# Gestion des risques : une approche transverse par les processus

Gilles Teneau, formateur ITIL accrédité APMG, iCONS Innovative Consulting, chercheur associé Cnam LIRSA
Nicolas Dufour, enseignant à l'Ecole nationale d'assurance, doctorant Cnam LIRSA

Comment pouvons-nous décrire le risque, la question est centrale comme en attestent divers cas ces dernières décennies : Seveso, Three Miles Island, Tchernobyl, AZF, plus récemment British Petroleum, Enron, Worldcom, Société Générale, AIG, JP Morgan, UBS. Ces différents exemples présentent une caractéristique commune : une prise de risque mal gérée qui s'est traduite par un potentiel d'accumulation catastrophique, allant au-delà du simple cadre des organisations concernées. Cette complexité peut être qualifiée de hors cadre à deux égards : l'évènement sort du cadre habituel de survenance du risque (débordement). Des risques jusqu'alors invraisemblables (hors échelle) se matérialisent et les risques dépassent leur simple lieu de survenance pour affecter des biens ou personnes hors de l'organisation ou de leur cadre d'apparition.
Face à une complexité croissante, qu'il s'agisse des risques extrêmes comme des risques de moindre importance, le rôle de la gestion des risques (en tant que politique d'entreprise) et de son représentant le Risk Manager est :

- de cerner cet objet frontière qu'est le risque ;
- de le ramener dans le champ de l'identifiable ;
- de l'évaluer correctement ;
- d'envisager les moyens de traitement : prévention, protection voire transfert via des mécanismes d'auto-assurance (captive) ou de transfert de risque (alternativ risk transfer, assurance, etc.).

Cette identification est d'autant facilitée si l'entreprise retient une approche par les processus comme fondement de l'approche par les risques.

L'objet de cet article est d'étudier le lien entre la gestion des risques, envisagée ici comme un objet frontière, et l'approche par les processus. Après avoir présenté ces notions, nous nous livrons à une analyse de leurs voies de rapprochements.

## 1. La gestion des risques et ses corrélats : objet frontière et processus

### 1.1. La notion de risque, un enjeu de gestion

Simon (2000) définit le risque comme un évènement imprévu ou un ensemble de conditions réduisant de manière importante l'habileté des gestionnaires dans la conduite de la stratégie d'affaires envisagée. Cette approche rassurante pour certains (les managers) ne l'est pas forcément pour tous. Ainsi, les enjeux d'audit et de contrôle du risque participent « *d'une politique plus large de l'angoisse et de la peur* » (Power, 2005, p.254) et ont une dimension quasi-prophétique (Pesqueux, 2011). La notion de risque, bien qu'ayant fait fortune ces dernières années, est ambigüe et bien souvent, plusieurs collaborateurs d'une entreprise traitant du sujet croient parler de risque alors qu'ils abordent en fait des notions distinctes (évènements redoutés, menaces, vulnérabilités, pertes…).

Les risques sont des évènements définis par une distribution de probabilités objectives (c'est-à-dire des probabilités établies à partir d'informations statistiques). Le risque est donc une incertitude objectivement probabilisable mais aussi une incertitude mesurable (Cleary, Malleret, 2006). Il est alors question de risque avéré. L'incertitude quant à elle ne peut être cernée par une distribution de probabilité objective, il s'agit du hasard avec des probabilités inconnues. On parle alors de risque potentiel. Le risque peut cependant se résumer de manière assez simple, selon une approche juridique notoire, comme un événement dont la survenance, aléatoire, est susceptible de causer un dommage aux personnes ou aux biens voire aux deux à la fois. Cette approche est souvent complétée par une vision

duale séparant les risques avérés et probabilisables des risques potentiels (latents) et non probabilisables. Une autre manière de résumer le risque consiste à l'appréhender comme la convergence d'une menace, le plus souvent externe à l'organisation, qui exploite une vulnérabilité interne, en vue de causer un dommage aux actifs ou aux personnels.

La question des risques est souvent sujette à difficulté, elle suppose l'expertise en même temps que la rationalité instrumentale mais est source d'ambigüité, de controverse (Beck, Kropp, 2011). Le risque se situe clairement entre ce sentiment public qui veut que l'organisation adopte une perspective gestionnaire et ce vice privé qui implique que l'individu soit par nature réticente adhérer à une telle approche (Cingolani, 2001). Cette controverse rend difficile une réponse organisée face aux nombreux risques entourant une organisation au quotidien (Darsa, 2011).

### 1.2. Risque et objet frontière

Nous envisageons le risque comme un objet frontière. C'est-à-dire un enjeu de communication permettant à des parties prenantes distinctes et issues de métiers différents de parler dans un langage commun dans le but de répondre à un objectif similaire. Il s'agit d'un moyen d'évoquer un sujet complexe et de faciliter l'action par rapport à ce dernier. Le risque répond à cette définition car cette notion permet « de satisfaire un besoin de compréhension de différentes communautés, conservant le même nom sans pour autant recouvrir les mêmes réalités. » (Pesqueux, 2011, p.461). Le risque permet en effet à différentes communautés de parler de la même chose, mais ces derniers ne parlent pas forcément le même langage, faisant référence à d'autres notions voisines telles que les évènements dommageables, les menaces, les vulnérabilités, les défaillances. L'absence de langage commun dans une organisation sur cet ensemble de notions rend la question des risques complexe et contribue à créer de la technicité là où il importe de simplifier la réalité.

Pour ces raisons, la nécessité d'une politique dédiée aux risques a peu à peu vu le jour dans les organisations au même titre qu'il existe des politiques financières, RH, marketing, etc. La tendance dans la société du risque est donc à une institutionnalisation des organisations soucieuses d'assumer plus que jamais leurs risques afin de réduire l'incertitude tout en développant leur activité. Ce rôle institutionnel de l'entreprise moderne face au risque correspond à l'émergence d'une perspective où hommes, nature, économie et société sont intimement liés et dans laquelle l'importance de principes tels que la précaution ou la responsabilité est croissante.

## Le risque, vers une réponse organisée

Le risque est un combat incessant dont on ne connaît pas l'adversaire. Il suppose une attention de tous et de chaque jour. Il n'a pas fini de surprendre par la diversité de ses matérialisations : risques financiers, risques techniques, risques humains, risques politiques, etc. et par son caractère parfois invraisemblable, rendant difficile son anticipation (Guillon, 2009, 2010).

Il demande dans les entreprises modernes une réponse organisée, ce qui suppose un accompagnement des parties prenantes. Au centre de cette question figure notamment le Risk Manager, ce copilote essentiel des risques de l'entreprise dont le but est d'appuyer les différents membres de l'entreprise dans l'identification, l'évaluation, le traitement et le suivi de leurs risques.

Tout type de management comporte une dimension Risk Management (All management is Risk Management). Follett (1941, p.42) nous enseignait déjà que *« les meilleurs dirigeants ne se contentent pas de tirer des conclusions logiques de la masse des données sur le passé que leur fournissent leurs experts, ils ont une vision du futur. »*

Il n'existe cependant pas de solution miracle en gestion des risques, de boîte à outils apportant une solution satisfaisante dans tous les cas. Comme le rappellent Véret et Mékouar (2005, p.15), *« même armé, le risque n'a pas fini de nous surprendre »*, même avec des dispositifs construits et aboutis de gestion des risques, les risques futurs ne peuvent être complètement appréhendés. Saint Thomas d'Aquin nous apprend que l'expérience est une lanterne qui éclaire le passé. L'expérience que l'organisation a du risque est fondée sur le passé. Une approche uniquement basée sur le retour

d'expérience et la remontée d'informations en interne s'avère donc limitée. Elle peut permettre de cibler les risques connus, mais n'est pas suffisante pour les risques futurs.
La gestion des risques, en accompagnement de l'activité, permet non pas de prévoir dans tous les cas l'imprévisible mais de se préparer au risque et d'en réduire les effets lorsque sa prévention n'est pas possible.

### 1.3. La gestion des risques : une approche transversale orientée décision

La Federation of European Risk Management Associations (FERMA)[1] identifie la gestion des risques comme *« un processus continu d'amélioration qui commence avec la définition de la stratégie et se poursuit avec l'exécution de celle-ci. Elle devrait traiter systématiquement de tous les risques qui entourent les activités de l'organisation, que celles-ci soient passées, présentes et surtout futures. »*

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

L'Institut Français de l'Audit et du Contrôle Interne (IFACI) et PriceWaterhouseCoopers (PWC), reprenant le référentiel COSO II, définissent le management des risques comme un processus mis en œuvre par le conseil d'administration, la direction générale, le management et les opérationnels. Ce processus est pris en compte dans l'élaboration de la stratégie et dans toute l'organisation. Il vise à éviter les évènements potentiellement dommageables et à fournir une assurance raisonnable quant à l'atteinte des objectifs. Dans un contexte de flou des frontières de l'entreprise et de ses sous-traitants, notre période fait évoluer l'entreprise dans un monde de plus en plus incertain, un environnement de plus en plus agressif, de moins en moins prévisible. Face à cela, la gestion des risques vise l'atteinte des objectifs en répondant aux risques organisationnels et non seulement au risque pris de manière isolée (Ebondo, Zéghal, 2009). Dans ce cadre, une démarche d'anticipation est nécessaire pour identifier les évènements pouvant potentiellement affecter les objectifs stratégiques. Les prendre en compte par une visée anticipatrice permet donc de mieux les intégrer dans les processus de fonctionnement de l'entreprise.

#### Une compréhension globale des risques

La gestion des risques suppose une compréhension globale des risques de l'entreprise (Guillon, 2009). L'entreprise, se veut une pluralité de risques faisant interagir des domaines divers (droit, économie, gestion, ingénierie…) et mobilisant une multitude de compétences dans le cadre de ce qui peut être appelé le *« total Risk Management »*. En la matière, l'interdisciplinarité est nécessaire, en particulier au Risk Manager. Cet homme de terrain, *« touche-à-tout »* (Véret, Mékouar, 2005, p.52) intervient dans des domaines stratégiques, organisationnels et techniques, et participe à la transformation de son entreprise[2] (sécurité des personnes et des installations, problèmes environnementaux, contrats avec les sous-traitants, dimension informatique, gestion de crise…).

L'image et les futurs marchés de l'entreprise sont soumis à l'incertitude et aux risques, lesquels revêtent plusieurs formes. La dimension stratégique du risque sera concrétisée par l'incertitude liée au lancement d'une activité donnée. Cette dimension suppose l'anticipation des évènements futurs ; il en va de même pour la gestion des risques, liée à la stratégie. En procédant ainsi, en permettant un bon déroulement des activités stratégiques pour l'entreprise, le Risk Manager répond aux besoins de la

[1] FERMA. Fédération regroupant les associations traitant des problématiques de gestion des risques, à l'instar de l'AMRAE, de l'Institute of Risk Management. Elle identifie les différentes pratiques en termes de risk management et organise des séminaires et conférences sur les actualités de ce domaine. Site officiel de la FERMA : www.ferma.eu

[2] Entreprise, vue ici sous l'angle de l'organisation, entité soumise aux risques et émettrice de risque de par son activité. De par son caractère technique et la nécessité d'un regard transverse mais également d'une analyse approfondie, la fonction de Risk Manager s'est professionnalisée depuis une trentaine d'années.

direction générale quant aux impacts des décisions managériales de même qu'aux demandes d'informations des analystes financiers.

La gestion des risques comprend encore une dimension organisationnelle et participative, incluant un ensemble de parties prenantes. Le Risk Manager participe à l'évolution de l'organisation dans laquelle il évolue, il analyse et gère le risque, non pas en tant que fonction déconnectée de l'entreprise, mais en tant qu'activité transverse liée à toutes les branches d'activités de l'entreprise. Le risque n'est pas géré en tant que tel, mais ce sont les activités qui sont gérées et de ce fait le risque qui en découle. *« La gestion des risques est plus un art qu'une science, chacun comprend cette fonction à sa façon. C'est ce qui fait la force et la faiblesse de cette fonction »* précise encore Baron[3] (2009) pour qui le Risk Management est autant le fait de risques liés à chaque activité qui intéressent ceux qui les exercent que de risques *« orphelins »* non rattachés à une activité précise, que personne n'assume et qui incombent au Risk Manager en parallèle à sa fonction de coordination dans la prise en compte des autres risques.

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

Le Risk Management peut être défini comme un processus transversal de création de valeur (Morlaye, 2006, p.60) au centre du processus organisationnel et impliquant toutes les fonctions de la chaîne de valeur au sens de Michael Porter (1986). Cette approche globale aussi qualifiée d'ERM (Enterprise Wide Risk Management) suppose de déterminer en accord avec l'objet social de l'entreprise, ses valeurs et sa stratégie, le profil de risque que cette dernière souhaite adopter et mettre en œuvre dans la conduite de son activité courante (voir Figure 1). Cette approche suppose dans un second temps le transfert ou la prévention et la protection contre les risques se situant hors de ce cadre et que l'entreprise n'entend pas assumer en tant que tels. Cette notion d'acceptation du risque apparaît comme fondamentale. Elle découle de l'appétit au risque des décideurs d'une organisation (ou *a contrario* de leur aversion). Sitkin et Weingart (1995) analysaient les comportements de prise de décision en univers risqué pour démontrer que la variable risque devient un paramètre dont la prise en compte va nécessairement croissante à notre époque, en raison du poids des parties prenantes autres que le seul *« Top Management »* (poids des actionnaires, dimension responsabilité environnementale, opinion publique, rôle des médias, etc.).

[3] Frank Baron est Business Development Manager chez AXA Corporate Solutions Risk Consulting, il est également administrateur à la FERMA. Propos tirés de l'article du magazine RiskAssur-hebdo, article du 01/12/2009.

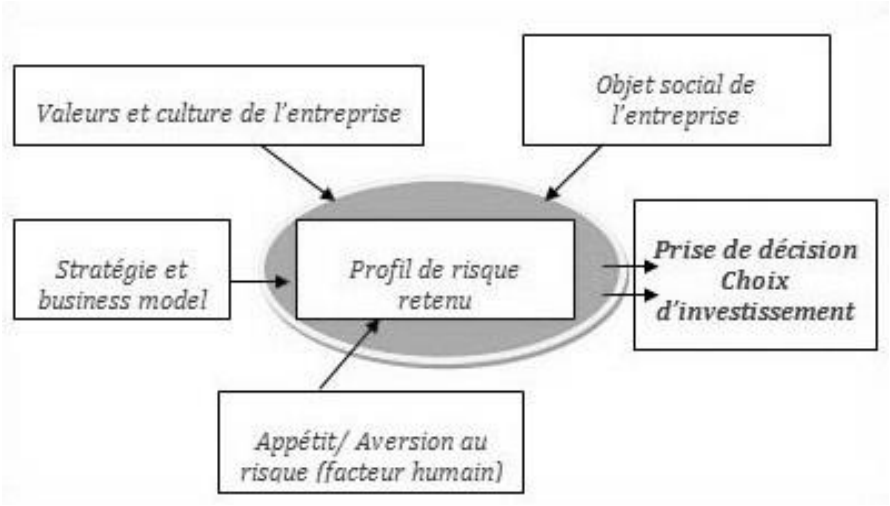


Figure 1. Profil de risque et décision

## 2. Gestion des risques et processus, la transversalité des approches comme nécessité

### 2.1. L'anticipation des risques est facilitée par une approche processus

A l'origine les organisations étaient gérées de manière fonctionnelle (système de gestion), ce qui signifie qu'il y avait absence de transversalité entre les différentes fonctions. Avec l'ouverture des marchés à l'international, avec les alliances, les partenariats, rapidement nous sommes passés d'une logique fonctionnelle à une logique de processus. Les systèmes de gestions orientés « fonctions » ont évolué vers des systèmes de management, orientés « processus ». Ainsi l'organisation avait la possibilité d'assurer une sécurité optimale des données, de l'information, des actifs tant à l'intérieur de l'entreprise que dans ses nombreuses relations extérieures, partenaires, fournisseurs, clients. De nos jours, cette vision transversale est appelée « entreprise 2.0 », elle intègre la transparence des services en toute sécurité, en toute confiance, tant au sein de l'organisation qu'en relation avec les parties prenantes (partenaires, alliances, associés, prestataires,…) Cela correspond à une vision collective et partenariale de la gouvernance.

Les organisations doivent identifier et manager de nombreuses activités de manière à avoir un fonctionnement efficace et efficient. Toute activité consommant des ressources a besoin d'être managée pour permettre la transformation d'éléments d'entrée en éléments de sortie en utilisant un ensemble d'activités corrélées ou interactives : cela est aussi connu sous le nom de « processus ». Les éléments de sortie d'un processus peuvent constituer directement les éléments d'entrée d'un autre processus et, généralement, cette transformation s'opère dans des conditions planifiées et maîtrisées. L'approche processus désigne l'application d'un système de processus au sein d'une organisation, ainsi que l'identification, les interactions et le management de ces processus (Raquin, 2009).

Cette transversalité, ce passage à la gouvernance d'entreprise, cette vision processus impliquent la mise en place d'une gestion des risques à l'ensemble des actifs (matériels et immatériels) d'une organisation (Naciri, 2011). Souvent, nous faisons une analyse rapide de la situation et des risques possibles par rapport aux bénéfices ; une évaluation est faite et, à partir de celle-ci, une décision est prise. Par rapport à cette prise de décision, aucun formalisme n'est mis en place. Quand il s'agit d'une entreprise grande ou moyenne, d'un gouvernement, de plusieurs pays… on recourt toujours à la gestion des risques. Ainsi, les décideurs peuvent choisir la solution qui offrira le plus de gains et le moins de risques. Cette démarche implique l'ensemble des acteurs de l'entreprise, depuis les organes de gouvernance jusqu'aux opérationnels, elle couvre à la fois la notion de risques et d'opportunité (bénéfice) et contribue à l'atteinte des objectifs de la structure en incluant l'ensemble des activités.

L'identification prospective des causes de risques peut être facilitée par une approche processus (voir Figure 2). L'analyse d'un accident (arbre des causes…) est un bon moyen de comprendre quels sont les facteurs de risques, mais elle intervient *ex post*, une telle approche ne peut donc prévaloir seule. En amont de la prévention, traiter des causes de manière proactive suppose de remonter aux origines du risque en agissant pour changer l'exposition au risque : au-delà des causes propres au risque, il est question de se demander quels peuvent être les risques en fonction des choix opérés. On est donc bien avant les causes d'un risque : on se demande quels sont les risques si tel choix est fait et l'on en tient compte dans l'arbitrage. C'est à ce stade que se caractérise une vraie politique de risque efficace, ce qui peut être pour l'entreprise un vrai outil de différenciation.

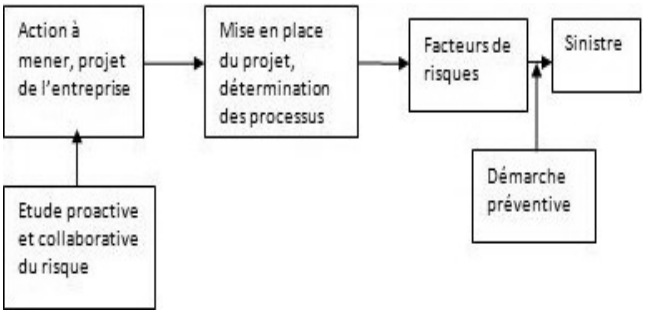


Figure 2. Processus de prévention-réduction du risque

Une approche caractérisant cette démarche de gestion des risques est l'approche dite IVTS (Identification, Evaluation, Traitement, Suivi).

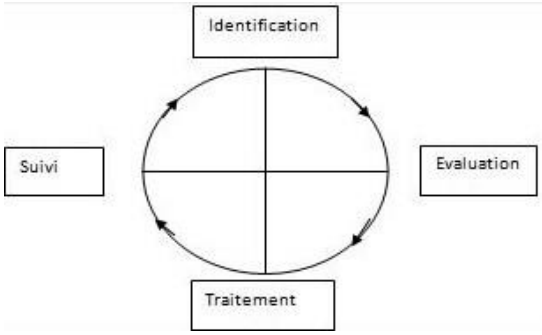


Figure 3. Roue du risque

Dans la lignée de l'approche qualité (roue de Deming), IVTS cherche à améliorer la démarche de gestion des risques de façon continue (voir Figure 3). À la première boucle (identification => évaluation => traitement => suivi), il est parfois difficile de mettre en œuvre l'identification des risques, de les évaluer et de les traiter. Toutefois, les procédés nourrissent les processus, et c'est par une implémentation continue des méthodes que l'on peut rendre celles-ci plus efficaces et opérationnelles. Ainsi, un traitement des risques à un instant T, fera l'objet d'un suivi en T+1 et le traitement sur cette même période T+1 en sera d'autant amélioré que l'organisation connaîtra (même partiellement) les meilleures manières de gérer certains risques.

### 2.2. Une bonne maîtrise des processus permet de mieux cibler les risques frontières : diversité des Risk Management

Si l'approche historique des risques est basée sur des mécanismes assurantiels et de transfert des risques, cette approche quantitative tournée vers les risques passés récurrents manque à elle seule de sens, notamment en ce qui concerne les risques organisationnels (tels que les risques humains ou les risques opérationnels). Il faut passer d'une approche en silo séparant différentes fonctions à une approche intégrée pour mieux prendre en compte *« l'agrégation des risques dans l'entreprise »*

(Mikes, 2009, p.24). Certaines recherches décrivent ainsi différentes approches caractérisant la gestion des risques que l'on peut retrouver dans les organisations (voir Tableau 1). On retrouve notamment, outre l'approche en silo où les fonctions dédiées au risque sont séparées, une approche intégrée visant l'intégration des risques, une approche basée sur une mesure de performance prenant en compte les risques (Risk-based Management) et enfin une approche holistique du Risk Management qui vise à tenir compte de manière significative des risques non quantifiables. Cette approche se veut encore plus englobante en intégrant la notion d'incertitude dans le processus de Risk Management.

Le Tableau 1 résume les 4 idéaux-types du Risk Management.

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

Tableau 1. Les idéaux-types de la gestion des risques
(Adaptation, d'après A. Mikes, 2009)

**Zoom sur l'approche Top Down-Bottom Up**

Le Risk Manager (ou responsable des risques) n'est pas décisionnaire, il possède un rôle largement consultatif, mais il doit néanmoins gérer les décisions prises. Son champ d'action décisionnaire couvre le traitement des risques associés à ces décisions. Pour être pleinement efficace à cet égard, il doit être un coordinateur entre la gouvernance de l'entreprise et les différents propriétaires de risques. Dans le cadre du processus de gestion globale des risques, notamment lors d'une étape essentielle vers la maîtrise des risques qu'est l'élaboration d'une cartographie des risques, l'approche *top down* ou *bottom up* sera privilégiée (voir Figure 4). Il s'agira alors de réaliser une cartographie des risques pour chaque entité, à chaque niveau (groupe/filiales), par activité, et de procéder à une mise en commun. Une approche Top Down aura pour avantage de mettre clairement en exergue la volonté de la direction générale de donner une impulsion dans la mise en place d'un processus de Risk Management. Les menaces seront mises en évidence au niveau global et l'accent sera mis sur la nécessité d'une adhésion du management décisionnel.

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


Figure 4. Approche Top-Down et Bottom-Up de la gestion des risques

## 3. Cas d'application

### Réorganisation d'un service de mutuelle

Afin de devenir un acteur primordial sur le marché des Mutuelles, la Mutuelle « AA » a décidé de s'associer par la réalisation d'un GIE à la mutuelle « BB ». Le projet concernait la simplification des méthodes de travail, en réorganisant les systèmes d'information, en redéfinissant les processus métiers et en facilitant l'interopérabilité des services (voir Figure 5).

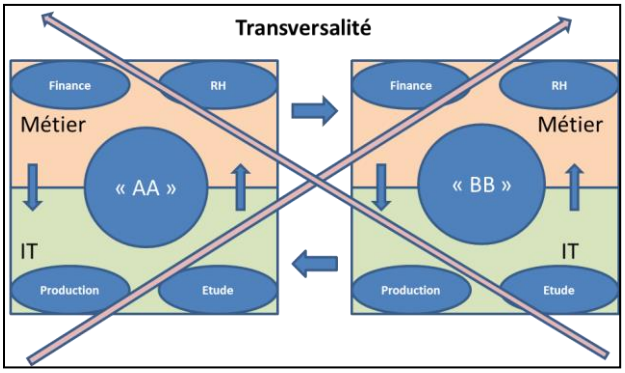


Figure 5. Transversalité, cas d'application

Pour faciliter cette tâche une équipe de direction fut nommée, elle a été divisée en trois parties, elle avait en charge la définition, la conception, la mise en œuvre de la nouvelle stratégie :

- la première équipe était composée de spécialiste de processus métier ;
- la seconde équipe était composée de spécialiste de processus IT ;
- la troisième équipe était composée de spécialiste en gestion des risques.

Au début du projet une partie de l'équipe travaillait sur l'unification et la correspondance entre les processus métier. Une seconde partie de l'équipe s'attachait à réaliser la cartographie des processus IT. Enfin la troisième et dernière partie se situait à la croisée des deux mutuelles et son rôle était de définir tous les risques (IT, outils, environnement, financiers, opérationnel, humain, politique, stratégique).

Pendant la phase cruciale du projet les deux premières équipes (métiers et IT) ont croisé leurs actions, afin de permettre la réalisation d'un processus transversal à toute l'entreprise, une gouvernance d'entreprise. Pendant cette phase importante, l'équipe en gestion des risques assurait la bonne réalisation du projet, tant la gestion des délais, des coûts, des risques.

Chacune des équipes a travaillé à une industrialisation des méthodes de travail, pour cela des outils, des technologies furent choisis, au travers d'un nombre de prestataires potentiels. L'équipe qui était en charge des processus IT, devait tenir compte de l'ensemble des fonctions des deux mutuelles,

la production, les études, la R&D, la gestion de projet, l'exploitation, chacune de ces entités devait être apte à communiquer avec toutes les autres entités. La transversalité processus retenue entre les deux mutuelles devait être aussi une transversalité entre fonctions. La totalité du projet était gouvernée par la direction des deux mutuelles, les outils choisis devaient s'adapter aux modes de travail et pas les acteurs de l'entreprise, s'adapter aux outils, la forme retenue était bien du Bottom Up.

L'équipe en charge de la gestion des risques a utilisé deux normes importantes de la gestion des risques, la norme de sécurité des SI, ISO 27001 (Teneau, Dufour, 2013a) et la norme générale de sécurité ISO 31000. Le modèle général retenu pour la gestion des risques était le modèle PESTEL (voir ci-après). Ce modèle a permis de cerner les principaux risques. Après avoir repéré les principaux risques, après avoir évalué ces derniers, une matrice fut réalisée pour atténuer les risques. La démarche entreprise par l'organisation de mettre en œuvre une gestion par les processus donna une réponse à de nombreux risques potentiels.

## Perspectives

L'intégration des risques à la gestion des processus (gestion, évaluation, application), peut se faire par le biais du modèle PESTEL. Ce dernier permet d'avoir une présentation des facteurs d'environnement (sociaux-légaux-économiques) ainsi que des impacts sur le fonctionnement et la performance de l'entreprise. En stratégie, il analyse les facteurs du macro-environnement externe dans lequel la société évolue. L'entreprise ne peut pas contrôler ces facteurs qui peuvent représenter des risques ou des opportunités de marché. Ce modèle permet de saisir les risques possibles et les familles de processus les concernant.

Politiques (P) : orientations politiques, actions des pouvoirs publics, politique fiscale…
Economiques (E) : inflation, conjoncture, chômage, taux de change…
Sociaux (S) : comportements ou attentes des clients et des salariés, éducation, santé…
Technologiques (T) : évolution des technologies, cycle de vie des produits, des méthodes de travail…
Environnementaux (E) : Météo et climat, catastrophe naturelle, développement durable…
Législation (L) : Propriété industrielle, norme, droit des contrats, réglementation de l'emploi…

Le modèle PESTEL peut être adopté pour l'analyse des relations entre l'entreprise et son environnement, de leur évolution, pour un futur proche, pour une démarche prospective également. Les facteurs liés à l'environnement sont utilisés dans une perspective plus temporelle, c'est le cas aussi des facteurs de changement. Il est possible de faire des analyses des facteurs d'environnement avec des analyses d'opportunités et de menaces. Des rapprochements sont possibles aussi concernant le positionnement de l'entreprise par rapport aux concurrents.

### Conclusion

Face à la transversalité que suppose la problématique du risque, la gestion des risques se fonde sur les différents processus afin de mieux identifier et cerner cet objet frontière (Teneau, Dufour, 2013b). Une approche par les processus tend à faciliter le repérage des zones de risques potentiels en vue de mieux anticiper leur survenance et de déterminer des moyens de protection, de prévention ou de transfert adaptés. Cette approche suppose cependant le nécessaire relais des organes de gouvernance sans lesquels la vision globale et stratégique de la gestion des risques reste un vœu pieu. Cette vision Top Down constitue un point de départ indispensable mais qui doit nécessairement être complétée par un relais des différents managers et opérationnels (approche Bottom Up) pour faire de la gestion des risques une politique d'entreprise effective et efficace, centrée sur les préoccupations des différentes parties prenantes.

## Bibliographie


Dufour N., Darsa J-D., Contrôle, qualité et maîtrise des risques (dir. Cappelletti L. et Hoarau C.), *Pratiques en or : Finance et Contrôle*, DUNOD, 2013.

Beck, G. & Kropp, C. (2011). Infrastructures of risk: a mapping approach towards controversies on risks. *Journal of Risk Research*, 14 (1), p. 1-16.

Cleary, S., Malleret, T. & Schwab, K. (2006). *Risques : perception, évaluation, gestion*. Eds Maxima, Paris.

Cingolani, P. (2001). Le risque, entre sentiment public et vice-privé. *Mouvements*, 14 (2), p. 55-60

Darsa, J-D. (2010). *La gestion de crise en entreprise*. Gereso, Le Mans.

Darsa, J-D. (2011). *Risques stratégiques et financiers de l'entreprise.* Gereso, Le Mans.

Guillon, B. (2009). Pour une approche globale du risque. *Responsabilité & environnement (Annales des Mines)*, 77, p. 7-8.

Guillon, B. (2010). Prise en compte de l'environnement naturel dans l'hôtellerie : à propos de l'intérêt d'une pluralité des normes. In : Bessire D., Cappelletti L., Pige B., Eds, Normes : origines et conséquences des crises, Economica, Paris.

Morlaye, F. (2006). *Risk Management et Assurance*. Economica, Paris.

Mousli, M. (2002). Mary Parker Follett, Pionnière du Management. *cahier du LIPSOR*, série Recherche, 2, Octobre.

Mikes, A. (2009). Risk Management and Calculative Cultures. *Management Accounting Researc*h, 20 (1), p. 18-40.

Naciri, A. Traité de Gouvernance d'entreprise. (2011). Presse Universitaire du Quebec, Quebec.

Sitkin, S.B. & Weingart, L.R., (1995). Determinants of Risky Decision-Making Behavior: A Test of the Mediating Role of Risk Perceptions and Propensity. *The Academy of Management Journal*, 38 (6), p. 1573-1592.

Pesqueux, Y. (2011). Pour une épistémologie du risque. *Revue Management & Avenir*, 43, p. 460-475.

Porter, M. (1986). *L'Avantage concurrentiel*. InterEditions, Paris.

Power, M. (1999, 2005), *The Audit Society: Rituals of Verification*. University Press, Oxford.

Raquin, M. & Morley-Pegge, H. (2009). *Piloter par les processus*. Maxima, Paris.

Teneau, G & Dufour, N. (2013a). Norme ISO 2700x : vers la gouvernance de la sécurité des systèmes d'information. *Revue des Techniques de l'Ingénieur*. G9060.

Teneau, G & Dufour, N. (2013b). *La gestion des risques, un objet frontière*. L'Harmattan, Paris.

Zéghal, D. & Ebondo, E. (2009). Management des risques de l'entreprise: Ne prenez pas le risque de ne pas le faire. *Revue des Sciences de Gestion*, 237-238, p. 17-26.

Annexe. Les principales classes de risques (d'après Dufour, Darsa 2013), axe mobilisé

| Classes de risques | Enjeux de qualité | Exemples | Axe mobilisé selon le modèle PESTEL |
|---|---|---|---|
| - risques géopolitiques ; | Veille géostratégique | Terrorisme, pays en guerre, « Printemps arabes » | Politique |
| - risques économiques ; | Dispersion de l'information | Volatilité du cours des matières premières, enjeu de maîtrise pour bâtir un modèle de marge | Economique |
| - risques stratégiques ; | Lucidité des modèles d'affaires | Rupture technologique non anticipée: General Motors, Kodak | Politique |
| - risques financiers ; | Relation avec les tiers de financement (qualité de la relation avec les investisseurs), longévité de la relation | Cas de LG, environ 60 000 entreprises en faillite par an (sous-capitalisation, trésorerie non structurée) | Economique |
| - risques opérationnels ; | Traçabilité des données | Affaire de la Société Générale, « fraude Kerviel » | Légaux |
| - risques industriels ; | Facteur humain (erreur) | Crises au sein de British Petroleum, Total | Technologique |
| - risques juridiques (une famille de risques opérationnels spécifiques) ; | Maîtrise de l'expertise face à l'inflation normative, confidentialité des données | Affaires Goldman Sachs (amende pour conflit d'intérêt), Enron | Légaux |
| - risques informatiques (une famille de risques opérationnels particuliers) ; | Qualité des infrastructures (vulnérabilité, détection de l'obsolescence et intrusion) | Sony, environ 200 millions de dollars de pertes | Technologique |
| - risques sociaux et psychosociaux (famille baptisée « RH » par commodité) ; | Pérennisation des pratiques et connaissances. Compassion et empathie comme rôles managériaux | Cas Orange-France Télécom ; Cas Renault | Sociaux |
| - risque d'image et de réputation ; | Confiance de clients et investisseurs, | Total, Marionnaud, ARC, Servier | Sociaux |
| - risque de *knowledge management* (ou de « gestion de la connaissance ») ; | Exhaustivité / pénurie (bonne documentation), stabilité des méthodes | Départs des sachants (départs à la retraite des populations de cadre dans le secteur assurance) | Technologique |
| - autres risques (famille à périmètre élargi : risque environnemental, de surqualité, de défaillance de contrôle et de pilotage...) ; | Gouvernance de l'entité et image renvoyée aux tiers | Cas de Barings (fraude du trader Nick Leeson et défaillance du contrôle interne) | Environnementaux |
| - risque d'intégrité (le risque individuel ultime). | Education sur le risque, sensibilisation | Cas Arthur Andersen, cas Nike | Social |