

Préface

L'ouvrage La Fonction Risk Manager de Caroline Aubry et Nicolas Dufour arrive à point nommé pour apporter des éclairages et des réponses aux tensions auxquelles les professionnels de la gestion du risque sont aujourd'hui confrontés, et qu'ils doivent pouvoir surmonter.

En premier lieu, la tension entre aider les managers et la gouvernance de leur organisation à mieux gérer les risques, à faire preuve de prudence et de rigueur en un mot, sans pour autant les empêcher d'agir et trop les freiner dans leur ardeur à créer de la valeur. Agent de conformité et de respect des normes, des procédures et des standards d'un côté, le Risk Manager ne doit pas, dans le même temps, corseter l'organisation sous une avalanche d'interdits et d'outils qui étoufferait son agilité nécessaire à sa survie et son développement. Le Risk Manager est également au centre de la tension entre les coûts et les gains : combien coûtent les cartographies, les contrôles, les actions préventives etc. qu'il suscite ? Et combien rapporte-t-il en termes de coûts des risques qu'il permet d'éviter ?

D'après nos observations, la capacité du Risk Manager à démontrer périodiquement, aux managers et à la gouvernance de son organisation, la rentabilité qualitative, qualitative et financière de ses actions - que son objet de risques soit financier, social, commercial ou autres - devient un enjeu fondamental. En somme, le Risk Manager doit savoir parler un langage « qualimétrique » avec ses business partners et ses clients internes, pour expliquer les gains qualitatifs, quantitatifs et financiers de ses actions, et les ajuster si ces gains n'étaient pas suffisants, et mieux vendre ainsi, en quelque sorte, ses préconisations, ses conseils et ses recommandations.

Également, le Risk Manager est au cœur des tensions liées à la « Tétranormalisation », c'est-à-dire les dysfonctionnements créés dans l'organisation par l'inflation normative et les contradictions qu'elle engendre. Sur cette tension, on attend du Risk Manager qu'il aide son organisation, en concertation étroite avec les autres fonctions concernées

par la conformité comme l'audit interne, à mieux orchestrer, arbitrer, négocier l'application des normes multiples auxquelles elle est confrontée. L'inflation normative mal gérée devenant, en effet, une nouvelle macro zone à risques dans toutes les organisations et, au-delà, une source puissante de conflits éthiques internes.

Enfin, le Risk Manager doit aujourd'hui pouvoir répondre à la tension qui peut exister entre la technique et le comportement, puisque si, d'un côté, on lui demande d'être à la pointe des nouvelles technologies de l'information, intelligence artificielle et big data compris, pour être toujours plus efficace et efficient dans son métier, on lui demande « en même temps » de conserver une humanité et un sens du contact, non seulement avec ses équipes, mais aussi avec tous ses business partners, notamment pour des raisons pédagogiques, de concertation et de conviction.

On le voit donc, l'ouvrage de Caroline Aubry et Nicolas Dufour, en apportant des éclairages sur ces tensions complexes et multiples, avec, qui plus est, la sensibilité pratique - donc appliquée - et académique - donc rigoureuse - qui les caractérise, se révèle d'un apport indispensable au Risk Manager contemporain et ses équipes.

Laurent Cappelletti
Professeur titulaire de chaire
au Conservatoire National des Arts et Métiers (Le CNAM)
Directeur à l'Institut de Socio-Economie
des Entreprises et des Organisations (ISEOR)

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 empêchement 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,*

inconvéient 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.