des risques présentée comme globale et intégrée, dans lequel le rôle des

responsables opérationnels devient essentiel. Une gestion des risques qui met en place les cinq étapes relève de l'ERM ; ainsi décrite, elle est globale au sens de Louisot (2010)[1]. Elle est par essence transversale puisqu'elle est là pour servir les projets, les différentes entités et les processus opérationnels et managériaux de l'entreprise et qu'elle se positionne en accompagnement du processus de décision. Elle suppose l'implication du personnel opérationnel indispensable à une bonne identification des risques. La démarche de gestion des risques se doit d'intervenir en amont de la survenance des évènements, les anticiper et non pas seulement valider les expériences survenues. En cela elle n'est pas seulement une activité de contrôle : on ne cherche pas seulement la qualité de chacune des opérations mais la bonne articulation des activités entre elles.

Méthodes de gestion des risques : quelques exemples

Méric et al. (2009) dénombrent une centaine de méthodes chargées d'anticiper le risque. La réalité est qu'il existe souvent autant de méthodes, adaptées en pratique, qu'il y a d'entreprises. On note une vraie tendance cependant à la convergence des méthodes face à un souci de clarifier, faire simple, rendre pédagogique une science du risque qui souvent tourne au débat d'expert. Il est essentiel de mettre l'accent sur les risques eux-mêmes et non sur les méthodologies en elles-mêmes qui ne sont que des manières d'identifier, d'analyser, de se représenter le risque (Dufour, 2015). Conçues par des ingénieurs, elles reposent sur une chronologie d'étapes attribuant des rôles aux différents agents et conduisent à construire une mémoire des risques.

Nous présenterons plus particulièrement les méthodes des scénarios et les méthodes dites à dire d'expert couramment utilisées par les Risk Managers dans le chapitre 5 de l'ouvrage.

Méric et al. (2009) synthétisent les méthodes de gestion des risques en trois grands types.

---

1. Modèle anglo-saxon d'une gestion des risques présentée comme globale et intégrée, dans lequel le rôle des responsables opérationnels devient essentiel. La notion de globalité introduit tous les éléments d'incertitude liés au futur de l'organisation, ce que Louisot (2010) englobe sous l'expression « toutes causes, toutes conséquences, toutes opportunités et menaces » ; elle est « intégrée », car la gestion des risques doit effectivement l'être à tous les niveaux de décisions et dans tous les process.