Avant-propos

Le management du risque est un domaine où le vocabulaire employé emprunte très souvent à l'anglais. Pour des questions de lisibilité, la terminologie de *risk management* a été systématiquement remplacée par celle de management du risque. De même, la personne en charge du management du risque a été désignée dans le présent ouvrage sous la terminologie de responsable du management du risque. Cette terminologie s'assimile au terme anglo-saxon de *risk manager*.

Les commentaires relatifs au COSO ERM ont été établis sur la base de la version publiée en anglais. Il est possible que des expressions ou des intitulés de notion subissent des adaptations de vocables dans la parution de sa version française, qui reste à venir au moment de la publication du présent ouvrage.

Introduction

Le management du risque n'a cessé d'évoluer ces dernières années. Les attentes croissantes de la gouvernance, relayées par la parution des nouveaux référentiels COSO et ISO, conduisent à des changements dans la nature des analyses, ainsi qu'à une professionnalisation des acteurs. Le bon sens et la connaissance opérationnelle des activités ne suffisent plus. Le responsable du management du risque doit faire preuve de hauteur de vue et ses interventions l'amènent à naviguer entre risques opérationnels quotidiens et risques stratégiques de long terme.

La cartographie des risques reste un outil privilégié de restitution des résultats des analyses. Néanmoins, sa méthodologie de réalisation doit aussi progresser. La prise en compte de la stratégie de l'organisation, ainsi que l'analyse de son écosystème, est devenue essentielle. Elle s'impose comme la pierre angulaire sur la base de laquelle les risques doivent être appréciés. Cette évolution implique une meilleure prise en considération de l'environnement interne et externe. L'ambition voulue, la stratégie de déploiement, le pilotage de la performance et l'intensité concurrentielle sont autant d'éléments qui doivent être intégrés. La qualité et la pertinence de leur analyse améliorent la vision globale du responsable du management du risque, elles contribuent à son positionnement de *business partner*.

Or, à ce jour, l'incorporation de cette dimension stratégique reste encore bien souvent conceptuelle et peu apparente dans les cartographies des risques, quand ce n'est pas tout simplement oublié. Cette prise en compte ne saurait se réaliser sans évolution méthodologique et sans effort d'intégration.

Il était nécessaire d'accompagner les responsables du management du risque dans cette évolution méthodologique et de mettre à leur disposition des outils fonctionnels. Le présent ouvrage souhaite répondre de façon pragmatique à ce besoin. Il propose des outils concrets permettant à chacun, et en fonction de son niveau de compétence initial, de découvrir ou d'approfondir de nouvelles facettes d'analyse. Au travers d'explications, de focus pratiques et d'analyse

de cas, le lien entre management du risque et stratégie est illustré et s'insère dans une approche méthodologique structurée.

Les lecteurs trouveront aussi dans la présente parution des références utiles aux nouveaux référentiels COSO ERM 2017 et ISO 31000:2018. Au fil de la lecture et au travers des encadrés « nouveaux référentiels », les nouveautés sont explicitées et mises en perspective en fonction de thèmes clefs.

La partie 1, « Enjeux d'un rapprochement » (chapitres 1 à 5), s'attache à présenter les fondamentaux d'une démarche de management du risque, d'une part, et de stratégie, d'autre part. Les deux notions y sont mises en perspective permettant ainsi une bonne compréhension de la finalité de chacune et de leurs complémentarités. Les réflexions sur la place des parties prenantes et l'appétence aux risques seront notamment abordées dans cette partie.

La partie 2, « Un rapprochement amorcé » (chapitres 6 à 11), présente en détail la norme ISO 31000:2018. Les nouveautés y sont plus particulièrement mises en valeur. Cette partie permet au lecteur de s'approprier les bonnes pratiques, mais également de *challenger* sa méthodologie de réalisation des cartographies. Enfin, une comparaison de la norme ISO 31000:2018 avec le COSO ERM 2017 y est réalisée, les spécificités de chacun y sont mises en exergue.

La partie 3, « Donner de la hauteur de vue à sa cartographie des risques : modalités d'intégration des analyses de management du risque et de stratégie » (chapitres 12 à 16), propose des outils d'analyse pour intégrer une vision stratégique dans les analyses de risque. Des exemples et des focus pratiques illustrent la mise en œuvre de ces outils. Les modalités concrètes de travail entre les services risques et stratégie, ainsi que la question des compétences et des facteurs clefs de succès sont présentées dans cette partie.

Enfin, une riche bibliographie permettra au lecteur d'approfondir ses réflexions.

Les outils et les méthodes proposés dans le présent ouvrage sont issus de travaux que l'auteur mène depuis 2013 et qui ont été entrepris avec l'appui de professeurs en stratégie de l'école HEC Paris. Des réflexions propres, des recherches documentaires françaises et étrangères, ainsi que des interviews auprès de dirigeants, d'administrateurs et de responsables de la stratégie ont permis de bâtir et d'affiner ces outils de mise en relation risque/stratégie. Des professionnels du management du risque, appartenant à des organisations de taille variable, du secteur public et du secteur privé, ont été également associés à leur mise en œuvre pratique.

Partie 1
Management du risque et stratégie : les enjeux d'un rapprochement

L'incitation à une meilleure coordination entre le processus stratégique et le processus de management du risque est récente. Les raisonnements restent encore souvent menés en silo, notamment en raison de problématiques organisationnelles.

Pourtant, les deux processus ont des enjeux communs qui relèvent du plus haut niveau de décision de l'organisation. Il est intéressant de raisonner, non plus en silo, management du risque d'un côté, stratégie de l'autre, mais de façon transversale, par *item* d'enjeu.

Cette approche par enjeu fera apparaître des problématiques similaires et des acteurs communs. Inexorablement, sous la poussée des évolutions sociétales et réglementaires, l'analyse stratégique et l'analyse de risque se complètent et se renforcent. L'absence de mise en perspective entre les deux matières exposerait l'entreprise à une perte de cohérence ou d'opportunités inexplorées.

Le point de départ de ce rapprochement est déjà de comprendre la notion même d'enjeu dans le contexte d'aujourd'hui. La définition de l'enjeu : « Ce que l'on risque dans un jeu, en particulier une somme d'argent, et qui revient au gagnant[1] », induit l'existence d'autres joueurs. Ces autres joueurs renvoient, dans la vie de l'entreprise, à ceux que l'on qualifie usuellement de « parties prenantes ».

Ces parties prenantes sont bien sûr les actionnaires et les investisseurs, mais aussi les clients, les consommateurs, les ONG, les fournisseurs, les médias, les syndicats, etc. Le périmètre des « joueurs » s'est considérablement élargi.

Par ailleurs, ce n'est plus seulement « une somme d'argent » qui est en jeu, c'est aussi une qualité de vie et la recherche de la satisfaction de besoins plus qualitatifs. Ces nouveaux enjeux induisent des parties prenantes très différentes dans leur profil, leurs attentes et leurs comportements à l'égard de la prise de risques.

La coordination management du risque/stratégie trouve aussi son sens dans le pilotage au quotidien de l'organisation, dans la recherche du juste équilibre dans l'affectation des ressources et le déploiement du *business model*. C'est dans ce pilotage au quotidien que les réflexions sur l'appétence aux risques prendront toute leur ampleur et contribueront à un alignement des visions.

1 Dictionnaire Larousse.

1
Management du risque et stratégie : les fondamentaux en dix questions clefs

Management du risque et stratégie présentent des similitudes et, comme on le verra dans le présent ouvrage, une coordination entre ces deux matières est source d'enrichissement des analyses.

Pour bien appréhender les apports de l'une ou de l'autre de ces matières, quelques fondamentaux doivent être préalablement acquis. Leur rappel permet de faire le point sur les notions et les outils emblématiques qui les accompagnent.

1.1 Qu'est-ce qu'un dispositif de management du risque ?

Le management du risque comprend un ensemble « d'activités coordonnées dans le but de diriger et piloter un organisme vis-à-vis du risque[2] ».

Quel que soit le référentiel ou la structuration retenue, un dispositif global de management du risque doit comprendre les éléments suivants :

1. Une organisation qui définit le « qui fait quoi » en matière de risque. Les questions suivantes y sont notamment traitées : Qui pilote les analyses ? Qui y contribue ? Quels sont les rôles et les compétences des contributeurs ? Comment se matérialise l'implication de la gouvernance ? Etc.
2. Une méthodologie qui décrit les modalités pratiques de réalisation effective des analyses de risque et de cartographies des risques. Les questions

2 Termes et définitions : article 3 de la norme NF ISO 31000:2018.

suivantes y sont notamment traitées : Comment sont identifiés les risques ? Comment sont-ils analysés ? Comment sont-ils comparés ? Etc. Ces aspects méthodologiques doivent garantir un déploiement homogène et systématique de la démarche de management du risque au sein de l'organisation et au fil du temps. Une assurance raisonnable doit être donnée sur la fiabilité et la pertinence des comparaisons réalisées entre les risques, éventuellement entre les différentes entités d'un même groupe, ou d'une année sur l'autre.

3. Des modalités de pilotage qui déterminent la façon dont se pilotera le dispositif au quotidien, ainsi que les acteurs impliqués. Les questions suivantes y sont notamment traitées : Comment et par qui les analyses sont-elles portées ? Comment sont mis en œuvre et suivis les plans d'action de maîtrise des risques ? Comment sont mises à jour les analyses ? Comment sont mises en place les synergies avec les matières connexes telles que la stratégie, le contrôle interne ou la qualité ? Le pilotage doit prévoir les modalités pratiques qui permettent de s'assurer que la démarche de management du risque se réalise de façon effective et dynamique.

1.2 Qu'appelle-t-on « management global des risques » ou *enterprise risk management* (ERM) ?

La démarche de management global des risques, dite aussi en anglais *enterprise risk management* (ERM) traduit la volonté d'avoir une vision globale des risques d'une organisation. Il s'agit de donner une vue d'ensemble, recouvrant l'ensemble des risques auxquels une organisation, publique ou privée, cotée ou non, doit faire face.

Tous les risques sont pris en compte, quelle que soit leur nature ou la catégorie à laquelle ils appartiennent. Sont ainsi intégrés les risques à caractère opérationnel, juridique, stratégique, managérial, réputationnel, etc.

Les facteurs endogènes, générés par l'organisation analysée, ainsi que les facteurs exogènes, c'est-à-dire subis, sont intégrés à l'analyse.

L'analyse peut être menée au niveau d'une organisation, d'une entité, d'un projet, d'une activité, etc.

La démarche de management global des risques doit permettre, une fois les risques analysés, de les comparer afin de définir, en fonction du niveau d'appétence de l'organisation, d'une stratégie de traitement. De par sa finalité, le management global des risques concourt à la répartition des ressources de l'organisation.

La démarche de management global des risques est différente, tout en étant complémentaire, des approches du type AMDEC[3] qui ont, elles, vocation à faire un focus plutôt à caractère technique sur des composants ayant un caractère matériel.

1.3 Qu'est-ce qu'une démarche *top-down* ? Qu'est-ce qu'une démarche *bottom-up* ?

Quand une démarche de management du risque se met en place, deux approches sont possibles. Ces approches présentent toutes deux des avantages et des limites inhérentes. Avant de choisir l'une ou l'autre, il est fondamental de comprendre quels sont les attendus de la gouvernance.

- L'approche *top-down* : les attentes de la gouvernance portent sur la sécurisation des objectifs stratégiques. L'approche consistera à focaliser sur les risques susceptibles de menacer, ou d'aider, l'atteinte des objectifs stratégiques. On parle alors d'approche *top-down*. Il s'agit, dans cette approche, de partir des objectifs stratégiques et des enjeux de l'organisation en s'interrogeant sur les *scenarii* susceptibles de favoriser ou de compromettre leur atteinte. Le point de départ des raisonnements et des travaux se situe au niveau de la direction générale ou de son équipe.
- L'approche *bottom-up* : les attentes de la gouvernance portent en priorité sur la maîtrise des activités.

  Sont visées :

  - les activités qui concourent directement à l'atteinte des objectifs de l'organisation ;
  - et/ou les activités dont la bonne réalisation est la base d'une organisation saine. Dans ce dernier cas, indépendamment des enjeux et des objectifs de l'organisation, il est considéré comme indispensable que ces activités opérationnelles soient bien réalisées. Elles doivent être effectuées conformément à ce qui est prévu, quelle que soit la personne qui s'en charge. C'est par exemple le cas avec les activités liées à la facturation des clients, ou à la réalisation des offres de services. La maîtrise de ces activités concourt aussi à la maîtrise de la qualité fournie, à l'homogénéisation des services, à la maîtrise de la productivité, etc.

  On parle d'approche *bottom-up* car le point de départ des raisonnements et des travaux se situe au niveau des opérationnels.

  Les synergies avec le contrôle interne et/ou la qualité peuvent être pertinentes pour ce type d'approche. La description des processus contribue à la formalisation de cette approche *bottom-up*. Les risques

3 AMDEC : Analyse des modes de défaillance, de leurs effets et de leur criticité.

seront identifiés au niveau des processus et se rattachent à une étape de réalisation de l'activité décrite. Dans ce cas, les raisonnements doivent se référer aux objectifs du processus. Quelle est la finalité de ce processus ? Quelles en sont les étapes clefs ? Quels sont les événements susceptibles de compromettre leur bonne réalisation ? La relation risques/objectifs existe aussi, mais le niveau de granularité est différent de l'approche *top-down*.

Par ailleurs, afin d'éviter une description fastidieuse de l'ensemble des processus, certaines organisations décident de se focaliser sur les processus dits « processus clefs ». Il s'agit alors de s'intéresser en priorité aux processus à forts enjeux.

Dans un dispositif mature, les approches *top-down* et *bottom-up* doivent être combinées. Toutefois, les organisations qui démarrent ou initient leur dispositif de management du risque ont intérêt à faire un choix clair entre l'une ou l'autre de ces approches, sous peine de confusion méthodologique. En effet, l'approche *top-down* ne requiert pas le même type de raisonnement que l'approche *bottom-up*. Le niveau de granularité des analyses n'est que la partie visible des différences entre ces deux approches. La nature des réflexions, la pédagogie mise en œuvre, ainsi que le profil et les compétences des contributeurs sollicités en interne sont aussi très différents.

Le tableau 1.1 en illustre les différences.

Tableau 1.1 Comparaison pratique d'une démarche *top-down* et d'une démarche *bottom-up*

	Top-down	***Bottom-up***
Attentes de la gouvernance	Besoin d'une vision d'ensemble des risques susceptibles de compromettre l'atteinte des objectifs stratégiques ou des grands enjeux de l'organisation.	Besoin d'être rassurée sur la maîtrise des activités : souhait de maîtriser les risques susceptibles de compromettre la bonne réalisation des activités.
Niveau de granularité des analyses	Vision macro, analyse située au niveau des objectifs stratégiques et des grands enjeux de l'organisation.	Vision micro, analyse située au niveau des activités et des processus qui les décrivent.
Compétences sollicitées en interne	Personnes ayant une bonne vision d'ensemble de l'organisation et de ses objectifs ou enjeux stratégiques et/ou personnes ayant une connaissance des influences du contexte externe sur la stratégie.	Personnes ayant une bonne maîtrise de leur activité.
Types de risque identifiés	Tous les types de risque, quelle que soit leur nature : stratégique, juridique, opérationnelle, managériale, réputationnelle, etc.	Essentiellement des risques de nature opérationnelle : identification des menaces liées aux modalités de réalisation des activités analysées.