AMRAE

la Maison du risk management

La Cartographie : un outil de gestion des risques

Association
pour le Management des Risques
et des Assurances de l'Entreprise

La cartographie :
un outil de gestion des risques

Préambule

La cartographie des risques est un outil du processus de gestion des risques. Le mot "cartographie" recouvre parfois des pratiques différentes telles que la réalisation unique d'une cartographie des risques, ou la mise en œuvre d'une gestion des risques mais encore le processus de gestion des risques dans son ensemble…

L'AMRAE a souhaité, à travers ses membres et leurs savoir-faire en matière de gestion des risques, rédiger un ouvrage issu des pratiques du terrain sur l'élaboration d'une cartographie des risques. Pour ce faire, deux groupes de travail ont été constitués, chacun traitant d'une étape du processus :

– le premier a orienté ses travaux sur le thème "Faire une cartographie des risques : pourquoi, pour qui et comment ?",
– le second sur le thème "La cartographie des risques : et après ?".

Le présent ouvrage est la première réédition de la synthèse des travaux de ces deux groupes de travail agrémentée des évolutions contractuelles et réglementaires depuis l'édition originale.

Ecrit par des risk managers, **"La cartographie des risques : un outil de gestion des risques"** est un livre dans lequel les auteurs ont cherché à restituer un retour d'expérience d'hommes et de femmes du terrain qui ont déjà eu l'occasion de réaliser une première cartographie des risques ou qui en sont parfois à la troisième ou quatrième édition. Il tente de suivre et d'expliquer de manière pragmatique les différentes étapes de sa réalisation au sein des entreprises : de la prise de décision d'entrer dans cette démarche jusqu'à l'après cartographie. Le point de vue adopté met en valeur le "risk management" par rapport aux autres systèmes de management qui peuvent, dans l'entreprise, identifier et évaluer des risques.

Les méthodologies et outils qu'il présente ne sont pas normatifs. Il existe certaines différences d'application d'une entreprise à une autre mais les retours d'expériences montrent que les fondamentaux restent néanmoins les mêmes.

Conformément à l'esprit de la Collection Maîtrise des Risques, créée par l'AMRAE, **"La cartographie des risques : un outil de gestion des risques"** est un ouvrage pédagogique et pragmatique dont le but est de permettre à toutes les parties prenantes de la gestion des risques de l'entreprise de mieux comprendre les motivations, l'intérêt et les étapes nécessaires à la réalisation d'une cartographie des risques pertinente.

Table des matières

Troisième partie :

Après la première cartographie

Annexes

Introduction

Les entrepreneurs ont de tout temps cherché à évaluer les risques de leurs projets et de leur entreprise, sauf à passer pour des aventuriers. Sans référence au risk management, ils l'ont fait soit par simple bon sens, de manière globale et pragmatique, soit en utilisant des méthodes d'analyse particulières à leurs activités. Ces pratiques intuitives peuvent être optimisées avec l'irruption du risk management dans la gouvernance des entreprises. Les méthodologies de gestion des risques apportent en effet un mode de raisonnement indépendant de l'activité faisant l'objet d'une analyse de risques qui s'enrichit d'un recul transverse.

Les démarches de gestion des risques, ou de risk management, ont pour ambition de faciliter l'expression rationnelle des risques à leur juste niveau conduisant à une prise de conscience du management. Elles visent à rationaliser des objets émotionnels, imaginaires ou fantasmagoriques – angoisse face au risque ou envie de risque – qui n'ont pas leur place en tant que tel dans le théâtre de la rentabilité des opérations et d'optimisation des profits où évoluent les entreprises[1]. La démarche de gestion des risques doit donc intégrer la "visibilité" dans ses objectifs et ses moyens afin de pouvoir communiquer ses résultats de manière claire, intelligible et concise au management de l'entreprise… si elle veut être comprise et efficace. Dans cette optique, la cartographie figure parmi les vecteurs de visibilité des risques de l'entreprise.

La cartographie des risques est un outil du processus de gestion des risques qui permet de représenter de manière synthétique et graphique les risques de l'entreprise, hiérarchisés selon ses critères, quelle que soit leur nature : risque stratégique, financier, opérationnel, de mise en cause de la responsabilité, par exemple. Elle permet donc de classer des objets de nature très différente, qu'il serait difficile de comparer entre eux sans l'utilisation de cet outil.

La motivation à se lancer dans un exercice cartographique est donc liée au besoin d'identifier en une seule "photo", de façon claire et fiable, l'état des lieux des menaces auxquelles s'expose une entreprise et de pouvoir comparer cette vision à la "photo" précédente pour en établir rapidement l'évolution et, ensuite, prendre les décisions de pilotage qui s'imposent.

---

[1] *La bulle internet des années 2000 n'a probablement été possible que par une envie irraisonnée de profit incarnée par les start up, eldorado de l'ère virtuelle. La crise des subprimes de 2008 en est également un autre exemple.*

A ce titre, elle est un outil de pilotage stratégique et complète la boîte à outils d'aide à la décision. Elle est utilisée par le management stratégique et opérationnel mais ne doit pas s'y substituer, au risque de perdre le recul et l'indépendance qui en fait toute la valeur.

Comme le processus de gestion des risques, la réalisation d'une cartographie des risques n'est jamais un travail parfait, ni définitif. Elle doit être reproduite régulièrement pour prendre en compte les évolutions du contexte des risques, causes externes et internes, et pour corriger les erreurs d'appréciation détectées. Le processus de cartographie des risques fait partie des démarches d'amélioration continue au sein de l'entreprise.

Dans le cadre de la transposition de la 8ème directive concernant l'obligation du "suivi de l'efficacité du système de gestion des risques par le comité d'audit" (Conseil d'administration pour les VaMP), la réalisation d'une cartographie est une aide précieuse et utile qui permettra d'élaborer rapidement et simplement le reporting nécessaire pour que le dit comité puisse exercer son rôle.

Première partie

Besoins et objectifs

La cartographie, ses raisons d'exister

La cartographies des risques est entrée dans les entreprises entre 2000 et 2002. Un nombre croissant d'entre elles (surtout celles qui sont cotées) déclare aujourd'hui utiliser cet outil dans leur processus de gestion des risques.

D'après l'enquête *FERMA European risk management benchmarking survey 2008*[(2)], qui a recensé les pratiques de 555 membres de FERMA :

– 56% des répondants déclarent disposer d'une cartographie des risques au niveau global (58% pour les répondants français), tandis que 21% évoquent une cartographie des risques sur certains types de risques.
– 44% déclarent avoir mis en place un processus de management des risques intégré (46% pour les répondants français).

Les principaux facteurs externes encourageant la gestion des risques sont, par ordre croissant :

– Obligations légales et règlementaires pour 71% des répondants (64% pour les répondants français).
– Crises et catastrophes naturelles pour 63% (59% pour les français).
– Volonté expresse des actionnaires pour 35% (41% pour les français).

Les stimulations externes et internes

Connaître pour décider et aligner les organisations

La cartographie des risques n'est pas née de la seule initiative des risk managers mais d'un besoin réel des entreprises qui rencontrent de plus en plus de difficultés à avoir une visions globale et pertinente de leurs risques.

Ce besoin résulte de l'accumulation de plusieurs facteurs dont les principaux sont :

■ *La multiplication des événements catastrophiques :*

Qu'il s'agisse de phénomènes climatiques (tsunami, raz de marée, etc), de terrorisme, de crashs industriels ou financiers, les risques encourus par les entreprises changent de dimension régulièrement et font ainsi varier régulièrement les limites de leur assurabilité.

[(2)] *FERMA European risk management benchmarking survey 2008, en collaboration avec AXA Corporate Solutions et Ernst&Young. Pour télécharger l'étude : www.ferma.eu*

■ *L'environnement économique :*

L'entreprise évolue dans un monde en forte accélération (évolution technologique, transmission de l'information, crise financière…) et qui est de plus en plus complexe (mondialisation, restructurations, concentrations...). L'émergence de nouveaux risques et leur rapide évolution exposent l'entreprise à des menaces nouvelles et variées dont la gravité peut vite mettre l'entreprise en danger.

■ *L'importance croissante des systèmes d'information :*

L'omniprésence de la technologie en perpétuelle complexification dans le quotidien des entreprises est un facteur d'augmentation des failles de sécurité qui mettent en danger l'existence même de l'entreprise. La mise en place d'une procédure globale d'identification, de traitement et de suivi des risques de sécurité devient indispensable.

■ *La pression des marchés financiers :*

L'intérêt grandissant des marchés financiers pour les états prévisionnels des entreprises implique, pour la Direction générale, de sécuriser l'atteinte des objectifs annoncés. Il devient impératif d'éviter la volatilité des résultats et, pour cela, d'obtenir une image régulière de l'évolution des menaces et de leur traitement afin de pouvoir corriger la trajectoire rapidement.

■ *L'atteinte des objectifs et la rémunération :*

Il n'est pas facile pour un collaborateur ou un dirigeant d'échanger sur les menaces pouvant atteindre ses objectifs. Pour certains, cet exercice est synonyme de faiblesse et d'échec, pour d'autres, la culture de l'entreprise ne favorise, voir ne tolère pas l'exposition de quasi- faiblesses et la remise en question. Ceci est d'autant plus difficile lorsqu'une rémunération variable importante est adossée aux objectifs. Il devient alors difficile voir impossible d'obtenir une vision objective des risques et de leur poids relatif dans l'entreprise.

Être conforme et transparent pour rassurer

Aux facteurs économiques ou sociétaux s'ajoute une évolution des réglementations, des jurisprudences et des normes de marchés qui sont autant d'éléments de pression pouvant conduire à renforcer le besoin d'une cartographie des risques au sein des entreprises même si cet outil n'est jamais imposé, voire même mentionné explicitement, dans les textes.

Evolution de l'environnement réglementaire et normatif

NRE, LSF, SOX

Suite aux scandales Enron et Worldcom aux Etats-Unis mais aussi Vivendi en France, le législateur a souhaité renforcer et garantir la fiabilité et la transparence de l'information des sociétés, en imposant notamment la mise en œuvre de référentiel de contrôle interne.

Alors que les Etats-Unis votaient la loi Sarbanes Oxley (SOX) en juillet 2002, la France se dotait des lois dites NRE (Nouvelles Régulations Economiques) en 2001 et de la LSF (Loi de Sécurité Financière) en 2003. La LSF a, vocation à accroître la transparence et la fiabilité de l'information comptable et financière des sociétés. Elle a été modifiée plusieurs fois depuis sa création, et notamment par la loi du 3 juillet 2008 qui est la transposition de la directive 2006/46/CE du 14 juin 2006.

A l'origine, la LSF demandait que le président du conseil d'administration/de surveillance *"rende compte des procédures de contrôle interne"* dans un rapport publié. La loi du 3 juillet 2008 élargit le contenu de ce rapport. La principale modification porte sur l'obligation de décrire dans le rapport du président *"des procédures de contrôle interne et* ***de gestion des risques"***, notamment sur les parties relatives au traitement de l'information comptable et financière. Cela signifie que les sociétés soumises la LSF devront, à travers le rapport du président, rendre des comptes aux actionnaires de leur système de gestion des risques.

D'autres dispositions de la loi du 3 juillet 2008 revêtent leur importance :

- *"Lorsque les entreprises se réfèrent volontairement à un code de gouvernance élaboré par les organisations représentatives des entreprises"*, elles doivent préciser *"si des dispositions ont été écartées et les raisons pour lesquelles elles l'ont été"*. Ainsi, désormais, les entreprises qui décideraient de ne pas se référer à ce code de gouvernance devront expliquer les raisons pour lesquelles elles ont choisi de ne pas l'appliquer ;
- Les Sociétés en Commandites par Actions faisant Appel Public à l'Epargne rentrent désormais dans le champ d'application de la LSF ;
- Le rapport du président doit dorénavant être approuvé par le conseil d'administration/de surveillance.

Un autre texte a particulièrement marqué la réglementation en matière de gestion des risques, il s'agit de la transposition de la 8ème directive européenne transcrite par une ordonnance le 8 décembre 2008, applicable dès le 9 décembre.

L'article 14 alinéa 1 de l'ordonnance institue pour les *"personnes et entités dont les titres sont admis à la négociation sur un marché réglementé, ainsi que les établissements de crédit (…), les entreprises d'assurances et de réassurances, les mutuelles (…) et les institutions de prévoyances (…),* ***un comité spécialisé agissant sous la responsabilité exclusive et collective*** *des membres, selon le cas, de l'organe chargé de l'administration ou* ***de l'organe de la surveillance*** *assurant le suivi des questions relatives à l'élaboration et au contrôle des informations comptables et financières"*[3].

L'alinéa 3 stipule que, *"sans préjudice des compétences des organes chargés de l'administration, de la direction et de la surveillance,* ***ce comité est notamment chargé d'assurer le suivi :***

a) Du processus d'élaboration de l'information financière.
b) ***De l'efficacité des systèmes*** *de contrôle interne et* ***de gestion des risques.***
c) Du contrôle légal des comptes annuels et le cas échéant, des comptes consolidés par les commissaires aux comptes.
d) De l'indépendance des commissaires aux comptes."

Cette nouvelle mission attribuée aux administrateurs propulse la gestion des risques au cœur des préoccupations des conseils d'administration. La cartographie des risques, comme nous le détaillerons plus loin, est un outil de pilotage et non de gouvernance. A ce titre, elle ne pourra être présentée "en l'état" aux administrateurs mais devra être adapté utilement pour servir leur mission.

Devant cette nouvelle mission pour l'administrateur, l'Autorité des Marchés Financiers (AMF) a décidé de réunir un groupe de place afin de :

– Rédiger un guide sur les comités d'audit.
– Réaliser l'adaptation du cadre de référence.

La restitution des travaux est prévue pour juin 2010.

[3] *Ordonnance n° 2008-1278 du 8 décembre 2008.*

Réglementations encadrant les activités

De nombreux secteurs d'activité sont encadrés par des réglementations propres ou réglementations sectorielles : secteurs industriels (SEVESO II, réglementations techniques, Directive sur la responsabilité environnementale…), secteur bancaire (Bâle II), secteur de la santé et des médicaments (Autorisation de mise sur le marché, réglementations de santé, …), secteur de l'assurance (Solvency II, …), secteur agroalimentaire (réglementations sanitaires, …), …, sans oublier les secteurs régulés (Télécom, Energie, Ferroviaire, …) - la liste est longue.

L'identification des risques, leur évaluation et leur traitement doivent être examinés au regard des réglementations sectorielles applicables et du droit applicable en fonction du pays où s'exerce l'activité (ou du pays du siège de la maison mère), suivant le risque considéré. La gestion des risques devra inclure dans son objectif de conformité aux lois et règlements ces spécificités sectorielles et tenir compte, notamment, des risques dus :

– À l'évolution de la réglementation qui peut engendrer des coûts supplémentaires ou imposer de nouvelles conditions opérationnelles,
– Aux conditions de renouvellement des agréments ou autorisations,
– À la diffusion des bonnes pratiques permettant leur respect.

La méconnaissance d'une réglementation peut engendrer des risques de non-conformité qui se traduisent généralement par des amendes, des coûts de remise à niveau ou pire, des suspensions de l'autorisation d'opérer.

Dans certains cas bien précis, la loi fait obligation de désigner un responsable de la conformité ou "Compliance Officer", qui doit être indépendant et a le devoir de signaler aux Autorités les entorses à la loi : c'est notamment le cas en France pour la loi Informatique et Libertés, les pratiques et comportements sur le marché financier et pour la lutte anti-blanchiment (règlement de l'AMF). Cette loi s'applique aussi à certains fonctionnaires (police, enseignement,..), et au corps médical pour la dénonciation de crimes et d'atteintes à l'intégrité de la personne.

Lorsque l'entreprise exerce une activité hors de France, la loi peut être différente y compris dans les pays européens, et il appartient au risk manager de questionner les différents services en charge de la veille législative et réglementaire pour faire vérifier si des spécificités locales ne pourraient mettre en péril certaines activités en les rendant non conformes par exemple du point de vue de la production, de la vente, des règles douanières, des contrats de travail ou de l'accès au marché financier. Les services juridiques en particulier doivent être sollicités systématiquement pour réaliser un inventaire des spécificités des droits et réglementations locales.

Les particularités des réglementations applicables étant pris en compte, leur application ou leur méconnaissance dans l'entreprise devront être passées au crible de l'analyse des risques, quels que soient l'activité et le pays considérés. Les concepts et outils présentés ci-après aideront le risk manager à mieux les caractériser.

Durcissement du droit de la responsabilité civile et pénale

La responsabilité personnelle des administrateurs, déjà largement établie aux Etats-Unis, connaît un durcissement en France depuis 1998. En effet, à cette époque, la Cour de Cassation prononce que "Seules les fautes commises pour des mobiles personnels, ou d'une gravité exceptionnelle excluant l'exercice normal des fonctions peuvent engager la responsabilité des dirigeants".

En 2001, la Loi NRE[a] précise dans son article 106 qu' *"Un Administrateur ou Conseiller ne peut plus se prévaloir de ne pas avoir été informé pour s'exonérer d'une responsabilité. C'est maintenant une faute de ne pas avoir réclamé ladite information"*. En 2003, le Procureur Général de la Cour de Cassation (JP Burgelin) déclare qu' "Il faudra tôt ou tard que l'on puisse mettre en cause la responsabilité personnelle des administrateurs, et qu'ils aient à participer à l'indemnisation des victimes. Ce serait la manière la plus efficace de les responsabiliser".

Enfin, la Loi Perben II va encore plus loin puisqu'à partir du 1er janvier 2006, les conditions de mise en cause de la responsabilité pénale de la personne morale, édictées par la Loi de 1974, sont élargies.

Mais si la jurisprudence et l'article L 225-100[b] du code de commerce font état du devoir de mise en œuvre d'une analyse des risques, la cartographie n'est pas mentionnée. Néanmoins, la responsabilité des dirigeants, à qui on reprocherait de ne pas connaître ou maîtriser ses risques, pourrait être mise en cause au motif de la faute de gestion (article L225-251 du Code de commerce)[c].

Face aux nouvelles réglementations, l'AMRAE et l'IFA (Institut Français des Administrateurs) ont rédigé un ouvrage sur le "Rôle de l'administrateur dans la maîtrise des risques[4]" analysant, notamment, les nouvelles responsabilités de l'entreprise et de ses dirigeants en matière de contrôle interne et de gestion des risques.

---

[4] *Rôle de l'administrateur dans la maîtrise des risques" IFA et AMRAE en collaboration avec Pwc et Landwell &Associés.*

[a] *NRE : Nouvelles Régulations Economiques.*

[b] *Voir Annexes.*

[c] *"Les administrateurs sont responsables, individuellement ou solidairement, selon le cas, envers la société ou envers les tiers, soit des infractions aux dispositions législatives ou réglementaires applicables aux sociétés anonymes, soit des violations des statuts, soit des fautes commises dans leur gestion."*

Extraits de l'ouvrage "Rôle de l'administration dans la maîtrise des risques"

Les responsabilités de l'entreprise et de ses dirigeants en matière de contrôle interne et de gestion des risques

La judiciarisation renforcée de la vie économique se traduit par une mise en œuvre plus fréquente des responsabilités civile et pénale de l'entreprise, personne morale, et de ses dirigeants y compris des administrateurs.

Entreprendre a toujours été synonyme de prise de risques mais le contexte actuel réclame plus de transparence et de réactivité dans des organisations très souvent complexes.

Les dirigeants et les administrateurs voient leur rôle se transformer face aux risques

Ils doivent ainsi :

– Se former, s'informer et agir.
– Organiser la transmission de l'information au sein de l'entreprise.
– Prendre des mesures adaptées de prévention des risques.
– Rendre compte des procédures de contrôle interne mises en place.
– Respecter des règles et expliquer les raisons du non respect de celles-ci (Comply or Explain).
– Evaluer l'efficacité des procédures mises en place.

Qui est responsable en cas de défaillance du contrôle interne ou de la gestion des risques ?

La loi du 3 juillet 2008 impose que ledit rapport soit approuvé par le Conseil et étend son périmètre à la gestion des risques.

S'il est démontré une faute caractérisée, un préjudice et un lien de causalité entre faute et préjudice, la responsabilité civile du Président et des administrateurs peut être engagée.

De façon très exceptionnelle, leur responsabilité pénale pourrait également être mise en jeu sur le terrain du délit de communication d'informations fausses ou trompeuses, pour des sociétés dont les titres sont négociés sur un marché réglementé. Les responsabilités quant à la qualité du contrôle interne et de la gestion des risques.

C'est la Direction Générale qui est responsable de la qualité du contrôle interne et des processus de gestion des risques. Le Conseil pour sa part s'assure de l'existence et du suivi de l'efficacité des systèmes de contrôle interne et de gestion des risques.

…/…

…/…

En cas de carence dans la mise en place des procédures de contrôle interne, ou de procédures inefficaces, la responsabilité civile collective des administrateurs, des membres du Conseil de Surveillance et de la Direction Générale peut être mise en cause.

Par ailleurs, aux termes de l'arrêt rendu par le Conseil d'Etat le 5 octobre 2007, en cas de fraude, une carence manifeste des dirigeants dans la mise en oeuvre des dispositifs de contrôle interne peut être qualifiée d'acte anormal de gestion, avec les conséquences fiscales associées.

On observe ainsi une responsabilisation accrue des administrateurs en matière de suivi des risques. Ces derniers doivent se former, s'informer, agir et rendre compte des procédures mises en place. Ils doivent appliquer et/ou faire appliquer des règles, ou à défaut expliquer les raisons du non respect de celles-ci (concept du "Comply or Explain"). Ils doivent aussi s'assurer de l'efficacité des procédures mises en place par la Direction générale.

Le Comité est chargé, sous la responsabilité exclusive et collective du Conseil d'Administration ou de Surveillance, d'assurer le suivi du processus d'élaboration de l'information financière. Il suit aussi l'efficacité des systèmes de contrôle interne et de gestion des risques, du contrôle légal des comptes annuels et le cas échéant des comptes consolidés par les CAC. La Direction Générale est en charge de la mise en place des procédures et processus de contrôle interne et de gestion des risques.

La responsabilité des membres du Comité d'Audit ne devrait pas être accrue. En revanche, leur rôle évolue. Ainsi, pour suivre l'efficacité des systèmes de contrôle interne et de gestion des risques, le Comité va devoir aller au-delà de la cartographie des risques. En effet, cette évolution va amener le Comité à demander une information plus formalisée et plus régulière en matière de gestion des risques, de la part des différents acteurs majeurs au sein de l'entreprise et plus particulièrement de la part de la Direction générale, des Directeurs des Risques, de l'audit interne et, le cas échéant, du contrôle interne.

…/…

…/…

La conformité aux lois et règlements est un des objectifs clés du contrôle interne. Toutes les entreprises sont concernées et les sources de responsabilité sont nombreuses en raison d'une réglementation abondante qui se complexifie, et des actions judiciaires en accroissement. La DGCCRF, l'inspection du travail, les Douanes, l'administration fiscale, l'AMF… diligentent de nombreuses enquêtes qui peuvent aboutir à des sanctions lourdes.

Les entreprises et leur dirigeants en France comme l'étranger sont aussi exposés à des risques sensibles tels que les ententes, la corruption, le blanchiment, la présentation de comptes inexacts, le marchandage, plus généralement les fraudes diverses.

Ainsi, la gestion des risques de responsabilités civile, pénale et fiscale est devenue un véritable enjeu pour les Directions Générales. Les Conseils d'Administration et les investisseurs s'y intéressent de plus en plus. Un risque pénal mal géré peut être fortement dommageable pour la réputation de l'entreprise et son cours de bourse.

Le Conseil se doit alors de veiller à l'intégration des risques de non-conformité aux lois et règlements dans la cartographie globale des risques, et au suivi de l'efficacité des dispositifs mis en place pour la gestion desdits risques (Codes de conduite, procédures d'alerte, délégations de pouvoirs, formations…).

■ *Demande de transparence des parties prenantes*

AMF

Les entreprises sont soumises à une demande de transparence de plus en plus forte, notamment pour les entreprises cotées. Les principaux documents, demandés par le législateur et l'AMF, afférant notamment aux risques, sont :

– Le rapport du président sur le contrôle interne et la gestion des risques
– Le rapport de gestion
– Les annexes
– Le document de référence

Difficile pour les entreprises de rester cohérent dans sa communication tout en conservant la confidentialité de certaines menaces.

Pour répondre à cette problématique, l'AMF a publié en octobre 2009 sa recommandation sur les facteurs de risque mettant à jour le guide d'élaboration du document de référence. Cette recommandation a pour objectif de guider les émetteurs dans la rédaction de la rubrique "Facteurs de risques" du document de référence.

Le document est structuré comme suit : Après un rappel du cadre législatif et réglementaire, l'AMF recommande aux émetteurs d'appliquer un certain nombre de principes sur la présentation des risques avant de détailler, dans une seconde partie, les informations à fournir sur les principaux risques.

Certaines agences de notation comme Standard & Poors ont intégré dans leur évaluation la pertinence du processus de gestion des risques dans l'entreprise qu'elles analysent. A travers une série de questions, les agents se forgent une opinion quant à la qualité du processus d'analyse, de traitement et de reporting des risques et demandent parfois de justifier des réponses avancées. Par ailleurs d'autres agences de notations notamment sociétales ou environnementales examinent également comment les risques sont analysés, traités et communiqués.

Rationaliser pour augmenter la performance et la rentabilité

Enfin, il existe des facteurs financiers ou techniques qui peuvent également motiver la décision de se doter de l'outil "cartographie" pour illustrer les risques de l'entreprise.

Financiarisation croissante de l'activité des entreprises

Le contexte économique est aujourd'hui caractérisé par une financiarisation croissante de l'activité des entreprises. Cette tendance est induite par une exigence accrue des actionnaires en termes de retour sur investissement, de création de valeur et ce, avec la volatilité la plus réduite possible. Cette exigence concerne autant les entreprises que les assureurs et structure désormais l'offre et la demande d'assurance.

Le financement des risques est donc un enjeu stratégique pour l'entreprise qui doit gérer au mieux ses besoins en capital. L'entreprise a besoin d'optimiser la performance de l'échange avec le marché de l'assurance en arbitrant entre la rétention et le transfert de ses risques. Pour répondre à cet enjeu stratégique du financement du risque, l'entreprise a besoin d'un outil d'information précis et global sur ses risques.

Difficultés dans le transfert des risques

La prise de conscience que l'on ne peut pas tout assurer (ou tout transférer au marché financier) a renforcé le besoin d'identification et de suivi de ce qui n'est pas couvert par l'assurance pour éviter l'effet boomerang destructeur sur ce qui l'est.

Les risques non transférables, comme le risque d'image ou certains risques de responsabilité, étant supportés par les fonds propres de l'entreprise, leur identification, leur évaluation et leur traitement est un enjeu financier majeur[5].

Le caractère cyclique des marchés d'assurance qui peut se traduire par de fortes augmentations de primes comme ce fût le cas en 2001/2002 a provoqué une recherche d'optimisation des programmes par les entreprises via une analyse plus pointue des risques encourus pour n'assurer que les plus pertinents. La cartographie est un outil efficace pour :

– Opérer cette sélection,
– Atteindre l'objectif de limiter le périmètre assuranciel,
– Justifier une réduction des coûts[6].

L'impératif du retour sur investissement

Les allocations de ressources sont arbitrées au sein des entreprises par des critères de rentabilité auxquels le risk management est parfois en peine de répondre. Dans cette optique, la cartographie est une démarche efficace. La détection d'un risque et sa représentation dans une vision globale peut conduire à l'abandon d'un projet ou à le repenser si elle fait apparaître une gravité insupportable du risque ou la nécessité d'un financement pour le maîtriser qui remettrait en cause la rentabilité du projet envisagé.

D'une manière plus générale, la question est posée indépendamment de l'utilisation de l'outil cartographique : peut-on estimer un ratio coût / bénéfice de la mise en œuvre d'une démarche de maîtrise des risques ?

Il n'existe aucune étude qui évalue les coûts et les gains directs d'une telle démarche. Mais globalement, de nombreuses entreprises ont développé cette mission, notamment celles dont les actionnaires sont les plus exigeants en termes de retour sur investissement. Eviter des pertes dues à des dommages opérationnels, réduire les contentieux juridiques, éviter des crises, préserver la réputation, assure *a minima* le gain du traitement des litiges, des coûts des experts et des conseils, la mobilisation de ressources internes détournées de la création de valeur. En cas de crise, l'arrêt partiel de l'activité normale devra être rattrapé "si possible". Certes, les efforts particuliers de gestion de la crise sont très coûteux, les séquelles fréquentes. Mais il est question d'éviter des pertes de parts de marché, de reconquérir une image de marque malmenée et une capacité d'anticipation supérieure à celle des concurrents. Le coût de ces pertes, si elles étaient avérées,

---

[5]Rappelons qu'il ressort de plusieurs études que seuls 20 à 25% des risques d'entreprises sont assurables.
[6]Ce besoin s'affirme également dans un marché "soft" en raison de son caractère provisoire et de son absence d'impact sur l'inassurabilité des risques stratégiques. Les tarifs peuvent être bas mais le marché n'est pas prêt pour autant à offrir de nouvelles garanties ou des plafonds de garanties plus élevés.

est sans commune mesure avec celui de quelques hommes/mois pour une PME ou quelques hommes/ans pour un grand groupe dédiés à maîtriser ces risques.

Le risk management est donc moins un problème de comptabilité que d'état d'esprit. Si le chef d'entreprise a une position passive, négative, voire résignée, à l'égard de ses risques, l'aspect comptable du coût du risque prendra une importance particulière car la gestion des risques sera avant tout considérée comme une charge. Il subira alors les événements et peut s'attendre au déclin de son entreprise.

En revanche, si le chef d'entreprise a une attitude positive et proactive par rapport à ses risques et s'il considère que les maîtriser lui donne un avantage concurrentiel dans son positionnement sur le marché, l'approche du risque sera considérée comme une composante du plan de développement de l'entreprise.

Principes de la cartographie

Objectifs

Si la cartographie n'est pas une obligation, elle peut cependant être considérée comme une étape préparatoire importante aux décisions de maîtrise des risques. Mais lorsqu'elle entreprend une cartographie de ses risques, l'entreprise doit s'interroger sur la finalité de cette démarche et sur le type de cartographie qu'elle entend mener :

- S'agit-il d'un exercice de contrôle interne qui se focalise sur les processus ?
- S'agit-il d'une démarche qui s'inscrit dans un processus global de maîtrise des risques ?
- La cartographie a-t-elle pour finalité d'éliminer ou de réduire tout ou partie des risques identifiés ou seulement d'améliorer la connaissance de ces risques afin d'aider les managers dans leurs prises de décisions et d'être en conformité avec les exigences réglementaires ?

De la réponse à ces questions dépendra non seulement la conduite du processus cartographique mais aussi la phase post-cartographie. Les méthodes de recherche et de mise en œuvre de plans d'actions varieront également selon le mode de cartographie adopté.

Il faut avoir conscience qu'indépendamment de sa finalité, la cartographie n'est pas un exercice "neutre". Elle engage la responsabilité des managers. Après une cartographie, les risques sont identifiés, hiérarchisés : les dirigeants ne peuvent donc les ignorer. Leur décision de les traiter ou non, et d'envisager l'après cartographie est par conséquent cruciale. Néanmoins, ne pas identifier ses risques ne réduit en aucune façon la responsabilité des dirigeants.

L'entreprise peut donc se déterminer en fonction de différents objectifs :

- Répondre à l'obligation réglementaire de communiquer sur les risques (Document de référence, Loi NRE,…) en utilisant un outil approprié,
- Identifier et évaluer les risques liés à la non-conformité,
- Réduire les risques opérationnels (sécurité, informatique, …),
- Elaborer le plan d'audit,
- Identifier et piloter les couples : risques / opportunités,
- Hiérarchiser les risques et décider des mesures prioritaires, optimiser les ressources, définir le niveau raisonnable de prise de risques.

Quoiqu'il en soit, l'objectif ultime reste la prise de décision, le pilotage et une mise en perspective des éléments de la communication. La production cartographique à but esthétique ou pour se conformer à un effet de mode, est à bannir car l'absence de traitement des risques connus engagerait d'autant plus la responsabilité du dirigeant. Plus que l'élaboration de la cartographie des risques elle-même, l'usage que l'on en fait détermine sa véritable valeur ajoutée.

Valeur ajoutée par rapport aux autres outils

Notons tout d'abord que des alternatives à la cartographie peuvent exister dans l'entreprise :

En termes d'identification :

- Reporting des défaillances et base incidents (incidents, défaillance, non qualité…),
- Réunions et travaux de la Direction Générale (consacrés aux risques),
- Audit interne des activités,
- Outils de modélisation / quantification des risques.

En termes de reporting :

- Reporting des incidents (déclarations de sinistres, réclamations clients, arrêts de travail…),
- Auto-évaluations périodiques des risques par les opérationnels et contrôles,
- Tableau de bord périodique d'indicateurs de risques,
- Intégration des risques dans les reportings standards de management.

Ces différents éléments font donc clairement apparaître que d'autres méthodes d'identification et de reporting des risques sont utilisées par les entreprises. Toutefois, force est de reconnaître que le besoin d'une visibilité globale et hiérarchisée des problématiques de réalisations prévisionnelles ne permet plus de se contenter d'une analyse de risques sectoriels, ni d'une analyse de risques par projets. Il faut une approche transverse pour dépasser les effets de silo et apporter

au dirigeant le sentiment de connaître l'étendue des menaces avec une mise en évidence des priorités où doivent se porter les efforts financiers de l'entreprise.

Par rapport aux autres outils qui peuvent exister (voire co-exister), la motivation à se lancer dans un exercice cartographique est liée au besoin d'identifier en une seule "photo" l'état des lieux des menaces d'une entreprise et sans doute de pouvoir le comparer à la "photo" précédente pour en établir rapidement l'évolution afin de prendre ensuite les décisions de pilotage qui s'imposent.

Dans cette optique, si la cartographie des risques n'a aucun caractère obligatoire, elle présente une réelle valeur ajoutée par rapport aux autres outils d'identification et de reporting. Elle permet en effet à l'entreprise :

- D'obtenir un consensus sur une vision globale des enjeux.
- De se focaliser sur les sujets majeurs.
- D'organiser la transversalité : les échanges d'informations, la confrontation des points de vue (opérationnels, fonctions transverses).
- D'initier et de développer une appropriation à tous les niveaux de l'entreprise d'une culture du "risque" et de ne pas craindre d'appréhender les risques et positiver ses faiblesses.
- De rationnaliser les risques.
- De formaliser un langage commun et une démarche homogène.
- D'avoir une approche managériale et pas seulement technique du risque : au-delà du pilotage, la cartographie peut être utilisée en outil de management. En effet, elle peut parfaitement illustrer une situation intenable. C'est une façon concrète de partager la vision d'une menace et de fait, entraîner la nécessité du changement sans rencontrer la résistance habituelle[7].
- D'optimiser les ressources allouées à la prévention, les contrats d'assurances et autres couvertures financières.
- D'identifier le "sous-" ou "sur-contrôle" des risques identifiés.
- De communiquer sur ses risques en externe. La cartographie des risques apparaît comme une base très pertinente pour établir les publications exigées par les régulateurs[8].

---

[7] *La survenance d'une crise grave surmontée avec difficulté constitue souvent une forte motivation pour les décideurs internes à structurer la visibilité de nouvelles crises potentielles. Le "traumatisme" interne en débloquant la résistance au changement ouvre une large opportunité pour la mise en place justifiée d'un exercice cartographique.*

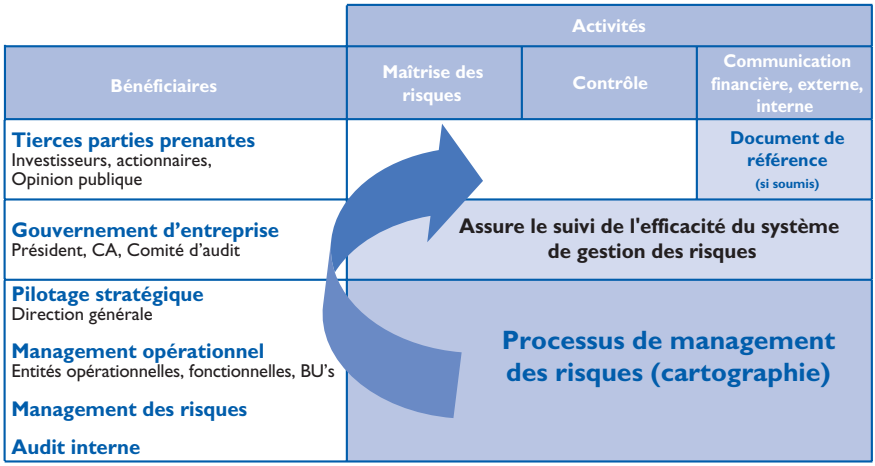
[8] *Cet exercice de communication reste néanmoins délicat compte tenu des enjeux de confidentialité autour de la cartographie elle-même. Cette question est traitée dans la 3e partie de ce document.*

Les pré-requis d'une cartographie

Identifier les bénéficiaires et choisir une méthodologie

Les bénéficiaires potentiels de la cartographie et leurs attentes

Le tableau ci-dessous indique les multiples bénéficiaires potentiels d'une cartographie des risques selon le besoin d'usage et de communication défini par les instances dirigeantes de l'entreprise.



Les entrées horizontales du tableau représentent les acteurs de l'entreprise et les entrées verticales expriment le rôle des acteurs face aux éléments cartographiques.

Le choix d'une méthodologie et d'une démarche

L'AMF recommande aux entreprises cotées de déclarer à quel référentiel elles se réfèrent pour organiser leurs démarches de gestion des risques. Il existe plusieurs référentiles de gestion des risques qui sont (voir en annexes pour plus de détails) :

– COSO II
– FERMA
– ISO 31 000 : 2009

Prendre en compte les "identités" de l'entreprise

La culture

Aucun changement, aucune évolution importante dans la vie d'une entreprise ne peut se faire à contre-courant de sa culture. La mise en perspective par une cartographie des risques n'est pas un simple tableau de bord supplémentaire parce qu'elle met en cause des points sensibles liés à la réalisation des objectifs avec des moyens souvent qualitatifs qui doivent être compris, acceptés et partagés par l'ensemble des acteurs. L'exercice cartographique ne peut pas être confondu avec un acte d'audit interne parce qu'il ne procède pas d'une "investigation" mais d'une démarche auto déclarative. Le processus ne s'impose pas, la transparence nécessaire demande un état de confiance établi et accepté en règle du jeu dans l'entreprise.

La psychologie

Il est fortement recommandé, avant de lancer l'exercice, de s'assurer de l'adhésion du management opérationnel, de la volonté et du soutien de la Direction Générale. Si l'exercice cartographique peut servir de levier à la mise en place du processus de gestion des risques d'une entreprise, il ne peut réussir que si chacun est prêt à affronter la vérité qui apparaîtra au cours du processus cartographique et d'en assumer les conséquences. Cette dimension psychologique est le courage de se remettre en cause sur toute l'échelle hiérarchique face aux risques générés par les activités et les prises de décision de chacun.

L'exercice de cartographie n'a de valeur à terme que si la totalité du processus est en place : en premier lieu, la définition par le Président et la Direction Générale de la politique de gestion des risques qui caractérise le seuil de tolérance au risque accepté pour permettre de faire ressortir les risques les plus importants, et en second lieu une méthodologie sous-tendant le processus de gestion de risque validée.
La notion de tolérance au risque a une dimension financière mais également psychologique qu'il n'est pas facile à déterminer car elle dépend souvent de facteurs très subjectifs.

L'organisation

Un processus de cartographie des risques relève avant tout du management de projet. Or la plupart des entreprises sont organisées en "silos" avec des structures de commandements et de gratifications verticales. La démarche de la cartographie en tant que management de projet peut se trouver potentiellement en conflit avec l'organisation de l'entreprise. Cette situation devra alors être gérée par la Direction générale de l'entreprise à qui il revient d'émettre des messages clairs attestant son soutien à la démarche de cartographie et d'approuver les mesures d'incitation destinées à motiver les contributeurs.

Le Risk Manager et la cartographie

La croissance incontestable de l'utilisation des cartographies pour avoir une vision globale des risques de l'entreprise, ne signifie pas pour autant que les risk managers sont en charge de ce processus dans toutes les entreprises.

Force est de reconnaître que la fonction de risk manager est très diversifiée selon les missions qui lui sont rattachées, selon la culture et la réceptivité de l'organisation et selon l'existence d'autres fonctions au sein de l'entreprise. Certains risk managers sont surtout reconnus comme experts dans le domaine de l'assurance et leur mission est avant tout de mettre en place des programmes de couvertures, d'autres sont déjà entrés dans une démarche d'analyse des risques et, à ce titre, peuvent se positionner comme acteur, voire pilote, de la cartographie.

Pluralité des cartographies

Parler de cartographie des risques au singulier vise davantage un idéal qu'une réalité et cela pour deux raisons :

– L'entreprise est une organisation complexe. Elle comprend souvent plusieurs niveaux (groupe/filiales), plusieurs activités, process et métiers. La cartographie peut donc être réalisée à chacun de ces niveaux selon la démarche adoptée, "top down" ou "bottom up"[9].
– Le risque étant désormais au cœur du management de l'entreprise, plusieurs systèmes de management (audit et contrôle interne, qualité, développement durable …) cherchent à identifier les risques de l'entreprise avec des méthodes et des objectifs différents.

Cette réalité confronte l'entreprise à relever deux défis majeurs pour s'engager dans un processus cartographique viable :

– La cartographie, en tant qu'outil "photographique" produisant une image globale des risques de l'entreprise, ne peut être un collage approximatif d'une panoplie de cartographies conduites de manière indépendante. La logique veut qu'il y ait des concepts et un langage commun entre ces différentes approches afin de pouvoir aboutir à une synthèse cohérente et pertinente.
– La menace de voir se multiplier les questionnaires et autres demandes de renseignements, diligentés selon des méthodes et des calendriers différents, adressés aux mêmes "propriétaires de risques" est réelle. Un tel embouteillage signerait la fin de toute tentative de réaliser une véritable cartographie des risques au sein de l'entreprise, ne serait-ce que pour des raisons de disponibilité des destinataires "propriétaires de risques".

[9] *Voir 2e partie : "Méthodologie" - "Choix préalables" - "Opter pour une démarche".*

La démarche cartographique étant par essence une démarche transversale coordonnée, il est donc indispensable d'avoir "un pilote dans l'avion". Le problème est de savoir qui peut prétendre piloter un tel projet ou tout au moins l'animer afin de l'organiser dans le temps et de faire converger les résultats obtenus.

Le danger est bien sûr de répondre à cette question sur le terrain des enjeux de pouvoir. Dans ce cas, le "canon étant l'ultime argument des rois", la question sera réglée par le positionnement hiérarchique des postulants. En revanche, si la question se pose dans un environnement plus détendu et dans une logique consensuelle d'efficacité, le risk manager aura quelques arguments à faire valoir pour piloter une démarche de cartographie des risques.

Les différents acteurs du management des risques

Le management des risques, au sens complet de son acception, fait partie, de facto, du fondement du management de l'entreprise car il consiste à maîtriser les obstacles qui s'opposent à l'atteinte des objectifs, soit en les réduisant, soit en les éliminant, soit en utilisant les opportunités offertes par ces obstacles.

Par l'amélioration de la connaissance des risques (menaces et opportunités) et de la prise de décision qui en découle, le management des risques vise à renforcer la confiance faite à l'entreprise par ses clients, ses actionnaires, ses salariés et les marchés financiers.

Si dans une entreprise, il n'y a qu'un seul système de management, celui qui permet de prendre les bonnes décisions, aux bons niveaux, en revanche, ses outils de maîtrise et d'appréciation sont "pluriels" et concernent ses deux aspects fondamentaux :

- La stratégie qui définit l'interdépendance de l'entreprise avec son environnement (audit, contrôle interne, risques externe et entrepreneuriaux),
- L'opérationnel qui tire la performance des activités de l'entreprise (sécurité, environnement, finance, immobilier, production, vente,…).

Les différents systèmes de management sont autant d'étapes d'appréhension de ces risques, d'évaluation de leur criticité et de la façon dont ils sont traités, c'est-à-dire maîtrisés.

Au final, le risk management de l'entreprise s'appuie sur la connaissance acquise au travers des différentes démarches de maîtrise. L'apport essentiel est de pouvoir représenter, pour les décideurs, les principaux risques et les enjeux qui s'y rapportent. Cette mise en perspective a pour vocation de les aider à interclasser les urgences, à mesurer les conséquences et de leur faciliter les prises de décisions et les arbitrages en matière de prises de risques.

Avant d'aborder la spécificité du risk manager, il est important de recenser les différentes fonctions qui, dans l'entreprise, contribuent à l'identification et à la mise sous contrôle des risques :

■ *Audit interne*

L'audit interne[10] intervient avec un regard distancié sur l'activité. Cette démarche est complétée par les audits externes (commissaires aux comptes, agences de notation financière ou en responsabilité sociale) qui interviennent "a posteriori" et qui complètent l'approche de l'audit interne.

L'audit interne est une activité indépendante et objective qui évalue l'efficacité des dispositifs de maîtrise des risques, 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[11].

Pour les auditeurs, la cartographie consiste à identifier les risques en termes de processus et de contrôle, non par mesure de fréquence et d'impact. De plus, le rôle de l'auditeur dans "l'après cartographie" est de constater mais pas d'intervenir dans le traitement des risques, ni en tant que conseil, ni à plus forte raison en tant qu'acteur.

■ *Fonction financière*

La direction financière a en charge l'identification et le traitement des risques de liquidité, de marché, de crédit et d'actifs. Elle est par ailleurs responsable des investissements, notamment de la validation du financement des plans d'actions pour réduire les risques identifiés et évalués des entités opérationnelles.

Outre le financement des plans d'actions, la fonction financière calcule les provisionnements. Sans entrer dans un débat sur les différentes normes comptables, seuls peuvent être provisionnés les risques de probabilité suffisamment importants, et rattachés à des évènements survenus : par exemple, les indemnisations futures liées à un dommage déjà survenu.

---

[10] *Le rôle de l'audit interne répond aux normes établies par l'Institute of Internal Auditors (IIA).*

[11] *Définition approuvée le 21 mars 2000 par le Conseil d'Administration de l'IFACI. Traduction de la définition internationale approuvée par l'IIA le 29 juin 1999.*

Contrôle de gestion

Le contrôle de gestion intervient durant l'exercice des activités, parfois un peu en amont. Il a pour vocation d'analyser et de fournir de l'information fiable d'aide à la décision permettant de piloter le résultat de l'entreprise et d'affecter les ressources financières nécessaires à la réalisation des objectifs de l'entreprise et d'évaluer la bonne utilisation de ces ressources. Les aléas sur les activités pouvant entraîner une volatilité des résultats seront pris en compte, notamment à l'occasion du retraitement des prévisions au cours de l'année, ou lors des résultats semestriels ou trimestriels. L'analyse des aléas pris en compte par le contrôle de gestion fournira une source d'information utile sur les risques opérationnels, techniques et financiers et enrichira ainsi les cartographies.

Contrôle interne

Le contrôle interne intervient simultanément à la réalisation des activités pour vérifier qu'elles sont "correctement" traduites en actes économiques. Sa vocation est d'apporter une assurance raisonnable sur l'optimisation des opérations, la fiabilité des informations financières et la conformité aux lois et règlements. Toute entreprise, soumise ou non au Sarbanes Oxley Act qui stigmatise plus particulièrement la conformité des comptes, doit réaliser un contrôle interne qui engage les mandataires sociaux.

Le plan de contrôle interne est fondé sur l'analyse des risques pour contrôler ceux qui peuvent avoir un impact plus important. Les écarts identifiés sont autant de risques opérationnels détectés par cette démarche, et les actions de traitement doivent aussi être considérées comme autant de moyen de réduction des risques.

Qualité - Sécurité - Environnement (QSE)

Les démarches QSE sont liées à la réalisation opérationnelle, pour que "tout se passe bien" et pour le garantir dans la quasi-totalité des cas. Elles concourent à la maîtrise des risques attachés aux processus opérationnels. Elles ont cependant leur limite car tous les risques opérationnels ne sont pas couverts par ce système de management, à commencer par les activités non traduites explicitement en processus, ou non soumises à la certification ou aux contrôles méthodiques.

La démarche QSE peut être caractérisée de la manière suivante :

– Depuis la fin des années 80, les entreprises ont été confrontées à une évolution de l'exigence des consommateurs, qui acceptaient de moins en moins les défauts de qualité. Elles ont alors voulu maîtriser leur qualité par l'installation de Cercles de Qualité, chargés d'identifier et de traiter les causes qui pourraient générer des défaillances. La normalisation a par la suite standardisé les bonnes pratiques avec par exemple les normes ISO 9000, d'abord en 1994 puis en 2000, selon lesquelles les entreprises ont recherché progressivement une certification. Ces normes recommandent d'identifier les causes internes et externes qui pourraient conduire à une insatisfaction des clients quant aux produits des processus. Il convient alors d'identifier des "points de contrôle" et des "points d'arrêt", qui déclenchent autant de mesure de traitement de ce risque de non-qualité.
– Les risques de pollution et de nuisances de toutes sortes (eau, air, sol, bruits,…), relèvent de la même démarche. Les normes ISO 14000 sur le management environnemental, bâties sur le même principe que les normes de qualité, conduisent elles aussi à identifier les risques qui pourraient causer une éventuelle pollution, et à en assurer un traitement préventif. Elles ajoutent l'obligation de préparer et de tester des "plans d'urgence", qui sont autant de plans de gestion de crise en cas de pollution.
– En matière de sécurité, les normes en vigueur adoptent encore le même principe (normes OHSAS[12] par exemple). En France, la loi fait obligation de décrire dans le "document unique" tous les risques de santé et de sécurité auxquels sont exposés les salariés à un poste de travail. Des mesures de prévention et de protection collectives et individuelles devront être prises, l'employeur est tenu de donner une formation adaptée à ses salariés. De la même manière, les réglementations qui ont fait suite à la directive SEVESO ont conduit à la mise en évidence de l'importance du "système de gestion de la sécurité" (appellation réglementaire qui revient à recommander l'intégration de la sécurité dans le management de l'entreprise). Elles ont entraîné la nécessité d'évaluer le système de management à partir de référentiels mis à jour en fonction de l'évolution des méthodes et pratiques (IFRS[13] par exemple) intégrant ainsi le principe d'amélioration continu commun à tous les dispositifs.

---

[12] *La spécification OHSAS (pour Occupational Health and Safety Assesment Series) précise les règles pour la gestion de la santé et de la sécurité dans le monde du travail.*

[13] *International Financial Reporting Standards.*

Responsabilité Sociale d'Entreprise (RSE)

Selon la Commission européenne, la RSE est "l'intégration volontaire par les entreprises de préoccupations sociales et environnementales à leurs activités commerciales et à leurs relations avec les parties prenantes". Un tel engagement de la part d'une entreprise suppose naturellement qu'elle respecte la réglementation sociale. De plus, il s'accompagne de démarches volontaires allant au-delà des normes réglementaires en développant des partenariats forts avec les parties prenantes concernées, à l'intérieur de l'entreprise (dialogue social), comme à l'extérieur. Des outils et référentiels (ISO, GRI[14], Pacte Mondial, OIT[15], ...) déclinent le concept et permettent de mesurer l'exposition de l'entreprise à des risques auxquels les investisseurs et agences de notation sont de plus en plus sensibles : risque de réputation, risque de cohésion (mauvais climat social dans l'entreprise), risque de malversation (corruption, délit d'initié, fraude, concurrence déloyale, contrefaçon,…).

Il faut avoir conscience que dans ce registre l'entreprise doit analyser de nouveaux risques et évaluer des risques connus selon des critères qui dépassent le droit de la responsabilité. Ainsi :

– En interne, les licenciements abusifs, la discrimination à l'embauche ou dans la parité hommes/femmes, toutes les formes de harcèlement, le travail des enfants, sont autant de risques de mise en cause en forte croissance du fait de lois de plus en plus sévères édictées dans les pays occidentaux. L'exposition à ces risques est encore plus importante pour les entreprises qui ont une activité internationale, notamment dans des pays où les valeurs morales et la culture sont bien différentes des nôtres, et où certaines pratiques douteuses sont tolérées bien que contraires à l'éthique. Mais en France, sommes-nous toujours irréprochables ?
– En externe, la RSE est mise en évidence lors d'évènements catastrophiques (pollution, risque alimentaire). Force est de constater que la gestion strictement juridique de ces risques n'est plus acceptée par l'opinion publique qui parle de responsabilité sociale de l'entreprise que les tribunaux se déclarent incompétents à juger. On peut avoir juridiquement raison, et moralement tort.

La RSE permet ainsi d'anticiper des risques stratégiques à long terme, et donne donc le temps à l'entreprise de décider des orientations qu'elle va prendre pour assurer sa pérennité. Nul doute qu'elle puisse contribuer à une cartographie des risques de l'entreprise.

---

[14] *La Global Reporting Initiative (GRI) a été établie en 1997 avec pour mission de développer les directives applicables pour rendre compte des performances économiques, environnementales et sociales de n'importe quelle organisation gouvernementale ou non gouvernementale.*

[15] *Organisation Internationale du Travail (OIT).*

Direction juridique

La direction juridique veille à identifier et à traiter les risques de mise en cause de l'entreprise ou de ses dirigeants dans les domaines du droit administratif (amendes) et du droit civil et pénal (responsabilité contractuelle, responsabilité civile, responsabilité des mandataires sociaux, risque de procédure pénale) ou d'atteinte à ses actifs (propriété intellectuelle ou industrielle). La "judiciarisation" croissante de la société civile renforce le caractère crucial d'une cartographie des risques juridiques.

Direction logistique

Les entreprises prennent de plus en plus conscience des risques liés à la "chaîne logistique". Ces risques sont parfois beaucoup plus importants en termes d'impact sur l'activité que les risques de dommages aux biens. Leur analyse ne peut se limiter à un inventaire dans la mesure où il s'agit de risques de flux. En fait, ces risques se prêtent particulièrement bien à un exercice cartographique puisque le but est de dessiner des parcours et d'identifier des points de rupture potentiels. De plus, le risque logistique peut être le risque majeur d'une entité de laquelle il ne dépend pas. Par nature transversale, son identification est essentielle. Les directions opérationnelles et les directions logistiques doivent donc s'atteler cette identification qui s'intégrera dans la cartographie des risques de l'entreprise[16].

Direction informatique

Le risque de défaillance des Systèmes d'Information (SI) est l'un des risques majeurs que rencontre la quasi-totalité des entreprises. Il ne se limite pas au risque matériel classique : incendie, bris de machine, incompatibilité des SI entre eux ou "panne sèche", entraînant à coup sûr l'arrêt de tout ou partie des activités, pour une durée variable.

Dans ce registre, les risques immatériels représentent plus de 70% du risque informatique total : pertes de données, fraude, piratage, virus, contrefaçons,… Ces risques n'affectent pas seulement l'organisation de l'entreprise mais toute son activité : sa capacité de production, sa chaîne logistique, la commercialisation de ses produits, la confiance de ses clients, bref son image.

---

[16] *Rappelons que le risk manager gère souvent les contrats d'assurance "transport de marchandises" ainsi que les sinistres générés dans le cadre de cette activité. Il identifie les faits générateurs de ces sinistres et leurs impacts directs. Il délivre son analyse et ses éventuelles recommandations au responsable Logistique.*

L'identification de ces risques est d'autant plus essentielle que l'offre du marché en termes de financement est peu abondante et couteuse. Elle pose néanmoins un problème dans la mesure où les directions informatiques sont beaucoup mieux armées pour maîtriser les risques matériels de leurs activités que les risques immatériels dont l'identification et l'évaluation dépendent des entités opérationnelles utilisatrices. C'est pourquoi, dans sa démarche de gestion des risques informatiques, la DSI devra associer les utilisateurs qui seuls peuvent :

– Prédéterminer la gravité des conséquences dues à l'indisponibilité des SI.
– identifier et tester les fonctionnements dégradés dans l'attente de la reprise des SI.
– Evaluer le coût de la reprise des données de la période d'interruption.
– Evaluer le montant des pertes d'exploitation consécutives au sinistre.

La DSI devra également associer le risk manager dans le cadre de la gestion de crise, de l'atteinte à l'image et du positionnement des risques SI par rapport à la globalité des risques de l'entreprise.

Spécificité de la fonction "risk management"

Dans tous les cas, le risk manager doit se positionner par rapport aux différents systèmes de management des risques en tenant compte de l'apport précieux d'information qu'ils lui apportent. La formalisation du positionnement des acteurs est nécessaire. C'est le seul moyen de décrisper les tensions qui pouvaient surgir dans les entreprises entre des fonctions s'attribuant parfois des responsabilités communes en préconisant une position qui augmente leurs performances respectives[17].

Ainsi, dans les entreprises où la mission du risk manager commence en amont du transfert du risque, son rôle n'est pas de refaire les analyses déjà faites, et encore moins de les contester, mais bien au contraire, de s'en servir pour construire, consolider et affiner toujours un peu plus la connaissance des risques de l'entreprise afin d'alimenter une cartographie globale.

[17] *Certains référentiels (voir Annexe) ont même positionné différents acteurs du management des risques. Ainsi, les champs d'intervention respectif du contrôleur interne et du risk manager sont définis par COSO II comme relevant de fonctions complémentaires : le risk manager initie et pilote la démarche de gestion des risques et le contrôleur interne vérifie l'efficacité de la démarche. COSO propose également une analyse fine des positionnements complémentaires des risk managers et des auditeurs internes dans son annexe. C'est une référence intéressante.*

C'est la raison pour laquelle, lors de la création d'une fonction spécifique dédiée à la gestion des risques, le risk manager, titulaire de cette fonction, prend en priorité appui sur les réseaux déjà en place et développe des liens et des interactions avec les systèmes de management existants avant de créer des dispositifs spécifiques. Cette approche permet en définitive une vision globale, transverse et totalement intégrée. La communication et le positionnement du risk manager sont ainsi plus aisés parce que non conflictuels[18].

Transversalité

Le risk manager a pour mission de développer la conscience du risque au sein de son entreprise. Il intervient pour assurer une cohérence transversale et une compréhension réciproque avec les autres systèmes de management en définissant notamment :

- Le langage commun à appliquer à travers le groupe en matière de gestion des risques,
- La méthodologie d'analyse et d'évaluation des risques, les outils appropriés et le suivi de l'efficacité de la gestion des risques au sein de l'organisation en s'assurant que le niveau global d'exposition est cohérent avec la politique de l'entreprise.
- Les responsabilités de chaque groupe de fonctions. Rappelons que les directions opérationnelles sont propriétaires et donc responsables des risques développés par leurs activités. Elles les identifient, les suivent, proposent des investissements en terme de prévention/protection pour les réduire. Le risk manager se positionne en support des directions opérationnelles pour le pilotage de leurs risques (évaluation et choix des mesures de traitement)[19].

Pour permettre une vision globale, il est donc nécessaire d'animer la démarche, d'agréger les données et de les harmoniser selon une méthode et des critères homogènes afin de parvenir ainsi à une synthèse cohérente de risques d'origine et de nature multiple.

---

[18] *Le référentiel COSO propose des exemples utiles de profil de postes liés à la gestion des risques ou des descriptions de fonctions précisant les rôles et responsabilités.*

[19] *Par exemple, il apporte la connaissance des expériences passées à travers les sinistres subis par les industries ayant la même activité (benchmark par les assurances), à travers les risques identifiés par les autres entités (interdépendances des sites entre eux…) alors que la Direction opérationnelle apporte sa connaissance du risque inhérent à l'activité qu'elle développe.*

Toutefois, le caractère transversal de la fonction de risk manager, c'est-à-dire sa capacité à animer un processus qui intègre l'ensemble des fonctions de l'entreprise autour de la captation du traitement des risques, est un objectif lourd qui n'est pas toujours atteint. Ainsi, l'étude FERMA 2006 sur les pratiques du risk management en Europe révèle que seuls 39% des répondants déclarent l'avoir atteint. Ce déficit de transversalité est confirmé par le score de la cartographie des risques qui ne concerne l'échelle globale de l'entreprise que dans 52% des cas.

La nature des risques identifiés dans la cartographie est donc également un domaine de réflexion pour les dirigeants de l'entreprise, l'objectif étant de cartographier les risques sur une échelle beaucoup plus large.

Neutralité

Le risk manager est le garant de la permanence de la gestion des risques dans l'entreprise. La crédibilité des résultats des actions qu'il entreprend est en partie construite sur l'indépendance de son positionnement dans l'organisation. S'il doit vérifier la fiabilité et la réalité des informations qui lui sont données, le risk manager n'a pas de rôle d'évaluation des activités ou des individus : c'est le rôle des dirigeants. Le risk manager inscrit sa démarche dans l'objectivité des faits et des actions et non dans la morale ni les jugements de valeurs.

Exhaustivité

S'il est reconnu qu'aucune garantie d'exhaustivité ne saurait sérieusement être donnée, seule une fonction dédiée à la gestion des risques permet toutefois de tendre vers celle-ci. Ainsi, en appliquant une méthode systématique, le risk manager pourra identifier certains risques non traités ou sous-estimés par les autres systèmes de management, ainsi que les moyens de traitement non mis en œuvre. Or, le plus dangereux pour une entreprise est le risque ignoré et non traité.

Compétitivité

L'exigence de perfection et la recherche systématique des responsabilités voulues par l'opinion publique sont telles qu'une entreprise peut perdre des marchés, de la valeur, voire disparaître si un risque important la touche et qu'elle se trouve alors dans l'impossibilité de fournir ses produits ou ses services. Réduisant ses défaillances, elle tire un avantage compétitif par rapport à ses concurrents.

Faire savoir que l'entreprise dispose d'un management de risques efficient incarné par une fonction clairement définie dans son organisation peut devenir un objet de communication car une des sources de plus-values d'une entreprise est de savoir gérer ses risques plus efficacement que ses concurrents.

La mise en place d'une fonction et d'une démarche de gestion des risques avec les moyens adéquats est le gage de la volonté de l'entreprise d'assumer, en pleine connaissance de cause, ses responsabilités et son devoir de transparence à l'égard des différents acteurs avec lesquels elle évolue : actionnaires, consommateurs, agences de notation, pouvoirs publics…

Responsabilité

Bien que chaque direction opérationnelle soit propriétaire et donc responsable des risques développés par son activité, le risk manager n'est pas pour autant dégagé de toute responsabilité. A la différence d'autres systèmes de management dont le rôle est strictement fonctionnel (comme l'audit), le risk manager est un opérationnel. A ce titre, sa responsabilité est engagée notamment :

- Lorsqu'il prend en charge le traitement de risques transverses ou externes,
- Dans l'animation et la coordination du réseau des risk managers ayant été désignés au sein de chaque entité ou filiale locale.
- Dans le compte-rendu (notamment cartographique) aux instances de direction et de contrôle, des risques identifiés et de leur évolution suivant les actions de maîtrise en place. Il est alors responsable depuis l'alerte jusqu'au veto.
- Dans la négociation du transfert des risques au marché de l'assurance.

Retour d'Expérience

Lors d'une série d' "entretiens dirigeants" conduits pour réactualiser la cartographie d'un groupe industriel important, les participants déclarent que "l'examen des risques permet de voir ce qu'on ne verrait pas autrement, et de poser des questions utiles au pilotage et à une prise de décision améliorée et plus globale".

*
* *

Deuxième partie

Méthodologie

S'appuyer sur un modèle existant

La cartographie est un outil qui s'inscrit dans le processus de gestion des risques de l'entreprise. Plusieurs référentiels[20] détaillent la mise en œuvre d'un processus de gestion des risques, référentiels qui suivent majoritairement deux grandes phases, à savoir :

– Identification et évaluation des risques adossés aux objectifs.

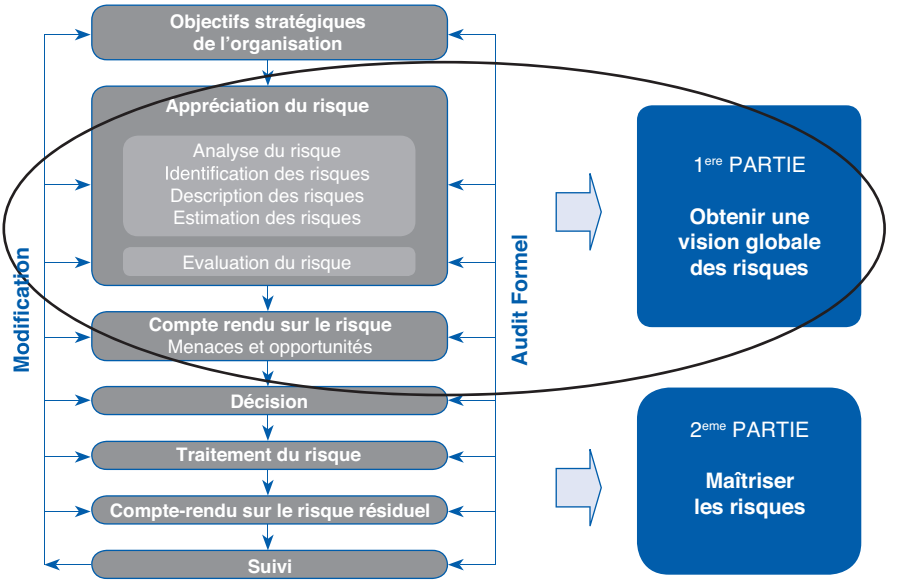
– Traitement et suivi des risques, compte-rendu aux parties prenantes du processus.

Nous proposons de présenter nos travaux suivant le référentiel présenté par FERMA, travail auquel l'AMRAE a largement contribué, et avons inscrit la cartographie des risques à deux moments distincts du processus qui sont :

1) *"Cartographie des risques : obtenir une vision globale des risques"*, qui se situe après l'identification et l'évaluation des risques bruts.

2) *"Cartographie des risques : maîtriser les risques"*, qui se situe après la mise en œuvre des plans d'action ou des contrôles en place.

[20] *Voir la présentation des différentes méthodologies existantes en Annexe.*



Opter pour une démarche

Pour exécuter les tâches définies par ce référentiel, deux méthodes sont possibles et se complètent :

– La démarche descendante ou "top down".
– La démarche ascendante ou "bottom up".

Top down

La démarche top down consiste à identifier et à effectuer une première estimation des risques auprès des dirigeants et de leurs principaux responsables puis à descendre vers les opérationnels.

Le risk manager implique les membres du Comité Exécutif, les directeurs de zone/des métiers, les directeurs fonctionnels et opérationnels,… jusqu'au niveau n-2 de l'organisation afin de recueillir leur perception des principaux risques de l'entreprise.

Auprès des dirigeants, l'identification des risques se réalise majoritairement sous la forme d'un entretien comprenant des questions ouvertes[21] telles que :

– "Quels événements pourraient entraver la réalisation des objectifs que vous vous êtes fixés pour votre activité ?"
– "Par rapport aux indicateurs de résultats et de pilotage de votre activité, quels sont ceux qui vous alertent sur les risques potentiels ?"

Cette démarche peut se réaliser au travers d'entretiens individuels ou d'ateliers[22]. En fonction de la culture de l'entreprise et de son mode de fonctionnement, le risk manager favorisera l'une ou l'autre technique (ou les deux). Notons seulement que :

– L'entretien individuel permet de "se livrer" plus facilement mais limite le sentiment de "partage collégial" des risques.
– L'atelier favorise la vision commune des risques et permet d'atteindre un consensus entre les participants mais peut limiter, voir censurer, la contribution de certains aux débats.

Le risk manager peut proposer un mélange des deux modes opératoires sous la forme d'un entretien individuel pour l'identification des risques et d'un atelier pour l'évaluation.

Avantages

La démarche descendante a plusieurs avantages. Elle permet :

– D'exprimer de la manière la plus forte, en interne, la volonté de la Direction Générale d'engager l'entreprise dans le processus.
– De favoriser l'adhésion du management décisionnel pour en faire le moteur de la démarche. Même si les résultats sont logiquement macroscopiques, ils constituent une base essentielle qui entraîne l'adhésion sur la nécessité d'aller plus loin.
– De conduire à une vision globale qui met en évidence des menaces sur des enjeux majeurs.
– D'échanger sur une vision transverse des risques indépendamment de la sphère de responsabilité à laquelle ils pourraient être rattachés.
– De partager au plus haut niveau la même compréhension des risques,
– De disposer de résultats rapides pour une mise en œuvre légère, favorisée par l'interrogation d'interlocuteurs ayant la compréhension plus claire des objectifs.

---

[21] *Voir Annexes : "Questionnaire pour un entretien avec un dirigeant dans le cadre d'une démarche Top down".*

[22] *Voir "Partie II - Obtenir une vision globale des risques" - "Appréciation du risque" - "Analyse des risques" - "Outils et techniques d'identification".*

Retour d'Expérience

Dans mon entreprise, il ressort que la façon la plus efficace pour lancer l'opération est de respecter trois étapes :

– Etape 1 :Réaliser une interview de chaque N-1 et N-2 de la Direction Générale en posant les mêmes questions à chacun : "En considérant vos objectifs, pouvez vous identifier quels sont les obstacles à leur accomplissement ? Quelle pourrait être l'incidence sur l'atteinte des objectifs en cause ?".

– Etape 2 : Une première liste de menaces va pouvoir être établie. Ces menaces seront reformulées, peut-être regroupées et synthétisées, sous forme de scénarios valorisés en utilisant l'échelle d'impact (*voir plus bas*).

– Etape 3 : Une deuxième interview des mêmes personnes va porter sur les questions suivantes :"Quel niveau de vraisemblance, quelle probabilité percevez-vous quant à la survenance de ces obstacles ? Quel est votre niveau de préparation pour réduire l'impact des obstacles s'ils surviennent ?", ce qui va permettre de définir l'occurrence en s'appuyant sur l'échelle de l'occurrence (*voir plus bas*) et la maîtrise opérationnelle en s'appuyant sur l'échelle de la maîtrise (*voir plus bas*) pour chacun des scénarios définis.

Bottom up

L'approche ascendante (ou remontante) consiste à interroger les niveaux plus opérationnels, au moyen d'outils plus directifs (tels que les questionnaires à questions fermées), l'analyse étant poursuivie en remontant jusqu'au niveau de direction opérationnelle ou fonctionnelle, c'est-à-dire jusqu'au responsable du processus ou de l'entité analysée.

Avantages

L'approche ascendante permet notamment :

– D'identifier des risques opérationnels qui, considérés individuellement, sont faibles, mais dont le cumul engendrerait un risque majeur, dépassant le seuil de tolérance de l'entreprise (ce qui suppose que ce seuil a bien été défini au préalable).
– De favoriser la détection des "risques orphelins" comme les risques situés à la frontière entre processus.
– D'identifier les menaces empêchant la bonne réalisation des activités et l'atteinte des objectifs opérationnels.
– De disposer d'une quantification reposant sur un historique ou une analyse concrète.
– D'obtenir des informations détaillées mais nécessitant des ressources.
– De bâtir un Univers de risques "commun", puis pour chaque entité.

Retour d'Expérience

Mise en place d'une démarche remontante, dans un groupe intégré couvrant une chaîne d'activités de plusieurs métiers.

A la suite de la publication de la loi LSF et après une étude d'opportunité, le COMEX a décidé la mise en place d'une démarche de cartographie et de maîtrise des risques. S'appuyant sur cette décision, le Group Risk Officer a travaillé sur plusieurs axes :

– Préparer une décision d'organisation, à la signature du Président Directeur Général, d'une filière Risques dans l'entreprise :
  • s'appuyant sur des risk officers dans les Divisions,
  • définissant le rôle des propriétaires de risque,
  • précisant les organes de décision et la mission de la filière Risques.
– Positionner la démarche Risques par rapport aux démarches de management stratégique et opérationnel, démarches qualité, sécurité environnement, et au cycle de gestion.
– Elaborer un référentiel méthodologique qui servira de mode commun d'échange sur les risques :
  • partage des finalités sur la maîtrise des risques,
  • définition de vocabulaire,
  • modalités d'évaluation.
– Diffuser la "Culture risque" et la démarche par des ateliers entre membres de la filière pour préciser, appréhender, s'approprier les concepts et leur mise en œuvre.

Ce travail a pris une année environ, à l'issue de laquelle les Divisions ont été en mesure de produire leur première cartographie. Au sein de ces divisions, des réunions ont également eu lieu pour identifier et confronter les risques, les évaluer, et à nouveau s'approprier les concepts.

Une fois les premières cartographies validées par les Comités de direction des différentes Divisions, assimilables à un métier, le Groupe a souhaité évaluer son exposition globale à ses risques. S'est alors posée la question de savoir comment "agréger" les risques de ces différentes divisions. Ils ont été regroupés par analogie de nature sur la base d'un modèle de risques génériques : défaillance des systèmes d'information, rupture d'approvisionnement clé, …

…/…

…/…

L'évaluation financière équivalent au "panier de risques" constituant un risque Groupe a été construite sur la base de la méthode d'analyse combinatoire, utilisée couramment en statistique financière pour évaluer les valeurs en risque (VAR).

In fine, une cartographie des risques Groupe a été constituée, hiérarchisée et validée par le COMEX.

Laquelle choisir ?

Comme on vient de le voir, la démarche descendante ou "top down" correspond plutôt à une identification des risques stratégiques alors que la démarche remontante ou "bottom up" correspond davantage à une identification des risques opérationnels.

S'il semble plus simple, parce que plus rationnellement chiffrable, de s'attacher à ne cartographier que les risques "opérationnels", l'exercice ne révèlera qu'une partie de la vérité, tant il est vrai que certains risques opérationnels ont pour origine des risques fortement stratégiques ou qu'ils débouchent sur des risques stratégiques beaucoup plus importants, dont la visibilité est nécessaire.

A ce stade, il faut comprendre que la cartographie des risques n'est pas un jugement ni un diagnostic mais un constat dont l'analyse, qui appartient au management décisionnel, reste à faire. Il doit être parfaitement clair que dans la démarche d'identification des risques, il n'est pas question de faire de la stratégie, ni de la remettre en cause, mais seulement, et c'est beaucoup, d'identifier et d'évaluer les risques de non réalisation de la stratégie, ou pire de mauvaise compréhension de la stratégie.

C'est pourquoi, convaincus des avantages des deux démarches, les auteurs se sont entendus sur leur complémentarité et leur utilité respectives et recommandent de :

– Commencer par une première cartographie en utilisant la démarche descendante.
– Obtenir l'adhésion de l'équipe dirigeante qui facilitera et soutiendra l'extension de l'exercice aux autres périmètres de l'entreprise.
– Initier la démarche remontante sans attendre[23].

[23] *Voir sur ce point la troisième partie : "Après la première cartographie".*

Quelle que soit l'option prise, on rappellera que le croisement des démarches "top down" et "bottom up" ne doit pas conduire à négliger la collecte d'informations existantes produites par les autres systèmes de management de l'entreprise[24].

Retour d'Expérience

Nous avons croisé la "cartographie des risques" qui est une démarche interne à l'entreprise, avec ce que nous avons appelé la "carte des risques" qui est le résultat de toutes les missions menées par des auditeurs. Cette dernière n'a pas l'ambition d'être exhaustive : elle ne fait que recenser et évaluer les risques observés lors des différentes missions d'audits. Le croisement de ces deux démarches avait pour objectif de vérifier qu'il y avait bien convergence dans le résultat final. En réalité, nous avons souvent constaté des écarts (risques ignorés ou évalués de manière différente), ce qui nous a permis de faire les corrections nécessaires.

Préparer la démarche

Que la démarche soit "top down" ou "bottom up", il est essentiel de prendre quelques précautions avant de l'entreprendre. La cartographie des risques, même soutenue par la Direction Générale, peut difficilement se concevoir comme une démarche d'autorité. Elle demande donc à être préparée pour éviter les malentendus et les obstacles inutiles. Pour mettre toutes les chances de son côté, le risk manager devra définir les notions de base de la cartographie, mettre en place un dispositif qui lui assurera des relais au sein de l'entreprise, expliquer le processus et motiver les contributeurs.

[24] *Voir première partie : "Le risk manager et la cartographie"- "Les différents acteurs du management des risques".*

Définir et organiser

Plusieurs initiatives pourront être prises par le risk manager pour établir un langage commun et une compréhension univoque des risques dans le cadre du processus cartographique et pour mettre en place un dispositif efficace d'animation et d'entretien de la démarche. A titre d'exemples, le risk manager :

- Doit définir ce que l'entreprise entend par "risque", et notamment choisir entre "un événement susceptible de porter atteinte à la pérennité, la réputation ou les résultats de l'entreprise", ou "tout événement susceptible d'avoir des conséquences négatives ou positives sur la pérennité, la réputation, le développement ou les résultats de l'entreprise". La première définition conduit à ne s'intéresser qu'aux menaces et aux dangers alors que la deuxième conduit aussi à s'intéresser aux opportunités favorables, notamment dans les risques financiers ou les projets de développements externes.
- Faire une communication préalable sur la démarche de gestion des risques.
- Choisir les éléments qui caractérisent un risque (causes, conséquences, catégorie,…).
- Caractériser les notions de survenance du risque (probabilité) et de gravité des conséquences.
- Face à la variété de vocabulaire et à la diversité de son utilisation par les différentes parties prenantes du risque dans l'entreprise, prendre la précaution de définir certains concepts permettant de parler le même langage.
- Définir un format de document de collecte : le registre des risques.
- Identifier les acteurs à impliquer et définir leurs responsabilités.
- Mettre en place un comité des risques au niveau central et au niveau des entités pour intégrer la cartographie au management courant de l'entité. Le positionnement de ce comité doit être suffisant pour responsabiliser ses membres et lui permettre d'arbitrer le cas échéant les problèmes de financement. La périodicité des réunions de ce comité peut être variable selon les entités opérationnelles.
- Prévoir une animation permanente du processus de cartographie par un réseau de correspondants.

Expliquer et convaincre

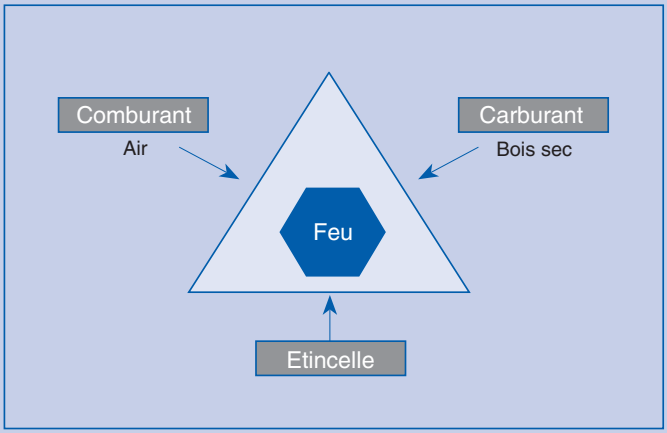
Le vocabulaire étant appris et les concepts définis, le dispositif ayant été mis en place pour disposer des relais nécessaire à la conduite du processus, reste à expliquer la démarche, à mettre en évidence sa signification et son intérêt et enfin, à convaincre les responsables opérationnels et tous les contributeurs à y participer.

Ce point est particulièrement sensible. Les arguments ont souvent une tendance à intellectualiser la démarche ce qui rend complexe sa mise en application sur le terrain. L'expérience ci-après nous a semblé apporter une vision simple, facile à développer dans tous les environnements.

Retour d'Expérience

Du triangle du feu au triangle des risques

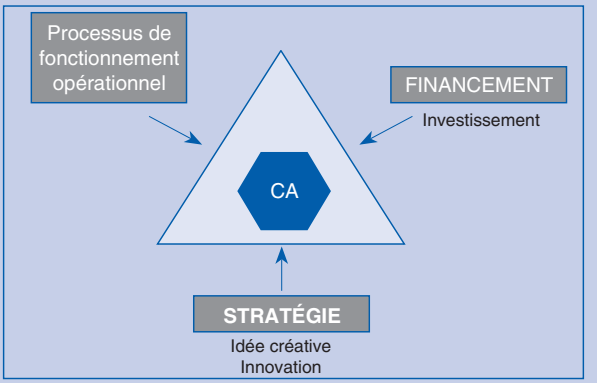
De façon à expliquer les risques, dans l'entreprise X, nous sommes partis du référentiel très connu des pompiers : Le triangle du feu.



…/…

…/…

Pour qu'il y ait un feu, il faut maîtriser le comburant, le carburant et l'étincelle. Transposé à l'entreprise, le raisonnement est le suivant : pour qu'il y ait génération de chiffre d'affaire, il faut qu'il y ait une idée stratégique (l'étincelle), un financement (le carburant), des processus opérationnels (le comburant).



Nous avons considéré ces trois éléments comme étant les génériques de l'origine des risques de l'entreprise.

L'actionnaire de référence souhaitait la mise en place d'un processus de gestion des risques. A la suite des conclusions d'une mission d'audit interne, le Président du Conseil d'Administration et le Directeur Général ont été demandeurs d'un pilotage par l'identification des risques. Ils ont nommé un directeur de la gestion des risques dont la mission était d'atteindre cet objectif et de pérenniser la démarche.

Même si l'organisation de l'entreprise est en mutation lente vers une gestion par processus, la culture reste fondamentalement ancrée sur les silos de métiers. Chaque mise en place d'une activité transverse est interprétée par les opérationnels comme un "reporting en plus" ou pire, une mode qui aura son temps, ce qui est évidemment destructeur des bonnes intentions de départ.

…/…

…/…

Le directeur, ancien opérationnel lui-même, a proposé d'utiliser la cartographie des risques pour structurer le processus et apporter rapidement un élément concret, utile aux responsables opérationnels dans le cadre de leur mission. De façon à présenter des résultats en peu de temps permettant d'entraîner l'adhésion du management, il a choisi de lancer une première opération d'identification et d'évaluation "descendante" (top down).

En réalisant l'interview des 80 premiers responsables de l'entreprise, basée sur les objectifs de chacun, les grands risques ont été identifiés. Après avoir mis au point, avec l'accord de la Direction Générale, un système extrêmement simple d'évaluation des risques, une deuxième interview des mêmes managers, centrée sur l'application du système à leurs risques a permis le calcul du niveau résiduel de chaque risque, une classification des risques entre eux et enfin une première vision globale des risques.

La présentation de ce premier travail, seulement six mois après la décision de lancement, a fait l'objet d'un débat interne passionné qui a ouvert largement la porte à la mise en place de la même démarche dans chaque entité de l'entreprise, poussée cette fois, par le management dont le besoin était de suivre l'évolution des plans de réduction de risques et d'identifier de nouveaux risques. Il est vrai que les occurrences de quelques crises dont les éléments avaient été identifiés ont donné une valeur forte à l'exercice cartographique.

La cartographie est maintenant entrée en phase itérative sur un rythme trimestriel. Depuis 3 ans, le management s'en est petit à petit approprié l'usage. Le fait qu'elle ait commencé en démarche descendante a permis la vision d'une large palette de risques dépassant les risques purement opérationnels pour inclure et hiérarchiser des risques stratégiques ou financiers.

Obtenir une vision globale des risques

Objectifs de l'organisation

Toute organisation a une "raison d'être". Selon le type d'organisation observée – l'entreprise, la filiale, l'unité opérationnelle, le processus – cette "raison d'être" va s'identifier sous des noms différents : mission, ambition, stratégie, niveau de service, résultats ou le plus souvent, objectif. La démarche de la gestion des risques a précisément pour objet d'identifier et d'évaluer dans un premier temps les menaces, les obstacles, appelés risques, susceptibles d'empêcher l'organisation d'atteindre sa "raison d'être" de façon à pouvoir mettre en place au mieux des ressources disponibles, les actions donnant à l'organisation une "assurance raisonnable" de sa réussite.

Appréciation du risque

Analyse des risques

■ *Identification des risques*

Outils et techniques d'identification

Selon la démarche utilisée ("top down"/ "bottom up") plusieurs outils ou techniques peuvent être combinés.

Les techniques d'identification et de première estimation des risques ont déjà été décrites ci-dessus[25]. Elles reposent principalement sur des entretiens individuels, des ateliers ou des questionnaires au cours desquels le risk manager cherchera à identifier les risques adossés aux objectifs ou issus d'indicateurs de performance ou encore d'événements susceptibles de menacer l'organisation[26].

Les principaux outils utilisés sont les suivants :

– Analyse du déroulement des processus.
– Appui sur l'expertise de tiers (ex. assureurs, courtiers, spécialistes, consultants).
– Synergies avec les autres systèmes de management[27].

---

[25] *Voir Deuxième partie : "Choix préalables" - "Opter pour une démarche".*
[26] *Voir Annexes : "Questionnaire pour un entretien avec un dirigeant dans le cadre d'une démarche Top down".*
[27] *Voir Première partie : "Le risk manager et la cartographie" - "Les différents acteurs du management des risques".*

– Base de données/bibliothèques d'événements/portefeuille de risques.
– Approche par scénarios qui consiste à cerner l'événement potentiel engendré par le risque et ses conséquences, en une définition simple. Il est utile d'envisager l'hypothèse de plusieurs scénarios combinant eux-mêmes plusieurs risques.

Ces outils ou techniques seront choisis par le risk manager principalement en fonction des ressources humaines, matérielles et financières dont il dispose.

	Avantages	Inconvénients
Questionnaires	Ressources nécessaires pour la mise en œuvre.	Utilisation de questions fermées. A mauvaises questions, mauvaises réponses.
Ateliers	Consensus, échanges et vision globale.	Censures de participants. Consommateur de ressources.
Entretiens individuels	Qualité de l'information recueillie.	Très consommateur de ressources (en entretien + en harmonisation des informations).

Quels que soient les outils ou techniques utilisés, il est important :

– De s'appuyer sur l'univers des risques pour tendre vers l'exhaustivité (*voir page 56*).
– De confronter les informations recueillies afin d'en assurer la cohérence.
– De procéder à une première estimation des risques identifiés : "Quelles en seraient les conséquences ?", "Quel niveau de vraisemblance, quelle probabilité ?"
– D'avoir conscience que tous les risques identifiés dans une cartographie ne sont pas susceptibles de se produire en même temps.

L'utilisation d'un système d'information

L'utilité et la satisfaction qu'apporte un logiciel informatique dépendent évidemment de la qualité du logiciel, mais encore, et peut-être surtout, de son adéquation avec les besoins de l'entreprise[28].

Il est recommandé de produire quelques exercices cartographiques par ses propres moyens avant de se lancer dans l'achat d'un logiciel. En effet, pour permettre une expression des besoins claire et précise, il est préférable de s'appuyer sur une expérience interne vécue. Pour s'installer durablement dans la culture d'entreprise, c'est bien le processus de gestion interne qui doit structurer le cahier des charges du logiciel et pas l'inverse[29].

Dans tous les cas, le risk manager désirant acquérir et mettre en œuvre une solution informatique supportant la gestion de ses risques devra identifier au préalable les attentes auxquelles l'outil devra répondre[30] et connaître les ressources dont il dispose (budget, temps, équipe projet interne…).

Retour d'Expérience

L'entreprise X a très vite été confrontée à la question de l'outil pour mener à bien l'exercice cartographique.

Un rapide tour d'horizon nous a permis d'identifier qu'il existait peu de logiciels complètement adaptés. Mais surtout le besoin de rapidité de résultat ne permettait pas, dans un premier temps, de nous laisser entraîner dans une étude complexe dans laquelle, n'ayant pas eu le temps de développer nos propres convictions, ce sont celles du prestataire de l'outil qui risquaient de nous être imposées.

…/…

---

[28] *Au sein de la Commission - "Systèmes d'Information" - de l'AMRAE, un groupe de travail SIGR (Systèmes d'information de Gestion des Risques) édite un panorama des logiciels tous les ans suivant deux axes :*
– Analyse de la couverture par le produit des 19 axes fonctionnels (assurances, audit, cartographie des risques…).
– Analyse de la couverture par le produit des composantes du COSO II.
Pour télécharger l'étude : www.amrae.fr

[29] *Afin d'aider les risk managers à analyser et à comparer les solutions informatiques disponibles sur le marché, nous proposons en annexe quelques critères qu'il conviendra d'adapter au contexte de chaque entreprise.*

[30] *Voir Première partie - "Les pré-requis d'une cartographie".*

…/…

Le maître mot de la stratégie de mise en œuvre étant la simplicité pour un meilleur partage, nous avons décidés de développer en interne un outil provisoire sur tableur.

Même si nous avions conscience qu'il n'était pas parfait et qu'il nous faudrait sans aucun doute en changer, l'outil que nous avons construit nous a permis de nous poser les bonnes questions, de corriger par nous mêmes les défauts, d'avancer en interne dans la compréhension de notre besoin, d'opérer plusieurs cycles d'exercices cartographiques pour caler l'étalonnage des évaluations, d'emporter l'adhésion des opérationnels avant d'engager un investissement important.

Nous sommes actuellement en recherche d'un logiciel et constatons la difficulté des fournisseurs potentiels à répondre précisément à nos objectifs avec un produit "sur étagère".

Description des risques

Alimentation de l'univers des risques/catalogue des risques

Le recours à l'univers des risques est un moyen de s'assurer de l'exhaustivité des domaines couverts par l'analyse. Des bases de données ou portefeuilles de risques sont utilisés. Ces "bibliothèques d'événements" recensent les risques inhérents à un secteur d'activité, à un projet ou à un domaine spécifique. Peuvent ainsi être recensés des risques, des sources de risques ainsi que les bonnes pratiques relevées pour y parer.

Obtenus à l'extérieur, ces catalogues de risques doivent être, bien entendu, adaptés aux spécificités de l'entreprise, objet de l'étude. Ils peuvent également être élaborés en interne. En tout état de cause, il convient de les enrichir régulièrement, notamment par l'expérience propre de l'entreprise. Cet outil, efficace, ne doit ni être figé, ni constituer la seule approche de l'analyse.

<table>
<tr><th colspan="3">Risques externes</th></tr>
<tr><td colspan="3">Concurrence - Lobbying social - Politique étrangère - Législation - Catastrophes naturelles - Réglementation - Crise sur marché clé - Terrorisme - Relations avec les parties prenantes - Partenaires - Innovation technologique</td></tr>
<tr><th colspan="3">Risques internes</th></tr>
<tr><td colspan="3">Risques stratégiques</td></tr>
<tr><td colspan="3">Labelling - Propriété intellectuelle - Stratégie de développement - Business model - Canaux de distribution Portefeuille - Perte de part de marché - Stratégie Marketing - Profitabilité - Fusion & acquisition - Intégration - Gouvernance</td></tr>
<tr><td>Risques opérationnels</td><td>Capital Humain</td><td>Conformité</td></tr>
<tr><td rowspan="5">Santé et Sécurité - Connaissance, savoir-faire - Développement - Cycle de vie des produits - Pollution - Accident majeur - Distribution - Arrêt de l'activité - Dommages aux tiers - Défaillance équipement critique - Qualité produit/service - Carence de fournisseurs - Dommages aux actifs - capacité - Carence Energie - Interdépendance entre sites - Erosion marque…</td><td>Externalisation – Personne clé – Communication – Compétences gestion du changement/recrutement</td><td>Législation & Réglementation – Contractuelle – Juridique – Communication financière</td></tr>
<tr><td>Gouvernance</td><td>Intégrité</td></tr>
<tr><td>Leadership – Délégation – Limites – Autorité – Performances incitatives</td><td>Fraude – Actes illégaux – Usage illégal – Ethique – Image de marque</td></tr>
<tr><td>Système d'information</td><td>Finances</td></tr>
<tr><td>Technologie – Infrastructure – Intégrité – Accès – Maintenance – Disponibilité – Confidentialité – Dépendance – Externalisation</td><td>Taux d'intérêts – Liquidité – Risque Crédit – Pension – risque de change – Management finance (budget, forecast, pricing, impôts…) Dépréciation d'actifs</td></tr>
</table>

Exemple de registre des risques

	Nom/ Description du risque	Estimation du risque*		Evaluation du risque*	
		Fréquence	**Gravité**	**Fréquence**	**Gravité**
1	**Echec à la mise en place du SI de gestion**	Moyenne	**Financier** → Fort **Réputation** → Moyen	Moyenne	**Financier** → Fort : Absence de Chiffre d'affaires sur 3 mois = environ 80 m€ Temps de panne système → Très fort : incapacité du système à fonctionner pendant 3 jours minimum
2	**Entente illicite**	Fort	**Financier** → Très fort **Réputation** → Moyen	Fort	**Financier** → Très fort : 10% du CA **Réputation** → Moyen
3	**Défaillance qualité**	Moyenne	**Financier** → Moyen **Réputation** → Moyen	Peu probable	**Financier** → Moyen : CA maxi par produit 10 m€ **Réputation** → Très fort : Crédibilité du groupe basée sur la qualité et la confiance

* Les notions d'"estimation" et d'"évaluation" sont définies page suivante.

Alimentation du registre des risques/journal des risques/fiches de risques

Dès l'issue des premières démarches d'identification, il va être possible d'alimenter un registre ou journal des risques reprenant les éléments essentiels des risques identifiés. Ces éléments seront affinés au fur et à mesure de l'analyse. Le tableau page ci-contre en donne un exemple.

Ce registre est en général enrichi :

– Des sources ou causes des risques analysés.
– Des mesures ou actions décidées pour en assurer la maîtrise.
– De l'évolution des risques constatée à l'issue de la réitération de la démarche.

Mise en perspective de l'information recueillie

L'analyse des risques se fait, comme on l'a vu sur une base déclarative, et c'est bien le propriétaire des risques qui en a, en règle générale, la vision la plus complète. Cette vision peut néanmoins s'avérer subjective, ce qui pourrait faire perdre toute crédibilité à la démarche. Il est donc fortement recommandé, à chaque fois que cela est possible, de confronter les informations recueillies afin d'en assurer la cohérence. A minima, il est en général possible de conforter une information émanant d'une direction opérationnelle auprès de la direction fonctionnelle concernée par le sujet (ex. risques RH, financiers, fiscaux, juridiques...).

Sous réserve de veiller à la confidentialité des données recueillies, il est également possible de s'appuyer sur l'expertise de tiers.

Enfin, certaines entreprises vont au-delà et instituent un comité consultatif des risques, dont les membres sont sélectionnés en fonction de leur compétence, de leur vision à la fois globale et transverse de l'organisation. Ce comité, réuni périodiquement, a pour fonction de revoir les risques majeurs identifiés et d'en valider tant la pertinence que les éléments d'évaluation retenus.

Estimation des risques

L'estimation est un moyen, au cours d'une interview, d'apporter une matière de réflexion complémentaire pour qualifier l'identification d'un risque. Au moment où l'interviewé exprime l'éventualité d'un risque, il doit pouvoir donner une estimation de la gravité selon sa propre échelle de valeur (grave, très grave, catastrophique). Il peut aussi donner sa perception de la capacité du risque à se produire dans son échelle de temps (maintenant, dans un an, dans 3 ans, dans 10 ans). Cette approche permet une réflexion propre à mieux définir les contours du risque en précisant une certaine idée de sa valeur.

L'estimation sera complétée ultérieurement par une véritable évaluation.

Evaluation des risques selon une méthode qualitative

La méthode d'évaluation des risques dépend des choix faits par les entreprises :

- Certaines décideront de raisonner selon une méthode qualitative qui consiste à suivre une échelle décrite et détaillée qui est la résultante d'un travail de groupe et non d'une étude d'expert ou représentative d'une vérité absolue. Il n'y a donc pas de niveau critique de risque universel qui serait identifié par la méthodologie. C'est à chaque entreprise de définir son échelle de risques. C'est une étape importante dans le processus de gestion des risques car elle permet de donner une gravité potentielle à la réalisation d'un risque. Néanmoins, la hiérarchisation des risques est plus importante que leur évaluation. En effet, pour un risk manager il est plus urgent de pouvoir communiquer sur les priorités de l'entreprise plutôt que sur une évaluation potentielle "exacte" des risques.
- Il existe aussi une autre approche qui n'est pas fondée sur la notion de niveau de risque mais sur celle de scénarios. L'impact est alors évalué non par rapport à l'intensité d'un risque spécifique mais par rapport à une corrélation de risques qui, en soi, peuvent être d'une intensité faible ou moyenne mais dont le cumul dans une chaîne de causalité produira un événement critique. Cette méthode est empruntée au secteur des assurances. Elle consiste à estimer le sinistre raisonnablement escomptable (SRE) ou le sinistre maximum possible (SMP) pour choisir les actions à mener.
- L'entreprise peut aussi opter pour une évaluation quantitative des risques (non détaillée dans le présent ouvrage) qui consiste à utiliser des bases historiques (incidents, sinistres, …) pour évaluer d'une manière plus "statistique" les risques de l'organisation. En résumé, cela revient à "se servir du passé pour prévoir l'avenir".
- Dans des cas spécifiques, l'évaluation "à dire d'experts" peut aussi être utilisée. Il s'agit d'une évaluation faite par … des experts. Par exemple, lors de l'évaluation de l'impact d'un tremblement de terre, il peut être utile pour un risk manager de s'en remettre à l'évaluation d'experts dans ce domaine.
- Enfin, le risk manager peut aussi avoir recours au modèle "bayésien". Les réseaux bayésiens sont un outil d'aide à la décision pour le risk manager. A travers une représentation graphique des sources du risque, des actions de réductions / de transferts, le risk manager peut calculer, sur la base de probabilité attachée à chaque élément, l'exposition, la survenance ou la gravité du risque mais également le coût du financement ou de la réduction du risque. Les réseaux bayésiens sont utilisés dans l'analyse de risques, mais également dans le diagnostic médical et industriel, dans la détection des spam et dans le data mining.

Mise en place des échelles de valeurs

La cartographie étant une visualisation graphique des risques, son élaboration passe par une démarche d'évaluation des éléments "impact, occurrence et maîtrise" sur des échelles de valeurs. Pour chaque risque seront calculés les enjeux, l'intensité ou l'impact, c'est à dire les conséquences directes et indirectes, à l'horizon retenu, dans un scénario "réaliste maximisé" (que peut-il arriver de pire ?). L'échelle de valeur doit permettre de décrire les conséquences financières ou autres, quantifiables ou non, d'un risque ou d'un événement identifié.

Ces échelles sont définies en interne pour chaque entreprise selon des critères qui lui sont propres. Elles doivent passer par une présentation et validation de la Direction Générale avant toute utilisation.

Le niveau de maîtrise du risque, élément indispensable pour caractériser le risque, est à prendre en compte dès les premières analyses. Il sera, par la suite, comparé au niveau de maîtrise cible souhaité par l'organisation pour, le cas échéant, être augmenté[31].

Echelle de l'impact

Il s'agit d'élaborer une graduation d'intensité de destruction (à l'image de la fameuse échelle de Richter pour les tremblements de terre), en partant de 0 (pas d'impact) pour arriver au degré le plus élevé tel que l'atteinte de ce dernier serait destructeur de l'entreprise (impact maximum). Certaines entreprises attachent à ces degrés des valeurs financières. Même si ceci n'est pas une obligation, l'évaluation pouvant parfaitement rester qualitative, la traduction financière de l'impact, lorsqu'elle est possible est recommandée : elle facilitera l'agrégation et la hiérarchisation des risques de toutes natures et, partant, la lecture de la cartographie.

Il est extrêmement important que les utilisateurs du processus de gestion des risques retrouvent le langage de l'organisation dans son échelle de gravité, notamment :

– En reprenant les termes majeurs du reporting interne tels que Cash Flow, Capex, ROI[32], …
– En intégrant des natures d'impact propres à l'organisation. En effet une compagnie aérienne n'aura pas les mêmes natures d'impact qu'une entreprise de distribution grand public.

---

[31] *Le lecteur est invité à se reporter à la partie II du présent ouvrage qui traite en détail de la maîtrise du risque.*

[32] *Capex (Capital Expenditure) : dépenses d'équipement. ROI : retour sur investissement.*

Il est également important de définir le vocabulaire qui exprimera l'intensité du risque comme par exemple :

- *Catastrophique* : Conséquences maximum qui provoqueraient en cas de crise, la destruction probable de l'entreprise, avec un retour au nominal impossible.
- *Majeur* : Conséquences entraînant la destruction d'une partie importante des ressources de l'entreprise, avec un retour au nominal long et difficile.
- *Fort* : Conséquences lourdes pour l'entreprise. les objectifs ne seront pas atteints et le retour au nominal sera complexe.
- *Modéré* : Conséquences indésirables mais n'affectant souvent qu'un secteur isolé de l'entreprise, avec un retour au nominal réalisable dans un temps relativement court.
- *Faible* : Peu de conséquence, avec un retour au nominal simple et rapide.

L'échelle de l'impact doit permettre d'évaluer l'ensemble des risques que l'on peut trouver dans l'organisation. Elle doit donc comprendre plusieurs natures d'impact et permettre aux utilisateurs d'évaluer facilement les risques identifiés. Toutefois, il est important d'avoir présent à l'esprit que trop d'informations tue l'information… Il est donc plus utile de proposer 4 ou 5 natures d'impacts bien ciblées qu'une vingtaine, ce qui désorienterait l'utilisateur et compliquerait son évaluation.

Cependant, si les degrés d'intensité s'apprécient généralement sur 4 ou 5 qualificatifs pour donner une position tranchée, certaines entreprises ont besoin d'un nuancier plus souple. Dans le cas d'un choix à 4 degrés, il suffit de réunir les deux degrés les plus proches, par exemple : risques modérés et faibles ou risque catastrophique et majeurs.

Exemple d'échelles

Natures d'impact	Faible	Moyen/ Modéré	Fort	Très fort/ Catastrophique
Financier	X € ou % de Chiffre d'affaires, Cash Flow / Capex / ROI			Y € ou % de Chiffre d'affaires, Cash Flow / Capex / ROI
Financier	Insatisfaction mineure des actionnaires, X% de chute du cours de bourse			Insatisfaction majeure des analystes, Y% de chute du cours de bourse
Gestion de projet	Retard de X mois			Retard de Y mois
Production	X unités produites en moins			Y unités produites en moins
Production	Insatisfaction faible de la qualité des produits (Taux de litige client < X appels par jour)			Interdiction définitive de mise en production (Taux de litige client >Y appels par jour)
Systèmes d'information	Temps de panne < X mn			Temps de panne > Y mn
Environnement	Danger pour l'environnement sur site, maîtrisé rapidement			Danger pour environnement hors site se traduisant par des effets dommageables
Client	X% de part de marché, abonnements, …			Y% de part de marché, abonnement, …
Réputation	Série d'articles dans la presse locale/ spécialisée du secteur			Couverture négative de grande ampleur par les médias nationaux
Responsabilité	Responsabilité engagée, événement réglé par un accord amiable			Responsabilité pénale des mandataires sociaux / de la personne morale
Personnel	Traitement médical nécessaire pour quelques employés			Nombreuses victimes au sein et à l'extérieur de l'organisation
Personnel	Démotivation dans un service / département / unité. Turn over de X%			Démotivation de l'ensemble du personnel de l'organisation. Difficultés majeures dans le recrutement. Turn over de Y%
…etc				

Pour chaque évaluation proposée, l'utilisateur devra justifier son appréciation. Il est important pour le risk manager de comprendre le modèle et les hypothèses d'évaluation suivies. Cette compréhension sera d'autant plus utile lorsqu'il faudra consolider plusieurs évaluations de sources différentes.

De plus, de nombreux risques peuvent s'évaluer sur plusieurs natures d'échelle (*voir l'exemple ci-dessous*). Cela complique le processus d'évaluation notamment au niveau de la réelle évaluation du risque.

Retour d'Expérience

Le risque d'"échec dans le lancement d'un nouveau produit" aura plusieurs natures d'impact telles que :

– La perte (l'absence) de chiffre d'affaires.
– L'atteinte à la réputation.

L'utilisateur évalue les deux natures d'impact et justifie de ses appréciations pour chacune d'entre elles.

Perte de chiffre d'affaires : Faible - le marché est nouveau, les prévisions de vente étaient de 20 000 unités par an, l'absence de vente représente 300k€.

Atteinte à la réputation : Fort - le lancement du produit doit rajeunir l'enseigne et initier une nouvelle stratégie de modernisation dans l'entreprise. Si les journaux nationaux font une campagne de dénigrement sur l'incapacité de l'enseigne à se rajeunir, cela va être très négatif pour l'entreprise en terme d'image.

En fonction de la politique d'acceptabilité[33] du risque établie par l'entreprise, les risques de réputation "fort" pourront être traités prioritairement par rapport aux risques évalués "faible" ou "moyen" en perte de chiffre d'affaires (voir Deuxième Partie - Maîtrise du risque).

[33] *Voir Deuxième partie : "Méthodologie" - "Maîtrise du risque" - "Décision" - "Politique d'acceptabilité du risque".*

Echelle de probabilité d'occurrence

Là aussi, il s'agit d'une graduation mais cette fois, elle correspond à la probabilité de survenance du risque dans le temps. Attention, chaque entre prise agit sur un marché avec un espace/temps propre à ce marché. Par exemple, la vitesse d'évolution d'un marché comme les télécoms est beaucoup plus forte que celle d'un marché de l'industrie lourde. Quand le premier va se positionner sur des degrés annuels en dépassant rarement une visibilité au delà de 5 ans, le deuxième le fera sur des tranches de 10 ans.

		Description de la réalisation	Réalisation calendaire	Probabilité de réalisation
4	**Quasiment certain**	Événement attendu dans la plupart des cas	Immédiat	> 50 %
3	**Possible**	Événement probable dans la plupart des cas	12 mois	> 20 %
2	**Peu probable**	Événement devant se produire à un moment donné	3 ans	> 10 %
1	**Rare**	Événement risquant de se produire à un moment donné	5 ans	< 10 %

Retour d'Expérience

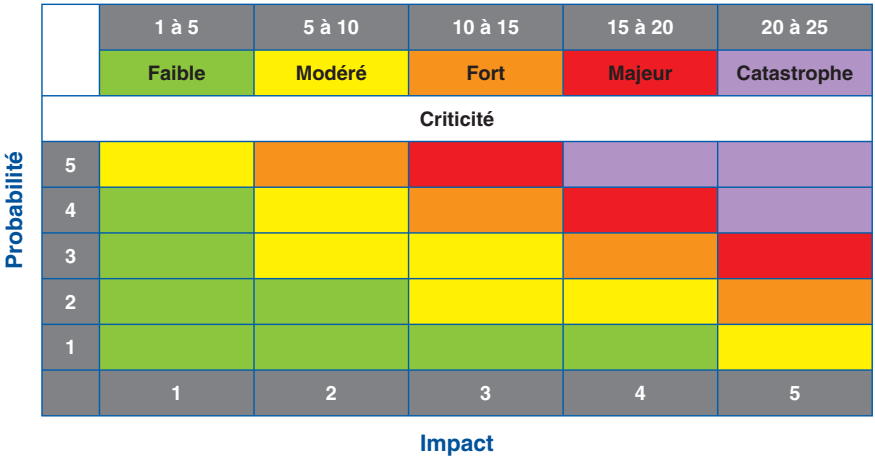
Dans mon entreprise, l'occurrence est un élément qui a longuement été débattu. Ce domaine d'évaluation, fortement conditionné par la perception de chacun, a été vu comme la partie faible de la méthode, dont le danger était de masquer facilement la réalité du risque par une confiance trop optimiste ou, sous la pression du moment, de crier "au loup" inutilement sur un risque faible. Sachant qu'en cas de crise, l'occurrence du risque devrait toujours être à son maximum, pourquoi ne pas donner cette vision là dès le départ ?

Le PDG a tranché en demandant à ce que l'occurrence soit représentée uniquement sous la forme d'une couleur. Le risque surligné en rouge présente l'occurrence la plus élevée, le niveau inférieur est surligné en noir, le suivant en vert, le suivant en bleu et le dernier n'est pas surligné. La vision cartographique est produite sur l'axe de l'impact en abscisse et l'axe de la maîtrise opérationnelle en ordonnée. Elle permet de positionner le risque au niveau où il se situerait en cas de crise, la couleur venant apporter la notion d'imminence du risque. Le mode de lecture, adopté par tous, est aujourd'hui complètement intégré à notre façon de gérer les risques.

En fait il s'agit là d'une convention partagée qui démontre bien que l'exercice est lié à l'objectif recherché dans un référentiel de culture interne.

Le calcul de la criticité

La criticité est le résultat du produit de l'impact par la capacité de survenance. Elle exprime un facteur de vraisemblance donnant au risque une intensité plus ou moins grande. Il est parfois utile, selon les besoins internes, de visualiser la criticité qui est le premier stade vers la cartographie. Dans ce cas, il suffit de positionner sur un graphique les degrés de l'occurrence en abscisse et les degrés de l'impact en ordonnée et de positionner sur le graphique les risques évalués selon ces deux critères (Voir schéma ci-après).



■ *L'agrégation des risques*

La cartographie des risques Groupe est élaborée à partir des cartographies des entités. A l'échelle du Groupe, elle intègre une étape complémentaire qui est l'agrégation des risques des différentes entités cartographiées (voir également à ce sujet la Partie III).

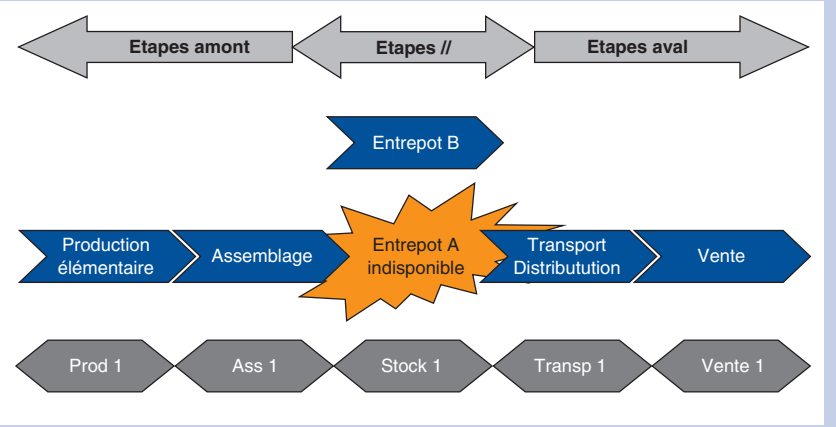
Les risques Groupe sont constitués de risques indépendants au sens statistique, c'est-à-dire dont la survenance n'est pas liée par une chaîne de causalités.

Il est donc nécessaire d'identifier en premier lieu les risques des entités dépendants entre eux, liés par une même chaîne de causalités, générée le plus souvent par les relations entre les activités des entités au sein du processus d'activité du Groupe.

Risques transverses

Les entités identifient les risques dépendants d'autres risques issus d'autres entités. Elles précisent si chacun de ces risques a des conséquences sur une étape amont du processus sur lequel le risque dépendant agit, ou sur une étape en aval du processus :

Retour d'Expérience



Dans cet exemple, considérons le risque portant sur un entrepôt indisponible, entraînant l'arrêt de la production et de l'assemblage, et une indisponibilité de produits finis à la vente : dans ce cas, l'entreprise va subir des coûts dus à l'arrêt de production et de l'assemblage, et des pertes de chiffre d'affaires. L'image de marque de l'entreprise sera altérée par l'impossibilité de répondre aux clients, c'est donc le risque commercial qui portera cet impact d'image.

Le risque transverse sera constitué en supposant que tous les risques dépendants sont liés entre eux à 100 %, soit avec un coefficient de corrélation de 1, ce qui permet de déduire ses impacts :

L'impact financier = la somme des impacts financiers
L'impact image = l'impact image maximum
L'impact humain = l'impact humain maximum

Il en résulte que :

- La probabilité d'occurrence du risque transverse est la probabilité du risque générateur.
- La criticité du risque transverse est la criticité maximum des trois criticités.
- La maîtrise du risque transverse est la moyenne des niveaux de maîtrise des risques dépendants.

Risques Groupe

La constitution de risques Groupe répond au besoin de disposer d'une vision synthétique de l'exposition du Groupe à ses risques. Cette approche se veut globale et synthétique, et doit permettre de rapprocher les risques Groupe des orientations et politiques générales.

Constitution du panier des risques

– Les risques Groupe sont constitués en regroupant un "panier de risques" similaires au sens du modèle de risques, ayant des conséquences similaires et, en cas de doute, des causes similaires. Le panier de risques comprend des risques transverses et des risques entités indépendants.
– Les entités ayant connaissance de la cartographie des risques Groupe, proposent le rattachement de chacun de leur risque à un risque Groupe pour garantir la cohérence du panier de risques.
– En cas de doute de la part d'une entité ou de la Direction de Management des Risques (DMR) quant au rattachement d'un risque entité, un échange aura lieu pour préciser le contour de ce risque. Le cas échéant, il pourra être décidé de le scinder ou de le préciser de façon à assurer la cohérence du rattachement.

Méthode d'agrégation

– L'agrégation se fait en déduisant un risque équivalent au sens statistique, qui représente les impacts et la probabilité d'occurrence d'exposition au panier de risques, sur la base d'un modèle statistique. Les statisticiens proposent différentes méthodes d'équivalence pour identifier la valeur en risque (VAR) telle que la méthode de Monte-Carlo :
– Criticité financière = l'impact financier et la probabilité attachée équivalents,
– Criticité d'image = l'impact image maximum et la probabilité attachée au panier réduit aux risques ayant un impact image,
– Criticité humaine = l'impact humain maximum et la probabilité attachée au panier réduit aux risques ayant un impact humain.
– La criticité retenue est la criticité maximum des trois criticités. La maîtrise du panier est la moyenne des niveaux de maîtrise des risques constitutifs.

Entités travaillant au périmètre du Groupe

– Les entités travaillant au périmètre du Groupe, en particulier les entités tête de filière (DSI Groupe ou DRH Groupe par exemple), réalisent leur cartographie sur leur périmètre de responsabilité. Attention, elles ne couvrent pas toujours l'intégralité du périmètre du Groupe.
– Pour ne pas compter deux fois le même risque (risques agrégés par les entités tête de filière et risques identifiés par l'entité), la DMR se rapprochera de l'entité tête de filière pour vérifier le périmètre qu'elle couvre et le compléter le cas échéant par des risques non inclus dans sa cartographie.
– De même, les plans de traitement qui déclinent l'activité opérationnelle des entités complèteront le plan de traitement identifié par l'entité tête de filière : plan d'affaires, plan de sauvegarde Groupe,…

Rattachement des risques entités

– L'évaluation des risques entités est cotée Impact(I) / Probabilité(P) / Maîtrise(M) de 1, niveau le plus faible, à 4, niveau le plus grave.

Entité	Risque Entité	RG SI	RG Qualité	RG Accidents
		I/P/M	I/P/M	I/P/M
Production	SI en panne > 1 jour	3/1/3		
Production	Dérive des machines outil		2/2/1	
Production	Accidents du travail			1/1/4
Assemblage	SI en panne > 1 jour	4/1/1		
Assemblage	Banc de montage en panne		4/3/1	
Assemblage	Accidents du travail			1/1/4
Entrepôt	Climatisation en panne		4/1/2	
Entrepôt	Robotique en panne		4/1/1	
Transport	Accident de circulation			3/2/3
Transport	Véhicules en panne		1/3/3	
Vente	Si client en panne > 4 h	4/2/3		
DSI	Centre de calcul en panne > 1 h	4/2/1		
DRH	Grève du personnel		4/1/1	
	Risques équivalents	3,7 / 1,8 / 2	3,2 / 2,1 / 3	2,4 / 1,8 / 3,5

Compte-rendu sur les risques bruts

Livrables

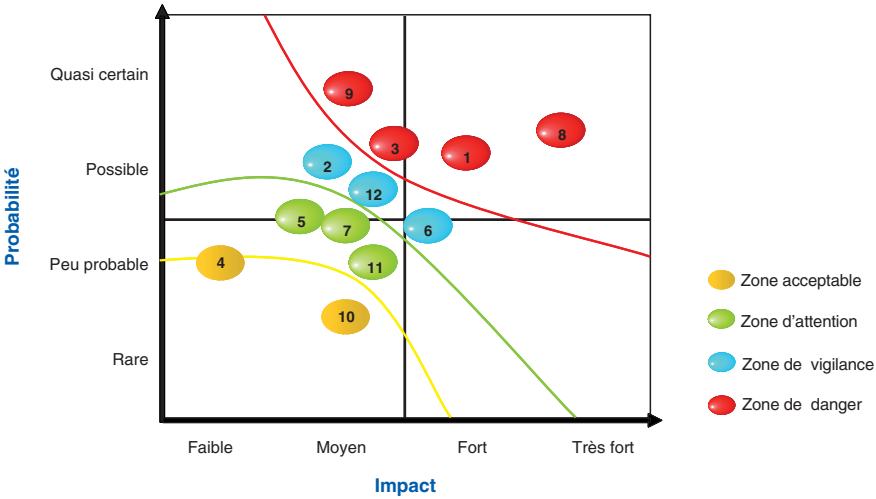
Une première représentation des risques bruts[34] encourus par l'entreprise peut, à ce stade, être réalisée.

Chaque organisation choisira la forme de sa cartographie en fonction notamment des éléments qu'elle souhaitera mettre en avant :

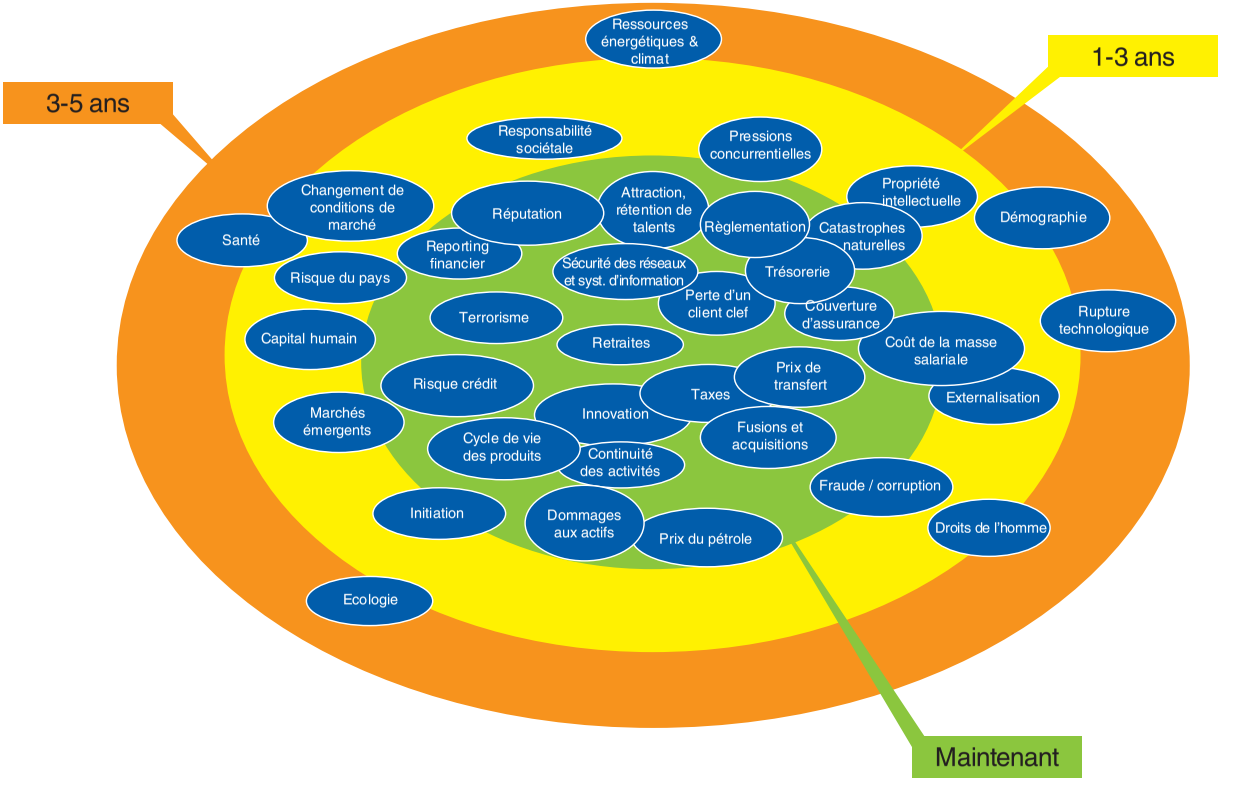
– Cartographie probabilité/impact.
– Cartographie des risques classés selon leur échéance (horizon des risques),
– Cartographie illustrant la part de chaque entité dans un risque donné (portefeuille des risques).
– Cartographie des risques classés selon leur nature (radar des risques).

En voici quelques exemples (l'expérience révèle que le plus simple reste souvent le plus pertinent) :

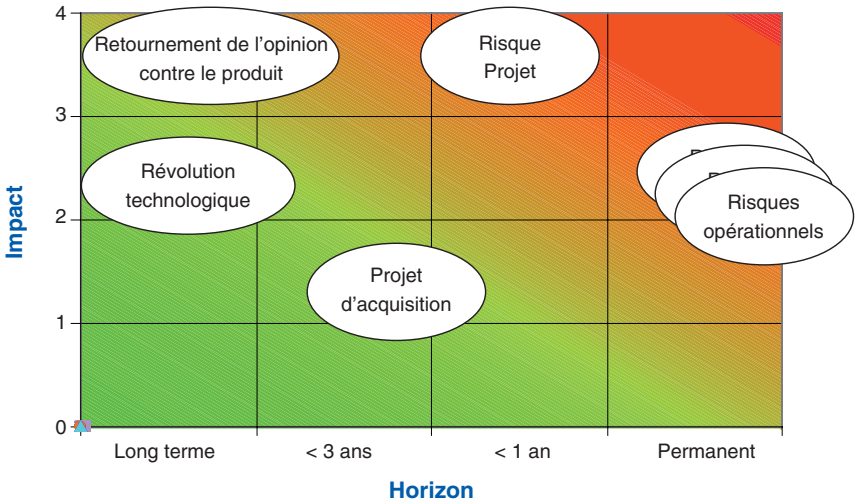
■ *Cartographie probabilité/impact*



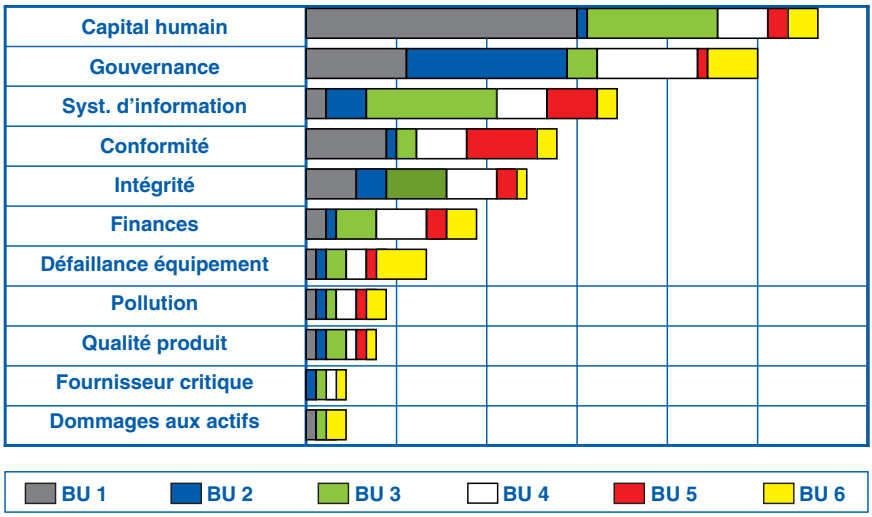
[34] *Est appelé "brut", le risque avant prise en compte des mesures de contrôle et de transfert à la différence du risque "résiduel" qui tient compte de ces mesures.*

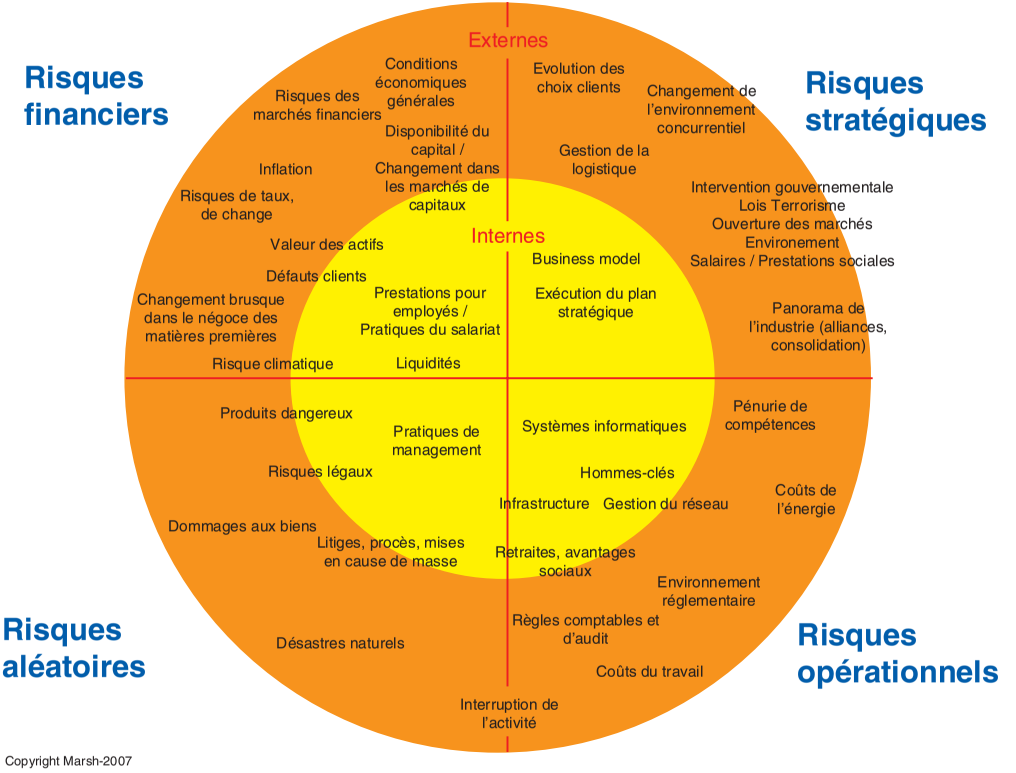

3-5 ans
1-3 ans
Maintenant
Ressources énergétiques & climat
Responsabilité sociétale
Pressions concurrentielles
Changement de conditions de marché
Réputation
Attraction, rétention de talents
Propriété intellectuelle
Démographie
Santé
Règlementation
Catastrophes naturelles
Reporting financier
Sécurité des réseaux et syst. d'information
Trésorerie
Risque du pays
Perte d'un client clef
Couverture d'assurance
Terrorisme
Rupture technologique
Capital humain
Retraites
Coût de la masse salariale
Prix de transfert
Risque crédit
Taxes
Externalisation
Marchés émergents
Innovation
Fusions et acquisitions
Cycle de vie des produits
Continuité des activités
Fraude / corruption
Initiation
Dommages aux actifs
Droits de l'homme
Prix du pétrole
Ecologie

Cartographie "horizon des risques"



Cartographie vision "portefeuille des risques"





Copyright Marsh-2007

Validation de la cartographie

La validation doit être faite par le manager de l'entité qui a participé à l'élaboration de la cartographie et qui en sera responsable. C'est une étape incontournable[35]. Elle permet de partir d'une base saine et d'éviter toute remise en cause ultérieure.

Cette étape préalable clôture l'exercice de cartographie des risques bruts et permet le lancement du plan d'action sur une base de risques acceptée par toutes les parties prenantes.

Le manager de l'entité doit confirmer formellement le résultat de la cartographie, pour :

- Reconnaître les conclusions de l'analyse réalisée et officialiser son engagement à mieux maîtriser tout ou partie des risques cartographiés.
- Définir des améliorations concrètes dans le traitement de chacun des risques prioritaires (interdire toute tentation postérieure de minimiser ou de nier ces risques).
- Informer le Comité Exécutif (ou la Direction générale) des risques que l'entité est impuissante à traiter et dont l'éventuel plan d'actions est du niveau de cette instance.

Ce principe de validation est unanimement reconnu par les entreprises consultées, sachant qu'une cartographie correspond à un instant "T" et peut comporter des lacunes.

A ce niveau, quelques écueils peuvent émerger :

- La sur-pondération d'un risque : le manager met un risque en évidence afin d'obtenir des ressources pour le traiter. Cette sur-pondération peut aussi être la conséquence d'une méconnaissance de certains types de risques comme ceux auxquels sont exposés les systèmes d'information. Le risk manager peut jouer ici un rôle de modérateur en tant que garant du processus de cartographie.
- Une formulation excessive ou pessimiste de certains risques comme la responsabilité pénale du manager qui valide la cartographie par exemple. La survenance du risque doit être formulée comme une probabilité et non comme une certitude. Le risque doit cependant être clairement décrit afin de permettre à la cartographie de jouer son rôle d'alerte et d'initiation du plan d'action.

[35] *Elle est même rendue obligatoire dans les procédures SOX (Sarbanes Oxley).*

– A l'inverse, il peut y avoir aussi une sous-pondération d'un risque. Il peut être difficile pour un manager de reconnaître l'existence d'un risque important dans son domaine de responsabilité. Cela pourrait être interprété comme un aveu d'impuissance ou comme une défaillance dans l'exécution de la mission qui lui a été confiée. La tentation de sous-pondérer le risque existe également lorsque le manager a soutenu personnellement un projet ou une décision particulière.

Enfin, une dernière question se pose : lors du processus de validation, le management a-t-il la possibilité de corriger les résultats des travaux du groupe de travail qui a réalisé la cartographie ?

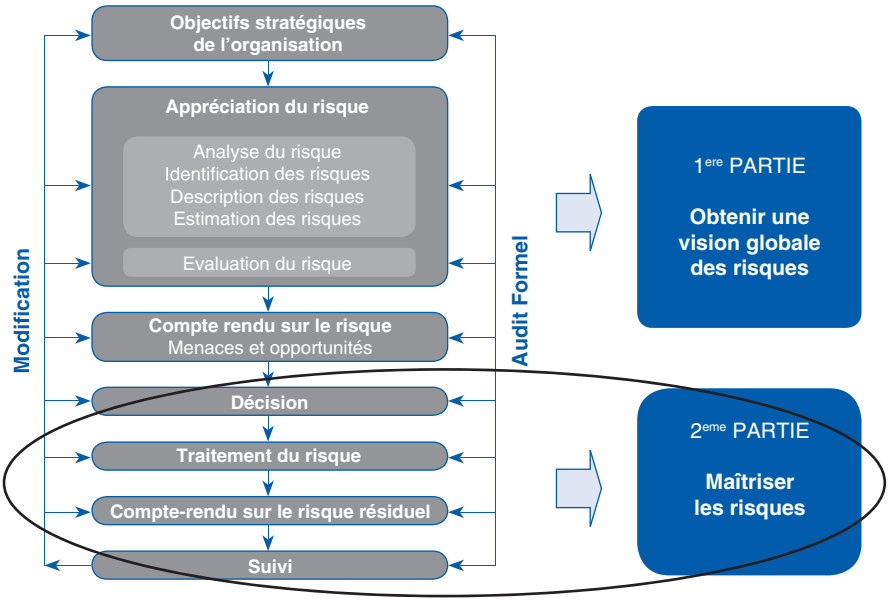
Le retour d'expérience semble montrer que les entreprises laissent souvent une latitude au management pour des corrections à la marge s'il estime que les membres du groupe de travail n'ont pas disposé de toute l'information nécessaire sur un point de détail. Toutefois, afin d'éviter toute dérive, il est fortement recommandé de prévoir un processus encadrant et limitant cette possibilité de correction dès lors qu'elle remet en cause les conclusions étayées. Il s'agit ici d'éviter deux extrêmes : la remise en cause totale ou une validation sans jugement.

Il peut arriver aussi que les entreprises réservent la faculté de modifier la cartographie des risques à l'audit interne.

Maîtriser les risques

A ce stade, les risques ont été identifiés et évalués mais leur degré de maîtrise, en l'état, par l'organisation n'a pas encore été cerné de façon précise.

Une fois cette étape franchie, les entreprises auront une vision globale de leurs riques et seront alors mieux armées pour mettre en place les meilleures actions de réduction et de transfert de ces risques.



Dans l'esprit du risk management, l'approche de la maîtrise des risques est résolument opérationnelle. Elle consiste à poser les questions suivantes :

– Comment traiter les risques cartographiés de manière exhaustive ou sélective ?
– Qui doit les traiter ?
– Quel est le rôle du risk-manager dans la mise en place des plans d'actions ?
– Comment motiver les responsables opérationnels ?
– Quelles ressources peut-on allouer au traitement de ces risques ?

Décision

La décision du traitement à réserver à un risque donné va tenir compte du degré de maîtrise qu'a d'ores et déjà l'organisation sur ce risque.

Politique d'acceptabilité du risque

L'acceptabilité est en fait une notion très variable selon le métier et la culture de l'entreprise, c'est pourquoi cette notion doit être définie par une politique validée par la Direction Générale.

En fait, il s'agit de préciser :

– *L'appétence pour le risque* qui consiste à poser des bornes (des limites) qu'il ne faut en aucun cas dépasser. Il s'agit de répondre à des questions simples : Quels sont les risques que l'entreprise est prête à prendre pour mener sa stratégie ? Jusqu'où ne pas aller trop loin dans l'exécution de la stratégie de l'entreprise ? En fonction des ambitions de chaque entreprise, son appétence pour le risque sera différente.
– *Le niveau (ou seuil) de tolérance aux risques,* c'est-à-dire la variation par rapport à ses objectifs que l'entreprise peut accepter, d'un point de vue stratégique mais aussi, et c'est très important, du point de vue de ses valeurs internes et de son éthique. Il s'agit ici de définir une marge de manœuvre.

La tolérance au risque peut être définie comme ce qui "peut" être assumé par l'entreprise à la différence de l'appétence pour le risque qui correspond à ce que l'entreprise "veut" assumer.

Ces critères expliquent qu'aucune politique d'acceptabilité n'est transposable telle quelle d'une entreprise à l'autre.

La facilité consiste à définir l'acceptabilité du risque de manière financière (x euros) en calculant le résultat d'une péréquation entre le coût de la réduction du risque et le montant du sinistre qui peut être absorbé par l'entreprise si le risque venait à se réaliser.

Mais ce seuil d'acceptation va dépendre aussi de la tolérance au risque de l'entreprise qui est variable selon :

- La nature des risques (nul ou très bas pour la réputation, la sécurité[36] ou l'intégrité des personnes[37]).
- Le cœur de métier de l'entreprise.
- Mais aussi les nouvelles activités ou les nouveaux produits envisagés dans son plan de développement.

Ainsi, l'impact financier du crash d'un avion de ligne, par exemple, est important mais pas destructeur des résultats d'une compagnie aérienne correctement assurée. En revanche, est-il envisageable que cette compagnie aérienne intègre comme "acceptable" un certain pourcentage de crash de ses avions ?

La part d'irrationalité dans l'approche d'une politique d'acceptation rend indispensable une réflexion profonde des décideurs et mandataires sociaux au plus haut niveau de l'entreprise. Il n'est pas possible, dans le cadre d'une saine gestion des risques, de faire l'économie d'une telle réflexion, parce qu'elle conditionne l'identification des priorités de traitement et donc de maîtrise recherchée des risques. Pourtant il n'est pas recommandé de concevoir une politique d'acceptabilité avant d'avoir réalisé une première cartographie. En effet, la première vision des risques de l'entreprise avec leur position relative dans la cartographie permet de rester dans le concret et d'établir de véritables règles de pilotage pour dégager les priorités réelles pour l'entreprise.

---

[36] Dans l'industrie nucléaire par exemple, la tolérance sera égale à zéro pour tous les risques de sécurité, même si la sécurité n'est pas identifiée comme un risque majeur par la cartographie.

[37] Certains risques ne peuvent être assortis de seuil d'acceptabilité comme ceux qui impactent la vie humaine (comment accepter des morts dans un accident ?). Néanmoins, même dans ce cas où la tolérance est nulle, on ne saurait négliger la préparation d'un plan de crise au cas où le risque "inacceptable" se produirait malgré tout.

Une bonne façon d'aborder ce sujet avec les décideurs consiste à leur montrer la cartographie globale du premier exercice et à leur poser la question : que voulez-vous voir ? Jusqu'où voulez-vous voir ? Tous les risques ? Une partie seulement mais à partir d'où ? Les réponses vont rapidement permettre de jeter les bases de la politique d'acceptabilité.

Choix des risques à traiter

Deux pratiques divergentes ont été notées :

- Certaines entreprises ne veulent pas faire de choix. Elles estiment qu'à partir du moment où un risque a été identifié, il doit être traité. Elles optent donc pour un traitement exhaustif de leurs risques. Cette position est souvent adoptée par des entreprises dont la culture est fortement inspirée par le contrôle interne. Son efficacité dépend cependant des ressources mises à la disposition des managers pour mener à bien les plans d'actions.
- D'autres vont opérer une sélection pour identifier les risques majeurs par rapport aux risques secondaires. Ces entreprises optent alors pour un traitement sélectif de leurs risques. Dans ce cas, la question est de définir des critères de sélection des risques à traiter en priorité. Par un souci de cohérence, cette sélection devra être validée formellement par la même instance que celle qui a validé la cartographie, afin d'assurer une suite logique entre cette étape et la mise au point des plans d'actions.

La cartographie est un des outils qui permettent d'opérer ce choix puisqu'elle hiérarchise les risques. Selon l'objectif qu'elle s'est fixée, la cartographie peut toutefois être insuffisante pour documenter entièrement la sélection des risques à traiter (Exemple : si l'échelle de cotation est uniquement financière, elle ne permettra pas de mesurer pleinement l'impact des risques sociaux ou d'image).

Idéalement, la sélection des risques à traiter prendra en compte les critères suivants :

- Les valeurs de l'entreprise (éthique, sécurité, politique sociale, respect de l'environnement, …).
- La réputation et l'image de l'entreprise.
- Le coût financier de la survenance du risque.
- L'impact sur la stratégie de l'entreprise.
- Les conséquences en responsabilité civile et pénale des dirigeants.

Traitement du risque

Choix des actions à mener

■ *Qui fait quoi ?*

Le choix des actions à mener relève de la responsabilité du management de l'entité. Cette responsabilité conduit à une double difficulté qu'il faudra surmonter :

– Les capacités de l'entité opérationnelle à financer les actions de maîtrise des risques.
– La tendance à ramener le plan d'actions de maîtrise des risques vers les processus habituels de l'entreprise. Les responsables opérationnels ont en effet du mal à apprécier la notion de risques majeurs car leur survenance est rare (bris d'une machine qui pourrait bloquer l'activité pendant plusieurs semaines) et privilégient le traitement des risques récurrents qui relève souvent d'un processus de maintenance (panne qui immobilisera une machine pendant trois heures).

Selon les entreprises, le risk manager peut avoir différents rôles dans le traitement des risques : animation, coordination, aide méthodologique, surveillance, alerte, …

Ainsi, pour favoriser l'"ancrage opérationnel" des plans d'actions à mener, le risk manager peut :

– Faire émettre par la Direction Générale un texte régissant les principes généraux de la gestion des risques de l'entreprise diffusé à tous les managers.
– S'assurer que la définition de fonctions/missions des managers opérationnels contient explicitement la maîtrise des risques parmi les outils de management standard.
– S'assurer que pour chaque plan d'actions, un pilote a été formellement désigné, ainsi qu'un responsable pour chaque action.
– S'assurer que le plan d'actions est pérennisé par des procédures auditées (en précisant par qui), par un reporting et une intégration dans les processus de progrès continu, de plan et de budget de l'entreprise.
– Rendre visible les actions de maîtrise de risque dans le plan stratégique de l'unité, et leur contribution aux objectifs stratégiques de l'entreprise.

Retour d'Expérience

Sur une dizaines d'entreprises interrogées, deux tendances majeures se dégagent :

- Une faible implication du risk-manager dans la mise en place des plans d'actions afin de responsabiliser les managers opérationnels. Cette position est surtout observée dans les groupes organisés en Business Units (entités dont les managers sont entièrement responsables).
- A l'inverse, dans d'autres entreprises, le risk manager va jusqu'à s'impliquer dans la mise en œuvre du plan d'actions sans toutefois en supporter la responsabilité. Cela se traduit par un accompagnement méthodologique et la mise à disposition d'outils de risk management.

L'implication du risk manager peut avoir un effet correctif mais elle doit faire l'objet d'un réglage assez précis car :

- Trop s'impliquer risque de transférer "de facto" la responsabilité du management de l'entité au risk manager qui n'a pas à l'assumer.
- Ne pas s'impliquer risque de démotiver le manager de l'entité locale qui y verra un manque d'intérêt des organes centraux de l'entreprise.

Compte tenu de cet avertissement, le risk manager intervient dans la plupart des cas en tant que conseil et garant du processus de management des risques. Il existe aussi des cas particuliers qui peuvent orienter ce réglage : de par sa position transverse, le risk manager pourrait être amené à piloter certains risques majeurs pouvant affecter plusieurs entités.

Méthodologie et outils

La multiplicité des causes et des conséquences possibles rend cette étape difficile… Il convient avant tout de fixer la cible à atteindre dans le traitement de ces risques en fonction du degré de tolérance de l'entreprise défini par sa politique d'acceptabilité du risque.

Dans cette démarche, plusieurs écueils sont à éviter :

- Ne pas fixer de seuil d'acceptation du risque peut conduire à ne pas prendre (ou accepter) assez de risques et donc à ne pas saisir des opportunités.
- Ne pas se fixer de cible à atteindre quand le résultat de toute action doit être mesurable.

Le seuil d'acceptabilité du risque et la cible à atteindre étant fixés, les actions à mener peuvent être déterminées par des méthodologies et des outils parfois empruntés à d'autres fonctions (qualité, sécurité, développement durable, environnement) :

- Arbre des causes.
- Méthode des scénarios[38].
- Mesure de l'écart entre le niveau de maîtrise et l'état de l'art (benchmark interne et externe).
- Le bon ratio coût/bénéfice des actions possibles (risques peu coûteux à traiter pouvant être réduits rapidement)[39].
- Approche causes/conséquences qui consiste à lister les actions agissant sur les causes (prévention/protection) et celles qui agissent sur les conséquences (transfert du risque/plan de continuité d'activité).
- Enfin, la facilité et la pertinence du choix des actions dépendent aussi de leur proximité avec un processus existant de l'entreprise[40].

Certaines entreprises vont jusqu'à intégrer directement ces critères dans l'échelle d'évaluation des risques de la cartographie. Dans ce cas, elles hiérarchisent les risques à traiter lors du processus de la cartographie en fonction de la nature de la réponse apportée en terme de traitement de ces risques : délai, facilité et coût des actions, efficacité sur la réduction du risque.

■ *Niveau d'intervention*

Le choix des actions à mener peut aussi rencontrer une limite liée à la nature même des risques : en effet, certains risques sont d'une nature ou d'une ampleur telles que l'entité exposée n'a pas les moyens de les traiter seule. C'est le cas :

- Des risques stratégiques (exemple : le renchérissement du coût d'une matière première ou la possible évolution d'une réglementation établissant un quota sur l'import d'une matière première) dont la solution ne peut être qu'une décision de la Direction Générale (rachat du fournisseur par exemple).

---

[38] Voir définition en deuxième partie : "Obtenir une vision globale des risques" - "Appréciation du risque" - "Analyse des risques" - "Méthode des scénarios".

[39] Voir plus loin : "Réalisation des actions".

[40] Les managers qui sont identifiés comme "propriétaires de risques" ont des difficultés pour construire un plan d'actions qui s'éloigne d'un processus qu'ils connaissent. Il est donc intéressant de tenter d'intégrer le traitement d'un risque dans une démarche déjà entreprise par le manager (démarche qualité par exemple).

– Des risques de nature transverse à plusieurs entités (exemple : risque d'approvisionnement par un fournisseur interne et en situation de monopole, dysfonctionnement d'un processus "corporate" comme la centralisation des achats, pilotage des projets R&D, les systèmes d'information) qui mettent en danger les objectifs d'une ou plusieurs entités.

Force est donc de reconnaître la non faisabilité d'une action de traitement d'un risque au niveau de l'entité concernée. La question est alors de savoir si le risque peut faire l'objet d'un traitement et, dans l'affirmative, de déterminer à quel niveau traiter ce type de risques (central ou local) et d'allouer les ressources en conséquence. Dans ce cas, il est recommandé au risk manager d'informer la Direction Générale afin qu'elle décide elle-même du plan d'actions ou qu'elle désigne un pilote approprié (entité client, fournisseur, service central,…).

Enfin, indépendamment du niveau de traitement des risques au sein de l'entreprise, certains risques ne pourront être traités ou optimisés que par un plan d'actions impliquant les parties prenantes de l'entreprise, c'est-à-dire des acteurs externes indépendants sur lesquels l'entreprise n'a pas de responsabilité directe. Dans ce cadre, "l'entreprise élargie" doit intégrer ses fournisseurs, ses clients (distributeurs), les communautés et collectivités locales, dans l'étude et l'exécution de ses plans d'actions. La difficulté est ici de trouver un juste équilibre entre les intérêts respectifs de l'entreprise et des parties prenantes.

Réalisation des actions

Blocages divers

La capacité de financement du traitement d'un risque dépend de son assurabilité (existence ou non de produits d'assurance sur le marché) et des capacités d'autofinancement de l'entreprise. La prise en compte de ce financement, quel que soit son mode, peut ainsi amener à réviser la classification de l'impact du risque. Les difficultés les plus fréquemment rencontrées peuvent être regroupées en deux registres :

– L'arbitrage entre l'investissement prévention et l'investissement production : même si un risque a été choisi, le financement du plan d'actions pour le traiter peut être un élément immédiatement bloquant. Les managers ont du mal à percevoir le retour sur investissement des plans d'actions qu'ils doivent financer car le risque est toujours aléatoire. Ce retour sur investissement est bien plus mesurable lorsqu'on investit dans l'accroissement ou la modernisation des moyens de production.

– Le manque de motivation ou d'adhésion sur un sujet mal compris et/ou trop souvent en marge des processus traditionnels.

Quelques solutions

Pour faire face à ces écueils, quelques pratiques utilisées dans certaines entreprises ont pu être recensées :

L'approche coût/bénéfice

Cette méthode consiste à mesurer les coûts (investissement de prévention par exemple) par rapport aux bénéfices obtenus (réduction de la probabilité de survenance du risque ou réduction de ses impacts). Toutefois, si le chiffrage "coût" est une approche classique et intuitive pour chaque investissement, en revanche, l'évaluation du bénéfice est plus difficile dans la mesure où la réduction d'un risque est rarement reconnue comme un gain par les entreprises. De plus, sur certains risques, le couple probabilité/gravité peut difficilement être quantifié dès lors que l'on touche à des risques sans fréquence.

Malgré tout, dans certains cas, cette évaluation est néanmoins possible. Ainsi, le bénéfice du traitement du risque de perte d'opportunité qui serait de ne pas investir dans un pays "sensible" peut être évalué par l'acquisition de parts de marchés rentables.

Le financement des risques transversaux

Vérifier que l'entité concernée est bien propriétaire du risque à traiter. S'il ne relève pas de cette entité, le financement de son traitement devra être supporté par une ligne budgétaire adéquate qu'il s'agit d'identifier[41].

La saisie d'une opportunité

Le traitement de certains risques peut demander des investissements importants considérés parfois comme "non rentable" (par exemple la prévention incendie, prévention des risques environnementaux, …) et de ce fait, ne sera pas considéré comme prioritaire. La bonne pratique consiste ici à saisir l'opportunité d'un nouvel investissement "métier" pour inscrire tout ou partie du traitement du risque dans l'enveloppe du financement de cet investissement (Exemple : sprinklers installés lors de la rénovation d'un bâtiment, traitement du risque environnemental ou du risque d'intrusion à l'occasion de travaux de réfection d'un bâtiment ou de la refonte d'une ligne de fabrication).

---

[41] *Voir deuxième partie : "Obtenir une vision globale des risques" - "Appréciation du risque" - "Agrégation des risques".*

La réduction du budget "assurances"

Certes, la finalité de la cartographie n'est pas l'assurance. La partie des risques assurables dans une cartographie est minime (elle représente 10 à 15% des risques identifiés). Mais on sait aussi qu'une bonne prévention de ces risques assurables permet de réduire le coût des primes d'assurances et/ou d'étendre les garanties des contrats[42].

Compte-rendu sur le risque résiduel

La maîtrise est une donnée fondamentale qui doit être retranscrite dans les outils de suivi des risques. Confrontée aux autres critères, elle va permettre l'élaboration de la version la plus aboutie de la cartographie, celle des risques résiduels.

Criticité et maîtrise

La criticité et la maîtrise des risques sont évaluées selon une graduation basée sur les niveaux de traitement des risques. En d'autres termes, c'est une échelle qui va permettre de mesurer les effets des actions (plan de secours, plan de contournement, plan de continuité d'activité, transfert à l'assurance) réalisées pour réduire le risque ou du moins en minimiser les effets.

		Degré de maîtrise	Temps maximum de retour au nominal	Description de la maîtrise
4	**Faible**	< 20%	> 1 mois	Non piloté
3	**Partielle**	< 50%	15 jours	Piloté, plan d'actions définis
2	**Forte**	< 80%	1 semaine	Piloté, plan d'actions en production
1	**Très forte**	> 80%	24 h	Piloté, plan d'actions testé, validé

[42] *Si tel est l'objectif, ou un des objectifs attendus, la cartographie peut aussi permettre un relevé topographique de l'assurance des risques. Pour chaque risque identifié, on peut se demander s'il est assurable. Dans l'affirmative, on vérifie qu'il est assuré. Si oui, on calcule le coût économique du transfert. Dans la négative, on cherche à savoir si cela relève d'une décision raisonnée. Si oui, on regarde s'il ne convient pas de la réexaminer.*

L'évaluation de la totalité des risques identifiés selon les échelles de risques[43] avant et après la réalisation des plans d'actions va permettre d'en déduire les risques bruts ou résiduels[44], tel que criticité moins maîtrise égale niveau résiduel du risque.

La matrice cartographique la plus répandue est celle qui, ayant positionné sur un graphique les degrés de criticité en abscisse et les degrés de maîtrise en ordonnée, permet de situer chaque risque selon ces critères (*Voir le schéma page 86*). La dynamique de cette évaluation réside dans la représentation de l'évolution des risques tel qu'il doit être possible de représenter le risque à son niveau initial, d'en faire une projection vers son point cible et d'en représenter sa situation actuelle, ce qui permet d'identifier rapidement le travail restant à accomplir ou le résultat du travail de réduction déjà réalisé (*Voir le schéma page 87*).

Inscription dans le journal des risques

Une fois les résiduels de chaque risque établis, il est possible de compléter le journal des risques qui peut avoir la forme d'une liste des risques classés par résiduels décroissants. Cette liste n'est pas une cartographie mais elle permet de visualiser une certaine cohérence dans la hiérarchie des risques entre eux et d'identifier rapidement les risques aux résiduels prioritaires (*Voir le tableau page 88*).

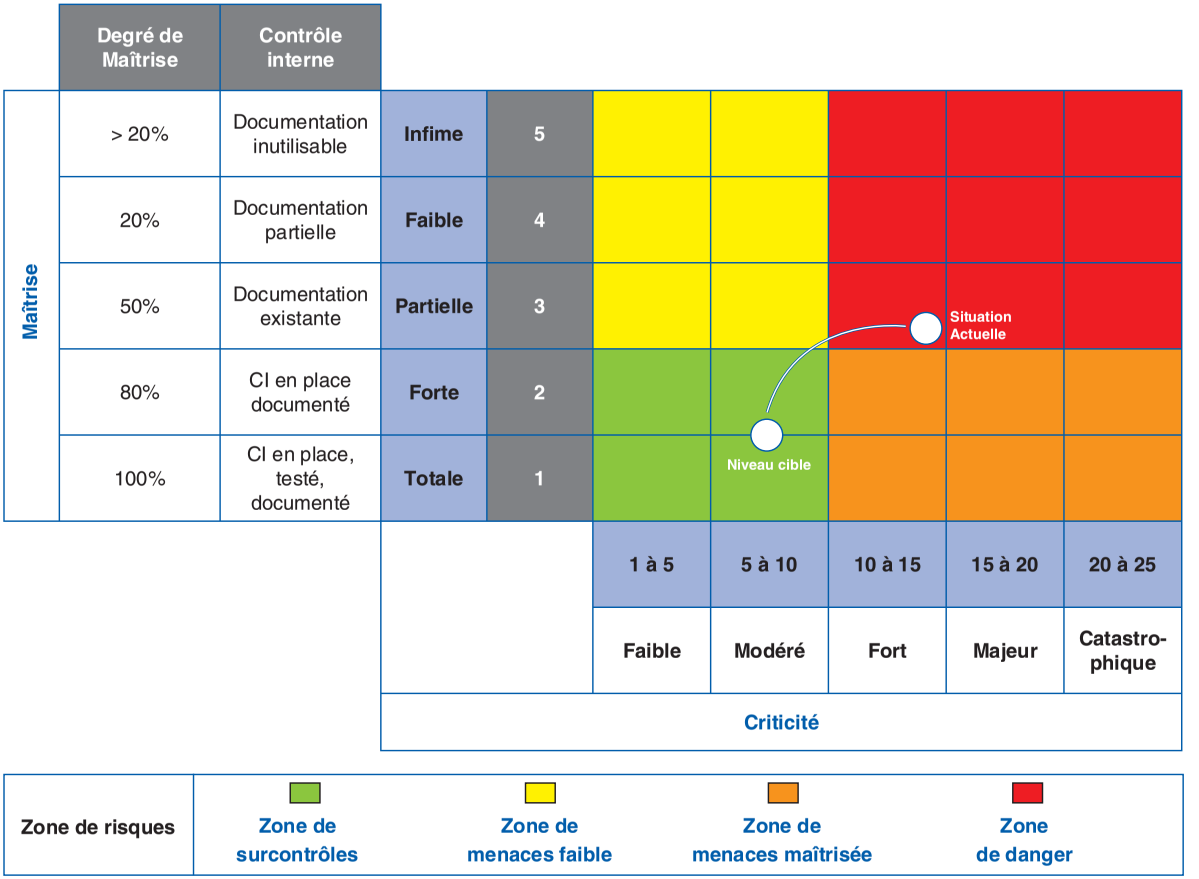
---

[43] Voir deuxième partie : "Obtenir une vision globale des risques" - "Appréciation du risque" - "Evaluation des risques selon une méthode qualitative".

[44] Voir la définition des risques bruts et des risques résiduels : Annexes - Glossaire.

	Degré de Maîtrise	Contrôle interne							
Maîtrise	> 20%	Documentation inutilisable	Infime	5					
	20%	Documentation partielle	Faible	4					
	50%	Documentation existante	Partielle	3					
	80%	CI en place documenté	Forte	2					
	100%	CI en place, testé, documenté	Totale	1					
					1 à 5	5 à 10	10 à 15	15 à 20	20 à 25
					Faible	Modéré	Fort	Majeur	Catastro-phique
					Criticité				

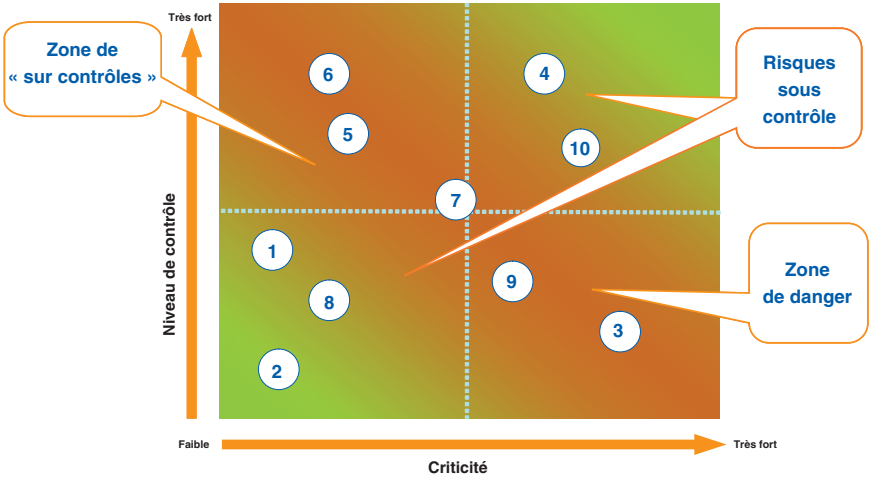
Zone de risques	Zone de surcontrôles	Zone de menaces faible	Zone de menaces maîtrisée	Zone de danger

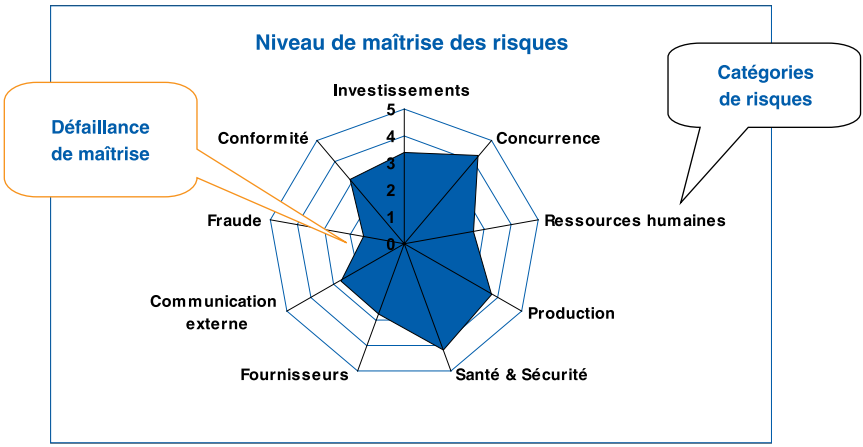

Degré de Maîtrise
Contrôle interne
Maîtrise
> 20%
Documentation inutilisable
Infime
5
20%
Documentation partielle
Faible
4
50%
Documentation existante
Partielle
3
80%
CI en place documenté
Forte
2
100%
CI en place, testé, documenté
Totale
1
Situation Actuelle
Niveau cible
1 à 5
5 à 10
10 à 15
15 à 20
20 à 25
Faible
Modéré
Fort
Majeur
Catastro-phique
Criticité
Zone de risques
Zone de surcontrôles
Zone de menaces faible
Zone de menaces maîtrisée
Zone de danger

	Nom/ Description du risque	Estimation du risque		Contrôles existants	Evolution N-1/N	Evaluation du risque		
		Fréquence	Gravité			Fréquence	Gravité	Maîtrise
1	**Echec à la mise en place de l'ERP**	**Moyenne**	**Financier** **Fort** **Réputation** **Moyen**		**Risque nouveau**	**Moyenne**	**Financier** : **Fort** – Absence de CA durant 3 mois = env. 80 M€ **Temps de panne système** : incapacité du syst. à fonctionner pendant 3 jours	**Forte** : Plans d'action en place / comité de pilotage mensuel
2	**Entente illicite**	**Fort**	**Financier** **Très fort** **Réputation** **Moyen**	**Procédure juridique**	**Absence d'évolution**	**Fort**		**Moyenne**
3	**Défaillance qualité**	**Peu probable**	**Financier** **Moyen** **Réputation** **Moyen**	**- Réglages machine - Visites fournisseur**	**N-1 : Criticité moyenne N : nouveau classement = Criticité forte (augmentation de la probabilité)**	**Moyenne**	**Financier** : **Moyen** CA maxi par produit = 10 M€ **Réputation** : **Très fort :** Crédibilité du Groupe basée sur la qualité et la confiance	**Faible** : Absence de contrôle depuis 2 ans/ Aucune visite fournisseur depuis 18 mois

Cartographie des risques résiduels (livrables)

A partir des matrices ci-dessus et du journal des risques mis à jour, il est possible de restituer le bilan de maîtrise des risques sous forme cartographique. Voici quelques exemples :





Suivi

Contrôle de la performance des actions

Sur la base de la cartographie des risques résiduels, une démarche qualité consistant à analyser la capacité des processus et actions mis en place à réaliser leurs objectifs de maîtrise des risques doit être initiée. Cette démarche implique l'identification et le traitement des risques de non performance liés à la pertinence du processus par rapport au résultat recherché. Comment contrôler la performance de la maîtrise des risques ?

L'entreprise dispose de deux leviers pour mener à bien cette tâche. Chacun de ces leviers opère selon une logique différente (opérationnelle pour le premier, réglementaire et procédurale pour le deuxième), ces deux logiques se complétant l'une l'autre. Ces leviers sont les suivants :

■ *Indicateurs de risques*

Le risk manager mettra en place des indicateurs de risque. Le contrôle sera réalisé une à deux fois par an afin de mesurer l'implication des entités et faire un reporting sur les points d'avancement et de blocage. Il existe des indicateurs de trois natures :

- Indicateurs de niveau de risques (pour les inondations par exemple).
- Indicateurs anticipateurs de crises (risques pays).
- Indicateurs de suivi de l'avancement des actions de maîtrise des risques (cet indicateur est fondamental pour mesurer le traitement du risque et documenter le reporting sur l'état d'avancement du plan d'actions)[45].

Ces indicateurs doivent être précisés dans un document de référence définissant les principes du risk management dans l'entreprise, et les acteurs concernés.

Contrôles internes

L'entreprise peut aussi s'en remettre aux contrôles réalisés par l'audit interne ou par les différentes fonctions spécialisées de l'entreprise comme la qualité ou l'environnement. Il s'agit alors d'une méthode classique d'audit : vérification de l'application des processus, contrôles dossiers par dossiers, test terrain, interviews des opérateurs, …)[46].

---

[45] *Par réflexe, les opérationnels ont tendance à s'en remettre aux processus de contrôle propres à leurs activités qu'ils ont déjà mis en place. Mais ces processus ne prennent pas toujours en compte le traitement du risque ou le font de manière incomplète.*

[46] *Rappelons qu'aux termes des réglementations en vigueur (SOX, LSF ; …), la maîtrise et la responsabilité du contrôle revient à l'audit interne et externe et non au risk manager, lequel peut toutefois être sollicité en tant qu'opérationnel de la gestion des risques.*

Afin d'éviter tout télescopage entre la démarche du risk management et celle du contrôle interne, il est recommandé de rédiger une Charte de "bonne entente" qui définira certaines règles[47].

Reporting

Une fois le contrôle fait, il s'agit de formater le reporting. Plusieurs pratiques ont été notées sur ce point :

- Certaines entreprises consolident l'ensemble des cartographies des entités et font une synthèse périodique du contrôle des plans d'actions et de leur impact sur les risques cartographiés. L'objectif est ici d'informer les destinataires du reporting.
- D'autres entreprises s'en tiennent à une synthèse des principaux risques de chaque entité. L'objectif est alors de permettre aux destinataires du reporting d'arbitrer les plans d'actions.

Il est nécessaire d'assurer un reporting au bon niveau de décision de l'entreprise : Comex, instances de Gouvernance (comité d'audit, conseil d'administration, …). La qualité de ce reporting est intiment lié à la performance dans l'atteinte des objectifs de transversalité du risk management de l'entreprise.

Nous insistons sur le fait que la cartographie est un document de travail de la même valeur qu'un tableau de contrôle de gestion. En tant que tel, c'est un document interne qui peut avoir un caractère confidentiel face à une possible interprétation déviante de personne non avertie du contexte évaluatif. Même si le livrable semble être un document accompli facile à transmettre, sa diffusion hors du management décisionnel est dangereuse. La décision du niveau de partage du document est du ressort de la Direction Générale. En tout état de cause, la diffusion d'un tel document ne doit pas se faire sans un accompagnement d'explications analytiques.

[47] *Cette Charte peut, par exemple, spécifier qu'aucun contrôle ne sera réalisé dans les six mois après réalisation de la cartographie afin de laisser le temps aux managers de mettre en place leurs plans d'actions.*

Les conditions de la réussite

Les facteurs clés de succès

Les facteurs clés de succès du déroulement des différentes étapes de la méthodologie et de l'utilisation de l'outil cartographique peuvent se résumer ainsi :

– Avoir le soutien de la Direction.

– Faire adhérer les participants en :
  • communiquant sur la démarche et sa valeur ajoutée,
  • faisant le lien avec les objectifs personnels des participants,
  • invitant les participants et la Direction à valider les résultats de la cartographie.

– Créer un climat de confiance en :
  • faisant preuve d'écoute,
  • garantissant qu'aucune information ne sera remontée sans en avoir préalablement discuté avec les intéressés,
  • respectant la confidentialité vis-à-vis des tiers.

– Mettre en place un dispositif efficace qui comprend :
  • un comité des risques au niveau central et au niveau des entités,
  • un réseau de correspondants.

– Faciliter la démarche en :
  • l'intégrant aux processus de l'entreprise (cohérence avec le développement durable, la qualité, …),
  • tenant compte du facteur "temps" (procéder à l'évaluation sur un délai court, avec présentation rapide des résultats).

Les écueils à éviter

– Faire une cartographie pour être à la mode.

– Démarrer la démarche par la recherche d'un système d'informations.

– Absence de rigueur illustrée par :
  • La remontée d'informations partielles à la Direction avant la fin de l'exercice.
  • La surévaluation des risques pour obtenir des ressources, ou leur sous-estimation par crainte d'être jugé ou de s'exposer à des représailles.
  • La tendance à ne pas objectiver les risques "biens connus" qui sont finalement sous-estimés.
  • Une mauvaise animation de la démarche qui réduit le processus cartographique à n'être qu'un réceptacle des doléances.

– Facteurs structuraux tels que :
  • Lourdeur, complexité de la mise en œuvre.
  • Coûts et manque de budget.
  • Résistance au changement et manque de motivation ou de disponibilité.
  • Difficultés à globaliser les cartographies.
  • Présence d'alternatives à la cartographie des risques.

*
* *

Troisième partie

Après la première cartographie

Les enjeux de la post-cartographie

Cette troisième partie s'adresse aux entreprises qui ont déjà réalisé une cartographie de leurs risques et qui s'interrogent sur les suites à donner à cet exercice. Le traitement de la post-cartographie concerne deux enjeux :

– La reconduite ou non du processus.
– L'impact de la cartographie sur la communication de l'entreprise sur ses risques.

En ce qui concerne la pérennisation du processus cartographique, l'objectif n'est pas d'établir une norme. Il s'agit plutôt de rendre compte des résultats d'un échange de pratiques entre industriels et consultants visant à identifier :

– Les questions qu'il faut se poser avant de s'engager dans l'étape post cartographie : Comment pérenniser le processus de cartographie ? Comment gérer la volumétrie croissante dans le déploiement de la cartographie ? Comment maintenir une bonne implication et garantir un bon niveau de contrôle ? Quels sont les moyens pour ancrer la cartographie dans le management opérationnel ?
– Les écueils que l'on rencontre lors du déroulement de cette étape.
– Les bonnes pratiques pour assurer le succès de la démarche.

En ce qui concerne la communication sur les risques, nous avons tenté de répondre aux questions suivantes :

– Comment communiquer sur les risques et sur les actions de maîtrise des risques ?
– Comment utiliser la cartographie à des fins de communication ?
– Comment utiliser la communication pour obtenir des résultats dans l'après-cartographie ?

Pérennisation du processus

Une cartographie est un diagnostic, une photographie globale des risques de l'entreprise à un moment donné. Par nature, elle est donc amenée à évoluer et l'entreprise ne saurait se référer indéfiniment à une première cartographie. La post-cartographie dépendra toutefois des objectifs qui auront été fixés lors de la prise de décision initiale d'entrer dans le processus cartographique[48].

Certes, la cartographie est une pratique encore jeune mais certaines entreprises commencent à avoir de l'expérience. Force est de constater que pour ces entreprises, la cartographie a évolué au fil du temps :

– Son périmètre s'est agrandi.
– Des acteurs plus nombreux y participent.
– Les outils et les méthodes s'affinent.
– Les bénéfices des résultats obtenus lors des exercices passés commencent à être perçus.

Retour d'experience sur les pratiques de mise à jour

Fréquence

Il y a un consensus général : la cartographie a une durée de vie limitée. Elle est un "arrêt sur image" dans la vie toujours changeante des entreprises. Certains vont même jusqu'à dire que la cartographie est déjà partiellement périmée le jour de sa publication. Aussi, n'est-elle pas un exercice "one shot". Elle évolue et doit s'inscrire dans une démarche récurrente. Reconduire l'exercice est une décision significative de l'importance et de la valeur ajoutée de la cartographie des risques[49].

---

[48] *Voir première partie : "La cartographie, ses raisons d'exister".*

[49] *Cette reconduction n'est cependant pas automatique. Si d'un point de vue intellectuel, tout le monde semble s'accorder sur le caractère éphémère d'une cartographie, le retour d'expérience a aussi mis en évidence certains cas où la reconduite de l'exercice est toujours en question après un premier exercice.*

A quelle fréquence faut-il renouveler la cartographie pour la maintenir à jour ? La réponse à cette question va dépendre de différents facteurs propres à chaque entreprise dont les principaux sont :

– La stabilité du business model qui dépend du contexte dans lequel une entreprise déploie son activité[50].
– La dynamique minimale pour conserver un bon niveau de motivation interne.
– La pression accrue des exigences réglementaires (celles de l'AMF notamment).
– L'acquisition d'une nouvelle activité ou le développement à l'international.
– La capacité des ressources internes à gérer les cartographies[51].

Les pratiques constatées montrent que la fréquence des cartographies est de six mois pour certaines entreprises et peut aller jusqu'à deux ans pour d'autres. Toutefois, il peut être intéressant d'aligner le renouvellement des cartographies sur les exercices budgétaires. C'est une manière de traiter simultanément le problème des allocations de ressources pour conduire les plans d'actions.

Un périmètre agrandi

La première cartographie, souvent initiée à partir du top de l'entreprise ("top down"), est fréquemment conduite comme un exercice pilote dont l'approche est globale et qui, parfois, ne concerne que quelques entités ou activités "test". Mais, si l'exercice est reconduit, on s'aperçoit qu'au fil du temps, la granulométrie des entités cartographiées devient plus fine.

Comment gérer cette évolution ? Deux logiques dominantes peuvent être observées :

– La première consiste dans le déploiement d'une équipe cœur (des professionnels de la cartographie) qui parcourt le groupe en se focalisant sur les entités les plus critiques sur lesquelles elle réintervient par rotation.
– La seconde consiste à démultiplier la démarche par la mise en place d'un réseau de correspondants qui touche des couches de plus en plus proches du terrain, ce qui revient à décentraliser la cartographie.

[50] *Les entreprises du secteur des nouvelles technologies, par exemple, ont des produits à durée de vie très courte et peuvent connaître une évolution rapide de leur business model.*

[51] *Il faut dimensionner la fréquence des mises à jour en tenant compte de la disponibilité des managers, par exemple.*

Ces deux logiques ne sont pas contradictoires et sont mêmes cumulées dans certaines entreprises.

Comment gérer la charge produite par ces deux démarches ? Le retour d'expérience fait état des solutions suivantes :

– Développer un outillage.
– Former des responsables locaux à l'exercice de la cartographie.
– Mettre en place des relais de contact pour suivre l'exercice.
– Ne revisiter qu'une sélection réduite des plus grands risques (exercice à deux vitesses : grands risques (fréquence 6 mois), tous les risques (fréquence 1 an).

Des outils et des méthodes qui s'affinent

La volumétrie croissante pousse vers des systèmes d'information dédiés. La réalité est contrastée à ce sujet. On note :

– Quelques expériences de bases de données intégrées des risques.
– Un rapport coût/bénéfice encore incertain pour beaucoup.

Avec le temps, les résultats gagnent en qualité. La maturité des managers dans le domaine de la maîtrise des risques a progressé et les évaluations sont mieux étayées.

A ce nouveau stade, l'extension du périmètre de la cartographie et l'augmentation de la volumétrie soulève la question de l'agrégation des risques. En effet, devant la masse d'informations ainsi recueillies, les entreprises ressentent le besoin de discerner les priorités et de détecter les problématiques transverses. Mais cette agrégation demandée, utile pour une communication synthétique des facteurs de risques d'un groupe multi-activités, se heurte à des difficultés techniques : homogénéité des risques agrégés, risque de caricature, rigueur discutable[52], généralisation excessive rendant impossible le traitement des risques.

[52] *Les agrégations de risques pratiquées ne se basent pas toujours sur de solides de fondements mathématiques. Et les indicateurs "naturels" peuvent être trompeurs. Une entreprise peut exporter 60% de sa production, cela ne veut pas dire pour autant qu'elle est exposée à un risque "pays" si ses zones d'exportation sont très diversifiées. Agréger ses risques sous cette bannière serait alors un abus. Voir sur ce sujet la Deuxième partie : Méthodologie - Obtenir une vision globale des risques - Appréciation du risque - Analyse des risques.*

Dans la pratique, on constate :

– Des synthèses de risques au niveau de la direction générale de l'entreprise.
– Des choix délibérés de ne pas agréger.
– Peu d'emploi d'outils à base quantitative[53], peu de gestion de type "portefeuille".

Faire évoluer la cartographie

Lors d'une nouvelle cartographie, comment exploiter les cartographies antérieures ? Comment faire le diagnostic de l'évolution d'un risque ? Comment identifier des nouveaux risques et mesurer l'efficacité des actions de traitement initialement menées ?

Il existe sur ce point des pratiques diverses :

– *La page blanche volontaire*. C'est une façon de se remettre totalement en question à chaque cartographie et d'éviter ainsi de s'enfermer dans les mêmes sujets.
– *L'analyse des évolutions*. Cette pratique part des résultats de la précédente cartographie. Elle permet de faire émerger et de mieux identifier les nouveaux risques par rapport aux risques persistants.

Ces deux pratiques tenteront de mettre en évidence les nouveaux risques ou l'évolution de certains risques pouvant résulter :

– D'une nouvelle activité ou de l'évolution du contexte (réglementaire, marché…).
– Du dépassement d'un seuil.
– De l'identification d'un risque qui n'était pas précédemment perçu.

A l'inverse, elles permettront aussi de constater la disparition d'un ou plusieurs risques[54].

[53] *Ces outils sont encore peu employés pour gérer des agrégations globales mais ils existent pour certains types de risques comme les risques financiers ou certains risques métiers.*
[54] *Il est essentiel de différencier ici un risque qui disparaît réellement pour une cause exogène, et un risque qui a fait l'objet d'un plan d'action. Dans ce cas, la question se pose de savoir s'il convient de rayer ce risque de la cartographie parce qu'au terme de son traitement il est considéré comme définitivement maîtrisé ou s'il faut maintenir ce risque dans la cartographie parce qu'il pourrait réapparaître.*

Il convient cependant de ne pas biaiser la démarche, ni interpréter trop simplement les résultats constatés. En effet, l'analyse demande du discernement car l'émergence de nouveaux risques, ou certaines évolutions des risques, peuvent être la conséquence de facteurs externes et ne sont pas, de ce fait, attribuables aux résultats du plan d'actions. La tentation reste malgré tout très forte d'attribuer une évolution positive au résultat du plan d'actions dont on a la responsabilité.

Maintien de la pertinence et du niveau de qualité des analyses

Eviter l'essoufflement et alléger la charge de travail de l'équipe centrale

L'implication du management est absolument indispensable pour maintenir la qualité de la cartographie et éviter un essoufflement possible. Conserver une bonne implication d'interlocuteurs de haut niveau reste un challenge critique. Après l'attrait de la nouveauté du premier exercice de cartographie, on observe parfois une baisse d'intérêt de la part de certains participants qui peuvent déléguer leur responsabilité à des collaborateurs, ce qui se traduit par une descente en gamme des interlocuteurs. L'identification des risques peut alors être incomplète et leur évaluation peut aussi manquer de hauteur de vue.

Les pratiques observées pour favoriser une implication au plus haut niveau sont les suivantes :

- Maintien de la supervision de l'exercice par un membre du management local.
- "Obligation de faire" venant du corporate avec un reporting attendu par le corporate.
- Faire évoluer la méthode de cartographie entre deux exercices afin d'alléger l'engagement du management en termes de disponibilité, de contraintes et de charge de travail.
- Visibilité donnée à l'exercice (nul doute que le reporting de l'exercice devant le Comité exécutif soit un stimulus important pour maintenir la pertinence et le niveau de qualité des analyses).
- Intégration de l'exercice dans les modèles de management du groupe. Il s'agit d'ancrer la cartographie dans la culture managériale des entreprises au même titre que l'exercice budgétaire ou l'exercice stratégique.

– Extension de l'exploitation des résultats de la cartographie à d'autres exercices dont elle maximisera les performances (input pour d'autres processus). L'erreur à éviter est d'en faire un exercice en chambre, déconnecté des autres processus managériaux.
– Réitérer l'exercice "top down" tous les 3 à 5 ans pour reconsidérer le contexte de risques au regard des nouveaux enjeux.

Contrôle de la qualité

Comment contrôler la qualité, en particulier à distance, via un réseau de correspondants ? Voici quelques éléments de réponse :

– Respecter les bonnes pratiques déjà citées (réseau, outils, méthodes, formation,…).
– Mettre en place un retour d'expérience sur l'exercice.
– Responsabilisation d'un manager local sur le résultat final.
– Obligation de validation formelle des résultats par le management local,
– Maintenir une étape de challenge des résultats par un tiers (étape de remise en cause, voire de contestation, pour éviter toute complaisance).
– Faire participer l'équipe centrale à certaines étapes clés.

A l'inverse, comment faire mourir la démarche ?

– Faire trop lourd.
– Piéger les participants (atteinte à la confidentialité, interprétation erronée ou utilisation inamicale des résultats, …). Il y a ici un enjeu de communication développé au chapitre suivant.

Communication externe

Exigences réglementaires et contraintes des marchés

La communication externe est essentiellement conditionnée par :

– Les obligations réglementaires auxquelles sont soumises les sociétés cotées (lois NRE, LSF et SOX, règlements européens…).
– La pression croissante des autorités boursières (AMF, SEC, …), des organismes financiers, sociétés de notation et autres.

Les résultats des travaux de cartographie peuvent constituer une base pour répondre aux exigences réglementaires et aux contraintes de marchés.

Quoiqu'il en soit, communiquer sur ses propres risques est un exercice particulier d'autant plus périlleux que le niveau d'exigence en la matière reste encore flou et mal stabilisé. Dans ce contexte, il n'est pas exclu que des forces de pression puissent conduire à des exigences toujours plus fortes comme la communication des cartographies et même des plans d'actions à des tiers (administration, organismes divers).

Une communication poussée à cette extrémité représenterait un vrai danger pour les entreprises car ces informations sont confidentielles, parfois incomplètes et peuvent prêter à interprétation pour des tiers éloignés de la réalité de l'entreprise. En outre, la cartographie est avant tout un outil de management des risques et n'a pas, à ce titre, vocation à être communiquée telle quelle à l'extérieur de l'entreprise.

La communication doit donc être considérée comme un risque à gérer. Le traitement de ce risque consiste à trouver un juste équilibre entre :

– Le droit à l'information des investisseurs (défini par les obligations réglementaires et les autorités de marchés).
– L'intérêt des entreprises.
– La confidentialité légitime de certains éléments.

Cet équilibre est propre à chaque entreprise qui doit définir sa stratégie en la matière.

La réglementation est très claire sur ce point. La responsabilité de la communication externe de l'entreprise sur ses risques revient à son dirigeant qui peut être mis en cause au civil comme au pénal pour toute erreur, lacune, falsification ou oubli graves dans la présentation faite aux marchés financiers.

C'est pourquoi il est important, dans ce cadre, d'examiner comment sont élaborés les éléments de communication externe en matière de risques tels qu'ils apparaissent dans les rapports annuels et les documents de référence des entreprises :

- Quel rapport existe-t-il entre la cartographie et la communication en matière de risques telle qu'elle est faite actuellement ?
- À qui est confié, dans l'entreprise, le soin de préparer cette communication ?

Force est de reconnaître qu'aujourd'hui :

- De nombreux contributeurs (direction financière, juridique, sécurité, environnement et développement durable, contrôle interne, etc..) participent, parfois sans concertation, à la rédaction des textes publiés dans la section réservée aux risques de l'entreprise des rapports annuels et des documents de référence.
- Aucune réflexion approfondie n'est menée sur le choix des risques sur lesquels doit porter la communication (risques avérés ou non, traités ou non, etc), sur la manière de les décrire et globalement sur l'utilisation des résultats de la cartographie dans cet exercice.

Il en résulte souvent un manque de cohérence dans les présentations qui sont faites et parfois aussi, de nombreuses lacunes. Il serait donc souhaitable que le risk manager participe davantage à la rédaction des rapports annuels :

- Afin d'éviter toute formulation inappropriée sur les risques.
- Pour aider à coordonner l'apport des autres fonctions de l'entreprise afin d'aboutir à un texte cohérent donnant une vision globale des risques de l'entreprise.
- Et, surtout, pour initier une réflexion sur l'utilisation des résultats de la cartographie comme une base commune de communication sur les risques.

La communication concerne également les risques visant les tiers tels que fournisseurs, clients (distributeurs), collectivités locales… L'entreprise doit prendre en compte cet aspect pour éviter qu'une mauvaise communication dégénère en crise (risque social ou environnemental).

Là encore, il s'agit de trouver un juste équilibre entre :

– Les intérêts respectifs des entreprises et des parties prenantes.
– La confidentialité de certains éléments (introduction systématique de clause de confidentialité dans les contrats).

Communication interne

Les contraintes et les enjeux

Le niveau de confidentialité de l'information délivrée aux collaborateurs est aussi la clé de voute de la communication interne. Il faut trouver le format adéquat et s'assurer que l'information est adressée au bon destinataire et ne soit pas divulguée à l'extérieur.

Le type de diffusion en interne est fonction des objectifs attendus de la cartographie. Les règles peuvent en effet varier en fonction de la nature du risque (sensibilité de l'information, "criticité" du risque…) et des acteurs concernés (diffuser la cartographie aux responsables des plans d'actions mais aussi aux directions ou entités qui sont parties prenantes). Pour éviter tout dérapage, ces règles peuvent être formalisées dans une charte de confidentialité.

La communication de la cartographie des risques provoque généralement un choc parce qu'elle révèle l'étendue des risques non transférables au marché de l'assurance et parfois non réductibles. C'est pourquoi il faut également veiller à ce qu'elle ne conduise pas à un "catastrophisme" qui décrédibiliserait la démarche et/ou déclencherait une crise non justifiée avec un impact pénal éventuel pour les dirigeants. Pour ce faire, la communication interne sur les risques de l'entreprise doit être considérée comme une opportunité de diffusion de la culture du risque.

Sous condition de respect des impératifs de confidentialité, cette communication permet :

– D'officialiser les objectifs de la cartographie.
– D'assurer une cohérence dans le langage "risque".
– De redéfinir les échelles de risques qui souvent mesurent la gravité des risques par rapport aux normes métiers en vigueur, et non en termes d'impact global sur l'entreprise (ou l'entité). La communication doit permettre de dépasser cette vision par silos en amenant l'entreprise à canaliser les priorités sur une liste commune de risques à traiter.
– De diffuser les bonnes pratiques existantes dans l'entreprise et de "benchmarker" les entités entre elles.

La communication au comité des comptes et de l'audit

Comme il a été dit précédemment la cartographie est un outil interne dont l'usage est destiné à l'exécutif. L'utiliser "en l'état" comme vecteur de communication sur les risques au comité d'audit ne nous semble pas de nature à aider ses membres à suivre l'efficacité du système de gestion des risques de l'entreprise. En effet la cartographie n'est pas un outil de gouvernance mais de pilotage de l'entreprise.

Nous recommandons de simplifier la cartographie des risques en :

– Présentant les 5 ou 10 risques majeurs.
– Montrant l'évolution de la criticité des risques entre deux périodes.
– Présentant succinctement les plans d'action adossés aux risques majeurs.

D'autres éléments utiles pour le comité d'audit seront nécessaires pour assurer l'efficacité du système de gestion des risques (politique de gestion des risques,…).

Conclusion

Quand elle n'est pas réalisée juste "pour la forme", la cartographie peut être un formidable outil de pilotage, d'aide à la décision et d'amélioration continue d'une organisation.

En faisant réfléchir les individus sur les risques et les opportunités de leur entreprise et en leur restituant une vision commune de ses risques, la cartographie permet de décloisonner les organisations, fédérer et mobiliser les ressources au service de la stratégie. Elle suppose d'avoir identifié ce qui est essentiel à la vie et au développement de l'entreprise, d'avoir défini ce qui est supportable et acceptable au regard des objectifs et de l'environnement global de cette dernière. Elle suppose aussi d'avoir rendu accessibles et compréhensibles ses résultats.

Cette démarche va inévitablement provoquer des questions de fond au plus haut niveau de l'entreprise et faire émerger des problèmes opérationnels qui auraient été ignorés ou négligés.

Accepter de voir ses risques, c'est déjà dépasser la peur de prendre conscience de ses limites. C'est se placer volontairement dans un mode de réflexion préventif face à la projection de l'image globale de ses menaces. C'est rationaliser ses inquiétudes ou ses angoisses, comme ses espoirs et ses envies.

Il devient rapidement évident que l'exercice cartographique participe largement à la mise en place du "contrôle interne" tel que défini par l'AMF dans le sens où elle met en évidence les zones prioritaires à placer sous contrôle pour en maîtriser l'évolution.

Au cours de leurs travaux, les auteurs du présent ouvrage ont constaté que leurs pratiques en matière de cartographie comportaient une certaine diversité propre au secteur d'activité de leurs organisations, à la culture de leurs entreprises, à la maturité des démarches de chacun, etc.. Néanmoins, deux constats ont fait l'unanimité :

– L'exercice cartographique n'est pas facile et son utilisation est toujours perfectible.
– Mais le résultat est à la hauteur de l'énergie dépensée et sa pérennisation fait entrer l'entreprise dans un cycle vertueux d'amélioration continue.

*
* *

Annexes

Glossaire

Criticité : Facteur de vraisemblance donnant au risque une intensité plus ou moins grande. Dans certaines méthodologies, la criticité est le produit de la probabilité par l'impact du risque (autre nom pour "espérance", terme mathématique).

Horizon : Vision de l'évolution possible du risque dans le temps. Echéance à laquelle le risque est susceptible de survenir.

Impact : Capacité maximum de destruction possible. Ensemble des conséquences d'un risque, financières ou non, appréciées dans le cadre d'un scénario "réaliste maximisé" : qu'est-ce qui peut arriver de pire ?

Maîtrise : Evaluation des moyens mis en œuvre permettant le traitement du risque.

Niveau de risque : Résultat de l'évaluation d'un risque prenant en compte sa criticité et sa maîtrise. Il peut se décliner en niveau de risque initial et niveau de risque cible.

Opportunité : Capacité de transformation d'un risque en réalisation positive.

Probabilité d'occurrence : Capacité d'un risque à survenir.

Risque : Eventualité d'un événement, d'une action ou d'une situation qui pourraient affecter l'atteinte des objectifs d'une entreprise. Le risque est caractérisé par sa probabilité d'occurrence et son impact.

Risque brut ou résiduel :

- Est appelé "brut", le risque avant prise en compte des mesures de contrôle et d'assurance. L'analyse des risques opérationnels se fait généralement par la notion de risque brut, de façon à identifier quel mode de traitement a été mis en place.
- Est appelé "résiduel", le risque après prise en compte des mesures de contrôle et d'assurance. En matière de risques stratégiques, l'analyse se fait sur les risques résiduels.

Risque opérationnel : Conséquences possibles d'un dysfonctionnement grave de la production de l'entreprise ou de ses processus opérationnels, en distinction des risques purement financiers ou stratégiques.

Risque stratégique : Conséquences possibles d'une décision ou d'une orientation initiée par le management engageant l'avenir de l'entreprise ou événement ayant des conséquences possibles sur la stratégie de l'entreprise.

Critères de choix d'une solution informatique

La commission Système d'information de l'AMRAE réalise chaque année une étude des caractéristiques techniques des outils de gestion des risques*.

Caractéristiques commerciales

Les performances du prestataire

- La qualité du partenaire (date de création de la société, chiffre d'affaires et effectif en France, budget en R&D, structure et organisation de la société, santé financière…).
- Ses références par secteur d'activité (et sur le progiciel de Risk Management en particulier).
- Sa connaissance du métier (orientation contrôle interne, gestion des risques dans le secteur financier, gestion des risques opérationnels…).
- Sa proximité géographique.
- La méthodologie de mise en place (cohérence du plan de gestion de projet, structure et qualité de l'équipe dédiée…).
- Les services proposés (conseils, paramétrage, formation, support de formation et documentation, accompagnement au déploiement, assistance, club utilisateurs…).

Maturité du progiciel

- Produit trop jeune : souvent synonyme de "bugs".
- Dernière version ancienne : peut être révélateur d'un manque de réactivité des concepteurs.
- Evolutivité : nombre de versions ou d'upgrades par an, intégration des besoins des clients…

Coûts de la solution

- Acquisition initiale / mises à jour.
- Coûts des licences (nominative, forfait, par type de licence…).
- Paramétrage (forfait pour le projet, coût moyen d'une journée de prestation).
- Formation, Assistance, Maintenance (taux et assiette de calcul).

Pour plus d'information sur cette étude : www.amrae.fr

Caractéristiques techniques

Couverture opérationnelle et fonctionnelle

Les fonctionnalités requises :

– Quelles sont les activités supportées par le logiciel (contrôle interne, risk management,…) ?

– Quelles sont les fonctionnalités génériques offertes par le progiciel ?
  • Processus de validation.
  • Alertes automatiques.
  • Extraction, reporting.
  • Administration fonctionnelle déléguée (périmètre).
  • Langue des menus.
  • Granularité et modularité de la structure des données (par régions, entités, pays, business units…).

– Quelles sont les fonctionnalités spécifiques au processus de cartographie des risques ?
  • Flexibilité (capacité d'accepter une identification des risques suivant les processus, les objectifs, les actifs de l'entreprise au travers d'entretiens ouverts ou de questionnaires fermés).
  • Echelles utilisées pour l'évaluation des risques (impact, probabilité, maîtrise etc.), limitation en nombre.
  • Gestion des consolidations et agrégations de risques.

Utilisateurs

Les niveaux de sécurité, confidentialité et faculté d'adaptation aux changements d'organisation :

– Quels sont les utilisateurs visés ?

– Quels sont les mécanismes d'authentification et les types de droits/rôles possibles ?

Intégration des SI

Les contraintes d'installation, d'intégration et de communication avec les outils informatiques et plateformes existants :

– Quel est l'environnement informatique requis pour l'installation du progiciel (équipement, architecture) ?

– Le logiciel peut-il s'intégrer et communiquer avec les autres logiciels/progiciels de l'entreprise ?

Interface homme-machine

Le plan de formation et de déploiement :

– L'interface est-elle conviviale, intuitive ?

– Quelle est la courbe d'apprentissage ?

Référentiels de gestion des risques

Pendant longtemps, les risk managers ont été hostiles à toute forme de normalisation. Ils étaient sensibles à la très grande diversité de leurs entreprises et redoutaient qu'on leur impose un costume trop étroit dans lequel il leur aurait fallu entrer.

Fort est de constater que l'application d'un référentiel de gestion des risques permet de structurer la démarche et de respecter les étapes clés favorisant ainsi le succès du projet.

Plusieurs référentiels de gestion des risques dont les principaux sont :

- AMF : Cadre de référence du contrôle interne et de la gestion des risques (en cours)
- COSO II : Le management des risques de l'entreprise
- FERMA : Cadre de référence de la gestion des risques
- ISO 31000 : Management du risque : principes et lignes directrices

Parmi les différents référentiels existants transparaissent des sensibilités différentes selon leurs origines. Certains sont très normatifs, d'autres définissent une démarche que les entreprises peuvent adapter à leurs particularités.

Nous décrivons ci-après, les principaux référentiels existants ou en cours d'élaboration[55].

[55] *Nous avons considéré Bâle 1 et 2 et Solvency 1 et 2 comme des référentiels de métiers spécifiques et non comme des méthodologies de management des risques.*

AMF

L'Autorité des marchés financiers a constitué un groupe de travail sur les comités d'audit dont la mission est :

En application de l'ordonnance du 8 décembre 2008, transposant la directive du Parlement européen et du Conseil de l'Union européenne du 17 mai 2006 concernant les contrôles légaux des comptes annuels et des comptes consolidés, les sociétés cotées sur un marché réglementé doivent se doter d'un comité spécialisé agissant sous la responsabilité du conseil d'administration ou du conseil de surveillance, pour assurer le suivi des questions relatives à l'élaboration et au contrôle des informations comptables et financières.

Sans préjudice des compétences des organes chargés de l'administration, de la direction ou de la surveillance, ce comité est notamment chargé d'assurer le suivi :

– Du processus d'élaboration de l'information financière.
– De l'efficacité des systèmes de contrôle interne et de gestion des risques.
– Du contrôle légal des comptes annuels et, le cas échéant, des comptes consolidés par les commissaires aux comptes.
– De l'indépendance des commissaires aux comptes.

Par ailleurs, la loi DDAC[56] du 3 juillet 2008 a étendu l'objet du rapport du président aux procédures de gestion des risques mises en place par la société, en détaillant, notamment, celles de ces procédures qui sont relatives à l'élaboration et au traitement de l'information comptable et financière pour les comptes sociaux et, le cas échéant, pour les comptes consolidés.

La nécessité d'avoir une interprétation claire des textes et d'en faciliter l'application, a conduit le Collège de l'AMF à constituer un groupe de travail chargé de rédiger un guide sur ces comités d'audit et de formuler des propositions d'adaptation du cadre de référence établi en 2007 par l'AMF sur les procédures de contrôle interne et de gestion des risques.

---

[56] *Loi portant diverses dispositions d'adaptation du droit des sociétés au droit communautaire, dite loi "DDAC" qui a modifié les articles L. 225-37 et L. 225-68 du code de commerce.*

Ce groupe de travail est animé par Jean-François Lepetit et Olivier Poupart-Lafarge, membres du Collège de l'AMF. Il est composé, notamment, de représentants de sociétés cotées, d'experts et de membres d'organisations professionnelles dans les domaines concernés.

Le groupe de travail qui a commencé ses travaux en octobre 2009, devra notamment :

– Décliner de manière concrète les missions du comité d'audit, dans le respect de l'ordonnance, en donnant un éclairage sur la terminologie employée par celle-ci ;
– Prévoir les adaptations nécessaires pour les valeurs moyennes et petites ("VaMPs") ; et
– Revenir sur la question du caractère évaluatif ou non du rapport du Président.

Les travaux du groupe qui seront soumis à consultation devraient être publiés à l'été 2010.

Le Président de l'AMRAE est membre du groupe de place.

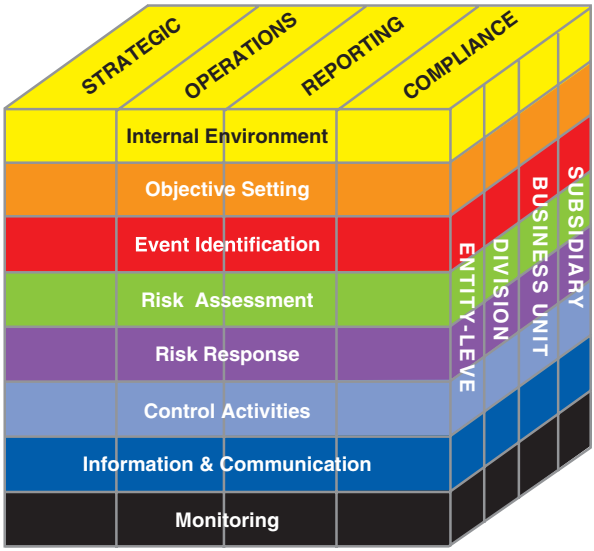
COSO II

La réflexion sur les risques menée par COSO dans son rapport intitulé "Le Management des Risques de l'Entreprise" (Enterprise Management - Integrated Frameworks[57]), dit COSO II, publié en septembre 2005, a été menée de telle sorte qu'elle puisse être comprise par tous les métiers internes et externes à l'entreprise qui sont concernés par la problématique du risque.

COSO I avait produit une codification qui permettait d'utiliser un langage commun dans le cadre du Contrôle interne. L'objectif de COSO II est de parvenir au même résultat pour le Management des Risques de l'Entreprise.

COSO II est une matrice tridimensionnelle qui distingue 8 composants de la gestion des risques. Ces composants peuvent être appliqués selon plusieurs angles de vue (axe de dimension, axe de nature d'objectifs). Il développe plus particulièrement l'identification, l'évaluation et le traitement du risque en comparaison avec le premier référentiel COSO qui visait le contrôle interne.

La cartographie est citée dans son chapitre "Représentation de l'évaluation des risques" en page 221 du document français cité plus haut. Elle est identifiée comme l'un des moyens de représentation visuel des résultats des évaluations.



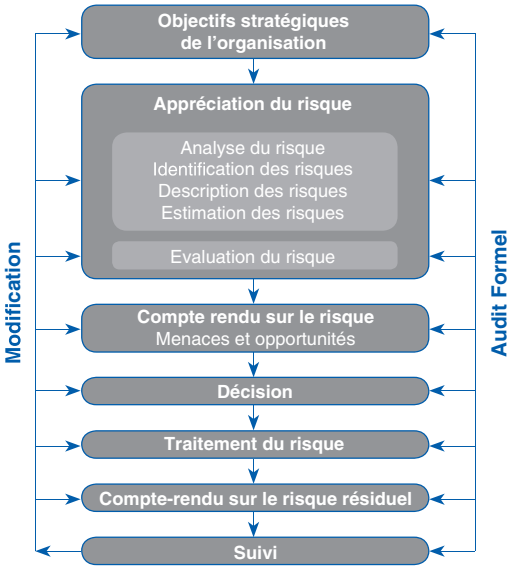
[57] *Traduction française réalisée par PWC.*

FERMA

Indépendamment des travaux de l'AMF, les associations de risk management ont adopté au sein de FERMA (Federation of European Risk Management Associations) un "cadre de référence de la gestion des risques" qui est antérieur à COSO II. Dans ce référentiel, on trouve des définitions et des approches qui convergent parfois vers celles de COSO II mais qui peuvent aussi s'en écarter. Il se base notamment sur l'expérience du Royaume Uni (IRM, ALARM) et des travaux de l'association professionnelle des risk managers anglais (AIRMIC). Le standard FERMA suit la terminologie ISO (FD ISO/CEI Guide 73 – septembre 2002).

Ainsi peut-on lire dans la méthodologie de management des risques préconisée par FERMA que :

- Le dispositif de management des risques est un ensemble d'actions continues et répétées, intégré à l'élaboration et à la mise en œuvre de la stratégie d'une organisation.
- L'objectif du management des risques est de préserver et de créer de la valeur durable pour l'entreprise.
- L'approche doit être globale par entités et activités et doit tenir compte des objectifs de l'entreprise (stratégiques, opérationnels, conformité, reporting, protection du patrimoine). FERMA fixe aussi des objectifs concernant la gestion des connaissances, donc proches de la sphère des Ressources Humaines, ce que ne fait pas COSO.
- La responsabilité opérationnelle incombe essentiellement à la Direction Générale sous la surveillance du Conseil d'Administration ou d'une instance équivalente.



ISO 31000

Le dernier référentiel de management des risques concerne la nouvelle norme internationale "ISO 31000 : 2009, Management du risque - Principes et lignes directrices". Cette dernière a comme principale vocation, à l'instar des autres référentiels, d'aider les organisations à gérer efficacement leurs risques.

Cette norme n'a pas vocation à servir de base à une certification.

La norme propose et décline les relations entre les principes, le cadre et le processus de management du risque.

■ *Les principes du Management des Risques*

Pour optimiser l'efficacité, il convient que le management des risques (MdR) d'une organisation adhère aux principes suivants :

1. Le MdR crée de la valeur
2. Le MdR est intégré aux processus organisationnels
3. Le MdR est intégré aux processus de prise de décision
4. Le MdR traite explicitement de l'incertitude
5. Le MdR est systématique, structuré et utilisé en temps utile
6. Le MdR s'appuie sur la meilleure information disponible
7. Le MdR doit être taillé sur mesure
8. Le MdR intègre les facteurs humains et culturels
9. Le MdR est transparent et participatif

■ *Le cadre organisationnel*

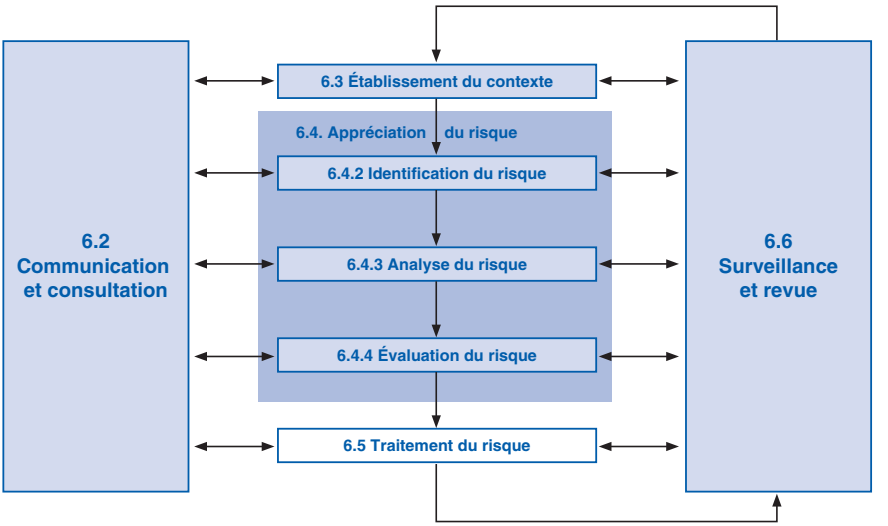
Pour être efficace, le MdR opère au sein d'un cadre organisationnel fournissant les bases et les dispositions utiles à son intégration dans une organisation. Ce cadre organisationnel se décompose en cinq étapes clés qui sont :

- Mandat et engagement : rôle et devoirs de la Direction vis-à-vis du management des risques.
- Conception du cadre organisationnel du Management des risques : Compréhension de l'organisation et de son contexte, Politique de management des risques, Intégration aux processus organisationnels, Responsabilité financière, Ressources, Etablissement de mécanisme de communication et de consignation internes puis externes.
- Mise en œuvre du management des risques : organisation du processus de management des risques.
- Surveillance et revue du cadre organisationnel.
- Amélioration continue du cadre organisationnel.

Le processus de management des risques

Ce processus doit faire partie intégrante du management de l'organisme. Pour cela il doit être intégré à sa culture, à ses pratiques et doit s'adapter à ses processus métiers. Le processus comprend cinq activités :

– Communication et consultation.
– Etablissement du contexte.
– Appréciation du risque.
– Traitement du risque.
– Surveillance et revue.



Questionnaire pour un entretien avec un dirigeant dans le cadre d'une démarche "Top down"

Présentation de l'entretien

Parmi les méthodes d'identification et d'évaluation des risques, il est courant de procéder à des entretiens avec les dirigeants.

Après trois à quatre cycles d'évaluation des risques, votre vision des menaces sur votre activité et le Groupe dans le contexte de cette année et dans la perspective des trois prochaines années, permettra d'établir ou de réactualiser la connaisance de ces risques.

Identification des risques

– Quels événements pourraient affecter gravement l'atteinte des objectifs que vous fixez à votre activité ou que le Groupe se fixe, par rapport à un événement externe, une crise, des facteurs humains, des courants d'opinion, une menace à long terme, par analogie à un événement de l'actualité, ou par rapport à une de nos parties prenantes,… ?

– Existe-t-il un risque important que vous ne retrouvez pas dans la cartographie de votre activité ou du Groupe ? (si réactualisation).

– Par rapport à ces risques, comment rebondir pour générer de la performance, maintenir notre réputation ou préserver notre pérennité (réduction du risque a priori comme l'anticipation de la réaction a posteriori) ?

– La définition des risques de votre activité (description et segmentation) doit-elle être substantiellement modifiée ou complétée – si réactualisation ?

Exposition des activités et du groupe

– Certains risques de votre entité pourraient-ils atteindre un niveau non supportable ?
– Dans ce cas, leurs impacts vous semblent-il suffisamment réduits ou contenus ?
– Une autre façon de réduire le risque est de le diversifier. Les facteurs de création de la valeur et de la réputation vous paraissent-ils suffisamment diversifiés ?
– Quel niveau d'aléa financier, juridique ou de réputation semble raisonnable pour votre activité et pour le Groupe ?

Risques transverses

– Certains risques d'autres entités pourraient-ils atteindre un niveau de menace non supportable pour votre activité ?
– Voyez-vous des risques de votre entité "cumulatifs" avec des risques d'autres entités (l'un entraîne la réalisation de l'autre) ?
– Voyez-vous des risques de votre entité se compensant avec ceux d'autres entités ?
– Certains risques nécessitent-ils un pilotage ou management transverse ?
– Dans ce cas, à quel dirigeant ou quelle entité suggérez-vous de confier le pilotage ?
– Dans ce cas encore, quelle part doit rester déléguée et quelle part doit être du ressort d'une instance de décision transverse ?
– Le principe d'agrégation permet une connaissance globale des risques par thématique, le pilotage restant de la responsabilité de leur propriétaire. Cela vous paraît-il satisfaisant ?

Si notre groupe était l'objet d'une fusion-acquisition

– Quels risques seraient réduits ?
– Quels risques seraient accrus ?
– Voyez-vous de nouveaux risques pour le nouveau Groupe ou pour votre activité dans le nouveau Groupe ?
– Les dépendances entre risques seraient-elles modifiées ?

Apports de la démarche risques

La démarche Risques vise à renforcer la confiance envers le Groupe, ses produits et la qualité de ses services, ainsi qu'à conforter la prise de décision, grâce à une connaissance globale et synthétique des risques et de l'exposition des entités et du Groupe.

– Pensez-vous que cette finalité est atteinte ?
– Attendez-vous d'autres apports de la démarche de maîtrise des Risques ?

Commentaires libres

Extrait du code de commerce

Article L225-100
Modifié par Ordonnance n° 2005-1126 du 8 septembre 2005 art. 22
(JORF 9 septembre 2005).

En vigueur, version du 9 Septembre 2005

LIVRE II : Des sociétés commerciales et des groupements d'intérêt économique.
TITRE II : Dispositions particulières aux diverses sociétés commerciales.
Chapitre V : Des sociétés anonymes.
Section 3 : Des assemblées d'actionnaires.

L'assemblée générale ordinaire est réunie au moins une fois par an, dans les six mois de la clôture de l'exercice, sous réserve de prolongation de ce délai par décision de justice.

Le conseil d'administration ou le directoire présente à l'assemblée son rapport ainsi que les comptes annuels et, le cas échéant, les comptes consolidés accompagnés du rapport de gestion y afférent.

Ce rapport comprend une analyse objective et exhaustive de l'évolution des affaires, des résultats et de la situation financière de la société, notamment de sa situation d'endettement, au regard du volume et de la complexité des affaires. Dans la mesure nécessaire à la compréhension de l'évolution des affaires, des résultats ou de la situation de la société et indépendamment des indicateurs clés de performance de nature financière devant être insérés dans le rapport en vertu d'autres dispositions du présent code, l'analyse comporte le cas échéant des indicateurs clés de performance de nature non financière ayant trait à l'activité spécifique de la société, notamment des informations relatives aux questions d'environnement et de personnel.

Le rapport comporte également une description des principaux risques et incertitudes auxquels la société est confrontée.

L'analyse mentionnée au troisième alinéa contient, le cas échéant, des renvois aux montants indiqués dans les comptes annuels et des explications supplémentaires y afférentes.

Le rapport comporte en outre des indications sur l'utilisation des instruments financiers par l'entreprise, lorsque cela est pertinent pour l'évaluation de son actif, de son passif, de sa situation financière et de ses pertes ou profits. Ces indications portent sur les objectifs et la politique de la société en matière de gestion des risques financiers, y compris sa politique concernant la couverture de chaque catégorie principale de transactions prévues pour lesquelles il est fait usage de la comptabilité de couverture. Elles portent également sur l'exposition de la société aux risques de prix, de crédit, de liquidité et de trésorerie.

Est joint à ce rapport un tableau récapitulatif des délégations en cours de validité accordées par l'assemblée générale des actionnaires au conseil d'administration ou au directoire dans le domaine des augmentations de capital, par application des articles L. 225-129-1 et L. 225-129-2. Le tableau fait apparaître l'utilisation faite de ces délégations au cours de l'exercice.

Les commissaires aux comptes relatent, dans leur rapport, l'accomplissement de la mission qui leur est dévolue par les articles L. 823-9, L. 823-10 et L. 823-11.

L'assemblée délibère et statue sur toutes les questions relatives aux comptes annuels et, le cas échéant, aux comptes consolidés de l'exercice écoulé.

Elle exerce les pouvoirs qui lui sont attribués notamment par l'article L. 225-18, le quatrième alinéa de l'article L. 225-24, le troisième alinéa de l'article L. 225-40, le troisième alinéa de l'article L. 225-42 et par l'article L. 225-45 ou, le cas échéant, par l'article L. 225-75, le quatrième alinéa de l'article L. 225-78, l'article L. 225-83, le troisième alinéa de l'article L. 225-88 et le troisième alinéa de l'article L. 225-90.

Publié par l'AMRAE
(Association pour le Management des Risques et des Assurances de l'Entreprise)
36 Boulevard de Sébastopol, 75004

© Copyright AMRAE – Toute reproduction, même partielle, de ce document est interdite
sans autorisation expresse de l'AMRAE

Achevé d'imprimer par l'Imprimerie Moderne de Bayeux
ZI, 7, rue de la Résistance, 14400 Bayeux
Dépôt légal : n° 31867 - Janvier 2010
Imprimé en France

La Cartographie : un outil de gestion des risques

La collection « Maîtrise des risques », éditée par l'AMRAE, a pour but de faire partager des expertises et des expériences sur les pratiques du risk management et de contribuer ainsi à l'enrichissement de leurs connaissances.

Après le thème des captives traité dans le précédent ouvrage, la cartographie des risques est apparue comme un sujet d'actualité important. Outil de gestion des risques de plus en plus souvent utilisé par les entreprises, le mot « cartographie » recouvre souvent des notions et des pratiques fort différentes. C'est la raison pour laquelle la Commission OGR (Organisation de la Gestion des Risques) de l'AMRAE a missionné deux groupes de travail sur le sujet, chacun traitant d'une étape du processus :

- **le premier a orienté ses travaux sur le thème « Faire une cartographie des risques : pourquoi, pour qui et comment ? »,**
- **le second sur le thème « La cartographie des risques : et après ? ».**

Le présent ouvrage est la synthèse des travaux de ces deux groupes.

Conformément à l'esprit de la Collection Maîtrise des Risques, il s'agit d'un ouvrage pédagogique et pragmatique. Son but est de permettre à toutes les parties prenantes de la gestion du risque dans les entreprises de mieux comprendre les motivations, l'intérêt et les étapes nécessaires à la mise en place d'une vision globale des risques par la cartographie.

Le point de vue adopté met en valeur le savoir faire apporté par le risk manager à l'ensemble de ses partenaires dans la réalisation de leurs objectifs en phase avec la stratégie de l'entreprise et témoigne que la gestion des risques s'inscrit résolument comme un outil essentiel de gouvernance et de management.

Gérard Lancner
Président de l'AMRAE

L'AMRAE regroupe 670 membres, gestionnaires de risques et d'assurance représentant 375 entreprises françaises publiques ou privées. L'ambition de l'association est d'apporter aux entreprises les moyens d'optimiser leur action dans le domaine de la gestion des risques. L'AMRAE aide ses membres dans leurs relations avec les acteurs du monde de l'assurance, les pouvoirs publics et les conseille dans l'appréhension des risques, la maîtrise de leur financement et de leurs achats de garanties d'assurance. La grande force de l'AMRAE repose avant tout sur les échanges d'information entre ses membres, au travers des nombreuses réunions d'information et travaux de commissions techniques ainsi que la mise en place de programme de formation et de manifestations telles que les Rencontres AMRAE.

www.amrae.fr

AMRAE
la Maison du risk management

Association
pour le Management des Risques
et des Assurances de l'Entreprise

Tél. : 01 42 89 33 16 - Fax. : 01 42 89 33 14
E-mail : amrae@amrae.fr

Prix conseillé : 23,00 €TTC

Création couverture Sigle Conception