100 Questions
POUR COMPRENDRE ET AGIR

Gestion des risques

Jean-Paul Louisot

2e édition

afnor ÉDITIONS

afnor boutique www.afnor.org/editions

Gestion des risques

100 Questions
POUR COMPRENDRE ET AGIR

Gestion des risques

Jean-Paul Louisot

2e édition

afnor ÉDITIONS

afnor boutique www.afnor.org/editions

L'auteur

Jean-Paul Louisot est notamment ingénieur civil des Mines de Saint-Étienne et titulaire d'un « Master in Business Administration » de la Kellog School of Management. Il est également titulaire de qualifications professionnelles, *Associate in Risk Management* de The Institutes (ARM, États-Unis) et *Fellow of the Institute of Risk Management* (FIRM, Royaume-Uni). Il a été successivement courtier, assureur et risk-manager.

Il est directeur pédagogique du CARM Institute qui assure la formation professionnelle ONR 49000 en France. Il a également été professeur associé à l'université Paris 1 Panthéon-Sorbonne de 2002 à 2010 et enseigne aujourd'hui la gestion des risques dans le cadre de différents masters, notamment à l'Institut catholique de Lille et à l'Institut international des Assurances (Yaoundé).

Il est l'auteur de nombreux ouvrages et articles, en particulier sur l'ERM — *Entreprise-wide risk-management* et conférencier régulier dans les rencontres internationales des professionnels de la gestion des risques et de l'assurance.

Vous voulez nous faire partager une remarque ou une suggestion ?
Contactez-nous :
fabrication-editions@afnor.org

Couverture : création AFNOR Éditions

ISBN 978-2-12-465461-1

AFNOR – 11, rue Francis de Pressensé - 93571 La Plaine Saint-Denis Cedex

Tél. : +33 (0) 1 41 62 80 00 – www.afnor.org/editions

Sommaire

Avant-propos

Depuis le début du XXI^{e} siècle, la gestion des risques connaît une véritable révolution culturelle. Jusqu'alors fonction technique, centrée autour de l'achat de couverture d'assurance, elle est devenue une discipline managériale et transversale : elle propose une valise d'instruments que chaque manager doit connaître et appliquer quels que soient son domaine de compétence et ses missions au sein d'un organisme.

Certains ont voulu voir dans cette évolution la conséquence directe des catastrophes en rafale des deux dernières décennies : La centrale nucléaire de Tchernobyl, les tempêtes en décembre 1999 en France, le tsunami fin décembre 2004 dans le Sud-Est, sans oublier les attentats terroristes du 11 septembre 2001 aux États-Unis, et l'explosion AZF à Toulouse. Et la litanie continue, alternant les catastrophes liées à des risques technologiques et celles dues aux événements naturels, voire une combinaison des deux comme au Japon en 2011 où les dommages du tsunami ont provoqué un accident nucléaire.

Sans sous-estimer leur impact, il s'agit, sans doute, plutôt d'une lame de fond dans l'opinion publique qui exprime son besoin de sécurité dans le temps et dans l'espace, selon un calendrier accéléré par les moyens d'information globaux et immédiats. On ne saurait, en effet, sous-estimer l'impact des médias sociaux. L'expression la plus aboutie est certainement l'exigence de développement soutenable, même si les instruments pour le mesurer et en faire un concept opérationnel manquent encore.

Avec le concept de gouvernance d'entreprise, dont les versions au niveau de l'Union européenne, mais aussi en Grande-Bretagne et en France,

exigent plus des managers qu'une conformité fiduciaire, un nouveau chapitre de la responsabilisation des dirigeants s'est ouvert.

Il débouche, naturellement, sur le développement de l'ERM (*Enterprise-wide risk-management*), dont la meilleure traduction en français serait sans doute gestion des risques étendue à tout l'organisme, c'est-à-dire une gestion globale et intégrée des risques. En effet, cette traduction rend bien compte de l'éclatement de la fonction de gestion des risques qui est devenue une des missions fondamentales de chaque responsable opérationnel, le propriétaire des risques qui pèsent sur l'unité qu'il dirige.

Bien entendu, dans les organismes de dimensions internationales, au niveau du siège, il faut un professionnel à temps plein pour coordonner et animer la démarche de gestion des risques dans sa totalité, et également, chez ses principaux partenaires économiques, pour en garantir la cohérence et l'efficacité.

Ce coordinateur a des alliés naturels : l'audit interne, la qualité ainsi que le contrôle interne, qui connaissent bien l'ensemble des processus et ont une légitimité reconnue par les opérationnels.

Les unités plus petites [les entreprises de taille intermédiaire (ETI) ou les PME/PMI, par exemple] ne peuvent plus faire l'économie de la gestion des risques qui devient chaque jour davantage une exigence de leurs donneurs d'ordre ou de leurs clients, un attribut de la qualité des biens ou services qu'elles produisent. Au niveau de la direction, il faut un champion, mais dans l'application sur le terrain, le responsable qualité avec une formation complémentaire adéquate ne pourrait-il pas être en mesure de remplir cette mission ? C'est avec les ETI et les petites structures à l'esprit que CARM Institute a mis en place, en 2014, une formation adaptée conduisant à une reconnaissance internationale l'ONR 49000 relative à la gestion du risque pour les organismes et les systèmes, véritable guide pratique d'application de la norme ISO 31000:2010.

Mais quelle que soit la structure répondant aux besoins et aux moyens de l'organisme, au travers d'un système niché au sein du système de management, la gestion des risques est un attribut de la culture qui doit être internalisée par chacun des acteurs.

Cette acculturation commence par une information et une formation des managers. C'est précisément l'ambition des 101 questions rassemblées dans cet ouvrage : apporter à chaque manager d'entreprise, de collectivité, d'établissement de santé, qu'il soit responsable d'un centre de profit, d'une unité, d'un processus ou d'un projet, des réponses

claires au « pourquoi » et au « comment ». Le but étant de leur montrer comment la gestion des risques est un instrument de leur performance qui leur permettra d'atteindre plus sûrement et plus efficacement les objectifs de leur organisme, voire les leurs !

Toutefois, la discipline est devenue si vaste qu'un auteur solitaire ne pourrait pas répondre correctement à toutes ces questions. C'est pourquoi cet ouvrage est le résultat d'un effort collectif, celui de l'équipe pédagogique de CARM Institute.

Une mention spéciale doit être attribuée à toutes les personnes qui ont directement contribué à certaines réponses par leurs conseils ou leurs révisions :

- Viviane Balland (questions 39 et 40)
- Guy Bellocq (questions 23, 24 et 25)
- Jean-Pierre Brioude (questions 22 et 32)
- Georges-Yves Kervern (question 100)
- Kevin Knight (question 81)
- Jacques Lautour (questions 28, 29, 33 et 38)
- Hugh Rosenbaum (questions 60 et 61)
- Erika Vincent (question 88)
- Michel Sfez (questions 93 et 94)

Le processus de gestion des risques proposé ici, directement inspiré de la norme ISO 31000:2010, conduit à une amélioration continue, un cercle vertueux qui est plus un voyage qu'une destination. Bon voyage donc à tous les lecteurs !

I
Diagnostic des vulnérabilités et « cartographie »

1
Les Concepts fondateurs du risk-management

1 *Risque ou opportunité, comment voir l'incertain ?*

L'avenir est incertain : « nous ne savons pas de quoi demain sera fait », mais la gestion des organismes repose sur des décisions, éclairées par des méthodes, pour discerner le futur.

Longtemps, les hommes se sont efforcés de s'assurer un avenir favorable et de se concilier les forces qui sous-tendent le futur, en offrant des sacrifices aux dieux. Depuis la fin du XVII^{e} siècle avec Pascal, Fermat et leurs successeurs, le passé et le présent servent à éclairer le futur sur la base des lois de probabilités, en utilisant soit par l'approche statistique soit les analyses de tendance.

Au cours des dernières décennies, on a pris l'habitude de ne considérer que l'aspect négatif de l'incertitude du futur, les menaces, en un mot la probabilité de pertes engendrées pas un événement aléatoire, en oubliant la possibilité de gains, et que l'on nomme aujourd'hui : opportunité.

Pour résumer, face à un avenir aléatoire, dans la pratique de la vie de l'entreprise, le risque « opportunités » et le risque « menaces » sont les deux côtés d'une même pièce : les issues favorables constituent une opportunité, les issues défavorables une menace.

C'est d'ailleurs ce qui est souligné dans la norme ISO 31000:2010 qui a retenu comme définition du risque : « l'impact de l'incertitude sur les objectifs ».

Dans la vie de l'entreprise, comme dans les théories économiques et financières, le risque est considéré comme inhérent à l'acte d'entreprendre.

La prise de risque est même la justification de la rémunération de l'entrepreneur, et la théorie financière définit le rendement d'un investissement comme la somme de deux facteurs :

- Le rendement de base, de l'investissement sans risque (assimilé, en général, aux bons du trésor de même maturité).
- Une prime de risque, c'est-à-dire un supplément de rémunération consenti à l'investisseur, pour le récompenser d'avoir accepté une volatilité dans son résultat.

Bien entendu, la littérature distingue l'avenir probabilisable et l'avenir non probabilisable.

Dans le premier cas, on dispose d'assez de données pour établir une loi de probabilité sur les événements futurs et définir un intervalle de confiance : les bornes entre lesquelles devrait se situer la variable aléatoire. Par exemple, en analysant le passé et les conditions économiques, on doit pouvoir évaluer un marché pour l'automobile, en France, l'année prochaine. Ensuite, en définissant un objectif de part de marché, un constructeur automobile peut prévoir son chiffre d'affaires avec un bon degré de précision.

En revanche, s'il lance un nouveau modèle, prévoir le coût de rappel ou de remise en état d'un véhicule (si un défaut se révélait lors de la première année de vente) est beaucoup plus difficile, en particulier s'il fait appel à des nouvelles technologies. Dans ce cas, s'il ne dispose pas de données fiables, ou ne peut pas travailler par analogie avec les anciens modèles, il ne peut pas définir de loi de probabilité. On parle d'avenir incertain non probabilisable, et le constructeur devra recourir à des scénarios pour estimer ce coût.

Au demeurant, l'exemple ci-dessus illustre les deux aspects du risque : évaluer le chiffre d'affaires futur examine bien une opportunité, l'aléa peut conduire à des ventes, en excédent ou en retrait par rapport à l'évaluation. Cependant, l'évaluation moyenne retenue est la base de tout exercice budgétaire sans lequel une entreprise serait condamnée à piloter à vue.

Au contraire, le coût des engagements de responsabilité produits potentiels, de remise en état de véhicules et/ou de frais de rappel, constitue bien une menace, plus ou moins contenue.

La tendance actuelle de la gestion des risques est de s'efforcer de gérer les menaces et les opportunités de façon globale, en analysant tout organisme comme un portefeuille d'aléas à équilibrer pour atteindre l'efficacité économique optimale.

Toutefois, il faut souligner que cette approche est surtout essentielle pour le volet « financement des risques » qui doit s'intégrer effectivement dans une stratégie financière. Au niveau de la réduction du risque, en réalité, ce sont les menaces qui doivent être identifiées, analysées et traitées par action pour réduire la probabilité ou contenir l'impact. C'est pourquoi la plupart des questions qui suivent seront focalisées sur les risques « menaces » qui demeurent le cœur du métier de la plupart des risk-managers.

2 *Quelles sont les différentes acceptions du terme « risque » ?*

Le terme « risque » est utilisé dans le monde professionnel pour refléter différents concepts, et peut donc prêter à confusion. Toutefois, il est tellement répandu qu'il est incontournable. Voici les principales acceptions utilisées en gestion des risques.

Risque (pur, spéculatif, mixte)

L'expression se rapporte à l'utilisation la plus répandue, à savoir : l'événement à l'origine du dommage subi par un organisme. Il s'agit, alors, d'un événement aléatoire dont la survenance entraîne une perte pour l'entreprise, le *risque pur*.

Par opposition, ceux dont la réalisation peut déboucher, soit sur un gain, soit sur une perte sont appelés *risques spéculatifs*.

Les autres, que l'on ne peut classer dans aucune des deux catégories, parce qu'ils ont des caractéristiques les apparentant aux deux, sont regroupés sous le terme de risques mixtes (recouvrement de créances).

Risque systématique et risque non systématique

Le risque systématique (risque non diversifiable) est engendré par un ensemble d'événements non aléatoires, c'est-à-dire dont la survenance tend à être simultanée, plutôt qu'aléatoire, ou due au hasard. De ce fait, le risque systématique ne se prête pas au traitement par la diversification (c'est-à-dire à la constitution d'un portefeuille de risques peu corrélés entre eux, voire anticorrélés).

Les pertes engendrées par les conditions économiques générales présentent un risque systématique, car l'ensemble de l'économie et des opérateurs économiques, est affecté au même moment. Lorsque les marchés monétaires deviennent tendus, les taux d'intérêt et le coût de l'emprunt augmentent pour l'ensemble des opérateurs.

Imaginons qu'une société d'assurance offre une couverture contre l'augmentation des taux d'intérêt, elle ne serait pas en mesure de se constituer un portefeuille diversifié de contrats du fait que l'ensemble de ses assurés serait frappé d'une perte en même temps.

Le *risque non systématique (risque diversifiable)* est engendré par un ensemble d'événements, dont la survenance sur un portefeuille de risques est aléatoire (c'est-à-dire qu'elle est due au hasard ou suit une loi de probabilité).

Ces risques sont également spécifiques à l'entité économique concernée. L'incendie d'un seul bâtiment est un événement aléatoire, et un portefeuille d'assurances du risque incendie, sur un ensemble de bâtiments suffisamment séparés, est constitué sur un risque non systématique.

Une société d'assurance peut donc se constituer un portefeuille diversifié ou équilibré, en assurant contre l'incendie un grand nombre de bâtiments répartis sur une zone géographique assez étendue.

La souscription d'un nombre important de tels « risques » permet à l'assureur, en application de la loi des grands nombres, de prévoir avec un degré de précision satisfaisant, le nombre (c'est-à-dire la fréquence) et les montants (c'est-à-dire la gravité) des sinistres qu'elle devra indemniser au cours d'une période d'assurance donnée. Elle sera donc en mesure de calculer une cotisation lui permettant de couvrir ses débours prévisibles (voir ci-après, le risque assurable).

Risque assurable

Certains acteurs sont encore plus restrictifs pour définir la sphère d'action de la gestion des risques, en se référant aux *risques assurables*, mais alors, le gestionnaire est pratiquement réduit au rôle d'acheteur d'assurances. En effet, un risque assurable est un risque pour lequel il existe un marché d'assurances, c'est-à-dire une offre (par des assureurs) et une demande (par des souscripteurs).

Les lecteurs non-spécialistes pourront se reporter aux ouvrages sur l'assurance. Il suffit de rappeler, ici, que l'assurance repose sur l'organisation d'une mutualité. Elle consiste à faire partager, par un grand nombre d'individus sur lesquels pèse un même risque, le poids financier de ce risque aléatoire (trop « lourd » individuellement) ne frappant qu'un petit nombre. C'est ainsi qu'une charge aléatoire exceptionnelle, dépassant la capacité financière de chacun, est transformée en une charge modeste, certaine et récurrente.

3 *Mais alors, qu'appelle-t-on vulnérabilité ?*

Pour les professionnels de la gestion des risques, l'ambiguïté du mot « risque » le rend difficilement opérationnel. C'est pourquoi il faut définir un concept nouveau : la vulnérabilité.

Une vulnérabilité se caractérise par les pertes financières induites par la réalisation d'un événement aléatoire frappant une ressource de l'entreprise.

Autrement dit, pour un organisme donné, une vulnérabilité est parfaitement identifiée par trois paramètres :

- ***Objet de risque*** : c'est la ressource qui est « en risque », résumée en cinq classes : humaines, techniques, informations, partenaires et financières (H, T, I, P, F) (voir question 4).
- ***Péril*** : c'est l'événement aléatoire dont la survenance prive l'organisme d'une ressource partiellement ou totalement, de façon provisoire ou définitive.
- ***Impact potentiel*** : il s'agit, le plus souvent, des pertes financières induites, et plus généralement de l'impact sur l'atteinte des objectifs fondamentaux de l'organisme (tous ne sont pas traduisibles en termes financiers). La littérature préfère souvent le mot « gravité » qui suppose une traduction en termes financiers.

Pour classer les vulnérabilités, on peut s'appuyer sur les catégories de ressources. On distingue alors cinq classes de vulnérabilités, à savoir :

- ***Les atteintes de personne H*** : elles génèrent des éléments de passifs (engagement de la responsabilité ou garantie) ou des pertes d'actifs potentiels (pertes de revenus) pour l'organisme (*perte d'un homme ou d'un groupe-clé*).
- ***Les dommages aux biens (physiques) T*** : c'est la perte d'un bien matériel ou immatériel dont l'entreprise a la propriété ou la garde. En général, elle se traduit par la perte d'un élément d'actif.
- ***Les pertes d'informations I*** : elles relèvent de tous les éléments d'information quel qu'en soit le support (informatique ou non) et consistent en des pertes, dégradations ou divulgations d'informations à des tiers, que cela soit dû à des erreurs ou à de la malveillance. Elles pourraient être intégrées dans les quatre autres classes.

L'importance de la valeur de l'entreprise « immatérielle », centre de flux et de traitement d'informations (et encore plus avec l'avènement des base analytics et de *big data),* a rendu indispensable un diagnostic et un traitement spécifique, que la plupart des opérateurs ont entrepris.

- ***Les dommages aux partenariats P*** : c'est l'ensemble des incidents sur la chaîne logistique, depuis l'extraction des matières premières jusqu'à l'utilisation de biens ou service produits par l'utilisateur final.
- ***Les pertes de revenus F*** : ce sont les pertes financières ou les pertes d'actifs potentiels engendrées, soit :
  - par la disparition d'une des ressources des trois classes précédentes (pertes consécutives) ;
  - par un événement extérieur, sans atteinte directe aux ressources de l'organisme (fermeture d'un hypermarché pour les commerçants de la galerie marchande attenante, notion de « site aimant ») ;
  - par une atteinte à la réputation ou l'image de l'organisme ou de ses marques.

La « ressource en risque » et le péril identifiés, la phase identification est terminée (voir question 14). L'analyse devra prendre en compte trois types de conséquences (voir question 15) :

- ***Primaires et secondaires :*** les dommages subis directement par l'organisme ; dommages directs et pertes de revenus induites.
- ***Tertiaires :*** les dommages subis par des tiers et l'environnement, qui se répercuteront sur l'organisation en cas d'engagement de responsabilité civile (pertes financières) ou pénale (amendes ou perte de ressources humaines, s'il y a mise en cause de collaborateurs ou de dirigeants).
- ***Quaternaires :*** les atteintes à la réputation (voir question 36).

On pourrait faire une représentation dans l'espace en reprenant les trois dimensions : les trois paramètres (voir questions 21 et 22).

4 *Quelles sont les ressources de l'entreprise ?*

L'entreprise peut être définie comme une combinaison dynamique de ressources, pour atteindre des objectifs. La définition de ces objectifs est donc au cœur de la gestion de tout organisme.

Il va toujours s'agir de combiner les ressources de la façon la plus efficace, pour atteindre l'objectif le plus ambitieux possible avec les ressources déterminées, ou d'atteindre l'objectif désigné avec le moins de ressources possibles. Il s'agit de la définition même de l'efficacité pour l'affectation des ressources dans une économie libérale.

Il existe de nombreux modèles découpant les entreprises ou les organismes en un nombre variable de classes de ressources. Pour l'exploitation du modèle, à des fins de gestion des risques, nous retiendrons cinq catégories qui permettent une approche globale de l'organisme, en distinguant des classes dont les modes de traitement des risques associés (voir partie II) sont spécifiques à chacune.

H = Humaines : il s'agit, ici, de l'ensemble des personnes liées à l'organisme par des contrats de travail ou des mandats, et dont les compétences, formations et expériences spécifiques, en font un véritable actif pour l'entreprise. Il faudrait prendre en compte, également, les données démographiques telles que : âge, sexe, situations de famille, qui peuvent avoir un impact sur la capacité de produire. En un mot, ce sont les éléments pris en compte, parce qu'il est traditionnel d'appeler : « *knowledge management* », gestion des compétences ou des talents.

T = Techniques : ce sont les bâtiments, équipements, outils… en un mot, l'ensemble des actifs physiques dans le périmètre direct de contrôle de l'organisme. La nature juridique de la détention est secondaire par rapport au contrôle direct. Certains appartiennent à l'organisme et sont inscrits à l'actif de son bilan, certains sont à sa disposition en vertu d'un contrat de location ou de leasing, d'autres sont en dépôt et appartiennent à des tiers, partenaires. Il peut exister d'autres situations qu'il serait trop long de recenser exhaustivement ici.

I = Informations : c'est l'ensemble des flux d'informations qui circulent au sein l'organisme, qui y sont transformées ou stockées, quel qu'en soit le support (informatique, papier ou humain). La ressource intègre aussi les informations concernant l'organisme lui-même : la perception que

les autres ont, les parties prenantes de l'organisme. On peut synthétiser l'ensemble dans le terme « réputation » qui sera explicité à la question 36, parmi les risques émergents. Il s'agit donc de tous les éléments au cœur de la mission d'intelligence économique.

P = Partenaires (amont et aval) : c'est l'ensemble des moyens des partenaires économiques de l'organisme, amont (sous-traitants et fournisseurs), aval (clients) et latéraux (cotraitants, connus ou non, dans un projet global) indispensables à l'organisme pour atteindre ses objectifs ou remplir ses missions. Il s'agit là des partenaires, pour l'essentiel, liés par contrat avec l'organisme et qui sont donc en transaction avec elle, sans oublier leurs propres réseaux de dépendances (voir question 6 pour plus de précisions).

F = Financières : c'est l'ensemble des flux financiers qui traversent l'organisme. Ils touchent aussi bien les flux à court terme (trésorerie, actifs liquides ou quasi liquides) que les flux à moyen et long terme (plan de financement, capitaux propres et réserves, ainsi que les dettes à long terme). En un mot, c'est la question de la gestion financière stratégique de l'organisme.

L'analyse ne serait pas complète si l'on ne tenait pas compte des échanges non transactionnels avec l'environnement, c'est-à-dire les ressources indispensables à la vie de l'organisme et dont il ne finance pas directement la disponibilité. En un mot, ce sont les « ressources gratuites », les externalités des économistes, qui ne laissent pas de traces dans les comptes de l'organisme, le bilan comme le compte de résultat. Leur importance dans le développement des organismes, encore plus aujourd'hui à la lumière des exigences du développement soutenable, justifie leur discussion à la question 6.

5 *Que sont les ressources partenaires ?*

La globalisation des marchés s'est accompagnée de la construction de réseaux, de plus en plus complexes, au travers de l'externalisation. Les grandes entreprises sont presque devenues des ensembliers, tandis que les plus petites ne sont qu'un maillon d'un réseau logistique complexe.

En effet, dans la plupart des situations, il s'agit d'une arborescence plutôt que d'une chaîne linéaire. En conséquence, la chaîne logistique est devenue l'épine dorsale de tout organisme produisant des biens et des services, intégrant un nombre croissant de tâches externalisées.

Les ressources partenaires sont donc l'ensemble des matières premières, produits semi-transformés, équipements et services dont les organismes ont besoin pour assurer leur fonctionnement quotidien.

Ces ressources peuvent donc être scindées en trois grandes catégories :

- ***Les ressources amont :*** elles proviennent des fournisseurs, des prestataires de services et des sous-traitants, y compris les transporteurs chargés d'apporter l'approvisionnement sur les sites de production.
- ***Les ressources latérales :*** ce sont les services et les produits apportés à ses clients ou donneurs d'ordres qui concourent à la réalisation des systèmes, projets et produits, auxquels l'organisme participe, sans nécessairement les connaître, alors qu'ils sont en fait « solidaires » au travers du donneur d'ordre commun. Par exemple, un fabricant automobile peut se procurer les moyeux des roues chez un sous-traitant, acheter des pneus adaptés chez un fabricant : les commandes de pneus chutent parce que le sous-traitant, en faillite, est remplacé par un autre sans que le fournisseur de pneus ne soit informé.
- ***Les ressources aval :*** ce sont les clients ou donneurs d'ordres (y compris les transporteurs chargés de livrer) et les institutions financières qui garantissent la bonne conclusion des transactions (cautions…).

Il est important d'identifier cette catégorie dans le cadre de la gestion des risques, car l'application des principes du risk-management s'accompagne d'aménagements spécifiques avec des similitudes entre les trois classes signalées. Dans toutes les situations de ressource « partenaire », le niveau de sécurité de l'organisme dépend, pour l'essentiel, d'actes de tiers sur lesquels elle a un contrôle limité, ou pas de contrôle.

En un mot, elle a transféré, consciemment ou non, une partie de la gestion de ses risques à des tiers. Dans ces conditions, que peut-elle faire pour garantir sa résilience face à une éventuelle carence de ces ressources ?

Les mêmes principes s'appliquent en amont et en aval avec la règle des « trois C » (voir version plus détaillée à la question 86) :

- **C** — pour **C**hoisir.
  - Évaluer avec attention si les produits ou les services offerts par le partenaire potentiel répondent effectivement aux besoins.
  - Valider la solidité financière et la compatibilité d'image et d'éthique (attention au cas des sous-traitants de sous-traitants utilisant des enfants, comme pour les ballons de football de la coupe du monde 1998 ou les incidents plus récents au Bangladesh ou en Chine).
- **C** — pour **C**ontracter.
  - Introduire des clauses contractuelles par lesquelles la qualité de la gestion des risques est un des critères de poursuite des relations donnant le droit de vérifier, sur site, les mesures prises.
  - Envisager les situations de rupture ou de difficultés et prévoir des solutions contractuelles de sorties de crise (indemnités forfaitaires, clause de médiation ou d'arbitrage…).
- **C** — pour **C**ontrôler.
  - Suivre l'évolution de la relation, en tenant compte des incidents, mais aussi des modifications du contexte (par exemple, changements de personnes, d'actionnaires ou de technologie…).

Dans tous les cas, la prévention commence en évitant toute dépendance trop marquée :

- Pour les fournisseurs et les sous-traitants, essayer de diversifier en tournant avec au moins deux ou trois (attention pour les sous-traitants avec échange de savoir-faire, cela peut être difficile ou risqué sur le plan de l'espionnage industriel).
- Pour les clients, éviter qu'un client ne prenne un poids trop lourd dans le chiffre d'affaires.
- Pour les ressources latérales, il faut passer par l'ensemblier, ou donneur d'ordre, et s'assurer qu'il a bien mis en place une gestion des risques du projet dans lequel des événements témoins ont été positionnés, pour alerter l'ensemble des partenaires très en amont des problèmes subis par un membre de l'équipe.

6 *Que sont des ressources gratuites ?*

Par-delà les ressources internes de l'organisme (voir question 3) et ses ressources externes, celles échangées avec des partenaires économiques amont et aval (voir question 5), il ne faut oublier de prendre en compte les échanges non transactionnels avec l'environnement. Ces ressources prélevées sur l'environnement sans échange financier direct ne sont pas le résultat de transactions, nous les qualifieront ici de « ressources gratuites », pour souligner qu'elles n'auront pas de trace dans les états comptables de l'organisme concerné. Elles sont donc liées à l'environnement physique, sociétal et concurrentiel :

- ***Environnement physique***, articulé autour de l'air, de l'eau et de la terre.
- ***Environnement politique, légal et social*** : conditions de vie et d'organisation de la société.
- ***Environnement concurrentiel*** : pression des concurrents, avancées technologiques, goûts des consommateurs et notion de site aimant (clientèle découlant de l'attraction d'une autre entité).

Comme il est souligné plus haut, ces échanges ne pourront pas être identifiés en analysant les partenaires économiques, puisqu'ils ne s'accompagnent pas de transaction commerciale.

Leur importance est particulièrement significative pour les entreprises se diversifiant et s'installant dans d'autres régions ou dans d'autres pays : les conditions qui ont conduit au succès d'une ETI ou d'une PME/PMI dans son environnement de naissance ne se retrouvent pas nécessairement réunies dans d'autres lieux envisagés, ou pour d'autres entreprises en cas de fusion/acquisition. Pour expliciter ces concepts, le plus simple est d'illustrer avec des exemples concrets :

- Certains processus font appel à un refroidissement par prélèvement d'eau dans un cours d'eau en amont, avec l'évacuation en aval de l'eau non polluée, mais avec une température supérieure. A-t-on pensé aux basses eaux d'été exceptionnel, où ni le débit ni la température en amont ne permettent des échanges corrects ? Que se passe-t-il si l'eau est en limite d'oxygénation pour les poissons ? La seconde implantation peut être dans une région qui connaît des périodes de gel prolongées…

- L'air doit être d'une qualité suffisante pour permettre la vie normale des salariés. Un voisin est-il susceptible de relâcher un nuage polluant ? Certaines productions doivent se faire en atmosphère totalement libre de poussière. Il y a des filtres, mais à côté d'un lieu proposé, il y a des industries relâchant des poussières fines que notre processus industriel ne sait pas arrêter…
- Un seul pont historique permet d'atteindre l'usine, il donne des signes de faiblesse. Les autorités décident de limiter l'accès aux véhicules de moins de 5 tonnes : nos proches fournisseurs se retrouvent maintenant à plus de 30, voire 40 km, ce qui engendre des délais de livraison incompatibles avec les produits transportés.
- Le pays est-il sûr ? Politiquement stable, sans parler de spoliations (nationalisations ?), le climat à l'égard des investisseurs étrangers restera-t-il favorable ?
- Le principe de précaution inscrit dans la Constitution française. Cela a-t-il des conséquences pour la compétitivité des entreprises installées en France ? Les produits innovants seront-ils encore vendus, en France, par les sociétés étrangères ?
- La culture du pays a un impact sur le rythme de travail. Quand une implantation a lieu dans un autre pays, quel est l'impact sur les conditions ou les rythmes de travail ?
- La clientèle que je reçois vient-elle pour nos qualités propres ou pour une situation que nous ne maîtrisons pas complètement ? C'est le cas d'un détaillant installé dans une zone commerciale dont l'aimant est un hypermarché d'une enseigne nationale. C'est le cas d'un restaurant, installé près d'une entreprise, qui attire un trafic qui lui procure sa clientèle.

1 *Qu'entend-on par péril ?*

Le péril ou aléa est le second des trois paramètres qui définissent une vulnérabilité (voir question 3). C'est un événement aléatoire, c'est-à-dire incertain, dont la survenance à l'instant « t » dans le futur entraînerait une atteinte aux ressources de l'organisme, le privant totalement, partiellement, temporairement ou définitivement de leur usage.

Le vecteur ressource/péril permet d'identifier la vulnérabilité, il reste ensuite à l'évaluer, en s'attachant à mesurer les conséquences induites par l'impact du péril sur la ressource recensée.

Idéalement, le péril est qualifié avec une probabilité mesurée à l'aide de lois de probabilités expérimentales tirées de l'expérience (historique) ou de modélisation. Dans certains cas, on devra se contenter d'évaluation approximative en classes de probabilité (exceptionnel, rare, peu fréquent, fréquent) selon une échelle à définir pour l'usage de chaque entité.

De nombreux phénomènes ont des distributions de probabilité qui suivent des lois dites normales (courbe en cloche) ou loi de Gauss, qui est définie par deux paramètres :

- L'espérance mathématique ou fréquence moyenne du phénomène (par exemple, les cyclones tropicaux frappent en moyenne sur le long terme, 4 fois par an, en Floride).
- Un écart-type qui permet de définir un intervalle de confiance, c'est-à-dire le nombre d'événements qui devrait se produire chaque année (dans le cas précédent, si l'écart-type est 1, il y a 68% de risques que l'on ait entre 3 et 5 ouragans par an en Floride, 95% entre 2 et 6, et plus de 99% entre 1 et 7).

En clair, il est « pratiquement certain » que chaque année la Floride sera frappée par au moins 1 et au plus 7 cyclones.

Pour des phénomènes mieux contrôlables que les événements naturels (par exemple, la fréquence des accidents de circulation dans une flotte automobile de taille suffisante, le nombre annuel d'incendies pour une grande multinationale avec un parc de sites significatifs), l'apparition de nombres sortant de l'intervalle de confiance déterminé est un élément significatif de diagnostic : la « dérive » peut révéler une amélioration ou une dégradation de la situation, qui exige une analyse des causes de cette évolution.

Les périls pour lesquels on peut établir une distribution de survenance représentent, dit-on, un avenir incertain « probabilisable », les autres un avenir certain « non probabilisables » (voir question 1).

Il est essentiel de connaître la distribution de survenance car, couplée avec la loi de probabilité de la gravité (traduction de l'impact en termes financiers), elle va dicter l'impact économique du péril pour l'organisme et justifier l'affectation des ressources à la réduction du phénomène (l'action de réduire la fréquence ou vraisemblance est appelée prévention et l'action de réduire l'impact, la protection).

On remarquera que, pour les phénomènes très rares, la valeur moyenne des sinistres « à long terme » (loi des grands nombres) n'a pas grand intérêt pour le décideur. La gestion se fait alors sur la base de l'impact rapproché d'une « vraisemblance » acceptable ou non, pour l'ensemble des parties prenantes. Par exemple, quand les dirigeants d'une entreprise, qui gère des centrales nucléaires, raisonnent sur l'accident nucléaire majeur, peu importe le coût moyen sur un million d'années, voire même un millénaire. La question est plutôt de savoir si l'accident, qui pourrait survenir demain, serait assez contenu pour ne pas mettre en cause l'ensemble de la filière aux yeux de la population, en particulier des riverains ?

La nature du phénomène détermine les instruments de prévention et de protections applicables à une situation donnée. Il est donc essentiel de les classer selon un mode, qui permet de déterminer pratiquement les instruments à prendre en considération (voir question 8).

En anticipant sur la question 8, on peut illustrer cette notion : pour les défauts de conduite, facteurs essentiels dans une flotte automobile, il faut, avant tout, modifier les comportements des conducteurs.

8 *Peut-on classer les périls ?*

D'autres classifications que celle retenue ici sont possibles (nature du phénomène, conséquences…). Celle que nous exposons ne vise pas à la rigueur scientifique, mais plutôt à faciliter l'identification des instruments de traitement applicables, en fonction de l'origine et de la nature même du péril (voir chapitre 2). Les périls sont classés selon deux critères :

1. La localisation de l'origine

- ***Endogène :*** généré par l'organisme lui-même ou à l'intérieur du périmètre qu'il contrôle (par exemple, un incendie prenant naissance dans les locaux de l'entreprise).
- ***Exogène :*** généré à l'extérieur du périmètre de contrôle de l'organisme (par exemple, une grève avec occupation dans un établissement voisin, bloquant l'accès de la zone industrielle où est installée l'entreprise).

2. La nature du phénomène

- ***Économique*****,** c'est-à-dire une variation brutale dans un paramètre économique touchant l'environnement de l'organisme et provoquant une contrainte lourde et immédiate.
- ***Naturel*****,** c'est-à-dire résultant de l'action des forces de la nature (par exemple, tempête, tremblement de terre…).
- ***Industriel***, c'est-à-dire ne résultant pas directement d'un acte humain, mais des activités productives développées par lui. Typiquement, on retrouve dans cette classe l'essentiel des risques « accidentels ».
- ***Humain*****,** c'est-à-dire dont le déclenchement est dû à l'action ou l'absence d'action de l'homme (par exemple, un incendie dans un entrepôt à la suite d'un travail avec un point chaud).

Pour l'origine humaine, il convient de préciser s'il résulte d'un phénomène non volontaire ou d'un acte volontaire.

- ***Le péril humain involontaire*** résulte d'une erreur, d'une omission ou d'une négligence. Ce peut-être au moment de l'événement lui-même (par exemple, un mégot non éteint près d'une matière inflammable) ou au préalable (par exemple, une inondation, pour défaut de cuvelage dans un sous-sol de bâtiment construit en zone où le niveau d'eau peut dépasser le niveau bas du sous-sol).

- ***Le péril humain volontaire*** résulte d'un acte volontaire ou conscient d'un homme ou d'un groupe d'hommes.
- ***Le péril humain volontaire : « petit malin »*** résulte de l'action légitime de certains acteurs d'un système. Ils le modifient pour faciliter le travail ou améliorer les performances, mais ne documentent pas leurs modifications. Par exemple, l'équipe qui suit, inconsciente des changements, respecte les anciennes consignes, ce qui provoque un sinistre (attention, ce phénomène est plus fréquent en France ou dans les pays latins que dans les pays anglo-saxons).
- ***Le péril humain volontaire : « malveillance »*** résulte d'une intention de nuire ou de la volonté de s'approprier les biens d'autrui. Il s'agit en principe d'actes illégaux, punissables par les lois des pays concernés (par exemple, l'espionnage industriel, l'incendie volontaire d'un salarié licencié…).

Il convient encore de distinguer si la « malveillance » est *à but lucratif* ou *à but non lucratif* :

- Dans le premier cas, il s'agit d'une entreprise illégale, mais dont les animateurs raisonnent selon des schémas économiques classiques. Pour les décourager, il suffit de détruire la « rentabilité » de leurs efforts, en augmentant le prix à payer (sanctions, surveillance…) ou en réduisant la valeur (par exemple, biens entreposés, informations diffusées).
- Dans le second cas, les malfaiteurs agissent pour une cause (par exemple, vandalisme, terrorisme…) leurs motivations et leurs raisonnements sont donc beaucoup plus difficiles à cerner et à circonscrire. Les attentats de New York et de Washington du 11 septembre 2001 rappellent, tragiquement, la nécessité et la difficulté de traiter ce péril, ainsi que tous ceux que nous avons connus depuis lors, y compris en Russie dans les semaines qui ont précédé les jeux olympiques d'hiver de Sotchi.

Le péril humain volontaire, sous ses deux formes, est en fait le plus difficile à combattre. Il suppose de reconnaître une volonté intelligente face à nous, qui exige une action et une adaptation continue. L'exemple le plus frappant est celui de la lutte contre les virus informatiques. Des « spécialistes » en génèrent chaque jour, ils doivent donc être mis à jour quotidiennement !

9 *Quelles sont les particularités des périls humains volontaires ?*

La principale particularité du péril humain volontaire est précisément qu'il résulte de l'intention d'êtres humains, utilisant leur intelligence, pour modifier le fonctionnement d'un système complexe. Dans la majorité des cas, il s'agit d'actes de malveillance visant à affaiblir l'organisme et/ou à s'approprier ses biens tangibles et intangibles.

Toutefois, il ne faut pas négliger la volonté de modifier pour faciliter la vie ou l'améliorer, mais que les acteurs « oublient de signaler ».

Pour illustrer simplement ce fait, en dehors du domaine des logiciels et des progiciels informatiques bien connus, on peut penser à une équipe de nuit dans une usine chimique qui doit suivre le fonctionnement d'un ensemble d'équipements à partir d'un poste de contrôle. On couple deux alertes, l'une visuelle sur le tableau, l'autre sonore.

Une équipe s'entend pour faire des roulements et déconnecte l'alarme sonore pour permettre le sommeil de ceux qui sont en « repos ». À la fin de leur semaine, ils oublient de remettre en l'état. La semaine suivante, la nouvelle équipe, assoupie, ne voit pas l'alerte visuelle et n'est pas réveillée, puisque l'alarme sonore ne se déclenche pas : l'usine explose. Ce péril demande donc la mise en place et la vérification régulière de procédures, afin d'éviter les dérives volontaires du système.

Pour l'essentiel, toutefois, le péril humain volontaire se manifeste par des actes de malveillance à l'égard de l'organisme. Ces actes confèrent à ce péril des caractéristiques propres, qui ont un impact sur les mesures de réduction applicables. Ces caractéristiques sont liées au fait que, quelle que soit la nature des actes de malveillance, ils partagent les éléments suivants :

- Ils sont développés par une intelligence organisée.
- Ils exigent des efforts de réduction permanents et tous azimuts.
- Ils proviennent d'un danger unique : un individu ou un groupe d'individus malveillants qui pensent pouvoir agir en toute impunité.

Le gestionnaire des risques doit anticiper les nouvelles possibilités de survenance d'actes de malveillance à l'encontre de l'organisme et doit imaginer des contremesures avant que les instigateurs ne frappent.

Des nouvelles possibilités de délits, et par conséquent des besoins particuliers pour augmenter la vigilance, résultent de toute modification dans l'organisme ou son environnement. Cela peut se traduire, par exemple, par l'acquisition de nouvelles installations, le développement de nouveaux procédés, l'embauche de nouveaux collaborateurs, en particulier dans l'équipe dirigeante… Chacun de ces changements est susceptible de générer des défauts dans le programme de sécurité de l'organisme que les malfaiteurs à l'affût sont toujours prêts à exploiter.

Le fait de développer un diagnostic complet sur les dangers de malveillance doit fournir le canevas logique pour recenser les mesures de réduction possibles, afin d'attaquer ces risques. Pour l'essentiel, les objectifs poursuivis seront :

- La réduction du niveau d'hostilité des personnes qui peuvent commettre des délits contre l'organisme ou contre ses partenaires (en particulier pour le péril de type vandalisme ou même « terrorisme »).
- La protection des biens et des activités de l'organisme contre les personnes malveillantes, par l'édification de barrières physiques, la mise en place des procédures et un management, afin de limiter leurs opportunités de nuire.
- La limitation de la perception d'impunité que les malfaiteurs peuvent avoir en préparant ou en commettant leur délit.

En résumé, pour les actes de malveillance, l'efficacité de la lutte passe par la vigilance de tous. Dans ce domaine, encore plus que dans les autres périls, c'est une véritable culture d'éveil et de précaution qu'il faut créer au sein de l'organisme, de façon à ce que tous se sentent partie prenante d'un dispositif en maille fine.

L'écueil inverse (à éviter, en France, en particulier) est l'esprit « shérif », dans lequel chacun prendrait le problème en main, avec des mesures musclées, mais contraires à la loi.

10 *Quels sont les objectifs de la gestion des risques ?*

Au cœur même de toute gestion des risques se trouvent l'atteinte des objectifs de l'organisme et l'optimisation de la performance. Les objectifs de la gestion des risques se déclinent donc à partir des objectifs des grandes directions qu'elle doit assister pour « passer les coups durs ».

Il s'agit de prévoir les moyens, de toute nature, qui permettent à l'organisme d'atteindre ses objectifs permanents, en toutes circonstances et, surtout, quelle que soit la sévérité de l'événement dommageable qui la frappe. En particulier avec l'appui direct du risk-manager, l'objectif financier est de mettre à la disposition de l'organisme, au bon moment, les montants de trésorerie nécessaires pour compenser l'impact des événements dommageables.

La gestion des risques s'intéresse, par essence, à une matière aléatoire, ou volatile. Donc, son résultat peut être lui-même aléatoire et dépend de l'horizon temporel retenu. C'est pourquoi les professionnels ont pris l'habitude de définir des objectifs « avant sinistre » et « après sinistre ». Ces termes font référence directement aux pratiques de l'assurance, mais ils sont retenus, ici, du fait de leur usage très répandu dans la profession. On aurait pu retenir également « dysfonctionnement » qui évite toute hypothèse sur l'origine de la rupture dans le fonctionnement normal, mais ce terme reste trop vague.

Il convient donc de préciser les objectifs, en distinguant l'avant et l'après sinistre. En réalité, dans la mesure même où la raison d'être de la gestion des risques est de réduire l'incertitude et/ou l'impact des sinistres, il faut analyser en priorité les objectifs d'après sinistre.

Les objectifs après sinistre (rupture de l'exploitation)

Dans tous les cas, l'objectif minimum est la survie de l'organisme. Mais, sur chacun des terrains évoqués précédemment, on retrouve un *continuum* d'objectifs plus ou moins contraignants.

- **Technique, informations et partenaires**

La continuité des opérations est un objectif exigeant qui peut être nécessaire dans certaines branches où l'absence même momentanée du marché est irrémédiable.

C'est également le cas des services publics (état civil d'une mairie, accueil des enfants scolarisés…) ou dans les services de santé (par exemple, l'alimentation électrique des salles d'opérations et des services de réanimation). Dans tous les cas, où une interruption est tolérable, il est vraisemblable que le coût sera moins lourd.

- **Financier**

Par-delà la survie, les objectifs peuvent être classés par ordre de contrainte croissante :

- ► Maintien d'une situation bénéficiaire (solde positif du compte de résultat, même au cours de l'exercice de survenance).
- ► Maintien du niveau de bénéfice moyen de l'organisme.
- ► Maintien de la croissance (du bénéfice).

On notera que le maintien de résultats financiers est particulièrement important pour les sociétés dont les actions sont cotées en bourse.

Les variations brutales de résultats sont lourdement pénalisées à la bourse et peuvent donc compromettre la pérennité, l'indépendance de l'organisme, mais également les mandats des dirigeants !

- **Humanitaires**

Il s'agit de minimiser l'impact de l'événement dommageable sur l'environnement de l'organisme, tant au plan de ses salariés que de ses partenaires économiques, en amont et en aval, mais aussi de l'ensemble de la société.

Les objectifs avant sinistre

Il est clair que l'objectif central, avant sinistre, est d'ordre financier.

Le programme de gestion des risques doit « consommer » le moins de ressources financières de l'organisme, tout en permettant de respecter les objectifs après l'événement.

Les objectifs annexes importants

- ► *Réduire l'incertitude,* c'est-à-dire la variabilité des résultats de l'organisme, à un niveau tolérable pour les dirigeants.
- ► *Respect des lois et des règlements* auxquels l'organisme est soumis.

- *Liaison avec les objectifs « sociétaux » :* on remarquera que les objectifs au niveau de la société se transcrivent, soit :
  - *Au niveau des lois et des règlements* qui doivent refléter la volonté populaire mise en forme par sa représentation législative.
  - *Au niveau de la citoyenneté et de l'éthique* par le dépassement de la stricte observance des obligations pour aller au-devant des attentes humanitaires ou culturelles de la société. Cet aspect est aujourd'hui le contenu même de la responsabilité sociale d'entreprise (RSE).

11 *Le coût du risque ou pourquoi faut-il gérer les risques ?*

Replacée dans la perspective des objectifs définis à la question précédente (en résumé, continuité d'activité en toutes circonstances), la gestion des risques a pour cœur de mission, ou pour enjeu stratégique, de mettre en place les moyens permettant à l'organisme d'atteindre ses objectifs quoi qu'il puisse arriver. Autrement dit, quelle que soit l'ampleur de la perte potentielle, le risk-manager doit veiller à ce que celui-ci dispose encore des ressources suffisantes pour respecter ses missions, comme cela a été exposé à la question 10. C'est la raison même de la nécessaire liaison entre stratégie et gestion des risques.

Dans ces conditions, le risk-manager doit remplir sa mission avec le minimum de ressources, en optimisant l'efficacité économique. En conséquence, il doit veiller à réduire le « coût du risque à long terme ». Les quatre composantes essentielles du « coût du risque » sont :

- ***Les coûts administratifs*** liés au processus de gestion des risques, qui comprend les frais engendrés par le service gestion des risques lui-même, les salaires des collaborateurs, les frais administratifs, les déplacements, la communication… En résumé, l'ensemble des postes de coûts à prendre en compte dans la gestion d'un service ou d'un département dans un organisme. Il faut également prendre en compte les honoraires des prestataires de services auxquels on aurait sous-traité certaines fonctions (par exemple, la gestion des sinistres, la visite technique de sites…). Ces frais sont relativement faciles à identifier et à chiffrer. En revanche, ceux exposés dans les services opérationnels participant à l'effort de gestion des risques peuvent être plus difficiles à identifier tout en étant significatifs.
- ***Les coûts des efforts de réduction des risques*** représentent les dotations aux amortissements des investissements, ainsi que les frais récurrents liés à ces processus de traitement des risques. Pour une installation de détection et/ou extinction automatique d'incendie (sprinklers), il y a, par exemple, un investissement initial significatif et ensuite des frais d'entretiens annuels. Les processus de protection des salariés peuvent comprendre l'achat initial de vêtements de sécurité et leur remplacement, ainsi que les conséquences d'un ralentissement des rythmes pour utiliser des procédures de sécurité. Il n'est pas toujours facile d'identifier tous les coûts induits.

- ***Les coûts des instruments de financement des risques par transfert*** sont, pour l'essentiel, des cotisations versées aux sociétés d'assurance ou de réassurance, en principe facilement identifiées. Tous les autres transferts à des non-assureurs (par exemple, clauses de protection ou d'abandon de recours dans les contrats) ont des coûts plus difficiles à chiffrer.
- ***Le coût des rétentions*****,** c'est-à-dire des sinistres ou des portions de sinistres dont le financement, non transféré à un tiers, reste à la charge de l'entreprise. Il s'agit des franchises sur les contrats d'assurance et des sinistres non assurés, ou non assurables.
- À ces quatre postes on pourrait en ajouter un cinquième : ***Le coût des investissements abandonnés parce que réputés « trop risqués »*****,** mais il est très difficile de chiffrer le coût de ces opportunités non saisies.

Les responsables sont toujours tentés par les comparaisons, le « *benchmarking* », avec des concurrents ou des partenaires : *« Notre coût du risque est-il en ligne avec celui de nos concurrents ? »*

Il faut être très vigilant et les limites de cet exercice sont doubles : deux entreprises n'ont pas le même profil de risques (leur portefeuille de vulnérabilités leur est propre) et deux équipes de direction n'ont pas le même appétit de risque.

Il a été souligné, au niveau des objectifs, que des objectifs après sinistre plus exigeants que la survie entraînent un coût du risque plus élevé : à court terme, une entreprise qui ne gère pas ses risques graves, mais peu fréquents, peut apparaître plus efficiente, jusqu'au jour où survient l'événement catastrophique qui l'emporte. C'est pourquoi il a fallu inventer un nouveau concept pour rendre compte de sa capacité à rebondir : la résilience.

12 *Avez-vous dit résilience ?*

À la question 10, nous avons exposé les échelles d'objectifs de gestion des risques après événement. Idéalement, la gestion des risques devrait assurer la survie de l'organisme en toutes circonstances. Pour ce faire, à la limite, il suffirait qu'elle dispose de la trésorerie nécessaire pour franchir le pincement de la période qui suit un événement dommageable, sous réserve d'avoir conservé la confiance de ses parties prenantes.

Toutefois, cet objectif « minimum » peut se révéler hors d'atteinte dans certaines circonstances exceptionnelles, en particulier en matière d'engagement de responsabilité et/ou d'atteinte à l'environnement, où il n'est plus besoin de citer l'Exxon Valdez, ainsi que les événements plus récents dans le golfe du Mexique pour illustrer le propos. Donc, dans ces scénarios de catastrophe extrême, il faudra peut-être se contenter d'en limiter la vraisemblance pour que les parties prenantes puissent vivre avec, et aient une perception du risque (voir le chapitre 1 de l'ouvrage *Diagnostic des risques — Identifier, analyser et cartographier les vulnérabilités,* publié chez AFNOR Éditions[1]) qui leur permette de l'accepter, en échange des avantages « sociétaux » et/ou financiers retirés. C'est ce que les Britanniques appellent la « licence sociale d'opérer ».

Mais un objectif limité à la « survie » peut être insuffisant pour répondre aux attentes des parties prenantes, en particulier pour les vulnérabilités que l'on pourrait qualifier de moyennes, dont la réalisation pratiquement certaine sur un horizon de cinq ou dix ans demeure très aléatoire d'année en année. En effet, la « survie » ne traiterait pas les conséquences sur les résultats et transformerait la vie de l'organisme en une montagne russe perpétuelle. Dans ce cas, les parties prenantes les plus proches, celles du premier cercle (actionnaires, dirigeants et collaborateurs), mais aussi les fournisseurs et les sous-traitants pourraient s'inquiéter sur la viabilité à long terme de l'organisme.

L'État, les collectivités locales et les citoyens « consommateurs » ou « spectateurs » pourraient, également, être alertés par la perception d'une gestion chaotique, à courte vue. C'est alors que les décideurs doivent envisager d'assigner à la gestion des risques, des objectifs plus

1 Sophie Gaultier-Gaillard et Jean-Paul Louisot, *Diagnostic des risques — Identifier, analyser et cartographier les vulnérabilités*, AFNOR Éditions, 2e édition, 2014.

contraignants évoqués précédemment (voir question 10), dans l'ordre de l'arrêt supportable, de la stabilité des résultats financiers ou de la prise en compte des intérêts de la société, relevant des choix éthiques et des valeurs de l'organisme. En clair, il s'agit de choisir les conditions d'un rebondissement optimum, même après un sinistre grave.

Sans qu'il soit nécessaire de développer longuement, monter dans l'échelle de la progression des objectifs après événement s'accompagne d'une mobilisation croissante de ressources, en particulier de ressources financières. De ce fait, il y a une contradiction croissante entre cette volonté de rebondir après un événement grave et l'objectif avant événement d'efficacité économique, c'est-à-dire de réduction du coût du risque.

Il convient de souligner à nouveau que l'analyse financière à court terme conduirait à préférer un organisme qui fait peu d'effort de gestion des risques, car ses résultats financiers seraient meilleurs. Il apparaîtrait à court terme, comme « plus rentable », procurant un meilleur rendement de ces investissements pour ses actionnaires.

C'est pourquoi il faut introduire un concept nouveau, permettant d'apprécier la gestion à long terme et de rendre la notion de « développement durable » mesurable, même dans le cadre d'une analyse financière. Le terme retenu est celui de résilience.

Aujourd'hui, tout auteur sur la gestion des risques se croit obligé de le citer, à bon ou à mauvais escient. Le mérite de le définir pour la première fois, est revenu à l'Association des auditeurs canadiens, dans un guide destiné à ses membres, et publié au cours de la dernière décennie du siècle dernier.

Sans aller dans les détails, rappelons que le terme est repris de la métallurgie pour qualifier la capacité d'un métal à reprendre ses qualités, en particulier son élasticité après un stress, un choc thermique ou mécanique.

En matière de gestion des risques, la résilience mesure ou évalue la capacité d'un organisme à rebondir après un accident majeur, ou à survivre à une crise. Donc, cela revient vis-à-vis :

- de la société, à faire face à ses obligations ;
- des salariés, à garantir un emploi ;
- des partenaires, à sécuriser les échanges ;
- des actionnaires, à générer des dividendes.

2
Le diagnostic et la « cartographie » des risques

13 *En quoi consiste le diagnostic des risques ?*

Le diagnostic des vulnérabilités est la première étape du processus de gestion des risques. Il comporte trois phases distinctes, à savoir : l'identification, l'analyse, et l'évaluation des risques.

On notera que, dans la norme ISO 31000:2010, le terme d'appréciation du risque recouvre la même étape du processus de gestion des risques.

Dans la terminologie retenue, ici :

- « identifier » signifie reconnaître qu'un « événement indésirable » pourrait survenir ;
- « analyser » se réfère à une estimation chiffrée de l'ampleur des conséquences financières pour l'organisme étudié ;
- et « évaluer » à rapprocher le risque résiduel des critères définis pour définir si des mesures supplémentaires de traitement s'imposent.

Bien entendu, cette répercussion s'entend à la fois, du fait de la probabilité de survenance, généralement appelée *fréquence* et du fait de l'ampleur de l'impact, généralement appelée *gravité* des sinistres potentiels. Mais il convient de prendre en compte également le degré de *prévisibilité* de la survenance de ces événements. En définitive, l'analyse vise essentiellement à évaluer *la capacité de l'organisme à atteindre ses objectifs et les conséquences qui en résultent*. Plus récemment, certains praticiens ont introduit la notion de *vélocité* pour rendre compte de la vitesse à laquelle l'organisme est frappé, dès lors que l'événement devient inéluctable.

Cette étape est la pierre angulaire du processus de la gestion des risques : un risque mal ou non identifié ne peut pas être intelligemment géré. En revanche, si un risque a été identifié et quantifié avec précision, les contours du programme pour le traiter apparaissent presque naturellement. C'est pourquoi nous verrons, à la question 21, comment le diagnostic se transforme en démarche récurrente dite de « cartographie des risques ».

Bien entendu, un même événement peut avoir des conséquences pour plusieurs acteurs. Pour prendre un exemple simple, supposons qu'un stockage de pneus usagés, situé en périphérie d'une agglomération, subisse un incendie majeur avec émission de fumées noires et toxiques que le vent rabat vers une zone résidentielle et commerciale de la ville. On peut évaluer les conséquences de cet incendie du point de vue de l'entreprise

qui était propriétaire du stock : elle subit une perte de dommages aux biens, du fait de la destruction de son stock et vraisemblablement une perte de revenus à la suite de l'arrêt de sa production. On peut également imaginer une perte d'image ou de réputation pour avoir pollué l'environnement et interrompu les livraisons à ses clients.

Mais cette analyse en système semi-fermé ne suffit pas : l'événement aurait, également, des conséquences pour les voisins, la ville, voire les autorités préfectorales selon les répercussions. Pour poursuivre la réflexion, il faut donc faire des hypothèses sur les conséquences pour les tiers. Du point de vue de l'entreprise, il s'agira d'analyser les engagements de responsabilité, civile ou pénale, que l'incendie pourrait provoquer. Du fait qu'il s'agit d'un péril endogène, le risk-manager pourrait être conduit, naturellement, à envisager les conséquences.

En revanche, le risk-manager d'une clinique située à plus d'un kilomètre de l'incendie aura-t-il pensé à vérifier sur une carte le positionnement de sources de périls exogènes et se sera-t-il inquiété du sens des vents, surtout si la clinique est spécialisée dans des maladies pulmonaires ?

En résumé, le diagnostic des risques consiste en un exercice récurrent d'inventaire systématique de toutes les ressources de l'entreprise, y compris celles dont elle bénéficie sans en payer le prix directement et un recensement de tous les périls qui pourraient frapper ses ressources.

Dans la seconde phase, il faut imaginer des scénarios « catastrophes » pour évaluer l'impact des événements identifiés sur nous-même et sur les autres, en particulier lorsque notre responsabilité civile ou pénale pourrait être engagée.

On voit d'emblée, que la problématique du diagnostic sera beaucoup plus délicate à résoudre dans le cas des systèmes ouverts, comme les centres commerciaux, les établissements de santé et les collectivités territoriales, où l'ensemble des parties intéressées ne sont pas dans la dépendance des acteurs principaux, comme c'est le cas dans une usine où l'ensemble des acteurs peuvent être formés et entraînés au diagnostic des risques.

Il reste encore le mode projet, où différents partenaires sont impliqués avec un objectif commun (mener à bien le projet), mais parfois, des intérêts divergents qui imposeront un diagnostic croisé des différents partenaires contractuels ou non.

14 *Comment identifier les risques ?*

Nous avons défini les risques pesant sur un organisme, comme un portefeuille de vulnérabilités. Chaque vulnérabilité est caractérisée par trois paramètres : ressource, péril et impact.

L'identification, qui est la première phase du diagnostic, consiste à recenser l'ensemble des ressources dont l'entreprise a besoin pour fonctionner et à les rapprocher de tous les événements aléatoires, dont la survenance pourrait l'en priver de façon partielle ou totale, temporaire ou définitive.

Identifier les ressources internes à l'organisme, celles dont il a la maîtrise directe, ne devrait pas poser de difficultés majeures : les principaux outils d'identification sont passés en revue à la question 18. Toutefois, l'organisme est également un composant d'un système ouvert et dépend de ses échanges, contractuels ou non, avec son environnement physique, socioéconomique et concurrentiel.

La principale difficulté est de recenser ces ressources, que nous considérons comme des acquis dans les pays d'Europe de l'Ouest. Par exemple, la sécurité des biens et des personnes et l'établissement judiciaire équitable qui ne sont pas toujours garantis lorsque nous nous installons dans un monde global. En ce qui concerne l'environnement physique, sommes-nous attentifs, à la qualité de l'air requise pour certaines fabrications délicates, à la qualité de l'eau lorsqu'elle n'est pas la matière première que nous vendons ?

Pour garantir un recensement complet, il faut disposer d'une structure d'identification des ressources. C'est ce que nous nous sommes efforcés de donner, sous forme d'un outil pratique, dans les questions 4, 5 et 6 de cet ouvrage.

Le découpage en quatre catégories internes et deux catégories externes (« partenaires » pour celles qui relèvent de transaction avec des tiers et « gratuites » pour celles relevant des interfaces non accompagnées de contrat) doit permettre à toute entreprise d'éviter les omissions les plus graves.

En ce qui concerne, le second paramètre, « l'événement aléatoire indésirable », le seul bon sens ne permet pas de tout envisager. C'est pourquoi nous avons élaboré une liste de différents périls types dans

lesquels toute la spécificité de l'organisme et de son environnement doit pouvoir être pris en compte. Dans cette démarche, le principal obstacle est le refus de voir, ou de prendre en compte, certains aléas.

Une illustration récente en est la preuve : « Combien d'urbanistes et d'architectes avaient pris en compte le risque de tsunami dans la conception des stations balnéaires construites au cours de ces trente dernières années en Asie ? ». Et que dire des événements du Japon en 2011 ? Le risque de tremblement de terre sous-marin entraînant des vagues géantes a été cependant recensé par les géographes, comme il l'est pour certaines zones côtières de l'Atlantique. Malgré cela, les autorités locales n'avaient même pas investi dans un système d'alerte pour permettre à la population de trouver refuge dans les hauteurs, au moins sur certaines îles ! Pour ce qui est de l'Union européenne, le système d'alerte est-il opérationnel en Europe du nord du Danemark au sud du Portugal ?

L'identification des risques est donc une nécessité absolue dans laquelle il faut s'engager avec un esprit ouvert et la capacité de remettre en cause les idées reçues et les habitudes. Pour éclairer ce propos, voici quelques idées :

- *« On a toujours fait ainsi ! L'itinéraire suivi par nos camions est le même depuis vingt ans et nous n'avons jamais eu un pont coupé par une crue (décennale ? centennale ?) »*
- *« Lors des grèves, nous avons toujours pu nous approvisionner (quels étaient nos fournisseurs lors de la dernière grève ?) »*
- À quelle distance, avons-nous investi dans les pays émergents, en Europe de l'Est ?

Finalement, le plus grand danger d'une identification des risques n'est peut-être pas d'oublier une vulnérabilité initialement, mais de vivre avec l'idée que, puisque nous avons identifié à l'instant « t » dans la configuration « c » des risques, nous n'avons plus à faire d'effort. Un processus d'identification des risques est une « denrée périssable » qui doit être remise à jour avec une périodicité liée aux évolutions internes et externes des métiers et des environnements majeurs de l'entreprise. Il est difficile de citer un rythme idéal, mais on peut donner quelques règles : rafraîchissement annuel, revue de détail à chaque modification majeure du contexte (par exemple, cession, acquisition, changement de processus, installation dans un nouveau pays…). Au bout de trois à cinq ans sans révision, une identification est hors d'usage.

15 *Comment analyser les risques ?*

L'ensemble des possibilités de survenance d'événements aléatoires, qui auraient des conséquences négatives sur l'organisme, est pratiquement illimité. Les risques identifiés doivent donc être évalués et classés pour déterminer des priorités de traitement.

L'approche de l'évaluation de l'impact des risques est encore, aujourd'hui, le plus souvent limitée aux deux variables traditionnellement utilisées par les assureurs qui veulent évaluer la charge future de la sinistralité de leur portefeuille, à savoir :

- La probabilité de survenance, aussi appelée fréquence, puisque les sinistres surviennent, effectivement, dans le portefeuille d'un assureur.
- L'impact financier de l'événement, également appelé gravité, là encore mesuré dans le cadre de l'application de garanties d'assurance.

Lorsque la loi des grands nombres s'applique, dans un portefeuille suffisamment diversifié, le poids moyen annuel (espérance mathématique de perte), peut être calculé en multipliant les deux variables, sur l'hypothèse implicite d'une indépendance de ces deux variables.

Appliquée à un organisme unique, cette pratique, qui donne un coût moyen à long terme, ne rend pas compte de la réalité de l'aléa auquel il est confronté annuellement. Une illustration de cette limite peut être tirée du monde nucléaire : supposons qu'en France, chacune des centrales nucléaires (moins de 100) a une probabilité de sinistre majeure de 1 sur 10 milliards (chiffre qui résulterait d'une analyse de sûreté de fonctionnement), le parc aurait une probabilité de 1 sur 10 millions. Supposons, en outre, que la catastrophe entraîne des dommages à hauteur de 1 000 milliards d'euros, alors le « coût annuel » moyen serait de 100 000 euros par an. Pour EDF, c'est une charge tout à fait tolérable, mais pour le PDG et la population ce n'est pas le coût moyen sur 10 millions d'années qui compte, mais de savoir si elle peut vivre avec le niveau de sécurité atteint.

En clair, l'analyse des vulnérabilités doit inclure une évaluation de la dispersion, ou volatilité du résultat.

Pour les risques de fréquence qui surviennent régulièrement, mais avec des conséquences limitées (comme les dommages aux véhicules

dans une flotte automobile, les arrêts maladie dans une entreprise employant plusieurs milliers de personnes, les erreurs de livraison pour un transporteur ou la poste), l'approche historique par définition de lois de probabilités pour la fréquence et la gravité permet d'évaluer le risque.

Pour les risques exceptionnels, c'est la gravité qui sera la variable majeure, rapprochée de la probabilité de survenance, ou vraisemblance, uniquement pour définir des niveaux de « sécurité » acceptables à la lumière de la gravité du risque. C'est alors le vecteur probabilité, gravité, volatilité qui est la clé du classement.

Dans le cas des risques majeurs qui pèsent sur l'entreprise, comme un incendie total, un tremblement de terre, une explosion, une contamination du sol et des eaux, c'est en scénario qu'il faut raisonner pour déterminer les conditions de survie sous la forme de ce que l'on appelle aujourd'hui dans les institutions financières, une « valeur en risque », et dans les entreprises de production et commerciales, une « trésorerie en risque ».

L'évaluation de la gravité vise alors à déterminer, dans le pire des cas, l'ampleur de la saignée de trésorerie qui peut affecter l'organisme avant qu'il ne retrouve un régime de croisière. Bien entendu, cette analyse doit être revue, annuellement, à la lumière des projections budgétaires et en prenant en compte, non seulement les pertes immédiates, mais également les pertes induites, les pertes de revenus, y compris la perte de confiance des partenaires économiques et des autres parties prenantes (atteinte à la réputation).

Certaines conséquences ne sont pas traduisibles en termes financiers (atteintes à l'environnement) et doivent être replacées dans le cadre d'autres objectifs de l'organisme que purement financiers, (par exemple, développement soutenable, assistance aux personnes en détresse…). Pour les principales vulnérabilités, celles qui devront être prises en compte au niveau des dirigeants parce qu'elles sont stratégiques, il faudra sans doute pousser l'analyse sur d'autres plans que les trois variables identifiées ici. Un profil de vulnérabilités détaillé pourra être dressé en utilisant l'approche cindynique (voir question 99).

En attendant, tout ce qui peut être quantifié en termes financiers doit l'être !

On pourra se référer à la norme ISO 31010:2009 *Gestion des risques — Techniques d'évaluation des risques*, en cours de révision, pour un panorama des méthodes d'évaluation des risques.

16 *Quelles sont les valeurs des actifs physiques ?*

Les actifs physiques de l'organisme (bâtiments et équipements industriels, équipements de bureaux, fournitures et stocks pour l'essentiel) sont valorisés sur son bilan. La question fondamentale est : « Comment sont-ils évalués ? »

En ce qui concerne les bâtiments, ils sont entrés en comptabilité à leur prix d'achat ou à leur coût de construction historique, qui peut faire l'objet d'un amortissement à long terme. Cette valeur, ***coût historique*** moins amortissements, est la ***valeur nette comptable***.

En ce qui concerne les équipements industriels et les équipements de bureaux, ils sont entrés en comptabilité en coût d'achat, coût historique et amorti à moyen terme selon la catégorie, de 2 à 5 ans pour le matériel informatique, de 5 à 20 ans pour les équipements de production.

Les stocks sont évalués en coût d'achat pour les matières premières ou les pièces utilisées en l'état et en coût complet pour les produits finis (y compris l'affectation des frais généraux).

Ces valeurs ont-elles un intérêt pour la gestion des risques ? Pour répondre à la question, il faut reprendre les différents éléments, l'un après l'autre, mais on peut définir un principe général : le risk-manager doit se projeter dans l'après sinistre et s'interroger sur le niveau de financement qui sera nécessaire pour remettre l'organisme en état de marche.

Bâtiments

Si le bâtiment est totalement détruit alors que l'organisme l'utilise pour ses opérations courantes (production et/ou vente), elle doit trouver un financement à la hauteur du ***coût de reconstruction***. Là encore, il convient de distinguer :

- La reconstruction à l'identique (mêmes matériaux, mêmes plans) s'impose dans le cas d'un bâtiment historique et/ou en zone classée : c'est le ***coût de reconstruction à l'identique***.
- La reconstruction de même capacité fonctionnelle, en utilisant de nouveaux matériaux et un nouveau mode de construction, peut être plus judicieuse pour un bâtiment industriel : c'est le ***coût de reconstruction fonctionnelle*** (il convient alors de faire établir des devis prévisionnels pour évaluer ce montant).

Deux remarques spécifiques aux couvertures d'assurance sont à prendre en compte :

- La ***valeur d'assurance*** est la valeur de reconstruction à l'identique moins la vétusté à dire d'expert (si une valeur « fonctionnelle » est préférée, il faut l'indiquer expressément à l'expert et le préciser à l'assureur en cas de couverture).
- Il se peut que la reconstruction à l'identique et sur le même site soit impossible du fait de l'évolution du Code de la construction et du plan local d'urbanisme (PLU), il faudra alors envisager des aménagements pouvant être coûteux et/ou un déménagement (dans ce cas, un ajustement du contrat d'assurance pour tenir compte de ces données s'imposera).

Équipements industriels et matériels de bureau

Pour les équipements industriels et les matériels de bureau, on est confronté à un raisonnement similaire à celui de l'immobilier, en revanche, on retiendra le terme de coût de remplacement plutôt que celui de coût de reconstruction. La problématique de « remplacement » se pose alors ainsi :

- Doit-on reprendre les mêmes équipements ? Il s'agit alors d'un ***coût de remplacement à neuf***, sous-entendu à l'identique (même fabricant, même référence…).
- Doit-on prendre des équipements de même performance ? Il s'agit alors d'un coût ***de remplacement fonctionnel***.

La question du remplacement fonctionnel se pose de façon plus aiguë dans les industries à évolution technologique rapide.

À l'origine, c'est pour les équipements informatiques que le remplacement à neuf s'est révélé impossible : au bout de deux ou trois ans, les équipements achetés ne sont plus disponibles, et les nouveaux, moins chers, ont une productivité supérieure : « Que devrait-on acheter, et quelle est la juste indemnisation de l'assureur ? »

La question se pose d'une manière générale pour tous les composants d'un processus industriel : il faut se tenir à jour pour adapter les couvertures à la nécessité du redémarrage, le moment venu.

Stocks et fournitures

Pour les stocks de matières premières et de fournitures à rotation rapide, la question peut être assez simple, dans la mesure où les valeurs du

bilan et les montants des dernières factures d'achat sont assez récents pour servir de base d'évaluation.

Pour les stocks à rotation plus lente, il faut se référer au mode de gestion comptable. Sans faire un cours de comptabilité, les deux méthodes principales sont FIFO (*First In, First Out* ou premier entré, premier sorti) et LIFO (*Last In, First Out* ou dernier entré, premier sorti). En période d'évolution sensible des prix, la première méthode conserve en stock les achats les plus anciens donc fait ressortir une valeur de stocks plus inexacte. Dans les conditions qui prévalent dans les économies développées avec des inflations limitées à quelques pour cent, la question peut-être inutile, mais pour ceux qui opèrent dans des pays émergents avec des inflations à deux chiffres, il peut être utile d'envisager la situation, avant le sinistre !

Si on osait, on pourrait dire que le risk-manager s'intéresse au NIFO (*Next In, First Out*, le coût d'achat du remplacement pour remettre les stocks à niveau). Pour les stocks d'encours et de produits finis, en France, la règle est de les comptabiliser en ***coûts de production complets***, en incorporant une partie des frais généraux. Ces frais seraient-ils exposés, à nouveau, en cas de reconstitution ? C'est précisément une des questions qui se posent derrière la notion de ***coût de reconstitution***.

Et le risque de change ?

Dans tous les cas, pour toutes les classes d'actifs physiques, il existe une complexité supplémentaire lorsque les coûts de reconstruction, remplacement ou reconstitution sont exposés dans une monnaie, autre que celle de consolidation du bilan ou de disponibilités de l'entreprise. Ce risque n'est pas réservé aux grandes multinationales, même si la portée en a été limitée pour les ETI ou PME/PMI avec la mise en place de la zone euro, qui comprend le plus souvent leurs principaux partenaires économiques.

17 *Faut-il valoriser les actifs immatériels ?*

Un constat : la capitalisation boursière d'une entreprise (mesurée par le cours du jour multiplié par le nombre d'actions émises) rapprochée de la valeur totale des actifs physiques, même évalués en valeur de remplacement, est très largement supérieure. Cette « valeur de marché de l'entreprise » peut atteindre des multiples, allant de 3 à 20 fois la « valeur physique ». L'explication est simple par la théorie financière, où la valeur de l'entreprise est égale à la valeur actuelle du flux futur de dividendes, actualisé à un taux tenant compte du niveau de risque et de la croissance espérée.

Cependant, ce modèle rend difficile l'explication du haut niveau de certaines actions, en particulier au plus haut de la bulle Internet, pour des entreprises n'ayant jamais réalisé de bénéfices et ne prévoyant pas d'en dégager dans un futur proche. Alors, d'où vient la valeur que le marché leur accorde ? Cette valeur ajoutée, quelle qu'en soit la source, provient de l'image de l'entreprise et constitue ce que nous appellerons, ici, la ***réputation***. Quelle est la réalité de cette grandeur ?

La réponse est que, même en tenant compte des montagnes russes que la bourse a connues, la différence entre la valeur de marché, non seulement en bourse, mais également dans les transactions rendues publiques d'entreprises privées reprises par des groupes plus importants, demeure significative. L'image (ou la réputation), qu'elle ait ou non une réalité, a un impact significatif sur l'économie dont elle représente, sans doute, en moyenne de 60 à 70% de la richesse des pays développés.

En résumé, si le risk-management continuait à s'intéresser exclusivement aux actifs physiques, qui ne représentent plus qu'un petit tiers de la valeur d'un organisme donné, il laisserait de côté l'essentiel de la « valeur » pour les « actionnaires ».

Il est donc temps que les risques liés à l'image ou à la réputation soient diagnostiqués et traités. Pour ce faire, on ne peut pas se contenter de la valeur globale de la réputation constatée par différence, il convient donc, en premier lieu, de valoriser les principaux composants qui peuvent être identifiés, c'est-à-dire les actifs immatériels. Cette opération est singulièrement incontournable dans les ETI ou PME/PMI, et plus généralement, dans tous les organismes qui n'ont pas d'actions échangées sur un marché boursier établi.

Les principaux actifs immatériels valorisables sont :

- Les brevets et licences.
- Les marques.
- Les droits au bail.

Comment les valoriser ? On pourrait imaginer que pour certains, il existe un marché, et que ce prix de marché est utilisé comme référence. Toutefois, par essence, ils sont « uniques » et font donc rarement l'objet d'un marché stable et fiable.

Dans ces conditions, la seule possibilité raisonnable est d'évaluer leur contribution à la marge brute de l'entreprise et de la projeter dans un « futur raisonnable », en tenant compte de la durée restant à courir pour le bail, le délai avant la perte d'un brevet (pour un médicament, par exemple). Le flux net de trésorerie, ainsi projeté sur plusieurs années, doit être actualisé pour tenir compte de la valeur temps de l'argent. La question essentielle est le choix du taux d'actualisation. En général, tout organisme a défini un taux de rendements sur actifs, qui peut être pris comme base. Ainsi, pour les actifs immatériels, dont la contribution peut être identifiée et mesurée, la valeur à retenir est la valeur actuelle du flux de revenus nets potentiels dégagés par l'actif considéré.

Il faut évoquer le « fonds de commerce » qui apparaît sur certains bilans, pour autant qu'ils aient fait l'objet d'une transaction chiffrée.

En ce qui concerne les compétences du personnel, les savoir-faire individuels, il est très difficile de les apprécier, en dehors des personnes-clés (voir question 26).

Enfin, l'impact d'une part de marché, rapproché des coûts d'entrée sur un marché donné, peut devenir l'objet de spéculations, que les autorités de contrôle fiduciaire sont hésitantes à laisser entrer sur un bilan, surtout après l'affaire Enron et autres affaires similaires apparues depuis.

En résumé, il faut prendre en compte les actifs immatériels pour la gestion des risques, sous réserve de les valoriser avec prudence.

18 *Quels sont les outils d'identification et d'analyse des risques ?*

Les outils d'identification des risques, ou plutôt des vulnérabilités (voir question 3), sont tous les moyens à la disposition des professionnels de la gestion des risques pour recenser l'ensemble des ressources de l'organisme et les périls qui pèsent sur ces ressources. Généralement, on les scinde en sept groupes, autour d'instruments traditionnels de la gestion d'entreprise.

Documents comptables et financiers

La première rencontre avec les ressources d'un organisme se fait au travers de la lecture de ses comptes.

Voici quelques exemples significatifs des informations à retenir :

- ***Le bilan*** permet à l'actif de saisir les principaux biens immobiliers ou mobiliers dont dispose l'entreprise pour ses activités (mais attention aux biens en location et/ou *leasing*). Le passif peut révéler des conflits en cours (par exemple, engagement de responsabilités). Le rapprochement éclaire les liquidités et les ratios qui sont des indicateurs de santé générale. Le compte client peut être révélateur du risque « crédit client »…
- ***Le compte de résultat*** donne les flux transitant par l'entreprise et peut indiquer un client ou un fournisseur-clé (leur importance dans les achats ou les ventes). Il donne une indication sur la marge de manœuvre de l'entreprise et sa capacité à encaisser des « coups » (marge brute, marge nette…).
- ***Le tableau « emploi et ressources »*** éclaire la santé financière à moyen et long terme de l'entreprise : d'où viendront les fonds pour ses investissements, leur utilisation, et globalement sa dépendance des marchés financiers et/ou des banques.
- ***Les annexes au bilan*** représentent l'ensemble des commentaires et des engagements hors bilan.
- ***La trésorerie*** est le cordon ombilical de tout organisme : son âge de survie, puisqu'il doit à tout moment disposer des liquidités nécessaires pour faire face à ses obligations. C'est le garant financier ultime de sa résilience.

Documents administratifs et commerciaux

Tous les documents, qui circulent à l'intérieur et à l'extérieur de l'organisme, sont des éclairages des risques. Par exemple, un mode d'emploi mal rédigé peut déboucher sur des engagements de responsabilité produit, un tract syndical peut éclairer sur la situation des ressources humaines, la publicité d'un concurrent peut être annonciatrice d'une « guerre »…

Schémas de production et schémas de flux

Les schémas de production mettent en lumière les goulots d'étranglement (par exemple, les machines dont l'arrêt stopperait une grande part de l'activité). Les schémas de flux externes sont des révélateurs de clients ou de fournisseurs-clés, mais aussi de trajets incontournables…

Historiques de sinistres et retour d'expérience

Bien entendu, l'éclairage du futur par le passé est la clé de la gestion des risques : on apprend de ses erreurs, comme on développe des probabilités ou des analyses de tendance à partir d'historiques de sinistres, en recherchant les causes profondes d'accidents ou d'incidents, voire de simples comportements anormaux (arbre des causes, arbre des conséquences, analyse de criticité…).

Le retour d'expérience « anticipé » est aussi l'utilisation de modèles, de maquettes, de prototypes qui permet de simuler, en grandeur réduite, un système complexe et d'améliorer ainsi, par avance, le niveau de sécurité de la réalisation, en grandeur nature. C'est un des éléments de la réduction des risques en « mode projet ».

Questionnaires standards

Confronté à la nécessité de dresser un diagnostic rapide des principales vulnérabilités d'un groupe diversifié, d'un secteur industriel ou d'une zone d'activité, le risk-manager peut avoir recours aux compétences des dirigeants locaux, en canalisant cette connaissance au travers de quelques questions fermées et d'une question ouverte.

Il pourra ainsi disposer d'une première information consolidable (questions précises, avec un nombre limité de réponses) tout en laissant le soin à chacun de signaler son « souci » principal (« risque perçu ») qui peut lui être tout à fait spécifique.

Visites de site

La nécessité de communiquer sera soulignée à plusieurs reprises (voir question 22) : cela suppose un dialogue avec les responsables opérationnels. Il est encore plus indispensable dans le cadre d'un projet d'ERM qui repose sur la coopération éclairée de tous. La visite de site est l'occasion de porter un regard conjoint, parfois avec l'aide d'un spécialiste externe, pour engager le dialogue sur le diagnostic et la réduction des vulnérabilités.

Consultations d'experts internes et externes

Si le risk-manager est une personne de compétences transversales, en revanche celles-ci ne peuvent être universelles. Il lui faut alors faire appel à tous les experts internes et externes qui peuvent apporter des connaissances précises sur les phénomènes étudiés : un géologue pour la connaissance de sous-sols (mines, fondations…), un météorologue pour les vents, les marées, mais on peut aussi avoir recours à un œnologue pour la visite d'un producteur éleveur de vins…

19 *Quelles méthodes faut-il employer pour établir un diagnostic des risques ?*

Passer de l'outil (voir question 18) à la méthode, c'est concevoir et mettre en œuvre un processus systématique pour dresser le diagnostic des vulnérabilités d'un organisme.

Au cas d'espèce, il y a sans doute autant de méthodes qu'il y a de consultants, mais beaucoup demeurent des « secrets de fabrication ». Nous en avons retenu deux, qui ont fait l'objet de publications et dont les objectifs et les qualités sont très différents.

La méthode des bilans simplifiés

Dans le cas des PME/PMI, aujourd'hui, l'approche patrimoniale peut encore se révéler plus parlante pour les dirigeants et les responsables financiers. Dans ces conditions, il est possible de dresser un diagnostic des vulnérabilités, en partant du bilan simplifié. Cette méthode s'inspire d'une recherche effectuée, il y a quelques années, dans le cadre de la Fédération nationale des agents généraux d'assurance (aujourd'hui plus connue sous le sigle AGEA).

Elle s'appuie sur les quatre postes du bilan simplifié (actif fixe et actif circulant, passif long terme et passif court terme). Elle a le mérite de la simplicité, mais l'inconvénient majeur de passer à côté des échanges qui ne s'accompagnent pas d'une transaction, (voir question 6, « ressources gratuites »).

Par ailleurs, cette approche « comptable » pourrait conduire à se focaliser sur les risques assurables et les réponses apportées par les assureurs. Elle est, en effet, une illustration de l'approche par les « pertes », c'est-à-dire une réponse à la question : « *Quelles pertes pourrions-nous subir ?* »

Toutefois, elle doit déboucher, au moins, sur une opération de nettoyage du budget assurances de l'entreprise. La rationalisation de ce poste budgétaire s'accompagne, en outre, de la mise en lumière des vulnérabilités patrimoniales lourdes.

Elle pourrait être étendue à une approche « cinétique », en se référant au compte de résultats, mais elle perdrait en simplicité sans atteindre la dynamique de l'autre méthode proposée.

La méthode des centres de risques

Yves Maquet a publié cette méthode dans les années 1980. Depuis, l'équipe pédagogique du CARM Institute s'est attachée à la développer et à l'approfondir, en tenant compte de l'évolution des organismes et des grands chantiers de risques, en intégrant la gouvernance, le développement durable et la gestion de crise qui sont les grands sujets du moment. On trouvera ici un résumé de cette méthode à jour.

La méthode s'appuie sur un modèle de l'organisme conçu comme une combinaison dynamique de ressources pour atteindre les objectifs permanents assignés par les responsables (propriétaires ou délégués).

Les ressources sont regroupées en cinq classes (voir questions 4 et 5) soit, en bref : H = humaines, T = techniques, I = informations, P = partenaires, F = financières.

En partant de ce modèle élémentaire, la méthode s'appuie sur la logique de la direction participative, par objectifs. Nous rappelons, brièvement, qu'il s'agit d'un découpage des objectifs d'un niveau hiérarchique en sous-objectifs, assignés aux responsables de niveau inférieur lui rendant compte.

Ces « objectifs critiques », de niveau N, tirent leur nom du fait que, s'ils ne sont pas atteints, le responsable de niveau N ne peut pas atteindre son propre objectif permanent. Chacun de ces objectifs devient l'« objectif permanent » de l'adjoint (de niveau inférieur, N + 1) en charge de la ressource en cause.

De proche en proche, en descendant la ligne hiérarchique, on découpe l'entreprise en « entreprises » ou « cellules individuelles ».

On peut résumer, simplement, le principe de la méthode des centres de risques : lorsqu'un problème est trop lourd pour être réglé, il faut le scinder, de façon rationnelle, en problèmes plus simples, afin de pouvoir les résoudre.

En clair, elle vise à identifier tous les propriétaires de risques au sein de l'organisme pour leur confier la gestion de « leurs » risques.

20 *Qu'est-ce qu'un centre de risques, et comment l'utiliser ?*

L'exercice de découpage d'un organisme en sous-système, tel qu'il est décrit à la question 19, s'arrête à l'échelon de la cellule élémentaire, qui doit être encore une « mini ou microentreprise ». C'est-à-dire que la cellule « vivante » dispose des cinq classes de ressources pour atteindre un objectif. On sait que dans certaines industries la granulométrie est encore plus fine en descendant au processus (établissements financiers), mais généralement le niveau décrit ci-dessus est le plus approprié pour un programme d'ERM.

C'est l'objectif permanent de l'entreprise « monocellulaire », le centre de risque, la combinaison dynamique de ses ressources pour optimiser sa performance au sein de l'organisme.

Les contours (ou frontières) de ce centre de risques et le « champ de force » de l'environnement dans lequel il est plongé, peuvent être appréhendés par le « patron » qui dispose d'un minimum de délégation pour « gérer » sa « microentreprise ». On retrouve le dilemme posé dans l'ISO 31000:2010, la responsabilisation qui impose une délégation sur les moyens.

Les différents outils d'identification des risques cités dans la question 18 sont mis en œuvre, mais une fois les centres de risques identifiés, le principal est le recours à l'entretien, la visite sur place et le dialogue avec le responsable du centre.

Le fil conducteur de l'entretien reprend les points essentiels évoqués ci-dessus (voir tableau ci-après « Questionnaire d'identification des risques ») :

- La question n° 1 vise à cerner l'activité et le positionnement du centre de risques.
- Les questions n° 2 à 6 visent à identifier les ressources dont il dispose, y compris les « ressources gratuites » par les interfaces.
- Les questions n° 7 à 10 visent à déstabiliser le responsable sur deux fronts essentiels : celui des ressources techniques et celui des personnes, des compétences des collaborateurs. Il est visé au cœur de sa sécurité personnelle, au cœur de ses certitudes et doit « imaginer » immédiatement des solutions pour « réduire les tensions ». Elles doivent permettre également de recenser, parmi ces ressources,

celles qui sont vitales et qui devront être protégées en priorité ainsi que les actions à mener pour atténuer (réduire) les risques pesant sur le centre.

- Les questions n° 11 et 12 visent à trouver à l'avance le moyen de rétablir un équilibre objectifs/ressources, que le « sinistre » pourrait rompre. La problématique est donc en termes de « management », pour raisonner en déploiement stratégique. Dans ce contexte, les ressources vitales, en principe, devraient être préservées, quel que soit le coût, puisque les objectifs ne peuvent plus être atteints en cas de disparition.

Il s'agit de demander au « patron », sur le terrain, de définir un niveau de ressource minimum acceptable (de survie) et un seuil de tolérance individuel.

Questionnaire d'identification des risques

1 - Objectifs

1. Quelles sont les missions de votre « département », de votre « service », de votre *business unit,* de votre centre de profit… ?

2 - Ressources

2. Comment êtes-vous organisés ?
3. En quoi consistent vos locaux, votre personnel, vos matériels et vos équipements ?
4. D'où viennent vos produits, vos matières premières, vos informations ?
5. Où envoyez-vous vos produits, vos informations ?
6. Quels sont vos moyens de communication ?

3 - Questions stratégiques

7. Supposons que vos locaux brûlent cette nuit avec tout leur contenu, sans faire de victime parmi votre personnel.

   Demain matin, vos collaborateurs seront là, comment allez-vous vous organiser ?

8. Supposons maintenant l'hypothèse inverse.

   Demain matin, vos collaborateurs ne seront pas là (une grève, impossibilité d'accès), comment allez-vous travailler ?

4 - Comment s'organiser pour éviter ces risques ?

9. Dès maintenant (avant sinistre)
   - prévention/protection
10. Après l'événement (après sinistre)
   - « Plan de redéploiement après sinistre »
   - « Gestion de crise »

21 *Une carte des risques, pour quoi faire ?*

Le diagnostic doit déboucher sur un recensement et un classement des vulnérabilités. Traditionnellement, le poids financier d'un risque peut être mesuré comme le résultat de la prise en compte de deux paramètres : ***probabilité*** et ***gravité***.

Il est devenu usuel dans la profession d'appeler « carte des risques », à un instant donné, un tableau à double entrée : sur un axe, les probabilités (fréquence ou vraisemblance) et sur l'autre, l'impact. C'est de là que vient le nom de cartographie des risques, ou de cartographier pour nommer le diagnostic des risques.

Toutefois, pour que la lecture de cette carte éclaire les décideurs, il est important que les ordres de grandeur des deux axes aient un sens pour eux :

- Pour la probabilité, par exemple, 1 fois par jour, 1 fois par mois, 1 fois par an, 1 fois tous les 5 ans, tous les 10 ans, voire moins de 1 fois par siècle (comme les crues décennales, centenaires ou millénaires en matière d'inondation).
- Pour les gravités : pour les risques faibles ou moyens, une référence au bénéfice annuel donne un éclairage intéressant (moins de 1 pour 1 000 du bénéfice, 1% des bénéfices, 10%…), pour les risques catastrophiques, une référence aux capitaux propres est plus significative (20%, 50%, voire 200%, 10 fois les capitaux propres).

Le rapprochement de la probabilité et de la gravité donnera, d'un coup d'œil, la zone de l'acceptable et du non acceptable, en fonction de l'appétit pour le risque des dirigeants de l'entreprise. Si l'événement coûte 1 pour 1 000 des bénéfices et ne se produit qu'une fois par an, il peut être ignoré. Si c'est une fois par semaine, c'est une autre affaire.

À l'inverse, la crue milléniale, même dévastatrice, peut peut-être rester ignorée. La clé de toute gestion des vulnérabilités auxquelles est confronté un organisme passe par une connaissance de celles-ci, de leurs caractéristiques, et en particulier la probabilité de survenance et le poids économique de chacune.

La cartographie des risques est, précisément, cet outil qui permet d'illustrer la comparaison ou la hiérarchisation des risques. On utilise aussi parfois le terme plus approprié de profil de risques.

Cartographie des risques, une démarche permanente

Plus que la carte « instantanée » donnant un profil de risques de l'organisme, c'est la démarche de cartographie qui facilite l'appropriation des risques par les responsables de terrain. L'approche présentée ici est inspirée d'une démarche proposée par une grande société d'audit aux clients qu'elle accompagne dans ce processus. Elle souligne, précisément, la nécessité de l'appropriation des risques par tous les acteurs opérationnels (propriétaires des risques et *chief risk officer*). Elle est scindée en trois étapes :

- ***Collecte des données***. Il convient de rassembler les éléments pertinents à la gestion des risques, en les replaçant dans la perspective des objectifs stratégiques de l'organisme. La banque de données est le cœur du système d'information pour la gestion des risques (SIGR) (voir question 22).
- ***Atelier d'autoévaluation***. C'est une réunion de partage de l'ensemble des responsables d'une unité donnée pour mettre en commun les évaluations de chacun. Saisies de façon anonyme dans une banque de données, elles produisent un graphe présentant une synthèse visuelle d'un système constitué d'un grand nombre de paramètres, qui ne se prêteraient pas à une formalisation mathématique, ni même à une visualisation intellectuelle.
- ***Amélioration continue***. Les vulnérabilités reconnues comme « stratégiques », c'est-à-dire conditionnant directement la réalisation des objectifs stratégiques de l'entreprise, doivent faire l'objet d'un plan d'actions spécifique. Elles devront, parfois, faire l'objet d'un approfondissement de l'analyse de type cindynique, avec une définition claire de la situation dans le temps comme dans l'espace, des réseaux d'acteurs ou des parties prenantes impliquées. Le rapport final est, alors, seulement le point de départ de la démarche de gestion des risques qui doit, ensuite, être intégrée de façon itérative dans la gestion globale de l'entité, avec ou non l'assistance du consultant, le facilitateur initial du processus. Idéalement, l'organisme doit s'approprier le processus et, ensuite, n'avoir recours au consultant que pour la correction périodique, face aux dérives possibles.

22 *Pourquoi faut-il envisager de mettre en place un SIGR ?*

La gestion des risques est devenue un processus de gestion d'information et de communication. À chaque étape, du diagnostic des vulnérabilités à l'audit du programme de traitement des risques, il faut communiquer (pour obtenir les informations indispensables), gérer l'information (la rassembler et la comprendre) et communiquer encore (pour présenter les résultats et en tirer les conséquences pratiques). De ce fait, la mise en place d'un système d'information pour la gestion des risques (SIGR), c'est-à-dire d'un ensemble de matériels et de logiciels pour recueillir et traiter les données pertinentes, pour la prise de décision et le suivi de leur mise en œuvre est un instrument essentiel pour gérer efficacement les risques. Détaillons ci-après ses principales contributions.

Aide à la prise de décision

Les décisions qui doivent jalonner le processus de gestion des risques s'appuient sur des systèmes qui relient, efficacement, les données et les hommes. La liste qui suit donne quelques illustrations des apports d'un SIGR :

- Identification des vulnérabilités : la collecte des données sur les sites de production, les immeubles, les historiques de sinistres, les valeurs et les localisations des éléments d'actifs.
- Recherche des instruments de traitement applicables : rapprocher les sinistres passés avec les valeurs en risque et intégrer les tendances pour analyser et modéliser l'impact de différents instruments envisagés.
- Élaboration du programme de gestion des risques : utiliser des outils d'analyse et d'évaluation pour quantifier la matrice d'instruments, sélectionner et démontrer leur impact global ainsi que la valeur ajoutée.
- Mise en œuvre du programme de gestion des risques : transmettre aux souscripteurs des informations de haute qualité pour ajuster, au mieux, la tarification du programme d'assurances ou générer, en interne, les informations nécessaires au suivi du programme de rétention.
- Audit du programme d'assurance : production en temps réel de rapports exacts pour la direction, rendant compte à la fois des efforts accomplis (référentiels d'activités) et des résultats atteints (référentiels de résultat) pour permettre un suivi efficace et apporter les corrections qui s'imposent.

Réduction de l'incertitude

Un des défis les plus difficiles à relever, pour un professionnel de la gestion des risques, est l'incertitude qui entoure chacune de ses décisions.

Comment qualifier l'incertitude ? On pourrait retenir comme définition : « le doute concernant la capacité de prévoir », l'amélioration de l'information pouvant le réduire. La réduction du niveau d'incertitude et l'amélioration du processus de prise de décisions qui en résulte sont, sans doute, la principale contribution d'un SIGR à un organisme.

Amélioration de la gestion

Par-delà l'amélioration du processus de décision, le SIGR a un impact sur d'autres aspects de la gestion des risques.

En particulier il améliore la productivité, la rapidité et l'efficacité de mise en œuvre du programme de la gestion des risques sur les aspects suivants :

- Collecter l'information sur des sinistres individuels ou des séries de sinistres, sur les vulnérabilités et les couvertures d'assurance pour des contrats multigaranties.
- Tirer de l'ordinateur des informations nécessaires pour éclairer la direction, comme le coût des assurances ou des attestations d'assurance.
- Suivre les transactions, émettre les chèques de règlement, imprimer les correspondances et calculer les niveaux de provisions pour sinistres pour les programmes de sinistres gérés en interne.
- Sauvegarder de l'information pour un usage ultérieur comme les notes sur un sinistre, les données historiques sur les couvertures.
- Tenir un journal des événements importants, comme les dates d'échéance de contrat, drapeau pour analyser l'évolution d'un dossier, la fermeture de sinistre sans mouvement.

Amélioration de la communication

Les fonctions d'analyse et d'émission de rapports peuvent être utilisées pour informer les collaborateurs et les dirigeants de l'organisme sur le programme de gestion des risques, les tendances lourdes et l'apport de chaque service à la gestion des risques, et valider les résultats obtenus.

Coupler le SIGR avec les programmes disponibles, pour l'édition et la mise en forme de rapports, permet de montrer l'impact de la gestion des risques de façon à la fois exacte, claire et efficace.

Par exemple, pratiquement tous les organismes de tailles diverses ont mis en place des services d'intranet et de courrier électronique interne pour informer leur personnel. Nombre d'entre eux utilisent ce moyen pour informer les responsables hiérarchiques opérationnels et les dirigeants sur l'évolution hebdomadaire de la statistique « accidents du travail », le plus souvent en instantané ou sans un jour ouvrable de décalage.

La visibilité de la gestion des risques est nettement améliorée lorsque les responsables opérationnels reçoivent des informations sur les risques en même temps que sur tous les autres éléments de l'organisme. Cela place la gestion des risques à parité avec les autres sources de coûts contrôlables et les responsables la considèrent donc avec le même sérieux.

Le SIGR peut contribuer, efficacement, à l'intégration de la culture de gestion des risques au sein de l'organisme. Par exemple, dans une structure décentralisée, chaque entité pourrait avoir développé, au fil du temps, ses propres habitudes en matière de gestion des risques et de suivi des réclamations. Pour la gestion des risques, la diversité peut signifier : désordre, manque de cohérence d'ensemble et de coordination au niveau du siège. La mise en forme d'une taxonomie des risques est indispensable pour rassembler des données cohérentes.

La mise en place d'un SIGR peut rassembler en une base de données consolidée, en particulier tous les sinistres des unités opérationnelles. Le professionnel de la gestion des risques en charge de l'ensemble de l'opération peut alors rendre compte à un comité de pilotage où toutes les entités sont représentées pour analyser les résultats. Cette information synthétique permet de disposer d'un panorama complet des risques de la société et de prendre des décisions sur la base de cette connaissance garantissant une cohérence qui aurait été, sans doute, impossible sans le SIGR (et les interactions en acteurs que sa mise en place a impliquées).

Les limites du SIGR et l'avènement de l'ère de l'analytics

La nécessité, pour la réflexion stratégique de tout organisme, de prendre en compte la gestion des risques impose que les informations liées à la gestion des risques soient intégrées dans un ensemble plus vaste d'aide à la décision.

Les capacités architecturales de gérer l'information au sein des organismes ont évolué pour permettre de tirer avantage des transactions « *big data* » pour des calculs complexes. La référence à ETL (Extraction, Transformation et Chargement, *loading* en anglais) en termes d'intelligence économique

a été supplantée par la capacité de réaliser des calculs en transaction analytique directe sur les fichiers. Cela réduit les nécessités de stockage, le temps de processus et s'applique à la détection des risques en permettant une notification immédiate sur un éventail de systèmes financiers et opérationnels au sein de l'organisme.

C'est ainsi que le système analytique des risques d'entreprise (*Enterprise Risk Analytics Systems*) est défini comme l'ensemble des applications informatiques qui utilise les fonctionnalités d'intelligence économique pour préserver l'intégrité de la gestion des données lors de la mise en œuvre de calculs complexes à des sources de données transactionnelles et externes.

C'est pourquoi aujourd'hui la mise en place de SIGR de dernière génération ne peut s'imaginer que dans le cadre de l'analytics, pour fournir en temps réel aux décideurs les informations éclairant l'avenir, pour optimiser la prise de décision et suivre sa mise en œuvre.

II
Risques fondamentaux de tout organisme

3
Les risques traditionnels

23 *Les risques de personne sont-ils du ressort de la gestion des risques ?*

Il faut d'abord cerner ce que l'on entend par risques de personnes. Il s'agit, en application des principes posés plus haut, de tout ce qui peut rendre la ressource « personne » indisponible pour l'organisme.

L'organisme dispose d'un portefeuille de compétences humaines et de réseaux relationnels, avant même, ses brevets et son système de production. Si certaines de ces compétences sont disponibles sur le marché du travail, d'autres sont plus rares et difficiles à remplacer, ainsi qu'il est souligné dans la question 26 sur les personnes-clés.

Pour tout organisme, une ressource humaine est l'objet, d'un certain nombre d'incertitudes et de périls, que sont : la démission, la maladie ou l'accident. Ces périls se traduisent par une baisse de performances (maladie), une absence temporaire (incapacité partielle ou totale) ou un départ définitif (démission, invalidité, décès), et doivent être pris en compte.

Indirectement, les risques de santé ont une incidence sur les régimes de prévoyance et de frais médicaux, que la branche, le groupe ou l'entreprise met, généralement, en place après négociations avec les partenaires sociaux. Le caractère aléatoire des résultats et le recours à des mécanismes de mutualisation, pour les gérer et les financer, impliquent l'établissement des prévisions qui ressortent des techniques actuarielles utilisées dans la gestion des risques classique.

L'importance de la gestion des risques liés au « personnel » est illustrée par les trois questions suivantes, au niveau du péril pour les deux premières (retraite et santé) et au niveau de la ressource (compétences exceptionnelles pour le cas des collaborateurs-clés).

Un cas spécifique, est celui des personnels en poste à l'étranger, détachés ou expatriés. L'employeur a une responsabilité spéciale de sécurité qui s'applique tant au salarié qu'à sa famille, quand elle l'accompagne. La problématique peut aller jusqu'à la prise en compte des études des enfants et les loisirs sur place.

On pourra se référer aux ouvrages spécialisés sur ce sujet (se reporter à la Bibliographie et à l'ouvrage de Guy Bellocq).

Sans entrer dans le détail de l'évaluation des risques et des modes de traitement, il faut signaler le risque d'enlèvement pour rançon ou pour des motifs crapuleux ou politiques, qui sont beaucoup plus fréquents que ce que la couverture médiatique pourrait laisser prendre.

Les journalistes retenus à l'étranger font la une des médias pendant des semaines ; en revanche, des dirigeants dans certains pays émergents sont libérés après négociations, sans jamais faire parler d'eux. Lorsque l'on opère dans certains pays, c'est une composante normale du coût des affaires à prendre en compte lors de l'établissement des budgets : « *Mais alors, est-ce encore un risque, si c'est un poste de coût presque certain ?* »

Pour les questions relatives au personnel (voir questions 24 à 26), les fiches indiquent, non seulement les éléments de diagnostic, mais également, les pistes de traitement par réduction. Du fait de leur spécificité et de leur interaction directe avec la gestion des ressources humaines, ces mesures sortent du cadre des approches traditionnelles de réduction des risques traitées dans les questions de la partie III tout en s'inspirant des mêmes principes d'action.

24 *La retraite représente-t-elle un risque pour l'entreprise ?*

On pourrait soutenir que le départ à la retraite des collaborateurs d'un organisme n'est pas un risque mais un événement inéluctable. En réalité, il faut analyser la situation. Le départ est certain, mais la date du départ reste un élément aléatoire, donc relevant du champ du risque. Par ailleurs, les incertitudes qui pèsent sur les régimes de retraite, dans tous les pays développés, en font un élément important de l'évolution des négociations collectives. Enfin, dans certains pays, les fonds de pension par capitalisation, publics ou privés, avec leur cortège d'hypothèses actuarielles, font bien peser un risque de passif social sur les organismes. En résumé, les départs en retraite ou en préretraites constituent un vrai risque, qu'il est possible d'analyser et de traiter.

Les risques

Ils se présentent sous un double aspect :

- ***Risque économique de perte de compétences*** : le départ d'un employé « clé » de l'entreprise (voir Infra) dont le remplacement ne serait pas organisé et, *a fortiori*, le départ simultané en retraite de personnes exerçant une même fonction peuvent présenter des risques de perte d'expertise et de bon fonctionnement de l'organisme.
- ***Risques financiers*** : l'organisme est exposé à des risques financiers lorsqu'il prend, directement à sa charge, le paiement des indemnités de fin de carrière, des préretraites ou des pensions de retraite à prestations définies. Ces risques conduiraient à un déséquilibre de trésorerie en cas de départs simultanés en nombre, mais également à une diminution de la valeur de l'entreprise qui ne provisionnerait pas ses engagements échus.

Identification et mesure des risques

Le risque financier direct est le plus facile à mesurer. Il convient de faire calculer par un expert (actuaire, assureur), la « loi de sortie » des engagements de l'entreprise, c'est-à-dire les montants qu'elle devra régler et les dates de paiement.

En revanche, l'impact indirect sur la perte d'efficacité et de capacité de production de l'organisme ne peut être évalué que sur la base d'un recensement des compétences qui lui sont indispensables pour son

fonctionnement quotidien et la pérennité de son développement. Ensuite, en les rapprochant des compétences des différents salariés, et en prenant en compte la pyramide des âges, il doit être possible d'identifier les domaines de compétences « à risque » : ceux dont les rangs s'amenuisent et les effectifs atteignent les âges de départ (60-65 ans). La différence fondamentale avec la question des personnes-clés est qu'il s'agit ici d'une analyse globale et pas forcément d'une problématique de personnalité exceptionnelle. Lorsque le diagnostic est posé, l'évaluation, du point de vue financier, est moins essentielle que l'identification du risque pour permettre la mise en place de mesures préventives.

Les mesures à prendre

En ce qui concerne la perte de compétences et les pertes d'opportunité induites, voire de mise en danger de l'entreprise, aucune mesure de traitement financier du risque ne peut compenser l'absence de personnel. Dans ces conditions, l'essentiel est de réduire le risque, en portant une attention à la pyramide des âges et à la transmission des compétences, avec une méthode d'échevinage ou de parrainage. Un exemple d'instrument est le départ en sifflet, avec réduction de temps de travail, qui permet au « senior » de s'adapter et de se préparer à la retraite tout en transférant son savoir-faire à un plus jeune.

L'organisme qui aura su mettre en place des solutions de continuité pourra envisager, éventuellement, de les compléter par un contrat d'indemnisation des pertes financières liées au(x) départ(s) prévu(s), permettant de lisser les coûts dans le temps.

Sur le plan de l'indemnisation des salariés, la solution consiste à provisionner, année après année, les engagements échus de l'organisme, soit directement dans les comptes de l'entreprise en déduction fiscale, puisque la loi française l'autorise désormais, soit par l'intermédiaire d'un contrat d'assurance.

25 *Prévoyance et frais médicaux : faut-il s'en inquiéter ?*

On entend par prévoyance, les maladies et les accidents dont le salarié peut être victime. Ils se traduisent en termes de risque : décès (1), arrêts de travail (2) et frais médicaux (3).

1 Le décès

1.1 Les risques

Les conséquences peuvent être de deux ordres :

- ***Financières :*** le nombre de décès peut, d'une part dépasser statistiquement la moyenne enregistrée dans la catégorie professionnelle et la profession, et d'autre part, atteindre des coûts unitaires très élevés, pour les cadres dirigeants ou les victimes d'accidents professionnels, dans lesquels la faute inexcusable de l'entreprise serait reconnue.
- ***Perte de compétences :*** ce peut-être la disparition d'un salarié dont l'activité se révèle essentielle pour l'entreprise, ou d'une équipe entière (accident collectif d'un comité de direction ou d'une équipe commerciale voyageant ensemble, par exemple).

1.2 Identification et mesure des risques

Nous pouvons distinguer, selon le cas, l'analyse *a priori* des risques et l'analyse *a posteriori* des sinistres :

- Le nombre de décès n'est significatif que sur des populations importantes. L'échantillon doit regrouper plusieurs milliers de personnes, que l'on atteindra en cumulant, si nécessaire, les effectifs des salariés sur plusieurs années. Les bases de références peuvent être fournies par l'assureur du régime de prévoyance, qui dispose de séries importantes, de résultats ou par des études de l'INSEE.
- L'analyse des circonstances des décès pour chacun des risques maladie, accidents et accidents de travail, peut fournir des indications : ainsi, un restaurant d'entreprise séparé de l'établissement principal par une route à grande circulation était la cause d'un nombre élevé de décès par accident ; une passerelle a permis de résoudre le problème.

- Le lancement d'une nouvelle activité ou d'un nouveau processus de fabrication doit s'accompagner d'une recherche d'identification des risques et des dangers. Le syndicat professionnel, les ingénieurs conseils de la Caisse régionale d'assurance-maladie (CRAM), ou un concurrent ami, peuvent également fournir des informations intéressantes (*benchmarking*).
- Les déplacements collectifs (séminaire des dirigeants ou de l'équipe commerciale) peuvent présenter un risque « catastrophique » pour l'entreprise, lorsque ces personnes voyagent ensemble.

1.3 Quelques exemples d'actions possibles

- Le coût élevé d'un décès de cadre supérieur et leur rôle essentiel dans le fonctionnement de l'organisme justifient qu'elle prenne régulièrement en charge (tous les deux ans ?) un bilan de santé destiné à diagnostiquer, au plus tôt toute maladie, afin de déclencher les soins ou les comportements préventifs nécessaires.
- Lorsque la contribution d'un salarié se révèle essentielle au bon fonctionnement de l'organisme (un responsable commercial apportant une part importante des ventes, par exemple), la souscription d'un capital décès proportionnel aux conséquences estimées, suite à sa disparition, sera nécessaire pour assurer provisoirement les charges et la marge correspondantes.
- Les conséquences du risque « catastrophique » évoqué ci-dessus seront minimisées par l'interdiction de déplacements collectifs simultanés par le même moyen de transport (les membres du comité de direction voyageant ensemble dans le même avion, par exemple).

Pour éviter le risque « catastrophique » sur les lieux du travail (l'incendie qui pourrait atteindre plusieurs vies, par exemple), des exercices d'évacuation, jusque-là insuffisamment considérés par les entreprises et les salariés, devront être effectués périodiquement.

2 L'arrêt de travail

2.1 Les risques

Les conséquences sont également financières et économiques :

- ***Financières :*** l'entreprise finance directement l'indemnisation complémentaire due au titre de la mensualisation et celles des arrêts plus longs, au titre de l'incapacité ou de l'invalidité par le biais du régime de prévoyance.

► ***Économiques*** : l'absence du salarié occasionne des pertes de performance de la chaîne de production de l'entreprise ; celle-ci doit, parfois, embaucher du personnel temporaire pour assurer la continuité du travail.

2.2 Identification et mesure des risques

La première difficulté consiste à apprécier le caractère excessif de l'absentéisme dans l'entreprise. Les bases de données de la profession, celle de la Caisse régionale d'assurance-maladie (CRAM) devenue CARSAT, ou lorsqu'elles existent, de l'assureur prévoyance, peuvent servir d'appui.

L'historique, sur plusieurs années, des taux d'absentéisme de l'organisme fournit une base d'étude, en distinguant les taux par cause : maladie, maternité, accident de travail, grèves…

L'identification des causes peut être aisée (accidents), mais peut demander un important travail d'analyse. Ainsi en est-il du stress, souvent identifié comme la première cause d'arrêt de travail (un tiers des arrêts sur l'ensemble de la France).

Des entretiens avec le médecin du travail, les chefs de service ou de départements les plus affectés pourront fournir des indications. Il faudra différencier le bon stress, facteur d'adaptation au changement et à la performance qui n'occasionne pas d'arrêts de travail et le mauvais stress, qui se manifeste par des réactions psychologiques et comportementales (troubles du sommeil, de la mémoire, maux de tête…).

Les causes sont généralement liées à la perception « d'agressions » économiques (menace de perte d'emploi, fusions…), organisationnelles (restructurations, changement de l'environnement, de méthode de management…), physiques (postes à risque, salariés au contact d'un public agressif…).

La consultation du « document unique » légal d'évaluation des risques pour la santé et la sécurité des travailleurs peut révéler des informations très utiles.

2.3 Quelques exemples d'actions possibles

Les actions découlent souvent du diagnostic.

Parmi les mesures possibles, nous citerons :

► des campagnes de vaccination organisées dans l'entreprise pour répondre au risque d'épidémies de grippe ;

- l'accompagnement des personnes en arrêt de travail, en vue de leur retour à l'emploi (quelques entreprises sont spécialisées dans ce type de service) ;
- des formations régulières qui peuvent réduire les risques de stress dans certaines fonctions ;
- des cercles de qualité à thème ;
- la mise à disposition des personnes exposées, de services téléphoniques de soutien psychologique fonctionnant 24 heures sur 24 ;
- certaines entreprises proposent des programmes déstressants sur la base de cours de gymnastique, de séances de relaxation, de séances de massages…

3 Le bon état de santé des salariés et les dépenses de frais médicaux

3.1 Les risques

Le risque pour l'entreprise est double : économique d'abord, par la baisse de performance des salariés en mauvaise santé et financier ensuite, par l'accroissement des dépenses de santé du régime complémentaire, qui depuis une vingtaine d'années varie entre deux et trois fois l'inflation.

3.2 Identification et mesure des risques

Une grande majorité d'assureurs proposent des analyses fines de la consommation médicale de chaque groupe assuré, pour chaque catégorie d'actes, avec souvent une décomposition en fréquence (nombre d'actes) et en amplitude (montants moyens).

L'identification des causes de dérapage des dépenses de santé est parfois difficile, mais les difficultés économiques d'une entreprise et les barèmes de remboursement de type « frais réels » sont toujours à l'origine de fortes consommations.

3.3 Quelques exemples d'actions possibles

Les actions possibles, outre les vaccinations et les bilans de santé évoqués précédemment, consistent essentiellement en mesures de sensibilisation :

- Des campagnes d'information sur les bons comportements de santé (tabac, alcool, alimentation…) peuvent être organisées, à travers des expositions ou des remises de documents dans l'entreprise. Des sociétés de service sont spécialisées dans ce domaine.

- En cas de dérapages de consommation sur certains postes, une information générale, sensibilisant le personnel sur les données observées, permet toujours un ralentissement de la dépense médicale. Cette mesure a un effet limité dans le temps, aussi convient-il de la renouveler régulièrement.

Certains organismes développent des programmes actifs et ciblés. Pour prendre l'exemple du tabac, les responsables concernés (DRH, médecin du travail, infirmière, responsable sécurité) forment des groupes de travail de personnes intéressées par le sevrage tabagique. Après une sensibilisation et un diagnostic (spiromètre…), ils posent des patchs antitabac, fournis par l'entreprise, et effectuent un soutien psychologique régulier.

Selon l'activité de l'entreprise, des programmes cibles sont développés par thèmes (vision, surdité, troubles musculo-squelettiques, obésité…).

26 *Qu'est-ce qu'une personne-clé ?*

Nous avons souligné, plus haut, que l'ensemble du personnel, avec ses compétences et son réseau relationnel, est une ressource essentielle de tout organisme. Toutefois, certains membres du personnel sont plus facilement remplaçables que d'autres. Les personnes les plus difficiles à remplacer ont en principe certaines caractéristiques dont :

- ► des talents, une créativité ou un savoir-faire exceptionnel ;
- ► la responsabilité de décisions stratégiques dans l'entreprise ;
- ► l'encadrement et l'animation du personnel.

Les conséquences financières de leur disparition, temporaire ou définitive, partielle ou totale, peuvent être très lourdes sur l'organisme. Elle peut même mettre en péril la survie de celui-ci et c'est pourquoi on a pris l'habitude de les appeler des « personnes-clés ». Les dirigeants doivent porter une attention particulière à la gestion de ces ressources humaines.

Pour dresser le diagnostic, on peut s'intéresser au bilan et à l'organigramme, ainsi qu'aux actionnaires majoritaires, aux dirigeants et aux cadres supérieurs.

Mais il faut aussi utiliser l'analyse par les flux pour envisager les conséquences dans le temps. On se concentre alors sur la détermination des « goulots d'étranglement humain » : ces personnes dont la disparition mettrait effectivement en péril les objectifs de l'organisme. Cette approche permet de dégager les personnes-clés qui ne seraient pas dans l'organigramme général, c'est-à-dire autres que les dirigeants ou les cadres supérieurs. En particulier dans les entreprises de nature artisanale, les « savoir-faire » peuvent se perdre avec le départ de compagnons anciens, qui ne figureraient pas, naturellement, dans un organigramme.

Dans les commerces ou les professions libérales, pour les sociétés en nom propre, en nom collectif ou les SARL, les propriétaires jouent un rôle essentiel dans la vie de l'organisme. Cela est encore vrai dans de nombreuses sociétés anonymes de taille moyenne. En revanche, dans les sociétés anonymes cotées en bourse, dont l'actionnariat est très dispersé, et dont aucun des dirigeants ne détient une part significative, ce lien traditionnel entre la propriété et la direction de l'entreprise a été coupé. Dans ces groupes, il est clair que les actionnaires ne représentent aucune vulnérabilité pour l'entreprise, au niveau des risques personnels.

Bien entendu, les commerciaux qui produisent une part significative du chiffre d'affaires doivent faire l'objet d'une attention particulière : *« Les clients sont-ils attachés à notre marque, nos produits ou notre représentant qui pourrait les "emmener" avec lui en cas de démission ? »*
Dans tous les cas, il convient de se poser deux questions :

- Que serait amené à faire l'organisme si cette personne venait à ne plus être disponible subitement ?
- Quel serait l'impact sur la réalisation des objectifs de l'organisme ?

La première question vise à déterminer les conditions et les délais nécessaires pour le remplacement de la personne en question. La première réponse qui vient à l'esprit est : donner une promotion à son (ou l'un de ses) adjoint(s), mais on pourrait également recruter en externe (ou en interne), supprimer le poste tout simplement ou encore répartir les tâches entre plusieurs autres personnes.

La seconde question doit permettre d'analyser la perte (éventuelle) d'efficacité de l'organisme en cas de disparition de la personne. Soyons précis, il s'agit, pour tout organisme, de repérer ces collaborateurs dont la perte entraînerait une baisse de la qualité ou de la quantité des biens ou des services produits, dans l'immédiat ou dans le futur.

Dans certaines situations, chaque individu pris séparément n'est pas « critique », mais la perte de tout un groupe deviendrait grave. Pour identifier les vulnérabilités face à un « groupe de collaborateurs », il convient d'envisager les périls risquant de les produire. Il peut s'agir d'un péril collectif, un événement unique comme un accident d'avion. Ce peut être aussi un problème ou un intérêt commun (repensons au cas où plusieurs salariés démissionneraient simultanément pour créer leur propre entreprise). Il peut s'agir, enfin, d'une combinaison de facteurs comme dans le cas d'un licenciement obligeant un certain nombre de salariés à chercher du travail ailleurs.

Enfin, les personnes-clés ne sont pas forcément liées à l'entreprise par un contrat de travail ou un mandat de dirigeant. On peut souligner deux situations :

- dans une société fermée, la disparition d'un actionnaire, investisseur dormant, peut créer les conditions d'une reprise par un tiers (pactes d'actionnaires) ;
- dans le réseau de partenaires, sous-traitants ou clients, certains peuvent dépendre de personnes-clés dont la disparition aurait un impact en ricochet sur l'organisme.

27 *Quels sont les principaux risques de dommages aux biens ?*

Pour répondre de façon complète à cette question, il faudrait passer en revue l'ensemble des biens matériels de l'entité : terrains, immeubles, mobiliers, équipements et stocks et les valoriser ainsi que nous l'avons exposé à la question 16. À ce stade, donc, la question posée est plutôt celle de l'événement qui peut atteindre ses ressources et les rendre indisponibles pour l'entité qui devra s'en passer ou les reconstituer.

Dans ces conditions, ce sont les principaux périls qui nous préoccupent, ceux qui peuvent conduire à une destruction lourde, voire totale. En clair, il s'agit d'être plus spécifique à l'intérieur des grandes classes de périls exposées à la question 8 et de donner une liste des plus graves périls qui menacent les biens matériels d'une entité.

Périls « naturels »

En principe, les périls naturels étant répertoriés et les « zones à risques » identifiées, les organismes doivent s'inquiéter de l'état de la région, au moment où se développe un projet de construction ou de rachat, sur les plans suivants :

- Éruption volcanique.
- Marée.
- Raz-de-marée (tsunami).
- Tremblement de terre.
- Vent (tornade, ouragan, typhon, tempête…).

En effet, ces événements ne sont pas contrôlables et peuvent dévaster une région entière, comme la rafale de quatre ouragans dans les Caraïbes pendant l'été et les événements du Sud-Est asiatique en décembre 2004.

Périls « industriels »

Ces périls, qui n'existent que du fait de l'activité humaine, résultent essentiellement de choix de construction, de procédés et sont liés à l'évolution industrielle de l'économie.

Pour l'essentiel, ce sont des périls assurables qui peuvent être contrôlés en appliquant des méthodes développées par les assureurs. Le cas le plus direct est celui de l'incendie, où un bâtiment équipé pour être classé en Risques Hautement Protégé est rarement l'objet d'un incendie accidentel majeur.

Voici une liste non exhaustive des principaux risques à analyser :

- Corrosion, rouille.
- Bris de machine.
- Effondrement.
- Explosion.
- Fuite de produits chimiques.
- Incendie.
- Pollution.
- Surtension et incidents électriques.

Périls « humains »

Les périls humains « involontaires » comme une omission, une erreur ou une négligence peuvent avoir un impact sur les biens de tout organisme.

Toutefois, ce sont les périls « volontaires » qui sont les plus difficiles à contrôler, car il y a derrière eux une intelligence qui vise, en permanence, à contourner les éléments mis en place pour la frustrer de son objectif.

Une seule relève des périls humains « non volontaires », ce sont les erreurs. La liste est toujours provisoire en attendant de classer le prochain scénario :

- Détournement de fonds.
- Erreur, omission, négligence.
- Fuite de produits chimiques.
- Grèves, émeutes et mouvements populaires.
- Incendie criminel.
- Sabotage.
- Terrorisme.
- Vandalisme.
- Vol, fraude, falsification.

Périls « économiques »

S'ils échappent à l'action des acteurs individuels, toutefois les prévisionnistes, économistes et autres futurologues essaient d'éclairer les décisions des dirigeants en améliorant leurs informations sur les phénomènes suivants :

- Chute des cours de bourse.
- Confiscation.
- Conséquence de grèves.

- Dépression.
- Évolution des goûts des consommateurs.
- Expropriation.
- Guerre.
- Inflation.
- Percée technologique.

Toutefois, quand on analyse les dommages aux biens, il faut garder à l'esprit que, dans la grande majorité des cas, la disparition du bien lui-même n'est qu'une partie de la perte réellement subie. L'essentiel est la perte de revenus induite, soit par l'impossibilité de produire ou de livrer, ou pire encore, à cause de la contrepublicité que l'événement entraîne avec la perte de confiance des partenaires économiques, ce que nous avons appelé ici la réputation (voir questions 36 et 37). C'est ce que certains professionnels appellent aujourd'hui analyse d'impact sur l'organisme ou BIA (*Business Impact Analysis*).

C'est pour cela que la question de pertes de revenus net (le produit d'assurance est appelé pertes d'exploitation), ne peut pas être traitée séparément (voir question 31). En effet, ces pertes de revenus sont, en général, engendrées par la perte d'une autre ressource, et doivent être analysées dans ce cadre. Pour les dommages aux biens, l'essentiel est de comprendre la chaîne de production interne et de la replacer en liaisons avec les chaînes amont et aval (voir question 86). En interne, c'est-à-dire dans le périmètre directement contrôlé par l'organisme, il faut identifier les « process », machines ou sites sans lesquels la poursuite de la production serait impossible. Ces « goulets d'étranglement » qui commandent un pourcentage important des capacités de production, voire cent pour cent doivent être analysés, non pas en tant que risque à hauteur de leur valeur propre, mais à hauteur de leur incidence sur la production et donc sur les revenus de l'organisme. Cela place les choix de réduction des risques de dommages aux biens dans un tout autre enjeu économique.

28 *Comment analyser les engagements de responsabilité ?*

L'identification des risques de responsabilité passe par le recensement, systématique, de tous les événements qui pourraient avoir un impact sur des tiers. Finalement, cette identification s'appuie sur la même grille « péril ressources » évoquée plus haut, chacun des couples, ainsi identifié, peut avoir des conséquences sur l'organisme lui-même. Ce sont les dommages primaires qui le privent d'une ressource, et des dommages sur son environnement et les tiers : elles sont potentiellement sources d'engagements de responsabilité, dès lors qu'un tiers lésé en demande réparation. Ces engagements de responsabilité sont généralement assurables dans leur volet « responsabilité civile » (RC). Toutefois, en France, on les a traditionnellement divisées en plusieurs catégories. La liste qui suit n'est pas limitative :

- ***RC exploitation*** (y compris la sécurité du travail) : les dommages provoqués directement par l'activité de l'organisme, au moment et dans les lieux où elle produit.
- ***RC produits/prestations*** (après livraison/prestation) : les dommages causés aux tiers, du fait de l'utilisation des produits fabriqués et/ou des prestations effectuées (voir question 29).
- ***RC pollution*** (environnement) : les dommages provoqués sur l'environnement par une pollution accidentelle ou graduelle et pour lesquels la société, au travers d'une législation spécifique, a prévu des sanctions et des remèdes pour la remise en état.
- ***RC maître d'ouvrage*** : la responsabilité spécifique, en France, de celui pour lequel on construit un immeuble ; le propriétaire final.
- ***RC propriétaire d'immeuble :*** le volet spécifique de la RC exploitation où sont directement impliqués des immeubles, propriétés de l'organisme, et qui peuvent toucher des tiers ou des locataires.
- ***RC mandataire social :*** les dommages causés aux parties prenantes, et particulièrement aux actionnaires, notamment par la conformité fiduciaire et légale des décisions prises par les mandataires sociaux (qui exclut, bien entendu, la couverture de la RC pénale).
- ***RC locative :*** la responsabilité du locataire d'immeuble essentiellement vis-à-vis du propriétaire et des colocataires.
- ***RC automobile :*** les dommages de toute nature causés à autrui par l'usage de véhicules terrestres à moteur.

Analyser ces risques suppose d'évaluer les conséquences pécuniaires pour l'organisme si sa responsabilité est recherchée. Il faut rappeler les principaux postes de coûts :

- Les frais de justice et/ou de suivi des affaires.
- Les honoraires des avocats.
- Le temps et les efforts internes.
- Les dédommagements des « victimes ».

Le poste le plus lourd et le plus difficile à évaluer est, bien entendu, le dernier. En droit français, les dédommagements, « dommages et intérêts » comprennent :

- ***Les préjudices corporels :*** il s'agit des atteintes physiques subies par des tiers et débouchant sur des frais médicaux, des incapacités ou des invalidités, voire des décès subis par les victimes (et donc leurs « ayants droit »).
- ***Les préjudices matériels :*** il s'agit de toute atteinte ou perte de biens immobiliers, mobiliers et d'animaux.
- ***Les préjudices immatériels :*** ce sont les pertes de revenus, de chance, un préjudice esthétique, un préjudice moral, l'atteinte à la réputation pour les particuliers, et pour les organismes, les pertes de revenus ou les atteintes à la réputation. Dans le monde anglo-saxon le terme générique est celui de « pertes financières ».

En pratique, il faut imaginer des « scénarios catastrophes » pour évaluer ces postes, et tenir compte des évolutions de la législation et de la jurisprudence pour évaluer des montants, sans oublier les différences entre les États, les régions.

Cette démarche est indispensable pour fixer les plafonds d'assurance souhaitables dans les différents domaines et justifier les efforts de réduction des risques, en amont par les efforts de qualité entre autres, en aval par le recrutement de spécialistes internes et externes, afin de gérer les situations avant qu'elles ne dégénèrent dans toute la mesure du possible (traitement rapide des réclamations, services après-vente…).

29 *Quelle est la différence entre responsabilité civile contractuelle et responsabilité civile délictuelle ?*

Tout d'abord, rappelons que la responsabilité civile s'oppose à la responsabilité pénale pour laquelle la « société » est victime, et les tribunaux répressifs sont en charge de la réparation. En matière de responsabilité civile, la personne lésée est une personne privée (physique ou morale). Dans ces conditions, il lui revient d'introduire une action civile pour obtenir réparation.

Il peut arriver qu'une ou plusieurs personnes privées soient lésées dans une situation où l'ordre public est mis en cause par une même faute, alors, les responsabilités, civile et pénale, sont engagées simultanément. Traditionnellement, donc, le droit est basé sur la réparation de la faute.

Si la faute est le non-respect d'une obligation contractuelle (contrat de vente, contrat de service, contrat de travail…), il s'agit de ***responsabilité contractuelle***. Elle ne peut donc être engagée qu'à l'égard d'une partie à un contrat (non-respect des délais de livraison promis à un client, non-paiement dans les délais prévus d'un fournisseur…).

Dans tous les autres cas, on parle de responsabilité délictuelle ou quasi délictuelle. La ***responsabilité civile délictuelle*** s'applique donc à un très grand nombre de cas de responsabilités civiles, où les parties en conflits ne sont pas liées par un contrat, ou dont le conflit ne résulte pas de l'application des clauses du contrat.

Des « obligations », ayant pour but et fonction de protéger les droits et libertés de chacun, n'ont pas été respectées, le non-respect d'un tel devoir, qui provoque un dommage à une autre partie, est un « délit » (que l'on appelle « *tort* » en américain).

En résumé, traditionnellement en matière civile, les deux grands ordres de responsabilité sont la responsabilité contractuelle et la responsabilité délictuelle. Toutefois, une des grandes évolutions du droit contemporain est, sans doute, le développement d'une responsabilité professionnelle, par l'émergence de deux acteurs essentiels de la vie économique : le ***professionnel*** et le ***consommateur***, perçus par l'opinion publique comme parfaitement antagonistes :

- ***Le « méchant »*** qui abuse de sa puissance économique, ***alors qu'il sait***, pour mieux tromper son cocontractant et les tierces victimes.

Il est entendu qu'il doit supporter toutes les conséquences de son activité puisqu'il en retire le bénéfice réalisé ou espéré (le « risque profit »).

- ***La « malheureuse victime »,*** à qui est due, nécessairement, réparation du préjudice qu'elle a subi.

Cette distinction manichéenne reflète l'esprit du droit contemporain, qui aspire à plus de réalisme et à moins d'abstraction ou d'idéalisme éclairé, peut-être sous l'influence de plus en plus pénétrante du droit de la consommation qui devient toujours plus contraignant. Elle aboutit donc à une transformation radicale qui débouche sur un droit à réparation dans toutes les circonstances. C'est ainsi qu'est née la théorie de la « poche profonde », la recherche à tout prix d'un organisme solvable pour indemniser.

Le souci d'aboutir à une juste indemnisation des victimes a poussé les tribunaux, de façon parfaitement prétorienne, à faire preuve d'une sévérité renforcée à l'égard des professionnels et à ajouter au « contrat de confiance » (qui existait, normalement, entre le professionnel et son client) des obligations implicites, qui n'avaient été ni prévues ni acceptées initialement par les parties au contrat.

Ce faisant, la jurisprudence a fait éclater des distinctions traditionnelles entre :

- Responsabilité contractuelle et responsabilité délictuelle, ou quasi délictuelle, pour la raison bien simple que les victimes peuvent être les consommateurs ou les clients, parties au contrat souscrit avec le professionnel ou dans un rapport d'affaires plus large, mais aussi des tiers qui sont parfaitement étrangers au dit contrat.
- Obligations de moyens et obligations de résultat, en introduisant des gradations subtiles entre ces deux catégories ; la jurisprudence refuse de se laisser enfermer par un critère de distinction unique.

La jurisprudence a donc aggravé lourdement la nature des responsabilités civiles pesant sur tous les professionnels.

30 *D'où viennent les pertes de revenus ?*

Les pertes de revenus résultent d'événements provoquant des dysfonctionnements, dans l'activité normale de l'organisme, pendant un certain temps. Pour en dresser le diagnostic, il convient donc de focaliser son attention sur les dysfonctionnements eux-mêmes, plutôt que sur les périls les occasionnant.

Le diagnostic de ces pertes est essentiel dans toutes les situations et quelle que soit la ressource qui fasse défaut, certains la nomment aussi BIA, et en font une discipline séparée ce qui ne paraît pas indispensable : un diagnostic complet doit bien entendu inclure toutes les conséquences financières induites pour prendre en compte leur impact sur le résultat de tous les exercices futurs jusqu'au retour au taux de croissance « normal ».

Quelle que soit l'origine des pertes (revenus, dommages aux biens, collaborateurs-clés, information, ressources partenaires, engagement de responsabilités vis-à-vis de tiers, voire indisponibilité des ressources gratuites…), elles sont toujours associées à une forme d'empêchement, partiel ou total, provisoire ou permanent de l'organisme de produire et/ou de délivrer les biens ou les services qu'il propose à ses clients. Dans certains cas, il peut le faire mais en exposant un coût supérieur à la normale, réduisant ainsi sa marge bénéficiaire.

Pour mieux comprendre le mécanisme des pertes de revenus, on peut passer en revue quelques exemples, en les rattachant aux grandes ressources ou aux engagements de responsabilité.

Dommages aux biens

Un bien d'équipement ou un bâtiment d'un site industriel « à la disposition » d'un organisme est utilisé pour la production de biens ou de services. Parfois, la contribution de chaque équipement est claire, comme c'est le cas d'une machine ou d'un équipement intégré à la chaîne de fabrication dans un atelier.

En revanche, dans d'autres cas, il est beaucoup plus difficile de l'identifier (par exemple, un avocat aménage ses bureaux avec du mobilier ancien, en partie pour créer une ambiance rassurante de sérieux et de succès, voire de luxe : cette impression provoquée chez le client contribue, sûrement, à son succès commercial, mais dans quelle proportion ?).

Partenaires

Certains partenaires amont (fournisseurs) ou aval (clients) sont indispensables au fonctionnement de l'entreprise : ils sont des « partenaires-clés ».

Pour les fournisseurs-clés, un fabricant utilise des matières premières et des produits intermédiaires qui sont incorporés dans les produits finis. L'arrêt d'approvisionnement de ces matières provoquerait la cessation de la production, avec une perte de revenus consécutive. La loi du marché impose, de toujours rechercher le fournisseur donnant le meilleur rapport qualité/prix. Ce qui veut dire qu'en cas d'arrêt de livraison, au mieux, on pourra faire appel à un autre fournisseur qui, par définition, proposera un prix supérieur.

Parallèlement, il est clair qu'un organisme qui perd son marché n'a plus de raison d'exister. Produire, sans marché, n'a jamais généré de recettes (ou très provisoirement). Si l'on fait abstraction de la vie normale des affaires, la perte d'une part de marché importante ne peut résulter que d'un dysfonctionnement majeur chez un client important contraint à cesser ses activités, provisoirement ou définitivement.

Ressources gratuites

Il est fréquent que des organismes s'appuient sur la force d'attraction de passage ou de clientèle de voisins pour créer leur propre courant de clientèle. Un cas particulièrement fréquent est celui des boutiques de la galerie marchande d'un centre commercial. Elles profitent de la clientèle drainée par l'hypermarché.

Le volume d'affaires peut être directement induit par la proximité de cet « aimant ».

Il va de soi que, plus les clients sont attirés par cet aimant, plus les pertes induites seront lourdes pour les « satellites », en cas de suspension de l'activité de l'aimant. Quand bien même les boutiques ne subiraient aucun dommage matériel direct, leurs recettes diminueraient, alors que les charges fixes seraient inchangées. Ceci aurait pour conséquence une perte de résultat. Il y a donc bien une « vulnérabilité aimant/perte de résultat ».

Responsabilités civiles

Un engagement de responsabilité débouche sur des frais de justice, d'avocats, d'experts et autres, exposés pour organiser la défense.

Dans certains cas, il faudra aller jusqu'à faire une campagne de retrait de produits. Tous ces frais sont autant de flux financiers détournés d'investissements rentables qui réduisent le résultat courant.

Par ailleurs, la modification d'un cadre législatif ou réglementaire peut imposer à un organisme de modifier ses modes de production ou de contrôle, augmentant ainsi ses coûts de fonctionnement ou de production, voire même d'arrêter certaines activités. Les conséquences de l'augmentation des coûts ou de la perte de recettes sont les mêmes, à savoir une réduction du résultat net de l'entreprise.

En outre, si l'organisme décidait d'ignorer la législation, il engagerait sa responsabilité civile, et pénale (depuis le 1er mars 1994, en France), ainsi que celle de ses dirigeants, ce qui pourrait entraîner des pertes encore plus lourdes à terme : amendes, fermeture provisoire ou définitive, sous injonctions des autorités administratives ou judiciaires (il suffit de penser aux problèmes liés à l'environnement et à la pollution)…

31 *Comment analyser les pertes de revenus ?*

La question précédente a permis de recenser les modes d'identification des pertes de revenus qui trouvent leur source dans tous les autres incidents touchant les ressources de l'organisme, y compris les ressources gratuites, et le mettant dans l'impossibilité de poursuivre son activité normale. Il reste à quantifier l'impact de telles conséquences pour envisager d'agir. L'action sera dictée par l'ampleur de l'impact. La première dimension est la probabilité de survenance, la fréquence ; la seconde, l'importance des conséquences financières et la gravité.

Dans le cas d'un actif physique, le souci majeur de l'organisme est la reprise de la production dans des conditions (de volume, de qualité et de coût) équivalentes, et non pas la remise en état de l'actif lui-même. Les deux sont parfois liés, mais ce n'est pas toujours le cas. Des sinistres mineurs, au niveau des dommages directs aux biens, peuvent avoir des conséquences très lourdes sur les revenus s'il s'agit d'un équipement-clé (goulot d'étranglement). À l'inverse, la disparition d'actifs physiques lourds peut n'avoir aucun impact sur les résultats.

Il faut évaluer, avec précision, les conséquences financières des pertes de revenus pour visualiser le coût complexe d'un événement donné. Le poids économique de la perte de revenus résulte de la combinaison de six paramètres, à estimer séparément :

1. ***La durée de l'interruption :*** cette durée est liée au plan de remise en état des capacités de production, ou de capacités alternatives. Il faut donc bâtir des scénarios et envisager le planning (PERT) de remise en état. Une attention particulière doit être donnée aux activités subissant des variations d'activités cycliques ou saisonnières.
2. ***Le degré de l'interruption*** (pourcentage de la production atteint de 0 à 100%) : c'est le pourcentage de l'activité qui est neutralisée. Il est clair que deux situations sont possibles : ou bien l'arrêt est total, ou bien il est partiel. Il va de soi que, si l'arrêt n'est que partiel, la perte sera moins lourde. Dans ces cas d'arrêts partiels, il arrive fréquemment que l'organisme soit en mesure de trouver des sources extérieures pour réduire les conséquences de son sinistre, sauvegardant ainsi sa capacité à générer des bénéfices. Un accident partiel lui permet de continuer à engranger des recettes, mais à un niveau plus bas.

3. ***Les pertes de chiffre d'affaires :*** dans certains cas, l'organisme pourra faire face à un arrêt de courte durée ou de durée moyenne, en utilisant des stocks ou en recourant à des achats externes pour poursuivre ses livraisons. Dans ce cas, ses clients ne subiront pas de conséquences, et l'impact à moyen terme sera limité. Bien entendu, c'est un des aspects à prendre en compte lors de la mise en place de logistique de flux tendus.
4. ***Les charges liées à cet arrêt*** (y compris les charges fixes incompressibles et les charges exceptionnelles) : même en cas d'arrêt, l'organisme supporte des charges récurrentes (assurances, rémunérations des cadres et des dirigeants, loyers…). Par ailleurs, pour reprendre l'activité, rapidement, l'organisme peut exposer des frais spécifiques (transports rapides, approvisionnement express…).
5. ***Le niveau des résultats courants en activité normale :*** l'activité moyenne de l'organisme et son bénéfice dégagé sont la base de l'évaluation de ce qui peut être perdu en cas d'arrêt. Là encore, il faut prendre en compte la volatilité saisonnière et cyclique de l'organisme, mais la perte devra être analysée de façon dynamique. Le résultat comptable reflète le passé, et ce qui nous importe c'est le compte prévisionnel.
6. ***Le temps nécessaire pour reprendre l'activité au niveau normal précédant le sinistre :*** il s'agit du temps, à nouveau, mais dans la perspective d'une reprise d'activité normale, le premier paramètre se fixe sur la reprise, même dans des conditions d'exploitation provisoire, ou de fonctionnement dégradé.

Bien qu'il soit plus facile de visualiser ces paramètres, dans le cas d'un arrêt de production après un dommage matériel aux ressources physiques, ils sont applicables à toutes les situations décrites à la question précédente. Ils permettent d'évaluer la gravité d'un sinistre de flux, qu'il résulte d'un dommage aux biens propres, ou chez un tiers, d'un engagement de responsabilité, de la perte d'une ressource partenaire ou d'une ressource gratuite, ou de la perte d'un collaborateur.

4
Les risques émergents

32 *Les entreprises ont-elles des responsabilités pénales ?*

Certes, le Code pénal français prévoit, spécifiquement, la responsabilité pénale des personnes morales, avec des sanctions financières, pour l'essentiel. La plus grave des sanctions est l'interdiction de continuer l'activité, ce qui équivaut à une « peine de mort », sur le plan commercial ou industriel.

Toutefois, c'est essentiellement par ses hommes que l'entreprise se trouve impliquée dans des poursuites pénales, et tout particulièrement ses dirigeants.

Si dans les années 1980, on parlait de « dépénalisation » nécessaire, aujourd'hui, on constate une « surpénalisation » et une « recherche effrénée de culpabilité » (commentaire du professeur Olivier Beaud, université Panthéon-Assas Paris 2).

Un certain nombre de facteurs explique cette « prolifération » des poursuites pénales :

- La pugnacité des victimes et des associations de défense.
- La médiatisation poussée à l'extrême, et en particulier l'impact des médias sociaux.
- Le sentiment partagé dans l'opinion publique que cette responsabilité est la juste contrepartie de la rémunération perçue par le dirigeant.
- La recherche systématique d'un « bouc émissaire ».
- Le jeu de la complicité active ou passive et la reconnaissance des agissements d'immixtion de fait.
- Les opérations « *manu polite* » et la recherche d'un « espace judiciaire européen » par les juges d'instruction.

L'insertion d'un principe général de précaution dans le préambule de notre Constitution (charte de l'environnement) peut entraîner quelques dérives en servant de fondement à une « obligation de précaution renforcée », et ainsi permettre de justifier des condamnations plus sévères au pénal (mise en danger d'autrui) comme au civil (obligation générale de sécurité).

Il en résulte que l'on va réprimer l'apathie, la négligence fautive, l'inaction et l'abstention de toute initiative. Les fondements des poursuites pénales se multiplient.

1. Le droit commun

Des poursuites ont toujours eu lieu contre les homicides volontaires, les coups et blessures volontaires, le vol, l'escroquerie, l'abus de confiance, le recel, le faux en écriture publique ou privée, l'abus de biens sociaux et son recel. Ce n'est pas un phénomène nouveau.

Ce qui est nouveau, c'est que l'on passe de l'impunité de fait, à des poursuites plus systématiques sous l'influence des médias et de la doctrine.

2. Le droit pénal « spécial » du travail

Des poursuites sont de plus en plus diligentées, en matière :

- ► d'hygiène et de sécurité des travailleurs, de travail clandestin ;
- ► d'infractions à la durée du travail ;
- ► d'entrave au fonctionnement normal des organes représentatifs du personnel (délit d'entrave).

3. Le droit pénal des sociétés

Les poursuites, assez rares autrefois, deviennent plus nombreuses, en vertu des textes qui régissent ces agissements fautifs :

- ► articles L 242 à L 255 de la loi 66-537 du 24 juillet 1966 sur les sociétés commerciales ;
- ► articles 423 à 483 du Code des sociétés, en particulier les articles 431, 463 et 478 ;
- ► loi de 1990 sur la transparence boursière (délits boursiers d'initiés).

4. Le droit économique de la concurrence

5. Le droit répressif du consumérisme

Par exemple, vente par démarchage à domicile, facturation, affichage, non-communication des prix, étiquetage.

6. Le droit de l'environnement

7. La naissance d'une répression systématique de la criminalité organisée

Notamment la criminalité financière, dite « en col blanc », avec entre autres, la question du blanchiment de l'argent.

8. L'apparition d'un Code pénal plus moderne en 1994

Avec des infractions « fourre-tout », telles que la « mise en danger d'autrui » et l'incidence de la responsabilité pénale des personnes morales sur la responsabilité pénale personnelle des dirigeants[2]. On constate donc une multiplication des sources de responsabilité pénale, tant à l'égard des entreprises, que de leurs dirigeants.

2 Sur ce point, voir la circulaire de la chancellerie du 26 janvier 1999, JCP ed Gén 1999, III, 20035 et Claude Ducouloux-Favard, « Quatre années de sanctions pénales à l'encontre des personnes morales », Dalloz, 1998, chronique p. 395.

33 *La sécurité informatique est-elle une nécessité vitale ?*

Dans la plupart des organismes, l'outil informatique pilote l'ensemble des opérations de fabrication, depuis les approvisionnements jusqu'à l'ordonnancement des livraisons, en passant par la production elle-même, sans parler des études et de la conception de nouveaux produits.

La gestion elle-même et la comptabilité sont également informatisées. De ce fait, la question ne porte plus tellement sur la sécurité informatique, mais plutôt sur la sécurité de l'entreprise informatisée. Celle-ci fait l'objet d'un ensemble de normes ISO spécifiques (la série des ISO 27000:2013 *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information*).

La première remarque est que, trop souvent laissés à l'appréciation d'un conseil extérieur, sans maîtrise interne suffisante, les systèmes d'informations sont d'architectures trop complexes avec deux écueils extrêmes : la centralisation excessive bridant les évolutions ou les décentralisations trop vastes avec des divergences incompatibles.

Le premier facteur de sécurité informatique est de concevoir un système où un juste équilibre est respecté. En particulier il faut mettre en place une gestion des postes individuels, grâce à des procédures de surveillance régulière, comme par exemple, vérifier que tous les logiciels prévus sont effectivement présents, effacer les logiciels « pirates » introduits par les collaborateurs, même s'ils sont pertinents pour le travail. Il est essentiel que le pilotage des logiciels soit centralisé.

Il faut noter, également, que bien souvent les logiciels libres (ceux que l'on peut télécharger d'Internet sans payer) offrent un niveau de sécurité supérieur, du fait que l'on peut les analyser plus facilement.

L'informatique a aussi un impact direct sur la gestion des ressources humaines. En incidente, une retombée de l'e-administration dans les collectivités territoriales — constatée en Grande-Bretagne — est la crainte des administrés qui font un complexe « Orwell 1984 » et celle des fonctionnaires qui ont l'impression de perdre leur capacité d'autonomie de décision.

Cela dit, sans avoir de prétention d'exhaustivité, il convient d'évoquer les quatre vulnérabilités essentielles des systèmes d'informations et d'en citer quatre autres courantes, mais moins vitales.

Ces vulnérabilités essentielles sont les suivantes :

- ***Disparition d'un fournisseur-clé :*** un fournisseur de logiciel peut faire faillite, arrêter la diffusion d'un logiciel, cesser la maintenance… Sans document source, l'entreprise peut être complètement paralysée. Des mesures de précaution s'imposent :
  - Analyse de la situation financière du fournisseur.
  - Analyse du volume de vente du système, présent et potentiel (pour les logiciels, le matériel et les fournitures).
  - Modification du contrat-type, éventuellement, révision périodique, pour y inclure les sauvegardes et les garanties nécessaires.
  - Disponibilité des sources du programme (au sein de l'organisme ou chez un tiers garant).
  - Écriture des programmes dans un langage de programmation couramment utilisé.
  - Portabilité du logiciel sur des matériels courants et largement diffusés.
  - Étroite coopération entre le fournisseur et l'organisme avec des échanges quasiment quotidiens.
- ***Changement volontaire de fournisseur :*** chaque décision doit être analysée avec précaution, en envisageant toutes les conséquences. Si les précautions listées ci-dessus ont été prises, la question de changement ne se posera pas.
- ***Accès non autorisé aux données :*** les mots de passe sont un moyen généralement utilisé, et l'un des plus efficaces, encore faut-il prendre les précautions suivantes. Chaque utilisateur doit :
  - Avoir son propre mot de passe ou une série de mots de passe différents de ceux fournis automatiquement avec le système.
  - Modifier très régulièrement ses mots de passe et, au coup par coup, quand un incident le justifie.
  - Conserver son mot de passe secret, et respecter le secret des autres utilisateurs.

En dépit des mots de passe, d'autres procédures et des barrières physiques, il peut arriver que des accès non autorisés aient lieu. Chaque amélioration des sécurités génère la génération suivante d'astuces pour les contourner. De ce fait, il est essentiel de maintenir un niveau élevé de sécurité sur l'ensemble des opérations informatiques d'un organisme.

- ***Les virus, vers d'autres formes d'attaques informatiques :*** en matière informatique, un virus est une série d'instructions insérée, dans le but de nuire (comme un acte de vandalisme), qui fait réaliser, à l'ordinateur, des fonctions pour lesquelles il n'a pas été programmé.

  Certains virus sont insérés dans le programme des produits achetés sur le marché, comme une protection des droits d'auteur du concepteur, dans le but d'éviter les reproductions pirates, et sont activés par la duplication. Ils polluent alors l'ensemble du système.

  La sécurité totale n'existe pas, mais on peut, toutefois, réduire considérablement le risque en prenant les précautions suivantes :

  - Prudence à observer, quant à l'introduction de programmes venant de sources non totalement fiables, et en particulier venant de « tableaux d'affichage informatisés ».
  - Installation de programme « antivirus » et de pare-feu sur le système de gestion pour vérifier et détecter, au moins, toutes les formes connues de virus. Il faut, en particulier, tester tous les nouveaux programmes avant de les introduire et tester systématiquement l'ensemble du système périodiquement.
- ***Autres vulnérabilités liées à l'informatique pour mémoire :***
  - Écrasement de disque dur.
  - Erreur d'utilisateur.
  - Dommage aux logiciels et aux progiciels.
  - Dommage au matériel.

Il faut surtout garder à l'esprit que les avancées technologiques et la mise en place de « *big data* » et « *cloud computing* » entraînent des sources infinies de risques d'intrusion et que les organismes doivent redoubler de vigilance sur ce dossier.

34 *Pourquoi faut-il gérer les risques de la chaîne logistique ?*

La logistique est devenue l'épine dorsale de tout organisme produisant des biens et des services dans le contexte d'économie intégrée dans lequel nous vivons aujourd'hui, du fait de la globalisation qui s'est accompagnée de l'externalisation d'un grand nombre de tâches et du fonctionnement en réseau qui en découle. Si le terme de « chaîne » est souvent utilisé, aujourd'hui il serait sans doute plus exact de parler de réseau, voire de nuage, tant il est difficile d'en connaître la frontière. Les événements naturels qui se sont produits en Asie en 2011 ont mis en lumière des dépendances qui n'ont, souvent, même pas été identifiées par les organismes concernés.

La conséquence de cette structure est que la satisfaction du client final passe par le respect d'un cahier des charges « risques », par chacun des maillons, alors qu'il n'existe aucun standard reconnu internationalement pour valider la pertinence de la gestion des risques des acteurs, contrairement à la question de la qualité, dont une approche est possible, à tout le moins, à l'aide des normes ISO.

Cela a pour effet que la gestion des risques est laissée à l'appréciation de chaque acteur, sauf à s'appuyer sur de clauses contractuelles dans le cadre des relations bilatérales. De nombreux organismes globaux s'efforcent d'obtenir, de leurs sous-traitants et de leurs fournisseurs, des engagements pour garantir la résilience de la chaîne logistique. Cela est facilité dans le cas où il existe un « maître d'œuvre » global maîtrisant un ensemble de partenaires, comme dans le cas d'un avionneur. Les entreprises industrielles et commerciales complexes, dont les départements logistiques sont puissants, commencent à s'équiper de risk-managers spécialisés, rattachés directement au directeur logistique.

Il faut, en premier lieu, définir ce que l'on appelle chaîne logistique. Dans ce contexte, c'est un ensemble de plusieurs organismes, juridiquement distincts, et entre lesquels s'échangent des flux amont et aval de biens et de services, avec en contrepartie des flux financiers pour mettre à la disposition d'un client final des biens et des services. On peut scinder cette chaîne logistique en cinq phases :

- achats et acheminement ;
- stockage ;

- traitement des commandes des clients ;
- fabrication ;
- distribution (transport et livraison).

De nombreux praticiens et universitaires se sont penchés sur la question, et des solutions commencent à se dessiner, en particulier l'équipe du professeur Borghesi de l'université de Vérone qui proposait dès les années 1980 de se focaliser sur une des entreprises participant à la chaîne : c'est alors elle, l'objet de la cartographie.

Cette cartographie passe par la définition d'indicateurs de risques associés aux différents objectifs, définis ci-dessus, et le calcul d'un indice composite de risques pour la chaîne qui s'apparente à l'approche de criticité employée en sécurité des systèmes. On se contentera de donner, ici, les grandes lignes de ces objectifs :

- aboutissement de la commande, scindé en sous-objectifs ;
- respect des délais ;
- réalisation intégrale ;
- respect des éléments qualitatifs ;
- livraison intacte ;
- réaction, scindée en sous-objectifs ;
- intégrité ;
- rapidité ;

Les indicateurs sont définis pour chaque objectif, en regard de chacune des phases. L'indice composite est le produit de tous ces indices individuels selon les deux dimensions, phase et sous-objectifs, chacun ayant un poids identique.

La définition de ces différents indices donne, en fait, une grille d'identification, de définition et d'analyse des différents points « vulnérables » ou critiques, que l'on peut croiser avec la méthode des centres de risques, au sein de chacun desquels une partie de la chaîne logistique est traitée.

Cette approche permet de valider les résultats et d'intégrer au niveau stratégique, c'est-à-dire porter à l'attention des dirigeants une évaluation de la « solidité » de la chaîne. En outre, l'indice composite permet de suivre l'évolution des progrès accomplis. Il va de soi, que chaque entreprise pourrait revoir ces indices, en fonction de ses propres objectifs et de ceux de ses principaux partenaires « logistiques » amont et aval.

35 *Les atteintes à l'environnement font-elles partie de la gestion des risques ?*

La protection de l'environnement reste un thème porteur pour les hommes politiques, mais quelle est sa réalité au niveau de la gestion des organismes publics ou privés ?

Trop souvent, les risk-managers ont eu à s'intéresser à cette question, au travers de la couverture d'assurance de la responsabilité civile « pollution », en particulier dès les années 1980 pour la pollution graduelle et ensuite plus récemment avec l'exclusion de la pollution accidentelle. Toutefois, les atteintes à l'environnement dépassent largement le thème de la pollution et de l'indemnisation des victimes publiques ou privées.

Aujourd'hui, l'environnement est devenu une fonction à temps plein, dans de nombreuses entités, dans un système parfois intégré avec l'hygiène et la sécurité sous le nom de HSE, voire avec la qualité QHSE.

Bien entendu, pour les activités industrielles, l'enjeu de la gestion du risque environnement est rendu complexe du fait des nombreuses interactions de l'entreprise avec son environnement. Le risque « écologique » est présent dans tous les aspects d'une entreprise et de ses activités. Par exemple, l'implantation d'une usine sur un site particulier peut mettre en danger une plante ou un animal rare, la construction de cette usine peut entraîner des ruissellements et un phénomène de sédimentation de déchets dans un lac ou une rivière proche, son exploitation peut créer de nombreux risques liés aux matières premières, à leur transport et à leur stockage, aux déchets et aux émissions résultant des processus industriels, aux méthodes de traitement et d'élimination des déchets, ou encore, l'utilisation et l'élimination des produits peuvent créer les conditions du risque écologique…

Néanmoins, les activités tertiaires sont, elles aussi, susceptibles de créer ou de subir des risques liés à la pollution : l'air respiré par les employés peut contenir des produits chimiques, des particules ou des pollens auxquels certains peuvent être particulièrement sensibles. On peut penser également à l'empreinte carbone de chacun.

Les cheminées d'usines, les réservoirs ou les aires de stockage et les décharges ne sont que des exemples de risques classiques associés à la gestion des risques « environnement ».

Il n'est pas possible, ni souhaitable, que le risk-manager ait lui-même une connaissance scientifique des problèmes environnementaux. La complexité des risques de pertes liés à l'environnement oblige une entreprise à s'appuyer sur des informations, des compétences et des expériences diverses. Elle fera donc appel à des personnes venues d'horizons très différents, parmi lesquelles le directeur environnement.

Dans ce cadre, quel est le rôle du risk-manager en matière de gestion des risques d'atteintes à l'environnement ?

Pour travailler avec les spécialistes de l'environnement, le risk-manager doit connaître et comprendre les concepts-clés de l'écologie. Il doit être capable de recenser les principales catégories et les sources d'atteintes à l'environnement et d'accompagner les processus d'identification et d'analyse de ces risques. Il doit, également, être capable d'évaluer les différents processus de traitement de ces risques, tant au plan financier, qu'au plan de l'impact à long terme sur la biosphère (voir question 89). Les principales missions du risk-manager en termes d'environnement peuvent se résumer ainsi :

- Identifier et analyser les principales vulnérabilités « environnement » de son organisme, et en particulier les pertes, les sources des dangers.
- Définir, en accord avec la direction, un cadre de priorités pour traiter les risques écologiques et contrôler les pertes liées à l'environnement.
- Conduire, avec les spécialistes, le processus d'évaluation des risques.
- Maintenir une coopération efficace avec les responsables environnement et les autres spécialistes (juristes, exploitation, bureau d'études…) pour planifier et mettre en œuvre la stratégie de gestion « environnement du groupe ».
- Développer et mettre en œuvre un programme de financement du risque « atteintes à l'environnement ».

36 *L'image et la réputation d'une entreprise sont-elles sources de risques ?*

Les organismes, parfois aidés par l'opinion publique, les consommateurs ou leurs propres partenaires économiques découvrent l'importance de la gestion du risque à la ***réputation (risque d'image, de marque)***.

C'est le risque de voir la réputation ou l'image d'un organisme dégradée, au moins dans la perception du public ou de la communauté vis-à-vis de ses partenaires économiques.

Cette dégradation peut provenir de multiples sources : accident spectaculaire mettant en cause la « sagesse » des dirigeants, défaut de produit et rappel mal conduit, insinuations malveillantes, campagne de dénigrement, pour n'en citer que quelques-unes.

Par exemple, Exxon a souffert de la pollution provoquée par l'incident de l'Exxon Valdez, Shell a vu ses ventes chuter — en particulier en Allemagne — pendant l'incident de la plateforme Alpha, Perrier ne s'est jamais remis des traces de toluène…

Alors que la construction de l'image est l'aboutissement d'un long et patient processus, la réputation peut être ruinée en un éclair si un événement, parfois mineur en apparence, est mal géré.

Le défi est que les dangers peuvent survenir en tout lieu et à tout moment. « Père gardez-vous à droite, père gardez-vous à gauche », conseillait le dauphin Charles à son père le roi Jean le Bon, pendant la bataille de Poitiers.

Le tableau ci-après illustre quelques périls essentiels, en reprenant la classification déjà exposée (voir question 8).

Il montre bien que tous les périls pesant sur un organisme sont susceptibles d'avoir un impact sur la réputation, positif ou négatif. En fait, plus que l'incident lui-même, c'est la réactivité de l'organisme et de ses dirigeants face à ces événements, leur capacité à les affronter qui est déterminante pour la perception qu'en auront les parties prenantes.

En résumé, si la réputation n'est pas en elle-même source de risques, puisqu'elle est un actif, en revanche, la prise en compte de l'impact sur la réputation de chaque risque modifie considérablement leur impact, et donc leur prise en compte dans les décisions stratégiques.

Quelques risques significatifs d'atteinte à la réputation

Économique	Évolution soudaine des goûts des consommateurs : *la société est perçue comme non réactive, coupée des réalités (application au domaine politique !)*
Naturel	Inondation : *la société est mal gérée puisqu'elle a choisi de construire un site de production en zone inondable (et le maire l'a laissé faire !)*
Industriel	- Incendie : *comment ont-ils pu construire une usine si mal protégée, risque pour ses salariés et ses voisins ?* - Pollution : *cette société n'est pas sûre, un danger pour la santé des hommes et la sécurité de l'environnement !* - Discrimination au niveau des ressources humaines : *divergence entre les valeurs affichées et les pratiques constatées (cas IBM et de ses salariés de couleur aux États-Unis)* - Gouvernance : *absence de guides clairs ou non-respect des normes établies* - Concurrence déloyale : *attitude en décalage par rapport aux règles admises ou aux engagements pris*
Humain non volontaire	Défaut de produit ou de service : *danger d'actions judiciaires et attention médiatique*
Humain volontaire	Défaillance de sûreté : *la société n'est pas assez attentive à la protection de ses informations confidentielles, à la sélection de personnels fidèles*

37 *Peut-on gérer les risques de réputation ?*

Si elle n'est pas source de risque en elle-même, la réputation, le principal actif immatériel de la plupart des organismes, est vulnérable. Effectivement, elle peut se mesurer par l'excédent de valeur de l'organisme sur la valeur de ses actifs physiques, en particulier quantifiable pour ceux qui sont cotés en bourse. Ainsi mesurée, l'image ou la réputation représente, sans doute, en moyenne de 60 à 70 % de la valeur d'une entreprise dans les pays développés. C'est pourquoi il faut intégrer les impacts sur la réputation dans l'analyse des vulnérabilités. Dans cette perspective, la clé de la gestion des risques, d'atteinte à l'image et à la réputation, réside dans une gestion des risques proactive efficace et des règles de bonne gouvernance respectées, couplées avec une communication sans détour des problèmes rencontrés.

Cependant, par-delà ces risques « usuels », l'équipe dirigeante doit rester en permanence à l'écoute des parties prenantes, de façon à anticiper les changements, en particulier ceux dont la soudaineté pourrait entraîner des ruptures.

En fonction des paramètres de la réputation, qui visent à créer et à maintenir une différentiation par rapport aux pratiques de la concurrence, il faut garder à l'esprit certains risques spécifiques à l'image, comme :

- L'incapacité d'établir sa « différence », et donc de créer cet avantage compétitif, qui fait que le consommateur est prêt à payer plus, pour un produit ou un service spécifique.
- L'incapacité de maintenir cette « différence » dans le temps (c'est un risque structurel) face aux :
  - évolutions des attentes et des attitudes du public ;
  - nouvelles réglementations ;
  - évolutions économiques aboutissant à l'incapacité ou l'absence de souhait du public de payer la « prime » pour la spécificité des biens ou des services proposés.

Dans un nombre croissant de domaines, les organismes fonctionnent en mode projet, qui implique différents partenaires.

Dans ce cadre, le respect des délais et des enveloppes budgétaires devient un facteur primordial de réputation. Pour gérer de telles situations, les spécialistes de la recherche opérationnelle ont développé des outils

spécifiques rendus plus puissants grâce aux supports informatiques. Ils sont devenus de véritables outils de maîtrise des risques de réputation, en permettant de suivre, au quotidien, le budget et le calendrier. On peut en particulier citer le PERT, dont le suivi du chemin critique permet d'investir sur les tâches qui conditionnent le succès du projet, y compris celles relevant de l'hygiène et de la sécurité. Bien entendu, on pourrait citer tous les outils de la sûreté de fonctionnement tels que l'AMDEC, la méthode MOSAR… (voir *Maîtrise des risques*, Bibliographie).

En résumé, la gestion de ces risques relève d'un processus d'apprentissage continu et de vigilance. Ce processus doit s'étendre non seulement à tous les acteurs à l'intérieur de l'organisme, mais également à l'ensemble de ses partenaires externes (sous-traitants, fournisseurs et/ou clients) avec lesquels il a des contrats, mais aussi ses « cotraitants » avec lesquels il peut n'avoir aucun lien contractuel direct (donc aucun moyen d'action) autre que *via* le donneur d'ordre ou le maître d'œuvre du projet. De plus en plus, l'entreprise individuelle n'est plus qu'un nœud de communications au sein d'un réseau complexe, dans lequel la réputation de tous est entre les mains de chacun. Qu'un seul soit défaillant, c'est la réputation de tous qui peut souffrir.

En conséquence, tous ceux qui « sont en charge » de ce processus doivent apprendre à réagir, non seulement aux risques identifiés, mais aussi aux dangers inattendus tout au long du chemin. Cette attitude d'éveil est d'autant plus vitale, que pour les risques de réputation, le marché ne propose pratiquement pas d'instrument de transfert. En ce qui concerne les mécanismes d'assurance, il n'y a pas de solution « tous risques » pour les atteintes à l'image ou aux marques, il n'y a que des « rustines » limitées aux frais de retraits et à la prise en charge de quelques dépenses de publicité, sans commune mesure avec l'ampleur du « sinistre maximum possible » en la matière. C'est pour cela que la réflexion globale accompagnant la mise en place d'un véritable plan de redéploiement stratégique (voir question 49) est la condition de la résilience de l'organisme, au cœur de la maîtrise des risques de réputation. Dans toutes les branches industrielles, mais plus encore, dans tout ce qui touche directement le public (alimentation et médicaments), la gestion des crises sera une priorité absolue (voir question 48).

38 *En quoi consiste la responsabilité des dirigeants ?*

La responsabilité des dirigeants peut être recherchée dans deux voies fondamentales :

- La responsabilité pénale, et l'arsenal de répression et de sanctions.
- La responsabilité civile, visant à la réparation des dommages subis par les tiers lésés, en particulier le volet croissant de conformité fiduciaire avec les évolutions légales dans le monde entier en répercussion de l'affaire Enron.

On pourrait également évoquer le volet fiscal avec son cortège de sanctions pénales administratives, mais qui, pour représenter des risques réels, sortent un peu de l'objet de cet ouvrage.

Qui est visé par le terme de « dirigeant » ? Bien entendu, sont concernés les dirigeants de droit (PDG, DG, membres d'un directoire, d'un conseil de surveillance ou d'un directoire de société anonyme, gérants de SARL, administrateur délégué de GIE, présidents d'associations…).

On peut noter qu'un représentant de société, au sein des organes dirigeants d'une autre société, fût-il salarié, encourt les mêmes responsabilités.

Mais, à la suite d'une interprétation jurisprudentielle, désormais consacrée par la loi, sont concernés également les dirigeants de fait (« *celui qui, en toute souveraineté et indépendance, exerce une activité positive de gestion et de direction* », citation du professeur Rives Lange).

Pour que la responsabilité, civile, pénale ou fiscale d'un dirigeant puisse être engagée, il faut réunir certaines conditions :

- Être dirigeant de droit ou de fait.
- Avoir commis une infraction prévue dans le Code pénal ou commis une faute de gestion.
- Posséder son discernement (état de démence…).
- Être mis en cause.

Plutôt que de faire une liste des formes d'engagements de responsabilité des dirigeants, dressons ici une liste de quelques préceptes de bons sens à garder à l'esprit :

- ***Le respect des lois et des règlements :*** « nul n'est censé ignorer la loi, et personne n'est au-dessus de la loi ».

Cela passe par la mise en place de procédures de veille juridique permanente, car le paysage légal actuel est marqué par l'évolution rapide et la complexité (Code civil, Code pénal, Code du travail, droit de l'environnement, droit de la concurrence, Code des assurances, Code de la sécurité sociale, principe général de précaution et droit de la consommation…).

- ***La responsabilité pénale personnelle***, des personnes morales et/ou physiques, n'est pas assurable.
- ***Le droit et la morale ne sont pas confondus :*** tout ce qui n'est pas interdit est permis, sauf la fraude ou la mise en jeu de la théorie de l'abus de droit.
- ***L'appel au spécialiste du droit*****,** interne ou externe, qui dispose d'outils spécifiques pour identifier, aider à évaluer et réduire l'ensemble des risques juridiques. Son apport peut être résumé en quelques points-clés :
  - Choix de la structure juridique appropriée à un projet donné. En effet, le régime juridique applicable et souvent l'étendue des responsabilités des dirigeants en dépendent. Un administrateur de SA ou un gérant de SARL n'a pas les mêmes responsabilités qu'un membre de conseil de surveillance.
  - Préconisation du meilleur chemin de « sécurité juridique », après l'établissement d'un « diagnostic des risques juridiques » de la situation (en particulier la vérification des publicités tous médias).
  - Mise en place de contrefeux dont la forme est très variable : transfert contractuel de responsabilité (rédaction des contrats de vente ou d'achat, modes d'emploi, avertissements à la clientèle, clauses restrictives de responsabilités entre professionnels, technique de déclarations dans les clauses de garantie d'actif et de passif, délégation de pouvoir de responsabilité de signature…).

En résumé, tout en gardant à l'esprit l'apport des différentes couvertures de responsabilité proposées, tout dirigeant de droit ou de fait doit développer une stratégie proactive pour gérer l'incertitude juridique dans laquelle son action s'inscrit.

39 *Que penser des catastrophes naturelles ?*

En France, c'est la loi d'indemnisation des « catastrophes naturelles » qui a donné l'habitude d'utiliser ce terme, en référence aux dommages parfois catastrophiques provoqués pas des événements naturels d'ampleur exceptionnelle, de fréquence inhabituelle et pour lesquels les sociétés humaines n'étaient pas préparées. En fait, si on doit rétablir la vérité, c'est que la connaissance scientifique de ces événements est basée sur des données chiffrées, recueillies depuis moins de deux siècles, des mémoires historiques sur deux ou trois mille ans, suivant les régions et des « mythes », comme le déluge, dont l'histoire reste très jeune par rapport au temps géologique.

En clair, la question n'est pas celle des « catastrophes naturelles », mais plutôt celle de l'adaptation des constructions et des modes de vie des êtres humains à des événements naturels qu'ils ne peuvent pas maîtriser, et dont ils connaissent encore mal les faits générateurs et les schémas de développement qui doivent se mesurer à une échelle de temps dépassant largement le champ d'analyse même des philosophes les plus visionnaires.

Certes, le tsunami en Asie de décembre 2011, a provoqué un nombre record de morts, alors que les centres qui suivent ces phénomènes les avaient prévus plusieurs heures auparavant, sans avoir les moyens de prévenir les populations en danger.

L'année 2004 était apparue comme exceptionnelle pour les montants des sinistres de cyclones à la charge des assureurs et des réassureurs dans le sud-est des États-Unis et les Caraïbes. Mais les années « exceptionnelles » semblent se multiplier. En réalité, cela tient aussi à ce que les valeurs accumulées et assurées sur les lieux sont sans commune mesure avec celles de la fin du XIX^{e} siècle lorsqu'une même année, non pas quatre, mais cinq cyclones frappèrent le continent.

En résumé, quelle que soit la qualité des modèles développés par les spécialistes des sciences de la terre, en liaison avec les assureurs et les réassureurs, l'ampleur et la date des événements naturels restent largement aléatoires et la réduction de leur fréquence ne relève pas d'activités humaines, sauf des efforts à très long terme pour contenir les tendances historiques. La prévention des événements naturels n'existe pas. Alors que peut-on faire ?

Les leçons du passé récent sont importantes. Il est possible, dans une certaine mesure, de protéger populations, constructions et de limiter les conséquences :

- Les vies humaines peuvent être sauvées si des systèmes d'alertes sont en place, et si les populations exposées comprennent les mécanismes et apprennent à réagir correctement. La comparaison du nombre de victimes du tsunami de 2011 et celles des cyclones des dix dernières années sont de claires illustrations de ce phénomène.
- L'étude de la topographie des lieux peut permettre de choisir des implantations moins exposées aux périls naturels, qu'ils soient de nature sismique, volcanique ou la conséquence de l'activité des vents et des marées.
- Pour certains périls, il est possible de choisir des modes de construction plus résistants, c'est notamment le cas pour les effets de tremblements de terre (fondations, structure…) et des cyclones (bâtiment offrant moins de prise au vent et protégés).
- La mise en place de plans d'action adaptés, en cas de catastrophe, peut réduire considérablement l'impact, en particulier en matière d'arrêt de production. Attention, les plans sont différents pour les différents périls et doivent être remis à jour périodiquement.
- Tout le monde peut subir l'impact de ces périls, même les entités *a priori* non exposées, telles que les PME/PMI localisées, de deux façons complémentaires :
  - Ampleur exceptionnelle ou inhabituelle d'un péril, comme les deux tempêtes de décembre 1999, en France.
  - Effet domino sur une chaîne logistique sensible à ces risques qui contient des partenaires, directs ou indirects, (fournisseurs au Japon, clients en Floride…).
- Il existe des mécanismes de financement par l'assurance accessibles pour les entités de taille moyenne avec l'aide des pouvoirs publics dans certains États (comme en France). Les marchés privés sont parfois très onéreux du fait de l'antisélection (pas assez d'assurés, risque trop lourd).

40 *Qu'entend-on par risque climatique ?*

Pour les Européens, globalement habitués à des climats tempérés, on pourrait dire que l'exposition au risque climatique remonte aux expéditions en Amérique, en Afrique, et plus récemment dans les zones polaires.

Les températures extrêmes ont toujours exigé des adaptations, mais la question de l'évolution climatique recadre la question dans une urgence plus générale.

Ce risque se retrouve déjà en France métropolitaine. Il suffit de se souvenir de l'été 2003 et de l'hécatombe de personnes âgées du fait de la canicule, même si les statistiques de décès se sont pratiquement normalisées après dix-huit mois, pour démontrer que le climat, s'il n'a pas tué, a toutefois hâté des décès. Il n'en demeure pas moins que les images resteront dans les mémoires, ce sont, avant tout, celles d'une impréparation à une crise de nature spécifique. Et que dire des inondations de l'hiver 2014 en France ?

C'est pourquoi ce que l'on appelle le risque climatique a pour objet les variations climatiques que la planète connaît aujourd'hui, à la suite des abus de l'homme ou d'autres phénomènes naturels. On résume souvent la problématique aux conséquences de l'effet de serre et de la déchirure de la couche d'ozone. Qu'en est-il exactement et quel impact cela a-t-il sur les risques des organismes publics ou privés ?

L'effet de serre s'accompagne d'un réchauffement qui peut entraîner de multiples conséquences : désertification où l'eau sera insuffisante, fonte de calottes glacières et élévation du niveau des mers avec inondations de zones côtières, déviation du Gulf Stream apportant un climat beaucoup plus marqué en France, pour ne citer que ceux dont la presse se fait l'écho régulièrement.

Pour la couche d'ozone, l'élévation du niveau des rayons UV sur la Terre peut modifier les conditions de survie des espèces animales.

« Les climatologistes prédisent que l'évolution des zones climatiques liée au réchauffement global aura pour conséquence d'exposer à des risques d'événements climatiques exceptionnels qui n'ont jusqu'à présent menacé que des zones extrêmes », cite le mensuel *SIGMA* (Swiss Ré, février 2005).

En réalité, les scientifiques ne s'accordent pas tous sur les causes du réchauffement. Selon l'échelle du temps prise en compte :

- certains montrent que, depuis les enregistrements météorologiques, l'augmentation des températures est sensible ;
- d'autres, en se positionnant par rapport aux périodes de glaciations et de déglaciations, pensent que l'impact de l'activité industrielle est marginal par rapport au phénomène naturel ;
- d'autres enfin essaient d'analyser une périodicité sur un cycle de mille cinq cents ans.

Bien entendu, la perception par les parties prenantes est essentielle, mais l'image est encore brouillée même si tout le monde s'accorde sur la réalité du réchauffement : une canicule, et tout le monde s'affole, un printemps pourri, et tout le monde oublie !

Face à ce phénomène, que peuvent faire l'élu territorial ou national et le chef d'entreprise ? Fondamentalement, on retrouve les problématiques évoquées à propos des catastrophes naturelles (voir question 39), de l'environnement et du développement durable (voir question 35) et du principe de précaution. Devant les inconnues de la science, les responsables doivent s'entourer d'un maximum de précaution dans le choix des sites et leur protection contre les changements climatiques de façon à répondre aux besoins des utilisateurs (par exemple, des installations de climatiseurs dans les maisons de retraite), et surtout être prêts à réagir, rapidement, dans le cas où des événements inattendus surviendraient.

Il est indispensable de mettre en place des dispositifs de secours pouvant être activés dans le cas où des vies sont mises en danger à la suite d'événements exceptionnels. Car c'est à la rapidité et à l'efficacité de la réponse que les parties prenantes, y compris les marchés financiers, évalueront les qualités des dirigeants, et leur confirmeront ou retireront leur confiance. À ce titre, on peut citer à nouveau les deux tempêtes de décembre 1999, où les réactions immédiates de prise en charge des problèmes des clients, par les dirigeants de la SNCF et d'EDF, ont été exemplaires. Ce phénomène a généré chez ces deux prestataires la prise de conscience de la nécessité de réfléchir à des défenses en profondeur, pour les futures évolutions climatiques et leur cortège de conséquences « imprévisibles ». Mais on peut penser aussi aux phénomènes plus récents en Asie en 2011, et au cyclone Sandy qui a frappé New York de plein fouet. Toutefois, malgré l'urgence, le consensus mondial sur l'action à tenir reste encore un espoir et non une réalité.

III
Le traitement des risques

5
La réduction des risques

41 *Qu'entend-on par réduction des risques ?*

Si nous avons souligné l'importance de dresser un diagnostic complet et précis, celui-ci sert de base à l'action, seconde étape du processus de gestion des risques, que l'on appelle aussi traitement. Le traitement résulte de la combinaison de deux types d'instruments fondamentalement différents : les instruments de financement qui visent à trouver des compensations pour les pertes engendrées par la survenance des aléas (voir partie IV) et les instruments qui visent à agir sur la réalité économique et sociologique du risque (les instruments de réduction).

La réduction des risques consiste donc à agir sur la survenance d'un péril et/ou ses conséquences sur les ressources de l'organisme objet de l'étude. De même que l'on a souligné les deux dimensions fondamentales de l'impact d'une vulnérabilité (fréquence et gravité) ; de même, ces deux dimensions servent à caractériser les instruments et leur action. Dans la réduction des risques, on distingue donc :

- ***Les instruments de prévention*** qui visent à réduire la fréquence, ou la vraisemblance de survenance d'un sinistre. Le principe est donc qu'ils agissent sur les causes à l'origine du péril et réduisent la probabilité de survenance.
- ***Les instruments de protection*** qui visent à limiter les ***conséquences*** de la réalisation d'un sinistre pour l'organisme étudié. Le principe est donc qu'ils agissent sur les conséquences, sans prendre en compte la fréquence.

Dans toute situation donnée, il est indispensable de prendre le temps d'une réflexion approfondie sur les instruments de réduction applicables. Trop souvent, dans la précipitation, on ne se donne pas le temps d'envisager les alternatives. Bien entendu, il y a une pression certaine à s'occuper, sans plus tarder, des vulnérabilités diagnostiquées en mettant en place les solutions qui « crèvent les yeux ». Toutefois, celles-ci ne sont pas nécessairement les meilleures, et trouver la solution optimale passe par un effort de réflexion et de recherche. Pour éviter l'écueil de la précipitation, le risk-manager peut s'imposer la discipline suivante :

- Se référer à la liste des huit instruments de réduction évoqués dans le tableau qui suit. C'est la garantie de n'oublier aucune des grandes options. Les applications pratiques varient largement d'une situation à l'autre.

- ► Recenser ceux dont la faisabilité dans la situation justifie une étude plus poussée.
- ► Analyser leurs principaux coûts et leurs avantages.

Avec de la pratique, des automatismes se créent. À l'examen d'une situation donnée, les différentes alternatives viennent d'emblée à l'esprit, évitant ainsi une « impasse » majeure. Illustrons ces huit instruments avec une situation pratique.

Vous envisagez de mettre en place un parc de véhicules pour votre force de vente. Comment réduire le risque lié à l'utilisation de la flotte ?

Les instruments de réduction (pour réduire la fréquence, la gravité ou la volatilité de ces pertes)	
Instrument	**Exemple d'application**
Évitement/suppression	Renoncer à se déplacer (téléconférences, marketing téléphonique)
Prévention	- Programme de conduite défensive - Entretien régulier des véhicules - Sélection des collaborateurs
Protection	- Donner des instructions pour la limite de vitesse ou installer des limiteurs - Choisir des véhicules moins puissants
Ségrégation par séparation	Utiliser plusieurs véhicules de tourisme pour déplacer un goupe (plutôt que les transporter dans un seul véhicule comme un minicar)
Ségrégation par duplication	Garder en réserve quelques véhicules de pool
Transfert contractuel pour réduction	Utiliser un véhicule en location (voir question 45)

42 *Qu'est-ce que la prévention ?*

La prévention a pour objectif de diminuer la probabilité ou la fréquence de survenance d'un sinistre. En revanche, elle peut être sans effet sur la gravité des sinistres potentiels.

Rappelons la différence fondamentale avec la protection. Celle-ci s'adresse, avant tout, à la gravité en cherchant à la contenir, sans préoccupation quant à la fréquence.

En analyse systémique, on peut également dire que la prévention est l'action sur les causes, et la protection est l'action sur les conséquences.

Dans une situation concrète, la distinction n'est pas toujours aussi tranchée, et beaucoup de mesures ont un impact sur la fréquence et la gravité. Ainsi, quand les limites de vitesse ont été instituées en plusieurs étapes, 130 km/h sur les autoroutes, 90 km/h sur les routes hors agglomération et 50 km/h en agglomération, l'effet attendu a été double :

- Réduction du nombre d'accidents automobiles (la vitesse réduite laisse plus de temps aux chauffeurs pour réagir et éviter des accidents) = prévention, puisque la fréquence baisse.
- Diminution de la gravité des accidents (en cas de choc, les dommages sont créés par la transformation de l'énergie cinétique, et celle-ci est proportionnelle au carré de la vitesse) = protection.

L'évitement, cité dans la question précédente, vise à arrêter une activité jugée trop dangereuse. Il pourrait être vu comme l'instrument de prévention par excellence, puisqu'il ramène à la probabilité zéro.

Néanmoins, il faut souligner que l'évitement se suffit à lui-même pour traiter une vulnérabilité. Dans de nombreuses situations, il est impossible (par exemple, une municipalité peut trouver les risques associés, avec l'école primaire ou la tenue de l'état civil, trop lourds, mais ce sont des missions fondamentales des communes qu'elle ne peut ni supprimer ni externaliser).

Avec tous les autres instruments de réduction, il reste, au moins, un risque résiduel par principe accepté par le décideur.

Le risk-manager doit alors poursuivre sa réflexion pour mettre en place peut-être un autre instrument de réduction et, en principe, un instrument de financement pour la partie « incompressible » du risque.

La distinction entre prévention et protection est essentielle. Une mesure de prévention agit sur la fréquence, et ne va diminuer la charge économique de l'entreprise pour une vulnérabilité donnée, qu'à moyen ou long terme. Elle n'a aucun effet sur la gravité d'un sinistre individuel. C'est le cas de l'interdiction de fumer pour éviter l'incendie dans un local.

Ainsi que nous l'avons évoqué plus haut, les mesures de prévention sont, en général, des actions sur la chaîne de causalité, conduisant à un sinistre visant à la rompre à un endroit donné. Concrètement, elle peut prendre la forme d'une procédure ou d'un dispositif physique dont la mise en place (avant la survenance de tout sinistre) a pour objectif de rompre, dans un certain nombre de circonstances, un enchaînement de faits supposés conduire au sinistre. Cette rupture de chaîne est censée réduire sa probabilité de survenance.

Du fait du lien étroit qui existe entre prévention et chaîne de causalité, des mesures de prévention efficaces ne peuvent être conçues qu'en s'appuyant sur une analyse attentive des causes de survenance de tel ou tel type de sinistre.

En ce qui concerne les accidents du travail, par exemple, la théorie des dominos indique qu'ils surviennent à la suite de situations ou d'actes dangereux. Dans cette tradition, l'attention s'est focalisée sur l'élimination des situations ou des actes présumés dangereux.

La prévention incendie s'appuie sur la rupture du « triangle du feu » : trois éléments sont nécessaires à la naissance d'un feu, un comburant (oxygène), un carburant et une source (d'allumage). Par conséquent, le principe de la prévention incendie est de supprimer ou de réduire l'une des trois pointes du triangle (limiter les stockages de produits dangereux sur un site industriel).

En résumé, il faut retenir une leçon essentielle : les mesures de prévention sans effet simultané de protection ne diminuent en rien le niveau des besoins de financements exceptionnels en cas de sinistre. En conséquence, la mise en place de mesures de prévention, à elle seule, n'aura pas d'impact sur les besoins en couvertures d'assurance.

43 *Qu'est-ce que la protection ?*

Ainsi que nous l'avons déjà évoqué, la protection consiste en l'ensemble des mesures qui permettent de réduire l'impact, la gravité d'un sinistre lorsqu'il survient. Donc, le gestionnaire de risques doit se poser la double question :

- Que peut-on faire avant le sinistre, pour en limiter les conséquences éventuelles ?
- Que pourrait-on faire après sa survenance ?

Il y a donc deux catégories essentielles de mesures de protection : celles à mettre en œuvre « avant événement », celles à mettre en œuvre « après événement ».

- Les mesures de ***protection « avant événement »*** ont souvent un effet de prévention, comme le cas évoqué à la question précédente avec les limitations de la vitesse. Typiquement, ces mesures vont avoir pour objectif de réduire l'ampleur de l'objet de risque exposé lors d'un événement donné (par exemple, limitations des valeurs dans un lieu de stockage, nombre de personnes travaillant dans un site « dangereux »…).
- Les mesures de ***protection « après événement*** » sont typiquement les « mesures d'urgence » (procédures, sauvetage, réhabilitation, organisation de la défense), pour arrêter l'accumulation des dommages ou contrer les effets du sinistre.

En réalité, cette appellation pourrait être dangereuse si elle conduisait les décideurs à imaginer qu'il n'y a rien à faire à l'avance, qu'il suffit d'attendre la survenance du sinistre pour se préoccuper de la conduite à tenir et des mesures à prendre pour en limiter les conséquences.

Il vaut mieux envisager la question sous un autre angle. Toutes les mesures de prévention sont à envisager et à mettre en place, avant la survenance de tout événement, toutefois :

- certaines se suffiront à elle-même et agiront sans qu'il y ait nécessité d'une intervention humaine ou d'un déclenchement d'un mécanisme que nous appellerons des « mesures passives » ;
- d'autres mesures devront être activées en cours de sinistre ou juste après, et nous les appellerons « mesures actives ».

Illustrons ce concept par des mesures concrètes que l'on peut prendre pour la protection contre l'incendie d'un site industriel :

- Construire des murs coupe-feu est une protection « passive ». Une fois le mur construit, un incendie prenant naissance dans un bâtiment industriel ne se communiquera pas à la partie du bâtiment située de l'autre côté du mur coupe-feu protégée par le mur. Aucune intervention humaine et aucun mécanisme ne seront nécessaires pour que la protection soit efficace.
- Mettre en place un système de détection et/ou d'extinction automatique des incendies, aussi appelé sprinkler, est une mesure de protection « active ». En effet, pour être efficace, le sprinkler doit se déclencher automatiquement et, pour cela, il faut qu'il soit entretenu régulièrement et que les sources d'eau soient bien approvisionnées.
- Un plan d'évacuation permet de sauver des vies humaines en cas de nuage toxique, par exemple, mais il faut que le plan soit connu de tous, que des exercices soient programmés et peut-être même, que des masques soient à disposition : il s'agit bien d'une mesure « active ».

La protection ne sert pas que pour les risques accidentels, elle est également un bon instrument de traitement des risques d'entreprise, aussi appelés risques spéculatifs.

Dans ce cas, la protection consiste à réduire l'investissement initial dans l'activité envisagée ou d'arrêter les frais, si l'aventure s'avère ne pas remplir les espérances attendues. Par exemple, un fabricant de poupées pourrait réduire son risque sur sa nouvelle gamme, en ne produisant qu'une quantité limitée et en poursuivant sa ligne précédente.

En vérifiant, ainsi, la réception de son nouveau produit par les consommateurs, sans pour autant se couper de sa base de revenu traditionnelle, le fabricant de poupées réduit son risque spéculatif lié à l'introduction de la nouvelle gamme. Ses pertes seraient limitées en cas d'échec. Bien entendu, parallèlement, ses profits seraient également moindres en cas de succès.

44 *Quelles sont la théorie et la pratique de la ségrégation des risques ?*

Derrière l'expression de ségrégation des risques se cachent, en fait, deux instruments de réduction des risques voisins, mais différents : la duplication des risques (ou plus précisément la duplication des objets de risques) et la séparation des risques, illustrés dans le tableau de la question 41.

Dans les deux cas, l'objectif est de réduire la dépendance de l'organisme sur un actif physique, une activité ou une personne, avec pour résultat de réduire l'impact d'un sinistre éventuel et d'améliorer leur prévisibilité.

Le proverbe suivant résume le concept : « *Il vaut mieux ne pas mettre tous ses œufs dans le même panier.* »

Quand les sinistres sont plus modestes et mieux prévisibles, l'effet de rupture sur l'organisme est moindre, et la planification est rendue plus facile.

La séparation des risques consiste à diviser une unité de production existante en deux ou plusieurs unités indépendantes (par exemple, scinder un stock unique, en gardant une partie dans un entrepôt et l'autre dans un second, ou construire deux unités de production distinctes pour un composant donné plutôt qu'une seule).

La séparation est un instrument particulièrement efficace si un organisme peut encore atteindre ses objectifs, avec une partie seulement de ses ressources. À supposer qu'un sinistre total vienne frapper une des unités, il est encore possible de produire les quantités nécessaires, quitte à augmenter les horaires de travail sur les sites disponibles.

Remarque importante : la séparation s'accompagne d'activité, sur tous les sites, en fonctionnement normal.

La duplication des risques suppose la mise en place d'une véritable « unité fantôme », double de l'unité existante et qui demeure en « *stand by* » ou en réserve.

C'est seulement si l'unité principale est indisponible que l'unité de secours est activée. Cet instrument, lourd au plan financier, se justifie par les pertes évitées si l'organisme est totalement dépendant de l'activité « doublée ». Par exemple, conserver un double des archives

comptables, garder un stock de pièces détachées essentielles pour certains équipements, avoir des salariés en réserve (équipages en alerte pour les compagnies aériennes), ou encore mettre en place un « *back-up* » informatique (exemple le plus fréquent).

Les différences entre la ségrégation (séparation ou duplication) d'une part, et les autres mesures de réduction des risques d'autre part, sont résumées ainsi :

- La ségrégation n'agit pas sur le niveau de risque de chaque site.
- La ségrégation réduit la gravité globale d'un sinistre, mais l'impact sur la fréquence est variable selon la forme retenue.
  - La séparation peut accroître la fréquence (par exemple, quand on utilise deux entrepôts au lieu d'un, les risques liés à l'exploitation sont doublés).
  - La duplication ne la modifie pas pour les risques de fonctionnement, puisque, par définition, le second n'est pas en fonction normalement (par exemple, l'ambulance de secours, qui reste au garage, n'a pas beaucoup de risque de subir un accident de la circulation, mais elle peut brûler dans le garage en cas d'incendie !).
- La duplication tend à réduire le sinistre « moyen » puisque les sinistres sont individuellement diminués sans avoir d'impact sur la fréquence.
- La séparation peut réduire le sinistre « moyen » ou ne pas le réduire (à étudier au cas par cas).

Toutefois dans la pratique, peu d'organismes construisent un second entrepôt simplement pour réduire les risques de rupture en cas de sinistre. En revanche, si la construction d'un second entrepôt est à l'étude, s'il est envisagé d'augmenter le parc automobile, si le recrutement d'un adjoint pour le directeur de l'exploitation informatique paraît s'imposer, le gestionnaire de risques peut ajouter son analyse qui, dans certains cas tangents, pourra emporter la décision.

Entrer le paramètre « vulnérabilités » dans l'équation peut, également, modifier parfois les contours du projet (par exemple, la localisation ou la taille de l'entrepôt, la marque et la taille de l'ambulance, le profil du poste et de l'expérience de l'adjoint informatique).

En revanche, le cas de la duplication est différent. L'initiative revient presque toujours au gestionnaire de risques ou, à tout le moins, à la découverte d'une vulnérabilité dont l'ampleur à elle seule peut justifier la mise en place de la structure de secours.

Les « *back-up* » informatiques ou comptables, les stocks de pièces de rechange critiques, les formations croisées permettant à des employés d'être polyvalents, sont autant d'investissements réalisés exclusivement pour des motivations de gestion des risques. Ils supposent que les dirigeants aient mesuré l'importance des risques.

Il suffit de prendre conscience de l'impact financier de la duplication sur les charges de l'entreprise, pour imaginer que, dans la vie pratique, la séparation est beaucoup plus souvent utilisée.

En ce qui concerne les risques spéculatifs, bien entendu la ségrégation des risques consiste à « ne pas mettre tous ses œufs dans le même panier », en espérant que l'un au moins des paniers se révélera bénéficiaire ou efficace : s'il s'agit d'un organisme à but non lucratif.

Dans le cas du fabricant de jouets, évoqué à la question 43, il pourrait, également introduire une gamme de soldats en même temps qu'une seconde gamme de poupées. En introduisant les deux gammes simultanément, on pourrait dire que le fabricant pratique la séparation, tandis que s'il conservait en réserve la seconde gamme (pour le cas où), il pratiquerait plutôt la duplication. Pour son développement, il s'appuierait sur les poupées pour l'essentiel, les soldats ne seraient qu'un substitut en cas d'échec. Dans tous les cas, la ségrégation des risques suppose que les dirigeants acceptent que leur rentabilité soit la rentabilité moyenne du « portefeuille » d'activités entreprises.

La ségrégation est, à l'évidence, un des instruments de réduction des pertes de revenus, puisqu'elle permet de maintenir la production, au besoin avec des contraintes plus lourdes ou à un niveau réduit, alors même qu'une ressource vitale est en partie indisponible. La distinction entre séparation et duplication est un peu rigide.

Dans la réalité, on peut être amené à concevoir des systèmes avec une souplesse, sans parler de dupliquer un investissement lourd, on peut introduire un degré de redondance, et on parlera, alors, plutôt de ségrégation avec ou sans « redondance ». Par exemple, une entreprise, qui estime ses besoins à une capacité de 100, construit deux unités de capacité 60 chacune : elle s'est procuré une redondance de 20%. Bien entendu, l'excédent de capacité peut aussi être une anticipation de l'évolution du marché.

En clair, sauf rare exception, la ségrégation des risques résultera d'une décision stratégique complexe où la gestion des risques ne sera qu'un des facteurs.

Attention, ces concepts ont des applications spécifiques en fonction des aléas en jeu. Par exemple, on peut séparer en :

- Deux lignes de production contiguës si le péril redouté est le bris de machine.
- Deux bâtiments séparés sur un site si le péril redouté est l'incendie.
- Deux sites assez distants si le péril redouté est un événement naturel.
- Deux sites dans deux pays différents si le péril redouté est le mouvement social.

45 *Quelles sont les pratiques et les limites du transfert contractuel des risques ?*

Traditionnellement, on parle de transfert des risques aux assureurs. Mais qu'en est-il vraiment ? Les contrats juridiques sont un élément important de la vie des organismes et peuvent servir dans le cadre des instruments de traitement des risques, tant en réduction qu'en financement.

Par exemple, en matière de flottes automobiles, l'opérateur peut choisir d'acheter les véhicules ou de les louer (en général, pour les organismes, il s'agit de location à longue durée). Le contrat de location laisse, alors, une partie des risques liés à la propriété des véhicules à la charge du cocontractant. Dans ce cas, il y a transfert effectif de risques, c'est donc bien un instrument de réduction.

Toutefois, les contrats les plus fréquents prévoient qu'un tiers (le cessionnaire) prendra à sa charge les sinistres subis par un organisme (le cédant), ou se substituera à lui pour indemniser un tiers lésé. C'est bien entendu le cas des contrats d'assurance, mais il peut s'agir aussi de clauses de renonciation à recours ou d'accord d'indemnisation quand le cessionnaire n'est pas un assureur professionnel. Dans cette seconde situation, contrairement au cas de la flotte, le risque reste sur l'organisme, le tiers ne s'engage qu'à payer.

Les clauses contractuelles mises en place pour « traiter un risque » dans un organisme peuvent prendre des formes très différentes, et elles ne sont pas toujours rassemblées dans le chapitre « responsabilités et assurances » du contrat. Toutefois, on peut les regrouper dans les deux catégories évoquées ci-dessus.

Transfert contractuel pour réduction des risques

Un organisme externe prend en charge le risque par un transfert effectif d'activité ou de certains risques spécifiques nés de cette activité. Par exemple, externalisation auprès d'un spécialiste du traitement de surface jugé trop « dangereux », nettoyage pour des vitres d'un immeuble de grande hauteur…

Transfert contractuel pour financement des risques

Il s'agit d'un contrat par lequel un tiers, autre qu'un assureur traditionnel, accepte de prendre à sa charge les conséquences financières de certains

risques pesant sur l'organisme, en indemnisant celui-ci ou une tierce partie, selon le cas. En réalité, la mécanique est identique à celle d'un contrat d'assurance, il s'agit d'un contrat aléatoire à vocation indemnitaire. Toutefois, le partenaire au contrat n'est pas un assureur professionnel. On peut dire, en somme, que le contrat d'assurance est une forme particulière de transfert contractuel pour financement, dans lequel le cessionnaire est un assureur professionnel.

Un transfert contractuel pour réduction de risque suppose que la partie qui accepte le risque y participe physiquement par le transfert, soit d'un actif physique, soit d'une activité. Ainsi, les vulnérabilités associées se trouvent bien transférées. En réalité dans ce cas, il n'y aura aucun paiement d'indemnité, le cessionnaire entreprend, désormais, l'activité jugée trop lourde par le cédant. Le tiers gère l'activité « à risques » et en supporte toutes les conséquences en cas de sinistre, le cédant n'attend en retour aucune indemnisation.

Dans le cas de transfert pour financement des risques, il y a seulement la promesse d'une indemnisation financière si le risque se réalise effectivement, et dans les conditions et limites énoncées dans le contrat. L'organisme (le cédant) conserve bien le risque, en revanche, il perçoit une indemnisation pour les périls couverts.

Quelle que soit leur position dans un contrat, il est essentiel que les dirigeants sachent clairement distinguer si un transfert donné est pour réduction des risques et pour financement des risques. Pour ce faire, ils doivent se poser trois questions :

1. Est-ce le cessionnaire ou la cédante qui réalise, effectivement, l'opération « à risques », nous ou le cocontractant ?
2. Le cessionnaire s'engage-t-il à faire ou à indemniser ?
3. Qui supportera le risque si le cessionnaire ne remplit pas correctement son obligation contractuelle ?

46 *Le retour d'expérience est-il une nécessité pour les organismes ?*

Des accidents se produisent, et la plupart résultent d'erreurs commises par des hommes, mais toutes les erreurs ne provoquent pas des accidents. Il nous faut donc comprendre comment les accidents se produisent.

« *Ne jamais faire la même erreur deux fois* », c'est la sagesse populaire, mais le risk-manager d'une collectivité britannique (*Sunderland*) va plus loin en disant : « *Ne jamais refaire la même erreur, une fois* » ! Ce qui se cache derrière cette exigence, c'est une réalité de terrain : très souvent les catastrophes dues à l'action de l'homme résultent d'une série de petites erreurs sans conséquences prises individuellement, mais qui conjuguées débouchent sur une situation ingérable.

En quelque sorte, c'est l'inaction face à des événements indésirables, parfois mineurs, qui est à l'origine des ruptures graves. Comment les organismes peuvent-ils se prémunir contre de tels « sinistres » ? En conservant systématiquement la trace de ces accidents ou incidents, et en analysant les causes profondes pour les corriger avant que l'accident grave ou catastrophique ne survienne. C'est ce en quoi consiste le retour d'expérience.

Il peut revêtir des formes différentes et s'appuyer sur des techniques de sécurité des systèmes et de recherches opérationnelles, ainsi que le « *brainstorming* », selon la nature et la fréquence des prémices.

L'un des principaux outils est l'analyse des causes profondes, utilisée fréquemment dans les établissements de soins pour comprendre les événements « sentinelles ».

Voici résumé en dix principes, comment conduire une analyse des causes profondes après un incident (*Root cause network*, newsletters, octobre 2003 à septembre 2004) :

1. ***Décrire objectivement les événements :*** une description rigoureuse de ce qui s'est passé sans essayer de comprendre pourquoi à ce stade.
2. ***Ne pas demander « Pourquoi ? »*** : la réaction, face à un accident ou un événement indésirable, est d'interroger le « responsable » en lui demandant « pourquoi » il a agi de telle ou telle façon, ce qui le met sur la défensive. Il vaut mieux, simplement, lui demander d'expliciter ses choix.

3. ***Dégager les tendances :*** « L'événement est-il isolé ? Fait-il partie d'une tendance (à la détérioration) ? » Il faut alors regrouper les événements qui semblent de même nature.
4. ***Se préparer :*** l'analyse doit être préparée et suivre une procédure approuvée (exemple de l'entretien après tout accident dans le cadre d'un plan de gestion des risques d'une flotte automobile).
5. ***Savoir construire l'arbre des causes :*** comprendre les séquences et les enchaînements entre événements.
6. ***S'attacher aux faits, rien que les faits (pas d'hypothèse)*** : à ce stade, il ne faut transcrire que des faits, et ne pas chercher à les interpréter.
7. ***Savoir conduire des entretiens :*** respecter l'interlocuteur, et veiller aux conditions d'ouverture pour ne pas se conduire en procureur.
8. ***Faire attention aux conclusions rapides :*** il est souvent tentant de saisir la première cause, superficielle, qui apparaît, et ne pas conduire le processus jusqu'à sa conclusion.
9. ***Éviter la culture du blâme :*** l'analyse des causes profondes est une enquête, mais ni à charge ni à décharge. Elle ne vise pas à trouver un (ou des) coupable(s), mais à apprendre tous ensemble à ne pas renouveler les erreurs (culture de responsabilisation et non de bouc émissaire).
10. ***Récompenser les « enquêteurs » :*** si dans les services, les responsables font effectivement ce travail, il faut en tenir compte dans les éléments de calculs des bonus, pour souligner que cela fait partie des missions fondamentales et de la défense en profondeur de l'entreprise.

« La capacité d'un organisme à apprendre, et à transformer cette connaissance en action rapidement, est en définitive le seul vrai avantage concurrentiel », Jack Welch, ancien PDG de General Electric.

47 *Pourquoi et comment utiliser le plan de continuité ?*

La continuité est l'objectif au cœur de la gestion des risques puisqu'elle est la clé du développement de tout organisme. Encore faut-il comprendre le niveau de perturbation d'un organisme pour déterminer la réaction adéquate pour ramener le système à son équilibre.

S'il reste stable, en régime de croisière, un système complexe peut très bien fonctionner sans encadrement, tant qu'il se maintient en son point d'équilibre de « fonctionnement nominal ». Dans ces conditions, la responsabilité primordiale des cadres et des managers est de mettre en route les systèmes (mode projet) ou d'agir dans les situations de dérives, c'est-à-dire là où le système ne peut pas retrouver son équilibre par le jeu des forces naturelles et doit donc faire l'objet d'une action planifiée spécifique pour le retrouver (le même ou un nouveau), le plus vite possible. Bien souvent, il s'agit seulement d'ajustements simples (retard d'une livraison, absence d'un salarié, coupure électrique de courte durée) : c'est le quotidien des agents de maîtrise et de l'encadrement de terrain.

L'approche de la continuité proposée par les normes telles que la NF ISO 22301:2013 *Sécurité sociétale — Système de management de la continuité d'activité — Exigences* insiste sur la stabilisation du système avant d'essayer de revenir à un état d'équilibre, l'ancien ou un nouveau.

Les situations où il fait imaginer un nouvel équilibre sont évoquées dans les deux questions qui suivent : ce sont la crise et le plan de redéploiement stratégique. Les situations de retour à l'équilibre précédent, après une dérive significative, relèvent précisément de ce que l'on appelle un « plan de continuité ».

Une remarque liminaire s'impose : pour qu'il ait des chances de réussir, le plan doit être mis en œuvre rapidement, dès les premiers signes de dérive si possible, et donc au plus près de l'émergence de la perturbation. C'est donc, typiquement, une fonction des opérationnels. En fait, c'est même la prolongation naturelle de l'exercice de diagnostic des vulnérabilités conduit au niveau des centres de risques.

Il s'agit donc d'un fonctionnement alternatif qui doit avoir la rigueur d'un projet industriel et faire l'objet de mises à jour régulières, s'il doit être effectif le jour où les circonstances dictent sa mise en œuvre.

Dans les cas les plus graves, il peut débuter par une phase secours qui vise à mettre à l'abri, dans l'urgence, les personnes, la réputation et les biens (voir tableau ci-après « Les deux phases du plan de continuité »).

Pour l'essentiel, il s'agit de s'organiser de façon différente, pour permettre la poursuite de la production, avec le minimum de temps d'arrêt. Les éléments du tableau qui suit donnent une démarche. Il peut y avoir autant de plans différents pour un service donné qu'il y a de scénarios de périls graves dans une situation donnée.

Les deux phases du plan de continuité

Phase « Secours »	Au déclenchement du sinistre, il faut organiser les secours : – Protéger les personnes : > Appeler et accueillir les secours > Contrôler les sécurités > Prévenir les riverains (si nécessaire) – Protéger la réputation (communiquer en transparence) : > Autorités > Public > Partenaires économiques (clients, fournisseurs) > Actionnaires (et analyste financier) > Médias – Protéger les biens : > Gardienner le site > Organiser le sauvetage des biens
Phase « Redémarrage »	Suivant le niveau de la perturbation, il faut répondre aux questions : – Dans quels locaux ? – Avec quels équipements ? (mêmes, identiques, nouveaux ?) > Machines (performances, délais) > Outillages (remplacement, remise en état) – Avec quels approvisionnements ? > Origine > Qualités > Coûts – Logistique : > Acheminement des entrées > Conditionnement et expédition de la production **Attention, pour le redémarrage, le respect des délais (courts) est une clé essentielle du succès, d'où le souci du planning PERT**

48 *En quoi consiste la gestion des crises ?*

Certaines situations voient une dérive du système au-delà de la limite où il est possible d'assurer la continuité (voir question 47). Ces situations de rupture exigent des réactions des dirigeants pour reprendre le développement du système.

Une des difficultés de la gestion des crises réside, principalement, dans la compréhension du phénomène et la définition du moment où le processus de gestion doit être lancé. Il en va de même avec des actions plus limitées dans le temps et dans l'objectif, comme un plan de retrait pour un produit défectueux ou un plan d'urgence dans une situation où des vies pourraient être en danger. Le fait même de les déclencher est un vecteur de crise, mais ne pas les déclencher à temps peut entraîner une atteinte à la réputation bien plus grave encore.

Le lecteur intéressé par les situations de crise pourra se reporter aux nombreux ouvrages de Patrick Lagadec (voir Bibliographie). Ici, nous n'examinerons que certains aspects essentiels qui ont un impact direct sur les décisions à prendre. Il faut déjà distinguer différents cas :

- Les situations d'urgence dans lesquelles, effectivement, des actions décisives doivent être entreprises pour sauver la vie de personnes dans et hors de l'organisme (voir Infra, phase « secours » déjà évoquée à la question 47).
- Les arrêts de production qui impliquent la mise en œuvre d'un plan de continuité (voir Infra phase de « redémarrage »).
- Les situations de crise proprement dites, où l'ensemble des paramètres de gestion de l'organisme sont remis en cause ; elle perd ses repères internes et externes (au sens strict, elle « perd la boussole »).

Ce sont ces situations qui impliquent à la fois de repenser l'ensemble de la stratégie et de communiquer avec l'ensemble de parties prenantes pour reconstruire l'image (voir question 49).

Une situation de crise se caractérise, avant tout, par l'impact négatif important et durable sur les résultats financiers de l'organisme, sur ses marques et son image, ainsi que sur ses relations avec ses partenaires-clés (actionnaires de référence, fournisseurs et sous-traitants, clients), sans oublier l'ensemble du personnel et les communautés dans lesquelles il est inséré.

On peut penser, également, que pour certains organismes le monde est leur village, le phénomène de globalisation est au cœur de la crise.

Le danger est que les dirigeants pensent qu'ils pourront toujours voir venir la crise car ils s'attendent à un événement soudain et grave (risque accidentel). Dans ces circonstances, le déclenchement du phénomène s'impose pour essayer d'enrayer le phénomène ou de remédier au plus vite (par exemple, on essaie d'enrayer l'incendie, et de nettoyer au plus vite après un ouragan). Mais ce faisant, ils oublient qu'il existe plusieurs formes de crises.

Pour fixer les idées, on peut retenir trois types, y compris celui que nous venons d'évoquer :

- ***L'événement cataclysmique :*** un événement unique d'une ampleur exceptionnelle remet tout en cause et déclenche une crise (par exemple, une action immédiate par la mise en œuvre de la phase « secours », le suivi selon l'ampleur des trois autres phases évoquées).
- ***Les événements en cascade :*** une série d'événements significatifs sur plusieurs semaines, sans qu'aucun en soi ne paraisse majeur, viennent atteindre la firme en faisant des saignées répétées. Le danger est de ne soigner que les symptômes, sans aller aux causes profondes par manque de vision globale. À ce stade, c'est le plus souvent la phase « marketing de substitution » qu'il faut mettre en œuvre, dès que des signaux « sentinelles », définis à l'avance, se déclenchent. Il faudra peut-être, alors, déboucher sur un véritable nouveau projet industriel et commercial.
- ***La crise rampante :*** de petits événements, non nécessairement reliés entre eux, étalés sur plusieurs mois, finissent par entamer la confiance des parties prenantes. Le danger est que la direction estime que le traitement relève des différents opérationnels, sans besoin de réflexion stratégique. On peut essayer de mettre en place une phase « communication » pour tester le pouls des partenaires, et parfois mettre en place une réflexion encore plus en amont.

En résumé, une des principales difficultés de la gestion des crises est de mettre en place les événements « sentinelles », mesurables ou repérables, qui permettront aux dirigeants de s'impliquer dans une situation très en amont de la crise, à bon escient, avec des priorités claires, et sans être dans une perpétuelle agitation.

49 *Quand faut-il envisager un plan de redéploiement stratégique ?*

Le réflexe naturel est de penser que c'est la classe de vulnérabilités (fréquence faible et gravité forte) qui peut, effectivement, mettre en péril la survie de l'entreprise. Attention, cela dépend des modes d'évaluation retenus pour dessiner la matrice des vulnérabilités.

Ce sont les situations où l'image de l'organisme peut être endommagée de façon permanente, celles qui entraînent un risque de mort, plutôt que celles où l'impact financier est immédiat, les destructions de matériels massives. En clair, ce ne sont donc pas nécessairement des situations de sinistres catastrophiques au sens des assureurs. En revanche, c'est bien lorsque les objectifs ou les missions de l'organisme sont en jeu que s'impose la réflexion « plan de redéploiement après sinistre » et « communication de crise », qui y trouve sa justification, et même, sa nécessité financière. En effet, l'exercice doit prendre en compte, non seulement les intérêts des actionnaires, mais également ceux des salariés et même de l'ensemble des parties prenantes, présentes et futures (développement durable).

Il est essentiel de souligner à nouveau la différence entre le « redéploiement stratégique » et un exercice qui se développe rapidement en France actuellement sous le nom de « plan de continuité » (voir question 47). L'approche « redéploiement » va plus loin dans la réflexion stratégique et pourrait s'intégrer à la gestion de crise (même si ce mot est réducteur, car trop souvent employé en référence à la gestion de la période de l'événement lui-même et de ses effets immédiats). Certains praticiens ou consultants ont une approche encore plus réductrice en se limitant à la « communication de crise », développée pour diminuer l'impact de cet événement. L'exercice proposé ici est d'imaginer les situations où des mutations profondes exigent une action immédiate, replacée dans le cadre d'une stratégie proactive.

De ce fait, il va pratiquement falloir coordonner, de façon cohérente, un ensemble de mesures de prévention, de protection, des processus provisoires, de recours à la sous-traitance et aux achats, une logistique de redondance et les sources de financement qui permettront à l'entreprise de rebondir et d'atteindre ses objectifs stratégiques quelles que soient les circonstances. Dans certaines hypothèses extrêmes, il faudra même

littéralement redéployer l'organisme vers de nouveaux marchés, voire de nouvelles activités. Si sa mise en œuvre dépend, pour l'essentiel, d'événements hors du contrôle des dirigeants, le plan de redéploiement doit faire l'objet d'une réflexion systématique et globale, et être minutieusement pensé, mis à jour régulièrement en s'appuyant sur une plateforme analytics et des informations (*big data*) qui permettent effectivement d'éclairer le futur. Le plan de redéploiement après sinistre est scindé en quatre phases complémentaires, à savoir :

- Phase 1 : Secours (ou urgence).
- Phase 2 : Stratégie de substitution.
- Phase 3 : Redémarrage.
- Phase 4 : Communication institutionnelle (post-crise).

Le plan « Stratégie de substitution » est un processus de réflexion plutôt qu'un plan défini *a priori*. En effet, la situation critique ou de rupture qui va justifier son activation ne peut pas être anticipée avec précision, et donc la réaction adéquate ne peut être « planifiée ». Toutefois, cet exercice de « *brainstorming* » prépare l'équipe de direction à affronter l'inattendu, la surprise, équipée qu'elle est des informations indispensables pour prendre des décisions rationnelles et armée d'un esprit d'équipe positif qui résistera au temps des ruptures.

Mais, avant même le temps de crise, inéluctable aujourd'hui, on peut tirer de l'exercice une valeur ajoutée immédiate : les dirigeants sont amenés à réfléchir, à tout moment, au meilleur usage des ressources disponibles et à saisir les opportunités tout en installant les systèmes « sentinelles » qui permettent de capter les signaux faibles, souvent seuls annonceurs de processus de rupture en cours.

Bien entendu, dans toutes les situations où la phase 2 se conclut par une reprise des opérations, « *business as usual* », le plan de redéploiement se réduit à un plan de continuité, finalement constitué des phases 1 et 3 du plan de redéploiement. En effet, si l'organisme n'est pas mis hors jeu dans ses activités et marchés actuels, c'est alors la phase 3, aux mains des propriétaires de risques opérationnels, qui devient vitale. Il s'agit là d'un véritable projet industriel qui doit être détaillé et mis régulièrement à jour. C'est sur le terrain que cette opération doit se faire, ce sont donc les responsables des centres de risques eux-mêmes qui doivent les développer et les mettre à jour, à l'occasion du processus de diagnostic des vulnérabilités et de représentation matricielle des risques (cartographie des risques).

50 *Comment traiter les personnes-clés ?*

La problématique a été abordée précédemment (voir question 26) par le biais de la définition d'une personne-clé. En résumé, c'est une personne ou un groupe de personnes dont les compétences sont incontournables pour le fonctionnement normal de l'organisme. Leur identification est la première étape du traitement. Dans tous les cas, il faut s'interroger en premier sur la nature incontournable de ce « statut ». Dans ces conditions, les moyens de traitements sont de deux natures : éviter qu'une personne ne devienne « clé » ou veiller à la santé et à la continuité de service de la personne-clé.

Éviter les personnes-clés

Au sein des organismes, les personnes-clés peuvent être générées par des erreurs de gestion du personnel ou de procédures, en particulier de la rétention d'information par une personne qui, consciemment ou non, se rend incontournable pour protéger son emploi ou sa carrière.

L'exemple le plus classique est celui de l'informatique dans une entreprise de taille modeste. Il est économiquement impossible de doubler un tel emploi, et la direction devient dépendante du responsable pour le fonctionnement de l'entreprise. Il faut donc veiller à ce qu'une documentation précise soit mise en place et sans doute auditée, périodiquement, par un spécialiste extérieur qui pourra certifier être en mesure de procurer une solution de continuité si le responsable n'est plus disponible. Dans les entreprises plus importantes, il faut un adjoint capable de prendre la relève : ce qui impose, là encore, une documentation précise.

Le réseau commercial peut, aussi, conduire à des situations où un représentant ou un visiteur qui développe son chiffre d'affaires finit par détenir une part trop importante du volume global de la société : il faut des règles de scission de territoire pour éviter ce genre de situations, de recrutements d'adjoints pour éviter d'être dépendants par rapport à quelques individus. Tout ceci doit être prévu, et rémunéré, dans le cadre des contrats de travail des commerciaux concernés. La question peut se poser en termes de « distributeur indépendant », en particulier s'il s'agit d'une personne unique. En matière technique, la formation croisée peut permettre à des salariés de remplacer des absents, au pied levé, sans engendrer de pertes significatives.

Veiller à la continuité du service de la personne-clé

La perte d'une personne-clé peut résulter de la démission, de la retraite, du décès ou de la maladie, sans parler des congés qui doivent être suivis, de manière à éviter que les mêmes compétences soient absentes simultanément.

- ***Démission :*** ce péril est d'autant plus lourd, que la compétence perdue va, en général, alimenter la concurrence. Si une personne-clé a été détectée parmi les salariés, elle doit faire l'objet d'une attention particulière des ressources humaines pour garantir que son statut et sa rémunération restent attractifs par rapport au marché, sans pour autant que l'entreprise devienne l'objet d'un chantage.
- ***Retraite :*** même si l'âge de la retraite n'est plus un couperet, pour l'essentiel, on sait qu'un collaborateur partira vraisemblablement à la retraite entre 60 et 65 ans. Il y a donc un risque sur la date, mais on peut s'y préparer en développant des formules pour garantir la formation de successeurs.
- ***Maladie/accident :*** le suivi médical et le style de vie des collaborateurs ne sont pas du ressort de l'employeur, mais de la sphère de la vie privée. Toutefois, les valeurs et la culture de l'entreprise peuvent conduire les collaborateurs à adopter des styles de vie plus sains. Dans le cas de mise en place de couvertures accidents, l'assureur pourra interdire la pratique de certains sports pour l'application de la garantie, ce qui pourra induire une conduite « plus sûre », sans intervention directe de l'employeur.
- ***Décès :*** le décès peut être à la suite d'une longue maladie (les mesures prévues pour la retraite peuvent, alors, s'appliquer) ou d'un accident brutal (dans ce cas, il faut pouvoir remplacer rapidement les compétences, en ayant identifié des successeurs potentiels au sein de l'entité ou des sources externes : associations professionnelles, chasseurs de tête spécialisés…).

On le voit, quel que soit l'aléa redouté, il est important de prévoir des plans de succession pour tous les postes-clés d'un organisme, et à tout le moins, des procédures à déclencher immédiatement si la situation se produit.

Dans tous les cas, et pour les PME/PMI en particulier, la souscription d'une assurance « personne-clé » pour financer la transition et la perte de revenu peut être essentielle pour la survie de l'organisme.

51 *Peut-on rentabiliser la réduction des risques ?*

Que l'organisme soit à but lucratif ou non, l'efficacité économique est toujours au cœur de ses préoccupations. Il doit donc légitimement se poser la question de la rentabilité des investissements consentis pour réduire les risques auxquels il est exposé.

Toutefois, l'approche est très différente selon que l'on parle de risques de fréquence élevée, de fréquence moyenne, ou de fréquence très faible, car les conséquences financières mesurables pour les deux premières classes ne le sont pas pour les risques d'impact exceptionnel, mais qui ont une probabilité très faible de survenir (faible vraisemblance).

Pour les risques de « fréquence », il est possible de mesurer le coût annuel des sinistres et de suivre son évolution à la suite des programmes de réduction mis en œuvre. Dans ces conditions, la rentabilité de l'investissement peut être calculée sur les projections de flux de trésorerie et les méthodes d'actualisation s'appliquent comme à tout autre investissement. Par exemple, si une entreprise utilise un parc automobile d'une centaine, ou plus, de véhicules et dispose d'une statistique sinistre sur trois ans, elle peut envisager de mettre en place un programme de formation des chauffeurs à la conduite défensive.

Les coûts de la mise en place du programme et de la formation peuvent être projetés avec précision, et la réduction du nombre de sinistres et leur gravité moyenne peuvent être appréciées par analogie avec les résultats obtenus sur des flottes comparables, en s'appuyant sur une analyse de la sinistralité passée. Il est possible de faire une évaluation financière du projet et de vérifier, ensuite, les résultats. La stabilité relative à la loi des grands nombres permet de vérifier les résultats sur des périodes de 18 à 24 mois.

Dans le cas des risques moins fréquents, comme l'incendie, le temps n'est plus où un système de détection et d'extinction (sprinklers) se rentabilise en deux ans par la réduction de cotisation d'assurance consentie par l'assureur. Il faut se placer sur des horizons à 10/20 ans pour évaluer le résultat, mais les entreprises ont des difficultés à se placer sur des horizons aussi longs.

Cependant, pour les risques moyens dont la réalisation s'équilibre sur ces durées, en combinant des instruments de financement internes

et la réduction des risques qui protège « l'assureur-assuré », on peut justifier financièrement les choix, à l'aide de modèles mathématiques qui s'apparentent à ceux développés et utilisés dans le monde de l'assurance et de la réassurance.

Il reste la question des risques les plus graves, qui ne se produisent « jamais », mais qui sont dévastateurs en cas de survenance. Dans ce cadre, il faut définir un autre concept, introduit à l'origine par les auditeurs canadiens mais largement répandu aujourd'hui : la résilience. C'est la capacité de l'entité à surmonter toutes les situations de catastrophes auxquelles elle pourrait être confrontée, et à rebondir ensuite.

Pourtant, s'il est difficile d'affecter une valeur financière à cette résilience, elle est devenue, de fait, un concept important à la lumière des obligations légales de communication en matière de gestion des risques. Il reste aux auditeurs et aux analystes financiers à préciser ce concept, pour le rendre repérable ou mesurable.

Toutefois, les risques n'ont pas que des conséquences financières, mais également un impact sur les hommes et sur l'environnement, qui n'est pas toujours immédiatement traduisibles en termes financiers. Il s'agit d'un impact sur les valeurs affichées par l'organisme : l'éthique qu'il défend.

Les questions du développement durable ou soutenable et de l'environnement se rattachent à cette problématique. Par ailleurs, il ne faut pas oublier que certains éléments de réduction des risques relèvent de la conformité légale et réglementaire. On peut citer, en particulier, les questions d'hygiène et de sécurité, et les éléments qui mettent en cause la sécurité et la santé du public. Pour ce qui relève de la conformité, les coûts de réduction des risques doivent être inclus dans les frais généraux incompressibles pour gérer l'entreprise et il n'est pas nécessaire d'en chercher la rentabilité propre.

Bien entendu, *in fine*, c'est la réputation de l'organisme qui est en jeu, et mesurer l'impact de risques mal maîtrisés sur la confiance des parties prenantes est sans doute une gageure. En revanche, l'effondrement d'une réputation met clairement une entreprise hors jeu, avec pour conséquence la perte totale du potentiel futur, voire la possibilité d'agir en tant que dirigeants pour le personnel de direction.

6
Le financement des risques

52 *Pourquoi faut-il financer les risques ?*

Longtemps, le terme de « financement des risques » n'a recouvert que l'achat de couvertures d'assurance traditionnelles, dans un marché cloisonné et de nature oligopolistique où la multiplicité des opérateurs cachait mal l'entente tarifaire organisée par la profession, avec la bénédiction des pouvoirs publics. En effet, elle garantissait la solvabilité ultime des assureurs, sans représenter des charges mettant en jeu la pérennité des entreprises. L'ouverture des frontières, les regroupements des entreprises de tous secteurs et l'évolution rapide de l'environnement dans lequel elles opèrent ont profondément modifié le paysage.

Il s'agit toujours, avant la survenance de tout sinistre, d'organiser les financements qui viendront compenser les pertes après leur survenance, que ces financements soient effectivement mis en place avant l'événement ou que l'organisme envisage des solutions qu'il activera après. Toutefois, si l'assurance répondait parfaitement à la compensation de la disparition d'actif dans un monde stable, tel n'est plus le cas aujourd'hui.

La part des accroissements de passif (engagements de responsabilité de plus en plus lourd) d'une part, et la nécessité d'approcher la stratégie financière de façon beaucoup plus agressive (le bilan ne représente plus la réalité de la valeur économique d'une entreprise avec des capitalisations boursières atteignant ou dépassant 20 ou 30 fois l'actif net) d'autre part, exigent une révision en profondeur des stratégies de financement des risques qui doit dorénavant être intégrée à la stratégie financière globale de l'organisme.

Pour accompagner ce mouvement, le monde du financement des risques est devenu beaucoup plus complexe avec l'apparition de « nouveaux instruments » au gré des plans marketing des grands courtiers et de certains assureurs spécialisés, anxieux de se créer des niches, au moins provisoirement.

Cependant, la finalité de ces instruments est toujours de lisser les résultats dans le temps, de réduire les fluctuations de bénéfices, voire de croissance, que les marchés boursiers, auxquels les dirigeants des grandes entreprises doivent être attentifs, n'aiment pas et sanctionnent en réduisant le multiple, donc le cours de l'action, pas plus que les banquiers que les dirigeants de PME doivent convaincre pour obtenir les financements indispensables à leur croissance.

À cet effet, plus que de savoir d'où vient la trésorerie au moment du sinistre, une question préalable doit être posée : doit-on préfinancer les pertes exceptionnelles ou pourra-t-on les postfinancer ? Dans tous les cas où le « postfinancement » ne met pas en cause la survie de l'entreprise, cette énergie financière préservée alimentera le développement. Toutefois, il faudra y recourir dans le cadre d'une réflexion prudentielle (voir question 53). Dans la plupart des situations, il faudra mette en place un préfinancement et dans ce cas, deux questions cruciales sont à se poser quel que soit l'instrument retenu :

- Y a-t-il transfert de la volatilité sur un tiers, ou qui supporte la volatilité du résultat : en d'autres termes, du point de vue de l'entreprise, est-ce que je connais le coût de cet instrument *a priori* (avant tout sinistre, avant le début de l'exercice) ou *a posteriori* (après la fin de l'exercice lorsque le bilan des sinistres peut être dressé) ?
- Quel est le prix payé pour ce transfert : c'est la notion du chargement (en assurance) ou des coûts de frottement (pour les instruments financiers) ?

Tout actif, toute activité, se décompose ainsi en deux éléments de valeur : le fondamental (la valeur actuelle de l'espérance mathématique de flux net de trésorerie sur la durée de vie de l'actif ou de l'activité) et la valeur du risque. Pour chaque dirigeant, les questions deviennent : « *Quels sont les risques que je conserve dans mon portefeuille de risques pour bâtir le programme optimal pour mes actionnaires ?* » et « *Quels sont ceux qu'il est plus économique de transférer ?* » Il n'y a pas de réponse universelle.

À tout moment, il faut arbitrer entre son propre appétit de risque et celui du marché. Dès lors, on comprend qu'entre le « tout rétention » et le « tout transfert », il y a une échelle sur laquelle chaque organisme doit se positionner avec un cocktail d'instruments pour obtenir le « niveau confortable », où l'appétit de risque des dirigeants est à l'équilibre avec le coût marginal du transfert.

Dans la pratique, les PME/PMI ainsi que les entreprises de taille intermédiaire (ETI) s'appuient largement sur l'assurance pour le financement de tous les risques que ce marché est susceptible de couvrir. Toutefois, tout chef d'entreprise doit pouvoir évaluer les instruments nouveaux, souvent sophistiqués et complexes à mettre en œuvre, mais dont les mécanismes sont faciles à comprendre et dont les avantages peuvent être intégrés sous des formes simplifiées, même dans des programmes d'assurance pour des entreprises de taille modeste.

53 *Faut-il financer le sinistre avant, ou peut-on le financer après sa survenance ?*

Les deux objectifs fondamentaux de la gestion financière d'entreprise sont la solvabilité et la rentabilité.

L'optimisation de la rentabilité passe toujours par le fait de garder le maximum de flexibilité dans l'utilisation des fonds disponibles. En effet, les fonds qui sont « gelés » en liquidités ou actifs à court terme, ou versés comme charge à des tiers (cotisations d'assurance, par exemple) ne sont plus disponibles pour financer les investissements productifs de l'organisme. Ce qui amène la question suivante, décomposée en deux temps :

- Quelles vulnérabilités doivent s'accompagner de la mise en place d'un préfinancement pour éviter la faillite lors de la survenance ?
- Quelles vulnérabilités peuvent être financées après la constatation du « sinistre » sans mettre en péril l'organisme ?

La mise en place de préfinancement s'impose, si les flux de trésorerie négatifs générés par un sinistre majeur ou une série de sinistres rapprochés :

- sont importants par rapport à la trésorerie courante de l'organisme ;
- doivent être disponibles rapidement.

Dans ce cas, il faut qu'un mécanisme ait été mis en place avant la survenance de tout sinistre pour garantir la disponibilité immédiate de fonds et éviter le risque de défaillance de trésorerie.

Illustrons cet aspect avec des cas concrets : si l'unique usine d'une PME/PMI disparaît au cours d'un incendie, elle se trouve très vite sans rentrées, en supposant qu'elle a préservé sa comptabilité et que ses conditions de vente sont soixante jours fin de mois, au bout de deux mois. Par ailleurs, elle va devoir reconstruire le plus rapidement possible, voire mettre en place des mesures exceptionnelles pour continuer à livrer ses clients. Sa trésorerie disponible sera rarement de plus de deux ou trois mois, et elle ne sera en mesure de poursuivre que si un « investisseur » ou un banquier généreux lui fait confiance pour repartir.

En résumé, le risque incendie doit être préfinancé, en pratique, par l'achat d'une couverture d'assurance dans ce cas.

Dans tous les autres cas, le préfinancement est sans objet et réduit inutilement le rendement. Par exemple, un fabricant automobile peut être conduit à faire des rappels de véhicules pour réparer un défaut constaté. Ces rappels sont devenus des « processus de gestion usuels » chez la plupart des constructeurs, donc le coût éventuel doit être intégré dans le budget, mais ne doit pas nécessairement faire l'objet d'un financement exceptionnel. Dans la plupart des cas, la trésorerie courante pourra absorber les débours liés au rappel.

Certains événements exceptionnels ne se prêtent pas à un préfinancement dans des conditions économiques acceptables. L'exemple du tremblement de terre au Japon vient à l'esprit. Assurer la totalité du parc industriel ou provisionner, à l'actif, les sommes considérables pour reconstituer un outil de production pourrait mettre hors compétition un producteur japonais. S'il est engagé dans une politique de croissance et d'investissements vigoureux, il doit y engager tous ses fonds disponibles : si le sinistre survient, le flux de fonds, à moyen terme, pourra être provisoirement détourné pour reconstruire une usine prioritaire. Dans ce cas, ce n'est pas la trésorerie courante qui interviendra, mais le tableau de financement.

De même, les sinistres « responsabilité civile produits » peuvent être de résolution lente (plusieurs années) et, dans ce cas, la trésorerie pour les financer pourra être dégagée sur la durée. Bien entendu, il reste la question de l'impact sur le résultat !

Les responsables d'ETI ou de PME/PMI réagiront en pensant que cette approche ne les concerne pas et ne s'appliquent qu'aux grands groupes multinationaux. En fait, la question peut être envisagée à la lumière de leur capacité financière, et le « postfinancement » se ramènera chez eux à un choix judicieux de franchises pour contenir leur budget assurances tout en ayant des couvertures significatives quand leur survie est véritablement en jeu. Certains sinistres de gravité limitée (vol dans les voitures, bris de glace sur les véhicules et dans les bâtiments, les petits équipements…) pourront peut-être être exclus des contrats d'assurance, dans la mesure où leur remplacement en cas de dégradation ou de disparition pourra relever d'un budget « entretien ou maintenance ».

54 *Que choisir : un financement interne ou un financement externe ?*

C'est la seconde question qu'il faut se poser, quelle que soit la réponse à la question précédente sur le moment où le financement doit être effectivement disponible.

À chaque fois que l'on fera appel à un financement externe, ce sera pour atténuer l'impact du risque sur la volatilité des flux de trésorerie et des résultats. Mais la conséquence est toujours de diminuer les capitaux disponibles, à moyen et long terme, pour les investissements rentables.

En revanche, le recours à un tiers, le cessionnaire, pour supporter la volatilité des coûts des sinistres s'accompagne d'une rémunération légitime qui vient amputer le rendement à long terme de l'entité ainsi protégée, la cédante.

Pour reprendre le terme consacré de la profession, la rétention, le financement interne, est toujours plus économique à long terme que l'appel à un tiers, le transfert, pour autant que l'entité ait établi un profil de risques précis et envisagé les situations extrêmes : les professionnels font parfois appel à la notion de « trésorerie en risque » pour évaluer le maximum de pertes possibles et/ou probables sur le portefeuille global d'opportunités et de menaces que représente l'entité.

Effectivement, pour trouver le meilleur équilibre entre rétention et transfert compatible avec l'appétit de risque des responsables, il faut une approche globale, qui débouche sur la mise en place de différents instruments dans le cadre d'un programme de financement des risques cohérent et pour le coût minimum pour un niveau de risque accepté.

On retrouve la notion de frontière efficace définie pour une entreprise donnée, comme celle qui réunit les portefeuilles de projets optimisant le rapport risque/rendement.

Le financement des risques ne peut pas être traité en dehors de la stratégie financière globale de l'entreprise qui en définit les contraintes et les objectifs. Une fois les éléments stratégiques retenus, il revient alors au risk-manager, en collaboration avec les services de consultants externes, de mettre en forme sur le plan technique et opérationnel le cocktail d'instruments répondant au plus près à ces éléments.

Bien entendu, cette mise en forme passe par la souscription de contrats et le respect de clauses contractuelles relevant des opérations courantes : de ce fait, les conseils juridiques de l'entité doivent être associés à ces choix.

En ce qui concerne les transferts contractuels à des partenaires non spécialisés, ni institution financière ni assureur, il est clair que le rôle des acheteurs et des vendeurs est essentiel pour comprendre quelles sont les pratiques habituelles des marchés dans lesquels ils opèrent. À vouloir trop se décharger de risques sur un partenaire des pratiques courantes, de façon exorbitante, on risque de se priver d'une source d'approvisionnement ou d'un débouché essentiel. Là encore, la direction juridique doit être associée, de bout en bout, à ces transactions.

La question, posée comme une alternative simple, doit donc être décomposée sur le plan technique pour passer en revue toutes les possibilités et s'assurer du choix le plus judicieux à court, moyen et long terme. Bien entendu, les conditions du marché de l'assurance, la disponibilité et le coût des couvertures offertes, sont des éléments essentiels. Parfois, les entités sont contraintes de pratiquer la rétention de vulnérabilités qu'elles auraient préféré transférer, et cela a des impacts sur d'autres arbitrages.

Enfin, entre le tout transfert et la rétention totale, il y a une gamme d'options, appelées souvent hybrides, qui présentent des caractéristiques des deux : l'entreprise conserve les sinistres de fréquence, quitte à les faire gérer par un tiers, et transfère les sinistres dépassant ses capacités de trésorerie ou d'absorption des pertes, quitte à conserver le risque catastrophique, non assurable ou à des tarifs prohibitifs, mais en mettant en place des moyens de prévention et de protection pour ramener la vraisemblance de leur survenance à un niveau si faible que les « parties prenantes » peuvent vivre avec.

Pour illustrer les remarques qui précèdent, les principaux instruments de financement des risques par transfert et par rétention sont décrits, brièvement, dans un tableau (voir question 55).

55 *Qu'est-ce qu'un instrument de financement des risques ?*

Un instrument de financement des risques, qu'il soit de « pré » ou de « post » financement, est un moyen mis en place avant la survenance de tout événement, afin de prévoir la disponibilité de la trésorerie nécessaire pour compenser les pertes subies par un organisme ou pour indemniser les tiers lésés de son fait, au moment où la compensation doit effectivement intervenir. Pour qu'un instrument soit entièrement défini, il faut pouvoir répondre à cinq questions :

- Comment a-t-il été effectivement planifié ?
- D'où viendra la trésorerie au moment opportun ?
- Comment sont traités les mouvements comptables associés, aussi bien au niveau des charges que des produits ?
- Quelles sont les conséquences fiscales éventuelles ? (En particulier se pose la question de la déductibilité fiscale des charges liées à cet instrument.)
- Qui supporte le risque financier, c'est-à-dire la volatilité du résultat (provoqué par la sinistralité encourue) ?

Il y a une question subsidiaire pour laquelle nous nous efforçons de donner des éléments de réponse sur l'ensemble de questions de cette partie financement des risques : *« Dans quelle situation est-il judicieux d'utiliser tel ou tel instrument, ou telle ou telle combinaison de financement des risques ? »*

Bien entendu, de nombreux paramètres sont à prendre en compte pour y répondre. On peut citer les principaux : nature du portefeuille de vulnérabilités, stabilité des flux de trésorerie associés aux activités normales de l'organisme, structure de financement permanent, et objectifs financiers stratégiques.

À ce stade, il suffit de donner un tableau recensant les principaux instruments de financement des risques, tout en soulignant les limites de l'exercice : les partenaires des « assurés professionnels » dans ce domaine, et tout particulièrement les grands courtiers internationaux, ont une imagination débordante et inventent sans arrêt de nouveaux « produits ». Toutefois, le plus souvent, ce sont des variantes des principaux instruments cités dans le tableau ci-après.

Les instruments de financement des risques

Instruments de financement	
Les moyens de financement exceptionnels conçus pour apporter la trésorerie nécessaire pour compenser les pertes et atténuer l'impact sur les résultats par-delà les efforts de réduction entrepris pour limiter la réalité de l'impact des vulnérabilités sur l'organisme.	
Instrument	**Caractéristique**
Rétention par traitement courant	Payer les dommages au fur et à mesure (trésorerie courante) et les comptabiliser comme charge courante
Rétention par provisions non financées	Reconnaître les besoins en financement au niveau du compte de résultat
Rétention par provisions financées	Outre la provision comptable, conserver des actifs financiers quasi liquides
Rétention par recours à l'emprunt	Mettre en place une ligne de crédit à n'utiliser qu'en cas de sinistre
Rétention par captive d'assurance ou de réassurance	Créer ou adhérer à une société d'assurance ou de réassurance réservée à un assuré ou un petit nombre d'assurés
Transfert contractuel pour financement des risques	Trouver un partenaire industriel ou commercial pour assumer à votre place les conséquences financières des vulnérabilités
Transfert à un assureur	Souscription d'un contrat d'assurance
« Hedging » ou arbitrage	Recours à un tiers ou un marché pour compenser des risques contradictoires comme achat de devises à terme

56 *Que penser de l'assurance et de l'autoassurance ?*

Dès que l'on évoque la gestion des risques, la plupart des interlocuteurs pensent immédiatement « assurances », tant cet instrument de financement est resté synonyme du métier.

En fait, il est vrai que la risk-management moderne est né aux États-Unis, dans les années 1960, de la prise de conscience que les coûts liés à l'achat de couverture étaient un poste fixe important, en particulier en matière d'accidents du travail, et que les transactions d'assurance étaient en outre entachées d'un paradoxe.

Alors que les trésoriers mettaient en œuvre la trésorerie « zéro », avec une batterie de mesure pour faire payer le plus vite possible les clients, et payer le plus tard possible les fournisseurs, l'assureur est payé en début d'exercice pour une prestation dont l'essentiel des coûts ne se concrétisera parfois que deux ou trois ans plus tard (responsabilité civile produit et accidents du travail).

C'est au travers du recrutement d'un professionnel de l'assurance que le risk-management a vu le jour. De fait, l'assurance est l'instrument de financement des risques le plus répandu.

Face à une situation à risques, le réflexe recommandé est de considérer le recours à l'assurance comme le premier et le dernier instrument : le premier, car lorsqu'on ne sait rien des risques, l'achat d'assurance est le seul traitement « immédiat » possible et le dernier, car c'est toujours le plus cher, d'autant plus cher que le travail de diagnostic préalable et de réduction n'a pas été effectué.

Pour tous les risques « non systémiques », les risques mutualisables par la loi des grands nombres, et pour lesquels il existe une demande solvable, on peut penser qu'un opérateur (mutuelle ou société d'assurances) se constituera pour offrir des couvertures, en organisant la mutualité de façon économiquement efficace pour toutes les parties.

Pour le financement interne, le terme utilisé est celui de rétention, toutefois, de nombreux ouvrages retiennent celui d'autoassurance, qui porte une contradiction dans les termes, car pour qu'il y ait assurance, il faut qu'il y ait mutualisation avec des entités externes.

Il existe une forme de rétention « formelle », dans laquelle l'entité tient une comptabilité « sinistre » équivalente à celle d'un assureur.

Dans ce cas, le terme « autoassurance » peut être utilisé, mais il prête à confusion, car il n'est le résultat d'aucun mécanisme de partage, sauf dans le cas où un groupe possède un nombre important de filiales y participant.

Pour la clarté du débat entre assurance et rétention, voici quelques remarques de bon sens.

Les éléments favorables de la souscription d'assurances :

- Survie ou niveau tolérable d'incertitude.
- Valeur ajoutée des services annexes (gestion des sinistres, visite de prévention…).
- Obligations légales et réglementaires.
- Lissage des pertes dans le temps et dans l'espace (l'assureur compense la volatilité du coût des sinistres).
- Impact fiscal favorable (les cotisations d'assurance sont des charges fiscalement déductibles).
- Coût perçu comme faible par rapport à la rétention.
- Protection des actionnaires minoritaires dans le cadre de « joint-venture » ou de projets complexes.
- Besoin de trésorerie/impact sur la cotation crédit (l'assurance est perçue comme un « actif potentiel », lors du sinistre l'indemnité de l'assureur revient à une injection de capitaux propres).

Les éléments défavorables à la souscription d'assurances :

- Mauvais rendement de l'investissement mesuré en rapport cotisation/sinistre, en particulier si l'entité a peu de sinistres et un ratio sinistres à prime faible.
- Coût de transaction élevé (les frais administratifs et de commercialisation peuvent atteindre de 20 à 40%).
- Solvabilité de l'assureur (la cotisation est acquittée en début de période, l'assureur sera-t-il présent quand l'indemnité sera due ?).
- Bonne foi de l'assureur et du réassureur.
- Tous les risques ne sont pas assurables.
- Cycle et variabilité des marchés de l'assurance (l'assurance est soumise à des cycles qui font que, parfois, les couvertures ne sont pas/plus disponibles ou à des coûts prohibitifs).

57 *Quels contrats d'assurance souscrire pour « rassurer » le dirigeant d'une PME/PMI ?*

Pour un dirigeant de PME/PMI, l'assurance est un monde complexe auquel il n'a pas le temps de s'intéresser, toujours trop chère quand il faut payer les cotisations, souvent décevante lorsque l'indemnisation n'est pas à la hauteur du préjudice économique subi ou perçu.

Pour l'assister, il dispose d'un certain nombre de prestataires de services externes (voir questions 71 à 75), mais il est bon qu'il ait une compréhension minimum des couvertures « standards » qu'il doit souscrire et de leurs principales caractéristiques.

Pour simplifier la présentation, nous allons nous limiter aux assurances dites IARD (incendie, accident, risques divers), en laissant de côté les couvertures pour le personnel (évoquées brièvement aux questions 23 et 25) : elles sont généralement plutôt du ressort des ressources humaines.

Il ne s'agit pas, ici, de rédiger un traité d'assurance, mais de rappeler quelques points essentiels. Deux contrats sont essentiels : le premier pour protéger les actifs physiques et les sources de revenus de l'organisme, le second est pour le passif, en finançant les dommages provoqués aux tiers.

- Multirisque industrielle (tous risques) :
  - Volet dommages : il couvre le patrimoine physique pour les périls, tels que : incendie et risques annexes, dégâts par liquide, bris de machine. Attention à bien vérifier les capitaux déclarés et à la description des lieux et des activités.
  - Volet pertes consécutives (pertes d'exploitation, frais supplémentaires ou frais exceptionnels) : la remise en état des lieux peut être longue, et la « reconquête » des marchés encore plus longue. Pour survivre, l'entreprise a besoin de flux de trésorerie pendant toute la période. Attention, l'indemnisation ne suffira pas à garantir la survie sans un plan de continuité adapté (voir questions 47 et 48).
- Responsabilités civiles : il s'agit de tous les engagements de l'organisme à l'égard des tiers, du fait des dommages qu'ils subissent et qui sont la conséquence de ses activités :
  - RC exploitation : les dommages subis dans les locaux ou directement du fait de l'activité.

- RC produits/après travaux : les dommages provoqués après son départ par les travaux effectués ou les produits livrés.
- RC professionnelle : les dommages financiers résultant d'une prestation intellectuelle déficiente. Attention, en France, il s'agit des « pertes immatérielles non consécutives ». En pays anglo-saxons, on retient la notion de pertes financières.

- Flotte automobile : parfois, le loueur propose des solutions. Il faut vérifier si sont couverts ou non :
  - La responsabilité civile (à l'étranger vérifier les montants).
  - L'incendie et le vol.
  - Les dommages aux véhicules (en cas de collision avec un tiers identifié ou une couverture dite « tous risques »).
- Transport : le transporteur a des obligations limitées à l'endroit de ses clients. Pour ne pas être en difficulté en cas de transports de marchandises chères, en particulier, il faut envisager de souscrire une police « tous risques » (à aliments, par voyage, ou à l'année sur le chiffre d'affaires).
- Autres contrats :
  - RC mandataires sociaux : la couverture des erreurs dans les actes de gestion et qui ont des conséquences négatives pour les porteurs de capitaux et autres parties prenantes.
  - Personnes-clés : évoquées à la question 50.
  - Assistance : en particulier dans le cas de salariés se déplaçant à l'étranger.
  - Affacturage ou assurance-crédit pour garantir une rentrée rapide des factures clients.

58 *Comment souscrire des contrats d'assurance ?*

La souscription et le renouvellement des contrats d'assurance représentent une partie importante des activités d'un gestionnaire des risques, quel que soit l'organisme dont il a la charge. De plus, il doit assurer la gestion des affaires courantes dans son service. Pour atteindre ces deux objectifs, il doit veiller à fournir, aux représentants des assureurs potentiels, autant d'informations que possible sur ces risques, et ce, sous une forme qui présente aussi un intérêt dans le cadre des activités habituelles d'un organisme en matière de gestion des risques.

Il est donc impératif que la souscription des contrats d'assurance fasse l'objet de procédures clairement définies, en accord avec la direction de l'organisme et dans des conditions de transparence qui ne permettront que le choix du meilleur rapport qualité-prix, sans laisser trace à des présomptions de « favoritisme ».

La pression de l'opinion publique et des consommateurs, les attentes des partenaires ne laissent plus le choix aux dirigeants. Ils doivent définir une politique de gestion des risques visant, au-delà de la protection des actifs de l'organisme, la sécurité physique et financière de chacune des parties prenantes, personnes physiques ou morales, dont la vie est influencée par l'organisme.

Ce phénomène se reflète dans la montée en puissance des couvertures des pertes de revenus et des responsabilités nombreuses et variées qui pèsent sur les organismes. Les contrats d'assurance souscrits devront donc faire l'objet d'une réflexion approfondie, tant au niveau des couvertures, que des plafonds de garanties par événement et par an, ainsi que la sélection de franchises appropriées. En effet, l'enveloppe budgétaire consacrée aux cotisations d'assurances, nécessairement limitée, conduira à des arbitrages parfois douloureux.

La tentation pourrait donc être de « minimiser » les risques par des descriptions ou des représentations « améliorées » pour obtenir des tarifications avantageuses, voire tout simplement, pour les risques difficiles, un placement.

Toutefois, il convient de rappeler que tout contrat d'assurance est conclu en toute bonne foi ou, en latin, un contrat *uberrimae fidei*. Cette expression signifie que les parties au contrat, et en particulier

l'assureur, sont en droit d'attendre de leur cocontractant : la vérité et la sincérité dans toutes les déclarations faites au cours de la négociation préalable au contrat. En particulier l'assuré s'engage à divulguer toutes les informations qui pourraient raisonnablement présenter un intérêt pour la définition des termes et conditions du contrat.

Ainsi, en vertu du principe de déclaration, chaque souscripteur d'assurances est dans l'obligation de communiquer, à l'assureur et à ses représentants, toutes les informations qui pourraient, éventuellement, avoir des conséquences ou affecter les choix faits par l'assureur quant à sa décision d'assurer ou non le souscripteur, ainsi que les conditions de cette assurance. En France, cette obligation est sanctionnée par le Code des assurances et les décisions de justice : en cas de fausse déclaration « involontaire », c'est la déchéance, la non-couverture du sinistre, mais en cas de fausse déclaration « volontaire », c'est la nullité du contrat !

Les organismes se posent souvent la question de savoir à quel rythme il convient de remettre ses contrats « sur le marché », c'est-à-dire mettre en concurrence les intermédiaires et les assureurs en place. Il n'y a pas de réponse absolue. Il faut rester à l'écoute du marché, savoir entendre ceux qui font des offres, mais se rappeler que la qualité d'un assureur et d'un intermédiaire s'apprécie dans le temps. La relation de confiance qui s'établit peut se révéler essentielle en cas de sinistre difficile. Toutefois, il y a également un danger à s'installer dans une relation trop confortable.

Si l'on doit avancer un rythme « raisonnable », il y a toute raison de penser que, sauf incident majeur précipitant les échéances, le « quinquennat » est un bon compromis, tout en rappelant que pour ce qui relève des marchés publics le triennal est la règle.

Aujourd'hui, l'achat d'assurance ne doit plus être qu'un élément d'une politique de financement des risques dans le cadre d'une gestion des risques. C'est en effet à une gestion globale de leurs risques que sont appelés tous les organismes. Pour les ETI ainsi que PME/PMI, il s'agit de passer d'un seul saut, de l'artisanat à la stratégie, souvent pour répondre aux attentes de leurs partenaires globaux.

Mais, parallèlement, la plupart des organismes ne peut pas se passer d'assurance quand survient le sinistre grave. Il faut donner à son assureur les moyens de tarifer au plus juste prix. Aucun assureur n'aime le risque « en aveugle », il est rassuré par des renseignements précis et rigoureux, reflet d'une bonne gestion.

59 *Comment définir les « Alternative Risk Transfer » et quel rôle jouent-ils dans le financement des risques ?*

« *Alternative Risk Transfer* » ou ART est une expression anglaise par laquelle on a pris l'habitude de désigner tous les montages financiers visant à pré ou postfinancer les risques, en n'ayant pas recours aux mécanismes d'assurances traditionnels. Cela ne veut pas dire que les assureurs et les réassureurs ne sont pas associés, mais cela veut dire que le support du transfert ne sera pas un contrat d'assurance traditionnel où un assureur supportera les conséquences de la réalisation éventuelle de sinistre, en échange du versement d'une cotisation fixée en début de période de couverture.

Certains de ces produits, qui visent au partage du risque financier, incertitude sur les coûts des sinistres (risque de souscription), seront évoqués dans la question 61. Nous allons évoquer, ici, ceux qui s'appuient sur les marchés financiers.

Le rôle traditionnel des marchés financiers, au service de l'industrie de l'assurance, se limitait à l'apport de sources de placement. Plus récemment, ils ont contribué à l'apport de capitaux pour les sociétés d'assurance et de réassurance. Les capitaux levés permettaient aux sociétés de souscrire des contrats d'assurance pour couvrir les risques de leurs assurés. La question posée ici est entrée dans l'actualité plus récemment : « *Comment les marchés des capitaux peuvent-ils être utilisés pour offrir des solutions alternatives aux marchés traditionnels de l'assurance et de la réassurance ?* »

Les produits alternatifs offerts par les marchés de capitaux peuvent être regroupés en trois catégories.

Titres (obligations) liés aux opérations d'assurance

Ce sont des investissements financiers, le plus souvent sous la forme d'obligations, qui ont un risque assurable niché dans leur montage. L'investisseur reçoit une rémunération plus élevée, car le taux d'intérêt contient une « prime de risque de souscription » pour rémunérer ce risque niché.

Les pertes de l'investisseur sont liées au transfert de risques effectué par un autre organisme, qui utilise les fonds levés par ce moyen, pour compenser ses pertes provoquées par des risques assurables.

Produits dérivés d'assurance

Ce sont des contrats financiers dont la valeur est directement liée aux montants de sinistres subis pendant une période spécifique. Un produit dérivé d'assurance voit sa valeur croître lorsque le montant des sinistres subis au cours de la période augmente. L'acheteur du produit dérivé utilise les gains dégagés pour compenser ses pertes engendrées par des risques assurables. Le vendeur, quant à lui, accepte le transfert d'un risque en échange d'une rémunération raisonnable de ce risque. Les deux principales catégories de produits dérivés d'assurance sont les swaps et les options :

- ***Un swap*** est un accord entre deux organismes d'échanger leurs flux de trésorerie liés aux fluctuations dans la valeur d'un autre actif, le taux de rendement d'un actif, ou même un indice de valeurs ou de rendement.
- ***Une option d'assurance*** dérive sa valeur de celle d'un portefeuille de sinistres assurables ou un indice de sinistralité pour une branche de l'industrie d'assurance. La valeur de l'option d'assurance croît avec le montant des sinistres sous-jacents. L'organisme peut donc utiliser les gains de son option d'assurance pour compenser les pertes assurables subies. Une ***option hors bourse*** est un contrat privé, et taillé sur mesure, pour les besoins spécifiques de l'organisme. Les ***options placées en bourse*** sont échangées sur un marché financier organisé.

Ces produits sont couramment utilisés par les organismes pour arbitrer leurs risques financiers liés aux variations de taux d'intérêts ou les risques de change.

Accord de financement à long terme

C'est un accord passé avant la survenance de tout sinistre qui met un organisme en mesure de lever des capitaux, en émettant des actions ou des obligations dans des conditions déterminées à l'avance, dans le cas où son montant de sinistres dépasse un seuil précisé.

Les sinistres en cause peuvent être des dommages aux biens (par exemple, conséquences de tremblement de terre), des engagements de responsabilité résultant d'une atteinte à l'environnement… En échange, l'investisseur reçoit une rémunération d'engagement.

60 *Les captives, un sujet captivant ?*

Une captive d'assurance (ou plus souvent en Europe, de réassurance) est une société anonyme ayant le statut de société d'assurance (ou de réassurance), filiale d'un grand groupe industriel ou commercial. Sa spécificité est de n'accepter de souscrire que des garanties, au profit de sa maison mère et de ses filiales. Dans le cas de la captive de réassurance, les polices d'assurances sont souscrites par l'ensemble des sociétés du groupe auprès d'un (ou plusieurs) assureur(s) direct(s).

La société mère a passé un accord préalable avec les assureurs pour qu'ils placent leur réassurance auprès de la captive du groupe dans des conditions fixées à l'avance (excédent de sinistre/proportionnel, commission de cédante).

Dans le cas où la réassurance serait « au premier euro », l'assureur direct ne conservant alors aucune part du risque, on parle plutôt de « fronteur », mais le cas est relativement rare sur les marchés développés et le terme de « fronteur » est donc de plus en plus souvent utilisé pour des cas où l'assureur conserve une partie du risque.

Grâce à ce montage, une part significative des cotisations payées par l'ensemble du groupe, à ses assureurs, revient pour alimenter la trésorerie consolidée du groupe (*via* la captive). Dans certains cas, les assureurs ne reçoivent que la part de la cotisation leur revenant, la captive étant créditée par jeu interne des montants lui revenant.

Il arrive que les risques couverts dépassent les capacités financières de la captive ou le niveau de rétention souhaité par le groupe. Dans ce cas, la captive comme tout autre réassureur rétrocède ses excédents (la part du risque qu'elle ne veut ou ne peut conserver) sur le marché mondial de la réassurance. L'existence d'une captive n'implique pas que toutes les couvertures achetées auprès d'assureurs du marché soient réassurées par elle. Elle peut se limiter à certaines classes d'assurances et même, dans certains cas, opérer une sélection des risques (et refuser certaines filiales « à risques » que le marché classique peut absorber).

Les groupes industriels qui créent des captives poursuivent un certain nombre d'objectifs dont on peut résumer les principaux :

- Faciliter la remontée d'informations sur les sinistres des filiales dans un groupe très décentralisé.

- Obtenir une rémunération plus juste pour les efforts de prévention et/ou protection grâce à un niveau de cotisation reflétant la sinistralité propre du groupe.
- Disposer d'un accès direct au marché de la réassurance.
- Favoriser la maîtrise des programmes (internationaux) d'assurance.
- Conserver des revenus financiers dans le groupe (la captive bénéficie des revenus financiers liés aux flux conservés : primes et provisions, y compris les commissions de réassurance).

Création de « capacité » pour couvrir des risques non assurables sur le marché traditionnel. Le terme consacré du monde de l'assurance est de parler de la création d'une « capacité » de souscription. Parmi ces risques potentiellement lourds pour l'assuré, et dont la réalisation sans secours d'un financement extérieur mettrait en jeu sa survie, on peut citer :

- la pollution et les dommages à l'environnement ;
- le retrait ou le rappel de produits défectueux ;
- la détérioration d'image (et frais de restauration) ;
- la responsabilité civile produit (pour certaines industries exclues par les assureurs traditionnels) ;
- certains événements naturels ;
- certains risques économiques et/ou politiques.

En disposant d'une captive, le risk-manager peut interroger directement le marché de la réassurance et envisager l'établissement de réserves ou de provisions fiscalement déductibles. Ainsi, il peut lisser dans le temps l'impact financier de réalisation de ses risques, et peut par ailleurs faire ou non appel à la réassurance financière.

L'avenir des ART est devenu moins clair, du fait des incertitudes liées à l'application des nouveaux principes comptables (voir question 88) et malgré les conclusions favorables d'enquêtes dans l'État de New York sur les utilisations par des assureurs de premier plan de programmes « *finite* » et de réassurances financières pour renforcer leurs bilans et stabiliser leurs résultats.

61 *Les avantages d'une captive sans les coûts, est-ce possible ?*

Les principaux avantages de la captive ont été soulignés à la question précédente. Le principal inconvénient est lié aux coûts de mise en place, capitaux propres immobilisés et frais à exposer. De plus, c'est un instrument lourd à gérer et qui ne peut s'envisager que si le portefeuille d'assurances est d'un poids suffisant, sans doute, en excès de 10/20 millions d'euros par an, bien que ce chiffre n'ait rien de magique. Alors, comment les entreprises de taille humaine peuvent-elles en obtenir les avantages à un coût acceptable ?

Il existe une batterie d'instruments moins lourds qui relèvent de deux ordres : ou une captive « partagée », ou des contrats d'assurance qui prennent en compte la sinistralité.

Il existe, également, trois variantes importantes de montages captifs : les captives multiparentales, les captives en location et les comptes captifs (ou cellules étanches).

La captive multiparentale

Quelle que soit sa forme juridique, on peut assimiler son fonctionnement à celui d'une « mutuelle fermée », réservée à un certain nombre d'associés qui ont choisi de mettre en commun leurs capacités pour créer une société d'assurance dont ils détiennent les actions. Il faut bien choisir ses compagnons de route et régler la question du niveau de mutualisation des risques entre les participants.

La captive en location

Un organisme utilise les services d'une captive, mais sans détenir de part du capital social. Au contraire, il loue le « capital » de l'organisme qui a créé et financé la captive. L'organisme qui utilise l'accord de location paie ses cotisations à la captive et en reçoit le remboursement de ses sinistres.

L'assuré est associé aux résultats de son compte individuel, sans mutualisation entre les différents « locataires ». Dans certains cas, le contrat prévoit que l'assuré doit acheter des actions privilégiées de la captive, sans droit de vote, et perçoit un dividende calculé sur la marge de

souscription et les produits financiers dégagés sur les provisions pour sinistre et cotisations non consommées. Dans les contrats où il n'est pas prévu d'achat d'actions, le même « surplus » est rendu à l'assuré sous forme de ristourne ou de participation aux résultats.

Le compte captif (cellule étanche)

Il offre des montages qui ressemblent à une captive en location, où chacun des « propriétaires » de cellule fait l'objet d'une comptabilité séparée et reçoit le bénéfice dégagé par la cellule.

La différence fondamentale est que, dans le cas de la cellule (en anglais PCC pour « *Protected Cell Companies* »), chaque propriétaire est assuré que les autres assurés, ainsi que les créanciers de la société d'accueil n'auront pas accès au capital et aux réserves de sa cellule.

En ce qui concerne les contrats d'assurance qui organisent un partage d'expérience entre assureurs et assurés, par-delà les programmes dits à participation aux bénéfices ou aux résultats, on compte deux types de contrats : les plans « *finite* » et les rétroplans.

Le plan « *finite* »

Le contrat d'assurance pluriannuelle et portant sur un panier de risques prévoit que, sur la durée du contrat, l'assuré paie des cotisations dont le montant est proche du montant total garanti.

Il s'agit d'un programme par « capitalisation », car les cotisations payées par l'assuré sont entrées dans un compte de résultat : au débit, les montants des sinistres et aux crédits, les cotisations et les produits des placements. Le solde est remboursé à l'assureur, en fin de contrat, à la demande de l'assuré (commutation). En revanche, l'assuré dont la sinistralité dérive lourdement peut se trouver sans couverture pour la fin de la période. Il peut être en partie protégé par une couverture en excédent.

Le rétroplan ou rétrotarification

Il ressemble à un contrat d'assurance classique à cotisations garanties. La société d'assurances émet un contrat garantissant le paiement des sinistres jusqu'à concurrence d'un plafond spécifié dans le contrat.

La différence fondamentale réside dans le mode de tarification : l'essentiel de la cotisation est calculé à partir des coûts réels des sinistres

encourus augmentés d'une marge. Donc, le coût du risque est variable pour l'entreprise, qui conserve à sa charge une part importante de la volatilité du résultat. Il s'agit bien d'un programme hybride, plutôt que d'un « tout transfert ».

L'assuré est protégé par un écrêtement de chaque sinistre et la mise en place d'une cotisation maximum. Le contrat couvre une période donnée, mais l'exécution se poursuit jusqu'à la clôture de tous les sinistres déclarés.

IV
Programme de gestion des risques et audit

7
Le programme de gestion des risques

62 *Comment conduire un processus de gestion des risques ?*

La question est simple et peut se traduire ainsi : confronté à un nouvel organisme qu'il aborde pour la première fois, comment le professionnel de la gestion des risques peut enclencher le processus pour établir une gestion des risques globale et efficace au sein de cet organisme. La première condition est qu'il ait l'appui de la direction générale. Ensuite, l'engagement de l'ensemble des responsables, propriétaires des risques est un passage obligé pour la mise en sécurité de l'organisme. Mais il faut conduire un processus de décision systématique que l'on peut scinder en trois étapes, par analogie avec un acte.

Première étape : Diagnostic des vulnérabilités

Tout d'abord, il faut identifier les vulnérabilités de l'organisme qui pourraient l'empêcher d'atteindre ses objectifs fondamentaux et définir un profil de risques, en analysant les impacts financiers et éthiques de leur réalisation. Cette phase a été largement évoquée dans les questions précédentes, mais la principale difficulté demeure la phase de quantification des impacts alors que, très souvent, les données disponibles au niveau d'une entité ne le permettent pas.

Deuxième étape : Traitement des risques

La mise en place du traitement des risques suppose de respecter les trois phases qui suivent :

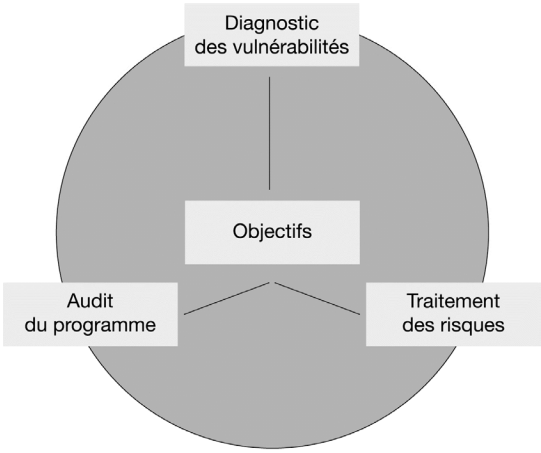
- ***Recenser*** les instruments de gestion des risques imaginables pour réduire ces vulnérabilités. Dans cette phase de « *brainstorming* », il faut éviter de se censurer par des habitudes ou des *a priori* de façon à ce que toutes les solutions, mêmes inattendues, soient effectivement passées en revue. La présence de spécialistes des métiers plutôt que de la gestion des risques peut ouvrir des voies nouvelles.
- ***Élaborer et faire approuver*** le programme de traitement des risques par la direction. C'est la phase d'interaction directe entre le professionnel et la direction, au cours de laquelle il doit présenter un programme cohérent de traitement de l'ensemble des vulnérabilités vitales de l'entité et justifier financièrement ses choix, dans le respect des objectifs fixés initialement. C'est cette approbation qui donne au programme sa légitimité à l'égard de toutes les unités opérationnelles.

- ***Mettre en œuvre***, c'est-à-dire suivre l'exécution du programme approuvé au niveau opérationnel. L'essentiel du travail est donc un travail de terrain. À ce stade, le professionnel de la gestion des risques doit convaincre les responsables opérationnels de mettre en œuvre les décisions prises, mais également les aider à les adapter dans le détail de leurs activités. La capacité de communiquer et le sens de la diplomatie deviennent ses armes essentielles.

Troisième étape : Audit du programme de gestion des risques

Il s'agit de contrôler les résultats obtenus et de vérifier l'efficacité du programme. Comme pour un acte médical, il faut une visite de contrôle pour s'assurer que les mesures décidées ont été effectivement mises en œuvre et que leur effet a été celui attendu. C'est donc naturellement que cette phase est appelée « audit du programme » puisqu'elle rejoint les principes de l'audit en entreprise.

En fermant la boucle de retour par l'audit, la troisième phase conduit à la révision de l'ensemble du processus. Le cercle « vertueux », repris ci-dessous, montre bien que le processus de gestion des risques mis en œuvre dans une entreprise s'apparente à une roue de Deming, où chaque tour de « roue » doit apporter une amélioration de la situation. On retrouve ici le principe de l'apprentissage organisationnel évoqué plus haut à propos du retour d'expérience.



Le cercle vertueux de la gestion des risques

63 *Qu'entend-on par traitement des risques ?*

Par analogie avec l'acte médical, le traitement des risques cherche à atteindre deux objectifs complémentaires : les mesures visent soit à limiter les symptômes, soit à traiter le mal en profondeur.

Le gestionnaire des risques dispose de deux trousses d'instruments pour atténuer les vulnérabilités :

- il peut intervenir sur le risque lui-même, en réduisant la probabilité ou les conséquences (trousse de réduction des risques) ou,
- il peut mettre en place les moyens financiers de compensation des pertes (trousse de financement des risques).

Concrètement, face à une vulnérabilité donnée, le plus souvent, le traitement va consister en une combinaison d'instruments issus des deux trousses évoquées.

En effet, seul l'instrument d'évitement ou de suppression exclut toute possibilité de sinistre futur, en échange du renoncement au profit qu'il y aurait à poursuivre ou à initier l'activité sacrifiée ; de ce fait, il n'y a aucun besoin de financement.

Par exemple, une entreprise fabriquant des équipements automobiles très spécialisés peut se voir offrir un contrat de fournitures d'une série limitée pour un constructeur aux États-Unis. Après vérification des conditions de mise en cause de la responsabilité civile produit dans ce pays, en particulier l'existence de dommages punitifs lourds, elle peut renoncer à ce marché. Et ce, pour ne pas devoir mettre en place une couverture d'assurance de responsabilité civile spécifique, nécessairement limitée, et d'un coût supérieur à la marge qu'elle pourrait dégager : la société renonce à ce contrat, mais elle peut renoncer par-delà, à l'opportunité d'un développement sur le marché américain. Dans ces conditions, elle n'a besoin d'aucun financement, puisqu'il n'y a pas de risque résiduel.

Pour tous les autres instruments évoqués à la question 41, même si on a réussi à diminuer la probabilité de survenance ou la fréquence par un instrument de prévention et/ou à limiter l'impact financier par un instrument de protection, il n'en demeure pas moins que des sinistres peuvent encore survenir : il faut donc, nécessairement, mettre en place un instrument de financement pour couvrir les débours induits et/ou limiter la volatilité du résultat qui en est la conséquence.

Pour illustrer ce propos, on peut prendre un exemple qui touche pratiquement toutes les entreprises : la flotte automobile. Sur la base d'une sinistralité enregistrée sur quelques années, on peut établir une prévision pour l'année prochaine : nombre de sinistres et coût moyen du sinistre. Avec un programme adapté et une conduite défensive, on peut diminuer la fréquence, par exemple en prévoyant un limiteur de vitesse sur les camions, on réduira l'énergie cinétique et donc la gravité des dommages en cas de sinistres.

Grâce à ce programme, l'entreprise pourra peut-être établir un budget pour les dommages aux véhicules de sa flotte (traitement courant), tout en maintenant une couverture de responsabilité civile pour les accidents corporels. Ces accidents sont rares, mais ont un impact très lourd sur la trésorerie de l'entreprise, et plus encore sur les bénéfices de l'exercice de survenance, en cas de non-transfert à un assureur. On voit que dans le cas de la flotte automobile, le traitement des risques consiste en la mise en place de quatre instruments : deux de réduction des risques et deux de financement.

Ces deux situations illustrent la réalité, d'où l'importance de l'étape de recensement systématique des instruments applicables à une situation donnée pour déboucher sur la solution la plus efficace, au plan économique pour l'entité concernée.

Il faut encore souligner qu'à chaque fois que l'on envisage un « traitement », ce doit être du point de vue d'une entité donnée. Le constructeur automobile peut se trouver en difficulté si le fabricant renonce à ses livraisons aux États-Unis, si c'est le seul fournisseur possible. Il pourrait alors revenir vers lui, en lui proposant une clause contractuelle de protection, dite « *hold harmless* », par laquelle il prendrait à sa charge toutes les réclamations que des clients poseraient contre les véhicules dotés de l'équipement en question. Si le fournisseur a confiance en la parole du constructeur et en sa santé financière, il peut accepter, ainsi la question du financement des risques qui l'arrêtait se trouve réglée.

64 *Comment la réduction et le financement concourent à la mitigation des risques ?*

Le terme de « *mitigation* » des risques est couramment utilisé dans le monde anglo-saxon et, par osmose, il apparaît dans la littérature française sur le risque. Généralement, il est compris comme synonyme du mot traitement ou même prévention, lorsque celui-ci sert à désigner l'ensemble des instruments de réduction.

En fait, l'utilisation de ce mot, qui rappelle le mélange d'eau chaude et d'eau froide pour faire une eau tiède, permet de souligner l'approche portefeuille ou holistique que suppose une véritable gestion des risques aujourd'hui. En effet, la mitigation fait référence à la protection contre les volatilités extrêmes qu'un risque seul pourrait apporter. Le rapprochement de différents risques, quant à lui, apporte une mutualisation élémentaire, dès lors que ceux entrant dans le portefeuille ne connaissent pas des lois de probabilités dont les variations sont en phase, mais au contraire en contrephase. Un risque maximum sur une vulnérabilité s'accompagne au contraire d'un risque minimum sur une autre, en un mot ce que les probabilistes appellent la covariance est nulle ou négative.

On peut expliquer ceci par un exemple simple : si une entreprise a des échanges réguliers avec un pays hors de la zone euro, comme les États-Unis, elle encourt un risque de change déjà évoqué plus haut.

Toutefois, si elle a des échanges dans la zone dollar avec des partenaires amont et aval (achat et vente), elle peut essayer de maintenir sa « balance » en dollars constamment proche de zéro, elle a alors réduit son risque à zéro, le risque sur le règlement futur des achats et celui sur la perception des montants des ventes s'annulant. Si le dollar s'apprécie par rapport à l'euro, l'augmentation du coût en euros de ses achats est compensée par l'augmentation du prix de ses ventes en euros. Elle a pratiqué une mitigation de son risque de change par la diversification de son portefeuille de partenaires économiques et un dosage judicieux.

Sur le plan du risque économique de croissance des marchés, elle peut obtenir une croissance moyenne en diversifiant sa clientèle dans les diverses zones géographiques pour échapper à une stagnation, voire à une récession locale. Bien entendu, le prix à payer pour cette protection, c'est de renoncer à la croissance maximale qu'elle aurait pu obtenir en « pariant » sur les zones ou les pays qui se développent le plus.

Dans certains cas, les risques sont contradictoires. La Chine offre un bel exemple de développement rapide, accompagné d'un risque politique et monétaire non négligeable. Il peut être tentant de « doper » sa croissance, en s'implantant en Chine, si on dispose de bases solides dans les pays développés qui permettront d'amortir le choc chinois si un virage intervenait dans les années à venir. Bien entendu, ce qui vaut pour la Chine vaut pour l'ensemble des BRICS (Brésil, Russie, Inde, Chine et Afrique du Sud).

Au niveau des risques « accidentels », l'illustration la plus classique en termes de chaîne logistique est le maintien de sources d'approvisionnement diverses pour éviter la dépendance et la carence de livraisons si un fournisseur ou un sous-traitant stratégique est en difficulté. En d'autres termes, la mitigation prend alors la forme d'un outil de réduction des risques que nous avons déjà évoqué plus haut, à savoir la ségrégation des risques, duplication ou séparation.

La mitigation s'entend surtout au niveau des conséquences financières d'un risque, et on touche alors au cœur de la réflexion sur ce qui s'appelle les ART, ou financement alternatif des risques (voir question 59). Tous s'appuient sur le principe de mitigation, car ils visent à rassembler sous un parapluie unique des risques, des menaces et des opportunités diverses pour réaliser un « portefeuille » dont les extrêmes sont « gommés », rendant couvrables collectivement des risques qui ne le seraient pas individuellement.

C'est aussi ce que l'on appelle les produits « multidéclencheurs » : l'illustration la plus classique est la couverture « catastrophe » pour un transporteur aérien, qui veut protéger à la fois son bilan, et dans une moindre mesure son compte de résultat, en plaçant un financement exceptionnel dont l'intervention ne se ferait que si, au cours d'un même exercice, les accidents d'avions et le cours du kérosène conduisaient à des pertes exceptionnelles. Le financement peut alors combiner emprunts pour la trésorerie et capitaux propres pour soutenir le résultat.

65 *Comment établir un programme de gestion des risques ?*

Le terme de « programme » est souvent utilisé pour faire référence à l'ensemble des mesures de gestion des risques mises en place à l'issue des décisions d'arbitrage entre le souhaitable et le possible (voir question 66).

En fait, bien que courant, le mot pose des difficultés, car il ne revient pas à la direction générale de prendre la décision sur les détails des mesures à prendre dans chacune des entités opérationnelles. De la même façon, il ne s'agit pas pour le risk-manager de détailler l'ensemble des mesures.

C'est pour cela que dans de nombreuses entités le programme de gestion des risques se ramène, en fait, à un ensemble de contrats d'assurance souscrits au niveau du groupe, de façon à bénéficier de l'achat groupé pour l'ensemble des filiales. Pour les organismes mondiaux ou globaux, les programmes d'assurances mondiaux permettent à la direction de maîtriser les couvertures de l'ensemble des entités, quelles que soient les conditions locales du marché.

Alors, quels sont les documents sur lesquels s'appuie la pratique de la gestion des risques dans un organisme ? Le point de départ sur lequel nous insisterons ici est la rédaction et l'approbation par les instances de direction d'un document de politique générale de gestion des risques. Ce document de références doit remplir les fonctions suivantes pour l'ensemble de l'organisme :

- Définir les objectifs de la gestion des risques au sein de l'organisme.
- Définir le rôle, les responsabilités et le positionnement hiérarchique du gestionnaire de risques.
- Coordonner le suivi des risques au sein de l'organisme, de façon à obtenir une approche cohérente dans l'ensemble des centres de profit, par-delà les différences techniques, géographiques, culturelles…
- Mettre en place ou améliorer la circulation d'informations entre les responsables.
- Donner les bases d'une politique cohérente et suivie, par-delà les évolutions dans l'organigramme et la personnalité des responsables opérationnels.
- Faciliter l'accueil et la formation des nouveaux collaborateurs et la continuité des missions « gestion des risques ».

En outre, pour le professionnel de la gestion des risques, le document de politique générale permet de définir ses missions et d'en fixer les conditions d'exercice, à savoir :

- Procure le cadre de référence pour fixer les responsabilités de chacun pour l'établissement des diagnostics vulnérabilités.
- Organise les responsabilités du risk-manager et des opérationnels pour le traitement des risques, réduction et financement.
- Souligne l'importance accordée par la direction à la fonction « gestion des risques », en lui procurant les moyens d'action.
- Donne un positionnement clair dans l'organigramme de la société, par-delà les compétences du titulaire.

La forme et le contenu de ce document sont le reflet des particularités de chaque organisme. Dans tous les cas, le document doit commencer par une description de la gestion des risques et de son importance pour l'organisme. Il faut également préciser le rattachement hiérarchique du risk-manager, l'étendue de ses responsabilités, et en particulier préciser la nature de ses relations avec les directions opérationnelles.

Il n'est pas absolument nécessaire que ce document d'orientation générale précise le fonctionnement interne du département. Ceci peut être laissé à l'initiative du risk-manager et peut varier dans le temps, en fonction de la composition de l'équipe.

Un élément essentiel est la définition claire et précise des objectifs retenus par les dirigeants, tant en matière de réduction que de financement des risques. Le niveau de détail des processus de décision doit refléter la politique générale en la matière et retenir les critères utilisés pour définir les fonctions des autres départements.

66 *Comment arbitrer entre les instruments de traitement des risques ?*

Le recensement de l'ensemble des vulnérabilités pesant sur un organisme global peut déboucher sur un catalogue imposant, de plusieurs milliers de pages. Le traitement intégral de chacune d'entre elles pourrait faire exploser le budget « risques » de l'organisme et dramatiquement réduire des marges opérationnelles, le conduisant peut-être à une mort certaine, plutôt qu'à une mort aléatoire si le risque se réalisait.

Au niveau global, il faut donc arbitrer entre les différents traitements possibles. Au niveau individuel, pour chaque vulnérabilité, après le recensement des instruments applicables, il faut également choisir le cocktail le plus approprié.

Comment cet arbitrage peut-il être effectué ?

Bien entendu, la priorité devra être donnée au traitement de toutes les vulnérabilités qui relèvent de l'application de lois et de règlements. Une attention particulière aux conditions locales peut modifier les priorités globales d'un grand groupe. Toutefois, cette catégorie recouvrera les domaines d'hygiène et de sécurité sur le lieu de travail, le respect de l'environnement et la sécurité des voisins et des consommateurs. En clair, la conformité est peu susceptible d'arbitrage !

Dans certains cas, les instruments de traitement seront dictés par le respect de ces dispositions obligatoires. Dans le cas le plus général, où le choix n'est pas ainsi dicté, ce seront les considérations financières qui imposeront les choix.

Pour l'essentiel, c'est l'approche des choix d'investissements, désormais usuels dans les entreprises, qui s'appliqueront au domaine des instruments de traitement des risques ; maximisation de la valeur actuelle, à long terme, des flux de trésorerie nets après impôts générés par les différentes solutions envisagées. Nous avons déjà souligné cette approche au niveau de la définition des instruments de financement et des choix entre pré et postfinancement.

L'avantage de cette approche est de placer les décisions de gestion des risques dans le moule financier utilisé pour toutes les décisions de l'entreprise. Cependant, elle comporte un certain nombre de limites dans ce domaine.

La première limite est l'hypothèse lourde que le seul objectif de l'organisme est l'efficacité économique. Par-delà les obligations légales et réglementaires déjà mentionnées, certains arbitrages peuvent s'imposer dans le cadre des valeurs définies par l'organisme. C'est particulièrement évident dans le cas des associations à but non lucratif et des ONG, des collectivités et des États où les engagements politiques pris à l'occasion des pactes électoraux s'accompagnent d'exigences. Mais le domaine concurrentiel n'est pas exclu de cette sphère, en particulier en fonction des vecteurs de réputation des différentes branches industrielles.

La seconde limite trouve son origine dans l'application même de la théorie financière. Par définition, les décisions en matière de risques touchent des flux financiers qui présentent une volatilité plus grande dans le temps que les domaines classiques : c'est cette volatilité relative ou extrême qui en fait un objet de gestion des risques. Or, l'approche des flux de trésorerie s'appuie sur des flux moyens espérés, sans prendre en compte la volatilité. Pour respecter l'équilibre risque/rendement de la frontière efficace, il faut donc trouver un remède pour les solutions les plus volatiles, les plus risquées.

Sans aller dans le détail des options, il est possible de réduire les flux des solutions les plus risquées pour donner une valeur à ce risque ou d'utiliser un taux d'actualisation (rendement attendu) supérieur aux situations à risque, et de comparer alors les résultats. La « prime de risque » envisagée doit refléter l'appétit de risques de l'entreprise. Certains préconisent une approche de trésorerie en risque pour mesurer la probabilité de « faillite » comparative des diverses solutions.

Finalement, dans certaines situations, la prise en compte des intérêts complémentaires et/ou divergents des différentes parties prenantes peut conduire à des arbitrages prenant en compte une « désirabilité » sociale, plutôt que des montants exprimés en unités monétaires. Toutefois, la difficulté est de se mettre d'accord sur les composantes et la mesure de cette valorisation sociale, des conséquences des choix effectués.

8
La mise en œuvre pratique de la gestion des risques

67 *Qui est responsable de la mise en œuvre de la gestion des risques ?*

Dans le passé, lorsque la gestion des risques se limitait à une fonction technique avec la mise en place et le suivi des couvertures d'assurance, pour l'essentiel, la responsabilité de la gestion des risques restait au sein de la direction financière, parfois de la direction juridique. Pour des raisons historiques, le volet trésorerie était privilégié et le trésorier était souvent le responsable hiérarchique du risk-manager.

Avec l'élargissement de la mission à la prise en compte globale de l'ensemble des risques et de leurs impacts pour toutes les parties prenantes, la responsabilité est clairement remontée au niveau du conseil d'administration. En particulier les administrateurs indépendants sont devenus d'autant plus demandeurs que leur responsabilité personnelle pourrait être mise en cause en cas de carence de gestion de l'entreprise.

Certes, le paysage n'est pas homogène, car parmi les pays développés, il existe des différences significatives qui sont la conséquence des règles de gouvernance non encore unifiées. Toutefois, on ne peut pas négliger l'impact de la loi Sarbanes-Oxley qui s'impose à toutes les entreprises cotées en bourse aux États-Unis, quelle que soit leur nationalité, et qui a conduit à une certaine unification des règles au niveau fiduciaire.

Clairement aujourd'hui,s le conseil d'administration et son président doivent veiller à la mise en place de processus garantissant une gestion des risques cohérente et efficace. Néanmoins, dans un organisme global, ce sont des centaines, voire des milliers de vulnérabilités qui pèsent sur l'ensemble des unités opérationnelles, et il n'est pas raisonnable de penser que le conseil pourra analyser et décider sur l'ensemble de ces éléments.

C'est pourquoi le rôle du conseil ou du directoire, selon la forme de l'entreprise, est de désigner un responsable qui devra rendre compte régulièrement des efforts de gestion des risques. Ce CRO (*Chief risk officer*) devrait être, dans l'idéal, entièrement consacré à la mission de gestion des risques, comme un véritable premier violon directement sous la baguette du chef d'orchestre.

Dans cette perspective, il revient au CRO de rédiger un document de politique générale qui sera discuté et approuvé par le conseil

d'administration pour servir de socle à tous les efforts en matière de gestion des risques. Ce document devra reprendre les valeurs et les éléments d'éthiques pratiques qui constituent la charte de l'entreprise, ainsi que les éléments financiers permettant de définir l'appétit de risques de l'organisme.

Ensuite, le rôle de consultant interne du CRO sera d'animer et de veiller à la mise en œuvre des opérations systématiques de diagnostic des risques dans toutes les unités opérationnelles. La consolidation progressive, au sein de l'organisme, doit permettre de faire remonter au niveau du conseil, par application du principe de subsidiarité, seulement les quelques vulnérabilités stratégiques, avec l'assurance que l'ensemble des vulnérabilités a été traité, chacune à leur niveau le plus proche du terrain.

Dans cette démarche, une des clés du succès à long terme est de préciser les conditions de continuité qui garantiront la résilience de l'organisme et les règles à suivre pour la mise en place, la mise à jour et les exercices de mise en œuvre des plans de continuité d'activité (PCA) au niveau de chaque unité. Ce volet est essentiel, car il faut que les PCA des différentes composantes du groupe soient cohérents et enchaînés les uns avec les autres, y compris avec ceux des fournisseurs et/ou des clients-clés.

L'exposé qui précède montre bien que, si le CRO est le coordinateur des efforts de gestion des risques, il travaille directement avec chacun des membres de la direction dans leur sphère de compétence pour que la gestion des risques soit mise en œuvre au sein des directions financière, production, marketing, logistique, ressources humaines, juridique. En résumé, la responsabilité de la mise en œuvre de la gestion des risques est une responsabilité collective du comité de direction générale dans lequel le rôle du CRO est d'assister chacun des membres dans sa sphère propre.

Chacun de ces responsables doit veiller à ce que l'effort soit prolongé, au niveau de tous les managers opérationnels et de leurs équipes, avec l'appui du CRO et sous le contrôle de l'audit interne, comme l'ensemble des vérifications de conformités.

68 *Avez-vous dit propriétaire de risques ?*

La révolution qu'a connue la gestion des risques au cours de ces vingt dernières années est une explosion d'intérêts due en partie à certains événements spectaculaires et, plus certainement, grâce à l'intérêt grandissant de tous sur la sécurité présente et à venir.

Parallèlement, la compréhension des systèmes complexes et le développement de l'approche qualité ont permis de mieux appréhender la nature complexe du risque et la nécessité de le traiter à sa source.

Dans ces conditions, la gestion des risques est devenue l'affaire de tous dans un organisme, et les responsables opérationnels sont apparus comme les plus proches du terrain.

C'est dans ce contexte qu'un nouveau terme, pour désigner ces risk-managers opérationnels est né : les propriétaires de risques.

Certes, les responsables de terrain ont toujours eu pour mission de gérer, au quotidien, les écarts de fonctionnement de leurs unités : l'absence d'un salarié, l'arrêt d'une machine, l'interruption temporaire d'une source d'énergie, le camion de livraison retardé par un accident sur la route… C'est même une des principales missions de l'encadrement : ramener un système complexe à son fonctionnement nominal, alors que celui-ci représente un équilibre instable.

Cela est différent lorsqu'ils doivent trouver, dans un emploi du temps déjà chargé, le moyen de placer une réflexion systématique sur l'ensemble des vulnérabilités (d'origine interne et externe) qui pèse sur eux et de mettre en place les moyens de parer la plupart d'entre elles, en évitant qu'elles surviennent ou en limitant les conséquences, essentiellement à l'aide de plans de continuité d'activité adaptés.

Cependant, toute l'architecture de la gestion des risques moderne (dite parfois ERM pour *Entreprise-wide risk-management*, c'est-à-dire étendu à toute l'entreprise) s'appuie sur une prise en charge, au niveau opérationnel, de tous les incidents et accidents qui trouvent naissance dans ces opérations quotidiennes et peuvent être traités plus rapidement et plus efficacement à ce niveau.

Il ne faudrait pas négliger pour autant les évolutions dans le contexte qui, pour ne pas être « soudaines », sont une source d'incertitude importante.

Bien entendu, il ne peut pas s'agir d'une génération spontanée, et l'intérêt pour la gestion des risques doit venir d'une incitation forte de la direction générale, accompagnée des méthodes et des moyens de mise en place des outils indispensables. Ce que l'on appelle parfois une approche « *top-down* ».

La communication et la formation de l'encadrement et de l'encadrement supérieur vont donc jouer un rôle essentiel dans cette évolution. L'appropriation, par les véritables propriétaires de risques, commence donc par une sensibilisation et un apprentissage de la maîtrise du processus de diagnostic des risques avec l'aide d'un consultant interne ou externe.

La mise en sécurité d'un système complexe, comme une entreprise globale ou une région économique, doit se comprendre non seulement comme la sécurisation des hommes et des biens, mais également des objectifs. Elle suppose, donc, que l'ensemble des acteurs aient véritablement une bonne connaissance de leur rôle dans la totalité du système, et des objectifs à long terme de ce système.

En d'autres termes, la mise en sécurité passe par une information transparente et honnête des acteurs internes et externes de l'organisme.

L'appropriation des risques, par les responsables de terrain, est la seule garantie que les dirigeants se concentrent sur les vulnérabilités de leur niveau, c'est-à-dire les vulnérabilités stratégiques qui engagent l'avenir à long terme de l'organisme, avec la certitude que les grains de sable opérationnels seront efficacement traités, grâce aux procédures mises en place à cet effet. Bien entendu, ces procédures doivent être acceptées et comprises de tous. Comme toutes les autres missions, elles doivent être clairement explicitées dans les définitions de fonctions et faire l'objet de sanctions et de récompenses dans l'évaluation des responsables. Toutefois, ces évaluations doivent s'appuyer sur des indices objectifs, non manipulables et compris de tous. L'audit des services opérationnels doit donc être étendu aux aspects gestion des risques dans des conditions comprises et acceptées par chacun, avec l'appui technique des professionnels de la gestion des risques internes ou externes. Ainsi les dirigeants ont-ils l'assurance raisonnable que tous les risques sont pris en compte, approche « *bottom-up* ».

69 *Comment instaurer une culture des risques au sein d'un organisme ?*

Il ne suffit plus de gérer les risques de « haut en bas », il faut également les gérer de « bas en haut ». Pour cela, il est essentiel de susciter une culture de risque dans tout l'organisme. Mais comment développer cette culture de risque de façon efficace et économique ?

Le véhicule privilégié est une communication sur le risque avec l'ensemble des parties prenantes. C'est pour cela que cette communication est devenue un instrument-clé de la gestion des risques au troisième millénaire.

Communiquer n'est pas l'apanage des relations publiques pour matraquer à coups d'annonces internes et/ou externes. Communiquer, c'est établir un processus d'échanges et de dialogues avec l'ensemble des parties intéressées.

« *La communication est un processus interactif d'échanges d'informations et d'opinions impliquant de multiples messages sur la nature des risques et de leur gestion.* » (« Manuel d'application du standard australien de gestion des risques HB 436:2009 »)

En conséquence, l'équipe dirigeante doit maintenir, à tout moment, un contact harmonieux avec l'ensemble des parties prenantes. Elle doit aussi démontrer sa capacité d'adaptation aux évolutions et aux changements rapides, y compris à ceux provoquant des ruptures.

Bien communiquer sur la gestion des risques exige un préalable : mettre en place une véritable gestion proactive des risques. Il faut donc « nicher » la gestion des risques au sein de l'entreprise, grâce à un apprentissage continu, pour que chacun soit sensibilisé. En pratique, nous avons déjà souligné que chaque manager opérationnel est le « risk-manager » de l'entité qu'il dirige. Le management des risques est une dimension de tout management. Cette réalité doit donc être reflétée dans toutes les descriptions de fonctions « cadres » (voir question 68).

Pour être efficace, cet apprentissage continu de la gestion des risques doit déborder l'organisme pour s'étendre par « contagion » à l'ensemble de ses partenaires économiques. C'est seulement dans ces conditions que ceux qui sont aux commandes peuvent faire face et réagir rapidement et efficacement, non seulement lors de la réalisation des risques identifiés, mais plus encore lorsque surviennent des développements inattendus.

Avec qui communiquer sur les risques à l'intérieur de l'organisme ?

- Le conseil d'administration (attention aux administrateurs indépendants) :
  - vulnérabilités stratégiques (moins de dix) ;
  - impact sur la confiance des parties prenantes ;
  - gestion des crises.
- Les directeurs d'unités et les responsables opérationnels :
  - vulnérabilités dans leur périmètre de contrôle ;
  - indicateurs de performance.
- La maîtrise et l'ensemble du personnel :
  - la responsabilité pour les risques individuels ;
  - les enjeux de leur mission « gestion des risques ».

Mais pour que cette communication soit efficace, il faut respecter certains principes, à savoir :

- Promouvoir un sens de « spécificité » dans l'esprit de parties prenantes (nos efforts pour tenir compte de tous les risques).
- Se focaliser sur un thème « central » (notre souci constant pour la sécurité tous azimuts).
- Veiller à la « cohérence » dans toutes les communications (chacun de nos publics reçoit l'information utile en cohérence d'ensemble).
- Se comporter avec « intégrité et authenticité » (dans la concertation avec toutes les parties prenantes).
- S'engager à la « transparence » (c'est le socle de toute performance financière et sociale soutenable, en encourageant le dialogue avec l'appui de toutes les parties prenantes).

70 *Allons-nous vers une gestion intégrée de tous les risques dans un système unique ?*

La gestion des risques est en pleine évolution et suppose une approche globale. Elle suppose donc, en particulier, de transcender les silos de risques gérés dans les différents secteurs d'un organisme. Dans la plupart des organismes, on gère déjà des pans entiers de la panoplie des risques.

Certains de ces risques relèvent d'un financement avec l'achat d'assurance, et les risk-manager ont développé de façon empirique une approche des risques « assurables » en s'appuyant non seulement sur les couvertures d'assurance, mais aussi sur l'expertise des assureurs et des courtiers en matière de réduction des risques nés des périls opérationnels tels que l'incendie, le bris de machine, le dégât des eaux, voire plus récemment les outils de réduction des risques liés aux engagements de responsabilité civile.

De plus, ils ont développé une approche liée aux classes d'assurance traditionnelles (dommages, pertes d'exploitation, responsabilités civiles, flottes automobiles…). Mais, tout en remplissant une mission effective, cette approche ne permet pas de déboucher sur un système global.

Depuis une vingtaine d'années, un certain nombre de normes ou de guides sont apparus pour assister les organismes dans la gestion de certains risques, en les incitant à mettre en place des systèmes partiels, tels que :

- ISO 9002:1994 *Systèmes qualité — Modèle pour l'assurance de la qualité en production, installation et prestations associées*[3].
- ISO 14001:2004 *Systèmes de management environnemental — Exigences et lignes directrices pour son utilisation.*
- BS OSHAS 18001:2007 *Systèmes de gestion de santé et sécurité professionnelles — Exigences.*
- NF ISO 31000:2010 *Management du risque — Principes et lignes directrices.*

Certains organismes ont développé des efforts pour intégrer hygiène, sécurité et environnement au sein d'un système unique, sous le nom de HSE, suivant différents modèles, soit en fusionnant la documentation

3 Cette norme a été remplacée par la NF EN ISO 9001:2008 *Systèmes de management de la qualité — Exigences.*

nécessaire pour les différentes certifications, soit en choisissant un système de référence et en le complétant avec les éléments nécessaires pour satisfaire les certifications.

Dans cette approche, la certification peut devenir une fin en soi, au lieu d'un moyen d'atteindre les objectifs d'hygiène, sécurité et respect de l'environnement qui devrait être au cœur du dispositif.

Aujourd'hui, des approches « globalisantes » sont offertes par le modèle COSO 2 ou « EFQM » qui semble être centré essentiellement sur la conformité fiduciaire pour permettre aux entreprises de répondre aux exigences de transparence de l'acte Sarbanes-Oxley. Il ne prend pas vraiment en compte les échanges avec l'environnement et les partenaires. Le modèle EFQM (*European Foundation for Quality Management*), dans la version 2005[4], intègre un vocabulaire spécifique aux risques.

D'autres auteurs proposent des systèmes ouverts visant à identifier et hiérarchiser les risques et évaluer la situation des mécanismes de réduction et de financement en place, pour agir sur les risques « orphelins » et améliorer l'efficacité économique des efforts de maîtrise de ceux déjà pris en compte.

Quelles que soient les qualités de ces approches, elles présentent deux limites :

- Elles présentent la gestion des risques, essentiellement sur l'angle sécurité et réduction des risques « négatifs » ou menaces.
- Elles tendent à présenter le système comme indépendant de la gestion globale de l'organisme.

La normalisation a l'avantage de procurer des références pour la pratique contractuelle et les échanges entre organismes interdépendants leur ouvrant ainsi la voie à une évaluation de leurs partenaires, présents ou futurs, pour valider la solidité d'un système de logistique (par exemple, la résilience d'un projet ou les conditions de soutien d'une réputation).

Elle trouve ses limites dans la dérive possible vers un respect formel, sans volonté stratégique de la direction, relayée à tous les niveaux pour l'atteinte des objectifs organisationnels et sociétaux de création de valeur pérenne.

C'est dans ce contexte que se pose la question de la définition d'une feuille de route ou d'un cadre de référence pour la gestion des risques,

4 Le modèle EFQM a été réactualisé en 2013.

validée et reconnue internationalement pour satisfaire les attentes de sécurité de tous, illustrée entre autres par le principe de précaution inscrit dans la Constitution française, intégrant à tous les niveaux opportunités et menaces.

En un mot, un système de management pour gérer efficacement l'ensemble des incertitudes pesant sur toute organisation humaine.

9
Les assurances et la gestion des risques

71 *L'expertise préalable a-t-elle une valeur ajoutée ?*

L'expertise préalable est une spécialité française. Elle consiste en un inventaire systématique des biens immobiliers et des équipements (objet de l'assurance) avec une évaluation en valeur de remplacement à l'identique, et une valeur d'assurance, égale à la première, sous déduction d'une vétusté « à dire d'expert » indiqué dans le rapport. Les expertises préalables sont réalisées par des experts dits « experts d'assurés » qui interviennent ensuite dans l'évaluation des dommages en cas de sinistre.

Les contrats d'assurance sont souscrits sur le principe de déclaration : les faits concernant les biens assurés, les qualités, l'activité et les valeurs sont la responsabilité de l'assuré. Si l'assuré donne des renseignements erronés, intentionnellement ou non, ou fait une fausse déclaration, lorsque le sinistre survient, il encourt des sanctions qui vont de règles proportionnelles à la nullité du contrat.

En ce qui concerne les valeurs, la sanction prévue par le Code des assurances français est : la règle proportionnelle de capitaux. En cas de sinistre partiel, le montant de l'indemnité versée à l'assuré est réduit, en proportion du déficit de valeurs assurées constaté au moment du sinistre. Par exemple, si un bâtiment assuré pour une valeur de 100 subit un sinistre partiel évalué à 50 se révèle avoir une valeur de 125 au jour du sinistre, l'indemnité versée par l'assureur ne sera pas de 50, mais de 40, c'est-à-dire :

$$(50 \times 100) : 125 = 40$$

Si l'assuré fait appel à un expert pour l'évaluation des bâtiments et des équipements, la présentation de cette « expertise préalable », annexée au contrat, conduit l'assureur à renoncer à l'application de la règle proportionnelle de capitaux.

Pour l'assuré, la première retombée de l'expertise préalable est la certitude d'être indemnisé, complètement, pour un sinistre partiel. On notera, toutefois, que le total des capitaux assurés reste le plafond de l'indemnité, donc en cas de sinistre total, si les valeurs dépassent le montant de l'expertise préalable, il y a aura un déficit. C'est pourquoi il faut choisir avec précaution le prestataire de service et veiller aux mises à jour régulières de l'expertise. Il faut également envisager une refonte du document tous les cinq ou six ans, du fait de l'évolution des techniques et des processus industriels.

L'expertise peut aussi être étendue à l'évaluation des capitaux à prévoir en cas de pertes d'exploitation. En effet, les assurés ont souvent des difficultés à identifier les postes comptables à retenir, les montants à projeter et la période de garantie à inclure dans le contrat.

En France, en cas de sinistre industriel, l'approche traditionnelle du règlement est la double expertise, le plus souvent à la charge de l'assureur. Chaque partie nomme un expert et les deux experts, assureur et assuré, doivent trouver un accord sur le montant des dommages subis.

La seconde retombée de l'expertise préalable est que, si l'expert préalable est choisi comme expert d'assuré, sa connaissance du dossier lui permettra d'assister l'assuré de façon beaucoup plus efficace. L'inventaire réalisé et les valeurs déclarées permettront de construire le dossier de demande d'indemnisation plus rapidement et plus rigoureusement. Après un sinistre, la rapidité d'indemnisation et de remise en état est un facteur essentiel de la résilience de l'organisme.

Certains experts préalables offrent maintenant des services complémentaires, comme le suivi de la gestion des actifs pour faciliter le travail comptable.

Il faut souligner que l'expertise préalable comme l'expertise d'assuré est une pratique française et il n'est pas toujours possible de l'étendre aux filiales à l'étranger.

À titre d'illustration, il faut souligner la pratique de la clause, dite de « coassurance » aux États-Unis. Outre que c'est un faux ami, car elle fait référence à la part que l'assuré accepte de garder à sa charge en cas de sinistre total, elle doit être comprise de l'assuré pour éviter une désillusion en cas de sinistre. L'assuré doit déclarer lui-même le montant des biens assurés et choisir un taux compris entre 70 et 100 % : il s'engage à ce que le montant assuré soit un pourcentage minimum de la valeur des biens assurés, évalués par l'expert unique au moment du sinistre pour que l'indemnité ne soit pas réduite en proportion du déficit de montant déclaré.

72 *Qu'est-ce qu'un « assureur-conseil » ?*

Le terme d'assureur-conseil est traditionnellement utilisé pour faire référence au commercial au contact des assurés, mais n'est pas une qualification professionnelle et n'a aucune valeur juridique.

En réalité pour les entreprises, les circuits de distribution de l'assurance sont indépendants des fournisseurs de garanties, et c'est pourquoi on les réunit sous le terme générique d'intermédiaires d'assurance. Ils sont constitués de deux groupes de professionnels qui diffèrent par le statut et le mode de fonctionnement dont les principales différences sont reprises dans le tableau ci-dessous. Certaines ont un impact sur les relations avec les assurés.

Les intermédiaires d'assurance

	AGA **Agent général d'assurance**	**Courtiers**
Statut	Profession libérale	Commerçant
Exclusivité	Oui	Non
	Lié par contrat d'exclusivité à un assureur, le « traité de nomination » lui concédant une exclusivité réciproque sur une zone géographique	Travaille avec de multiples assureurs comme un VRP « multicarte »
Mandataire	De l'assureur	De ses clients
Sa signature engage	L'assureur	Lui-même uniquement
Rémunéré	Par commission	Par commission
En cas d'arrêt	Perçoit une indemnité compensatrice	Vend un fonds de commerce
Remarque	Le portefeuille de clientèle appartient à l'assureur	Le portefeuille de clientèle appartient au courtier

Les entreprises importantes font plus souvent appel au service de sociétés de courtage, tandis que les PME/PMI peuvent faire appel à un agent général. Les missions des deux types d'intermédiaires sont en principe différentes, du fait de leur statut. Lorsque l'agent général propose les solutions « assurances » souscrites par la société d'assurances dont il est le représentant, le courtier quant à lui doit trouver la meilleure solution pour son client parmi les assureurs auprès desquels il a ouvert un « code », et avec lesquels il travaille régulièrement.

Le marché de l'assurance a connu récemment une concentration et les différences se sont estompées. Les agents ont cherché des mandats de compléments et/ou créé des sociétés de courtage pour offrir une palette plus large à leur clientèle d'entreprises.

Rappelons que la rémunération de l'intermédiaire revêt le plus souvent la forme de commissions reversées par l'assureur.

Toutefois, cette commission est incluse dans la cotisation versée par l'assuré ; il est donc fortement conseillé d'exiger la transparence : l'intermédiaire devrait porter les taux et les montants des commissions à la connaissance de son client.

Dans tous les cas, lors d'une transaction donnée, il faut savoir si l'intermédiaire agit en tant que courtier ou en tant qu'agent, car le statut a des conséquences importantes pour le client :

- Au niveau du placement : le souscripteur doit donner au courtier un mandat de placement.
- Au niveau de la souscription des garanties : un agent engage son mandant, un courtier n'engage que lui-même. Donc, avec un courtier, à défaut de recevoir un contrat avant la date de début de garantie, il faut exiger une note de couverture signée de l'ensemble des coassureurs.
- Au niveau du règlement des cotisations : la remise à l'agent vaut remise à l'assureur, la quittance vis-à-vis de l'assureur n'est acquise que lorsque celui-ci a reçu les fonds. Dans le cas d'un courtier, il est prudent d'établir les chèques au nom de l'assureur.
- Au niveau du respect des délais de déclaration des sinistres : la déclaration à l'agent vaut déclaration à l'assureur, dans le cas d'un courtier, il est recommandé de faire parvenir un double de la déclaration à l'assureur, sauf si le courtier dispose d'une délégation de gestion écrite.

73 *Quelles prestations attendre de son « conseil en assurances » ?*

Même si le terme de « conseil en assurances » n'est pas un label de qualité ou une reconnaissance, il n'en demeure pas moins que la législation s'est renforcée, en exigeant des courtiers en particulier, qu'ils aient des diplômes minimums pour apporter leurs conseils et des garanties financières.

La jurisprudence a consacré le devoir de conseil des intermédiaires d'assurance. Le devoir de conseil repose sur l'assureur lui-même en cas de vente directe, c'est-à-dire par des salariés des sociétés d'assurance dont le salaire est constitué de commissions (producteurs salariés) ou par les salariés (bureau des mutuelles sans intermédiaire).

Fondamentalement, on doit attendre de son intermédiaire : compétence professionnelle, créativité, transparence et loyauté. La confiance est au cœur de la relation intermédiaire-client. Mais en quoi consistent les conseils et les prestations que l'on doit attendre de son « assureur-conseil » ?

Pour le comprendre, le plus simple est de suivre la vie du contrat d'assurance :

- ***Définition des besoins :*** c'est la phase la plus délicate au cours de laquelle le conseil doit mettre en forme, compatible avec l'état du marché, les besoins en financement exceptionnels dérivés du diagnostic des risques établi par son client. Bien entendu, dans la réalité, le conseil est souvent conduit à participer à l'évaluation des risques, du moins ceux de nature assurables. La connaissance du métier de son client, s'il a déjà des clients dans la branche industrielle, et des contrats traditionnellement proposés doit lui permettre de l'assister dans le choix des garanties souhaitables, des montants de couverture et des franchises.
- ***Sollicitation du marché :*** sauf dans le cas des marchés publics (collectivités, hôpitaux), l'approche du marché peut se faire de gré à gré, sans recours à un appel d'offres formel (voir question 74). Toutefois, dans le cas d'un agent général, il peut être nécessaire de solliciter plusieurs participants, puisque chacun n'interroge que la société d'assurance qu'il représente. Dans le cas des courtiers, on peut le choisir sur la base des prestations qu'il apporte et le laisser approcher l'ensemble du marché. Cette méthode est recommandée dans les marchés étroits où le nombre d'assureurs potentiels est restreint. À défaut, il faudra organiser le partage du marché (voir question 74).

- ***Sélection de la meilleure offre :*** dans le cas d'un intermédiaire unique, il lui revient de dresser un comparatif des offres qu'il a obtenues, afin d'aider le client dans sa sélection du meilleur rapport couverture/cotisation. Pour éviter que les conditions de rémunération du courtier ne biaisent son jugement, elles doivent impérativement figurer dans le comparatif.
- ***Mise en place du contrat :*** l'intermédiaire doit veiller au texte des garanties et à la date d'effet pour que le client soit effectivement couvert en continuité. Il faut prêter une attention particulière aux contrats en coassurance, car plusieurs assureurs se partagent le contrat : tous les documents contractuels doivent être signés de chaque assureur, à côté de la mention de sa part dans le contrat.
- ***Suivi du contrat :*** une société évolue, ses besoins et les conditions du marché également. Il revient alors au courtier de suivre le marché pour s'assurer que son client est à tout moment assuré dans les meilleures conditions économiques.
- ***Assistance et gestion des sinistres :*** le suivi des processus d'indemnisation, pour que celle-ci soit équitable et rapide est une mission importante de l'intermédiaire. Rigueur de gestion pour les risques de fréquence et qualité des conseils pour les risques de gravité doivent être des facteurs du choix. On notera que le suivi des sinistres est parfois confié à un tiers gérant pour le compte de l'assureur et de l'assuré.

Il faut noter une tendance à l'évolution du mode de rémunération des intermédiaires avec une part croissante de versement d'honoraires par le client. Cette action peut paraître plus équitable : le courtier ne risque plus d'être suspecté de favoriser les assureurs qui donneraient les plus grandes commissions et ne verrait plus sa rémunération flotter au gré des cycles d'assurance. En Europe, à ce jour, seul le Danemark interdit toute rémunération directe de l'intermédiaire par l'assureur, mais une réflexion est en cours au niveau de l'Union européenne.

74 *Pourquoi et comment lancer un appel d'offres en assurance ?*

Les entreprises, régulièrement démarchées par des intermédiaires, peuvent étudier leurs offres et choisir celle qui leur paraît être la meilleure, qu'elle soit faite par un salarié de mutuelle, un agent général ou un courtier. Toutefois, elles peuvent juger utile de procéder à un « tour de marché », pouvant prendre la forme d'un appel d'offres, qu'elles définissent, spécifiquement.

Ces appels d'offres visent à organiser la concurrence à la main de l'assuré. Ils peuvent revêtir plusieurs formes, selon qui est invité à répondre, et ce que les candidats sont invités à fournir. L'appel d'offres peut être fermé ou ouvert. Dans un appel d'offres fermé, l'assuré sélectionne un nombre restreint d'intermédiaires choisis pour leur proximité, leurs compétences ou leur connaissance spécifique de l'activité industrielle concernée. Dans un appel d'offres ouvert, l'assuré invite, par toute voie qu'il juge utile (contact direct, presse…), les candidats intéressés à répondre. Quant à la prestation attendue, le candidat peut être face à :

- ***Un appel d'offres conceptuel :*** l'assuré souhaite recevoir une proposition de montage lui apportant une solution de couverture idéale des risques identifiés, sans que l'offre soit accompagnée d'une tarification précise. En général, il demandera aux candidats de ne pas approcher (on dit saisir) les assureurs. La qualité des solutions proposées sera un critère essentiel. Dans un second temps, un appel d'offres auprès des assureurs pourra être organisé, sur la base de sa « solution », avec l'intermédiaire retenu.
- ***Un appel d'offres de placement :*** le candidat est invité à donner une réponse chiffrée précisant le budget d'assurance, et garantissant le placement intégral. Le tarif sera un critère essentiel dès lors que la proposition remplira les exigences de couvertures demandées.

Dans tous les cas, les organismes qui ne disposent pas de spécialiste interne font appel à un prestataire externe, consultant en assurance, pour organiser l'appel d'offres en étroite collaboration.

Qui choisir ? Bien que l'achat d'assurance présente des particularités, notamment si la prestation est effectuée après l'achat, les règles de l'achat professionnel s'imposent : choisir des candidats compatibles en termes d'éthique, solvables, compétents dans les domaines où l'on intervient, et de taille telle, que l'on soit un client significatif mais pas indispensable !

Les opérateurs publics sont souvent obligés, par le Code des marchés publics, de procéder par appel d'offres ouvert.

Pour fixer les idées, le tableau qui suit donne une idée de ce qu'il faudra couvrir dans un appel d'offres de placement. Bien entendu, dans le cas d'un appel d'offres conceptuel, on omettra le résumé des garanties.

Les principaux chapitres à prévoir dans un appel d'offres en assurance

1	**Description des opérations :** description générale des opérations par filiales, divisions et branches, budget annuel et bilan, rapport annuel de la société.
2	**Description du service Gestion des risques et assurances :** politique générale de gestion de risques et d'assurances, organisation et structure, prestation du service, répartition des coûts, gestion des plaintes, prévention des pertes, prestations sous-traitées à des prestataires extérieurs…
3	**Analyse des risques de dommages aux biens :** base des valeurs retenues : remplacement à neuf, valeur d'assurances, plus date d'évaluation (il est souvent souhaitable de disposer d'une expertise préalable récente), valeur totale par site et par ligne de couverture, sinistre maximum probable et montant en jeu (perte maximum possible) par site, rapports individuels sur la protection contre l'incendie, photos et plans pour les sites de grande taille, valeur des biens en transit et sites non programmés, tableaux des frais supplémentaires à exposer (pour maintenir la continuité de service public après un sinistre).
4	**Analyse des risques de responsabilités :** données d'assurances quantifiées (recettes fiscales par classe, coûts salariaux, recettes d'activités de service à titre onéreux…), description des activités « à risque », risques incidents ou de type « parapluie », situations de garde ou de contrôle, responsabilité professionnelle, responsabilité potentielle résultant de lois et réglementations spécifiques, ports et activités concédées, autres risques décelés.
5	**Analyse de la sinistralité :** description de la procédure de gestion des sinistres : par l'assureur, l'expert ou en interne, montant total des pertes subies par classe de risque, description et analyse de tous les sinistres importantes (disons, supérieurs à 10 000 €), même s'ils ne sont pas clos (évaluation), découpage de la sinistralité par classe de couverture et cumulée. Il ne faut pas hésiter à donner un tableau qui parle aux assureurs (regrouper les sinistres par taille — moins de 5 000 €, de 5 000 à 10 000 €…), analyse prévisionnelle des sinistres et rétentions (franchises). Il ne faut pas hésiter à joindre des projections de sinistres futurs en fonction de la sinistralité passée et des évolutions en cours ou prévisibles.
6	**Résumé des garanties souhaitées** (elles sont en général divisées en lots) : dommages aux biens, et en matière de frais supplémentaires, responsabilité civile (flotte automobile), individuelle (accident des élus), couverture prévoyance et maladie complémentaire du personnel.

75 *Faut-il avoir recours à un consultant en gestion des risques ou à un risk-manager en temps partagé ?*

Au sein de tout organisme, il faut un gestionnaire de risques. Seule en Europe, la législation allemande en fait une obligation légale, mais la réalité économique le dicte. Toutefois, s'il y a un membre de la direction, dont la fonction comprend clairement la « gestion des risques », ce peut être un directeur général adjoint, un trésorier, un directeur financier, un secrétaire général…, dont ce domaine n'est qu'un volet de son activité.

Dans les organismes de taille plus modeste, c'est le PDG ou le gérant lui-même à qui cette responsabilité incombe. Dans ces conditions, il devra faire appel à des compétences externes pour la mise en forme et le suivi effectif du processus de gestion des risques au sein de l'organisme. Bien entendu, l'intermédiaire d'assurance (courtier ou agent) participe à la fonction, mais nous l'avons vu avec une capacité limitée à la mise en place et à la gestion des programmes d'assurance.

Dans les entreprises et les collectivités où, sur le plan économique, l'engagement d'un professionnel à temps plein ne se justifierait pas, il faut utiliser les services d'un consultant externe rémunéré en honoraires ou un cadre spécialisé en temps partagé.

Dans les collectivités publiques, aux États-Unis, la situation qui prévaut est celle des grandes entreprises avec au moins un spécialiste à temps plein. Dans les collectivités plus modestes (communes, syndicats, chambre de commerce ou autres), le recours à des compétences extérieures est utile, en appui d'un responsable administratif en charge du dossier.

En Europe, à l'exception du Royaume-Uni, la mise en place d'une approche de la gestion des risques en est encore à une phase de développement, dans les entités publiques et dans le tissu des entreprises de taille régionale. Néanmoins, des progrès sont à noter, en particulier en France, depuis la décentralisation qui a incité les maires à redoubler de vigilance. C'est pourquoi il faut susciter un métier de risk-manager consultant qui se partagerait entre plusieurs entreprises.

En revanche, la gestion des risques suppose un effort continu sur de longues périodes et s'accommode mal de la vision classique du consultant qui passe un temps limité dans un organisme, dépose un rapport et disparaît. Les risques qui pèsent sur les organismes de taille modeste

sont aussi lourds et complexes que ceux qui pèsent sur les grands, et suppose les mêmes compétences dans le temps mais à un rythme plus limité pouvant aller de 10 à 50 journées par an, par exemple. C'est pourquoi il faut procéder au « recrutement » du consultant en gestion des risques avec la même rigueur que celui d'un cadre dirigeant à temps plein, quel que soit le statut ultime (contrat de prestation pluriannuel ou contrat de travail à temps partiel). On notera que la législation française sur le travail ne facilite pas le recours au salarié en temps partagé.

Toutefois, étant donné son implication dans les réflexions stratégiques de l'entreprise, la constitution du portefeuille de clientèle du consultant est importante, si l'on veut éviter de générer un risque, même involontaire, d'espionnage industriel. Or, dans le même temps, on souhaite que le consultant connaisse le métier. On peut imaginer des solutions innovantes sous différentes formes, par exemple :

- Un risk-manager de zone, partagé par l'ensemble des PME/PMI implantées dans une zone d'activité donnée : il sera à même d'apprécier les interférences entre les activités et devra bien connaître les risques communs.
- Un risk-manager « d'association » recruté par un syndicat professionnel (une association départementale de maires), pour servir l'ensemble des adhérents.

Dans les organismes, même un professionnel à temps complet ne peut pas tout savoir sur tout en matière de risques. Si la responsabilité principale lui incombe, le gestionnaire de risques devra faire appel, ponctuellement, à des spécialistes qui viendront donner un éclairage et un point de vue spécifique : étude de faisabilité d'une captive, analyse et protection du risque de kidnapping dans des pays difficiles, évaluation des impacts fiscaux de certaines décisions. Dans ce cadre, seule la compétence technique avérée est essentielle, puisque la cohérence de la politique de gestion des risques est assurée par un salarié permanent.

10
L'audit de la gestion des risques

76 *En quoi consiste l'audit de la gestion des risques ?*

Comme tout processus de gestion, celui de la gestion des risques doit se conclure par une vérification des résultats atteints. Cette vérification correspond à la visite de contrôle d'un acte médical, où il convient de vérifier à la fois si le patient a suivi la prescription et si celle-ci a apporté l'amélioration de l'état de santé espéré. Traduit en termes d'entreprise, il est évident que l'une des trois possibilités se réalisera : les résultats atteints sont inférieurs aux objectifs, juste sur l'objectif ou supérieurs aux objectifs.

En fonction des résultats, il est possible qu'il faille envisager de modifier le programme de gestion des risques, de renforcer sa mise en œuvre ou de reprendre le diagnostic, bouclant ainsi le cercle vertueux de la gestion des risques.

La définition qui précède reprend le principe même de l'audit en entreprise : des mesures (ou des référentiels) ont été définies, une évaluation objective des résultats est effectuée, et les améliorations à apporter à la situation sont recherchées.

Les modifications doivent être décidées en commun par les dirigeants, le gestionnaire de risques et les responsables dont les résultats sont évalués.

On pourrait penser que si les objectifs sont juste atteints, la situation est satisfaisante et que l'on peut maintenir un *statu quo*. C'est souvent le cas, mais un praticien averti sait bien que si l'instrument de mesure n'implique pas l'excellence, la performance réalisée n'est pas non plus l'optimum pour l'organisme.

Il est clair que si les résultats sont en dessous des objectifs fixés, il convient de mettre en place des actions correctrices. D'abord, comment atteindre des références fixées ? Ensuite, peut-être faut-il s'interroger sur les référentiels ? Les objectifs sont-ils trop exigeants ? Faut-il fixer des objectifs plus raisonnables ? Abaisser les références peut être un facteur de motivation des collaborateurs, qui travailleront mieux, pour atteindre des objectifs qu'ils estimeront à leur portée alors que, précédemment, ils avaient baissé les bras devant l'impossible.

Si les résultats excèdent notoirement les objectifs, il est légitime de s'interroger. Ont-ils été incomplets ? Insuffisants ? Trop centrés sur un aspect

de la question, et les salariés se sont-ils concentrés sur cet aspect sans se préoccuper des autres ? Bien entendu, en gestion de risque, où la part de l'aléatoire est particulièrement sensible, il est possible que l'on soit face à un exercice hors du commun où tout s'est conjugué pour donner un résultat improbable. Dans tous les cas, il faut analyser le phénomène et, au besoin, maintenir les objectifs, en expliquant aux dirigeants les conditions d'une situation exceptionnelle. Si ces résultats se renouvellent, il faudra envisager une implication, hors du commun, des salariés et les en récompenser.

Tout organisme œuvre pour améliorer ses résultats futurs, non pour critiquer ou humilier ceux dont les résultats sont insuffisants. L'audit n'a pas pour objectif de punir, mais de responsabiliser les managers et de faciliter la mise en œuvre d'actions correctrices.

Remédier à une situation relève plus de compétences de terrain spécifiques que de méthodes générales qui pourraient faire l'objet d'un exposé théorique : à chaque situation, à chaque individu correspond un mode opératoire spécifique qui permettra d'atteindre le résultat souhaité. Il s'agit de tenir compte de l'objectif concerné, du type de risque, du type d'organisme, du caractère des responsables sur la sellette, ainsi que des différents moyens qui permettraient de l'atteindre. Voici deux illustrations de cette démarche :

- Face à une dérive de responsabilité civile produit, il faut s'interroger : quel produit ou quelle gamme est en cause ? S'agit-il d'un défaut dans la chaîne de production ? Il faut chercher un remède à la situation avec tous les acteurs impliqués dans le produit, la R&D, la fabrication, les approvisionnements, la logistique, le marketing et les ventes. La solution résidera peut-être dans une amélioration du service après-vente, la rédaction d'un nouveau mode d'emploi, la révision d'un contrat avec un sous-traitant…
- Une recrudescence de vols dans une chaîne de magasins est-elle liée à un point de vente, une région, une enseigne, un type de magasin ? A-t-on réduit le rythme des transferts de fonds à la banque augmentant ainsi les montants de liquides en caisse ? La solution serait alors de faire des dépôts plus fréquents à la banque.

77 *Qu'appelle-t-on un « référentiel » en gestion des risques ?*

En matière d'audit, les « référentiels » sont les instruments de mesure mis en place pour évaluer, objectivement, la qualité de la prestation auditée. Toutefois, la gestion des risques s'inscrit dans une perspective pluriannuelle, voire même au-delà de la décennie. Un audit annuel valide en principe des référentiels annuels. C'est pour répondre à cette dichotomie temporelle qu'il faut mettre en place deux types de référentiels pour contrôler la qualité de la gestion des risques : les référentiels de résultats (comme courir le 2 000 m en moins de 5 minutes ou réaliser un chiffre d'affaires de 100 euros) et des référentiels d'activité (comme courir pendant 30 minutes tous les jours ou faire 5 visites de clientèle quotidiennes). Les premiers se concentrent sur l'atteinte d'objectifs mesurables à court terme, sans se préoccuper des efforts déployés pour les atteindre. Les seconds reflètent les efforts fournis pour les atteindre, avec pour hypothèse implicite que ces efforts doivent conduire aux résultats escomptés.

Pour apprécier la qualité de la gestion des risques d'un propriétaire de risques, responsable opérationnel, les deux types de référentiels doivent être utilisés :

- ***Référentiels de résultats :*** les résultats de l'action de gestion de risques de chaque responsable comme ceux de l'organisme peuvent être mesurés en euros, en pourcentage, en ratio ou en nombre de sinistres. Tous ces chiffres peuvent être donnés en valeur absolue ou rapportés à des entités de référence comme chiffre d'affaires, valeur des actifs, nombre de salariés ou toute autre mesure pertinente de l'activité des services. Par exemple, le coût du risque d'un organisme donné peut être de 0,65% du chiffre d'affaires, l'objectif pour l'exercice suivant peut être de le ramener à 0,64%.
- ***Référentiels d'activité :*** la performance du responsable en matière de gestion de risques peut, aussi, être mesurée en termes d'efforts déployés pour atteindre les objectifs. Par exemple, en matière de sécurité des personnes, il faut organiser, au moins, une réunion sécurité mensuelle. Sur la sécurité incendie, une visite annuelle par un expert externe sera réalisée chaque année. Pour le département marketing, ce peut être de lancer une enquête de satisfaction auprès des consommateurs, chaque année. Pour les approvisionnements, une visite trimestrielle des installations de tous les fournisseurs ou les

sous-traitants-clés… L'importance de la culture de gestion des risques a été déjà soulignée, il n'est donc pas étonnant de retrouver dans les référentiels d'activité dans ce domaine, de nombreuses actions d'information et de formation pour créer et entretenir cette culture.

Nous avons déjà, indirectement, souligné les limites des référentiels de résultats, dès lors que le coût du risque n'est jamais mesurable d'une façon unique et absolue (voir question 11). Notamment en matière de gestion des risques, car les résultats sont très sensibles à des circonstances inhabituelles, en particulier les montants annuels de sinistres qui peuvent varier considérablement si un sinistre exceptionnel survient. Les référentiels de résultats basés sur les fréquences refléteront mieux les efforts développés.

De plus, certains efforts de réduction des risques ont des effets de retards et, à l'inverse, des relâchements ne peuvent se faire sentir que plusieurs mois, voire plusieurs années plus tard. Dans les grands groupes, où les managers restent en place fréquemment pour des durées inférieures à quatre ans, il peut y avoir une incitation à limiter les investissements en gestion des risques pour optimiser un bonus, si les conséquences ne doivent être ressenties que par les successeurs. C'est pour cela qu'il est essentiel que la gestion des risques soit auditée sur le terrain, avec une batterie de référentiels, qui comprennent à la fois des référentiels de résultats et des référentiels d'activité. Ces derniers sont la garantie des efforts sur le long terme pour maintenir le niveau de culture de gestion des risques chez tous les collaborateurs, quelle que soit leur ancienneté dans l'organisme.

Bien entendu, des référentiels doivent également être définis pour le service de gestion des risques. Dans la mesure où il maîtrise directement le financement des risques et plus spécifiquement le budget assurances, une tentation pourrait être de mesurer son efficacité uniquement sur la base du coût des assurances. Ce serait dangereux pour le risk-manager qui serait dépendant des cycles d'assurances et de l'engagement dans des activités nouvelles plus risquées. Mais ce serait encore plus dangereux pour les dirigeants, qui réduiraient leur évaluation des efforts de gestion des risques au sein de leur organisme au montant des cotisations d'assurances, alors que les parties prenantes attendent d'eux la mise en place de procédures garantissant le niveau de risque le plus réduit possible à court et à long terme pour leur contribution au développement économique, à savoir produits et services, salaires et dividendes selon les parties intéressées.

78 *D'où viennent les référentiels de la gestion des risques ?*

Quel que soit le domaine d'intervention, la source des référentiels utilisés pour un audit réside dans les objectifs, les plans ou les budgets qui formalisent la stratégie de l'organisme. Dans le cas de la gestion des risques, les référentiels sont donc directement tirés des programmes de gestion de risques, c'est-à-dire :

- ***Référentiels de résultats :*** le programme de gestion des risques doit indiquer les objectifs chiffrés qu'il cherche à atteindre, tant au niveau de la fréquence des risques que du coût annuel des sinistres subis, du coût du financement des risques, du budget assurances. Tous ces objectifs peuvent être traduits en référentiels mesurables ou repérables concrètement.
- ***Référentiels d'activité :*** pour atteindre les objectifs définis, le programme expose les efforts qui vont être développés en termes d'investissements, de charges récurrentes, et le tout détaillé par département, centre de profit… Les référentiels d'activité découlent donc des moyens indiqués dans le plan, comme nécessaires pour atteindre les objectifs souhaités.

Toutefois, les référentiels qui doivent avoir les qualités d'un bon instrument de mesure sont faciles à résumer. Un référentiel doit être :

- ***Juste :*** la mesure réalisée sur le terrain doit, effectivement, refléter la disparité entre la situation atteinte et la situation idéale planifiée. Par exemple, pour une flotte automobile ramener la sinistralité annuelle de 0,8 à 0,5 (réduire de 8 à 5 sinistres par an pour 10 véhicules).
- ***Fiable :*** les mesures doivent donner des résultats identiques dans le temps et dans l'espace, en cas d'entités dans différents pays. Par exemple, toujours pour la flotte automobile, réduire de 10% le coût moyen des sinistres, quel que soit le niveau original.
- ***Sensible :*** l'instrument doit rendre compte même en cas d'amélioration limitée. Par exemple, en matière de plan de continuité d'activité, un retour à l'activité normale en 2 jours en cas de dommages au site inférieur à 20%.
- ***Objectif*** (non manipulable) : il faut que le résultat de la mesure ne soit pas sujet à des manipulations par les managers audités. Si un retour d'expérience est en place, le nombre d'incidents déclarés

peut servir d'indice, mais pour le manager, il peut être tentant « d'oublier » des incidents mineurs afin d'améliorer sa performance.

- ***Économique :*** le suivi et le calcul des référentiels ne doivent pas exiger la mise en place de suivis lourds et onéreux. Par exemple, la fréquence mesurée par le nombre de sinistres déclarés, automatiquement introduits dans le SIGR (voir question 22) pour le suivi de l'indemnisation.
- ***Efficace :*** c'est-à-dire mesurer un facteur qui améliore, effectivement, la gestion des risques. Le nombre de visite de risques peut, en soi, être inutile si cela devient une routine. En revanche, il peut être utile pour la culture de gestion de risque que chaque visite soit accompagnée d'un séminaire de sensibilisation de tout le personnel aux problèmes de sécurité. Dans ce cas, il faut que la formation soit le référentiel, plutôt que les visites elles-mêmes.

Dans tous les cas, comme pour les opérations budgétaires, il faut que les managers, qui devront être audités, soient parties prenantes dans la définition des référentiels. C'est d'autant plus nécessaire que le programme global de gestion des risques est la consolidation de tous les programmes opérationnels au niveau des unités et que les référentiels doivent refléter les conditions locales d'exercice.

En revanche, certains référentiels, d'activité et de résultats, découlent du respect des obligations légales et réglementaires qui peuvent peser sur les activités de l'organisme.

Cette conformité de l'entreprise incombe aux dirigeants, qui ont une responsabilité personnelle, voire pénale, en cas de non-respect. Sans que cette liste soit exhaustive, les domaines qui doivent faire l'objet d'une attention particulière sont l'hygiène et la sécurité des lieux de travail, la discrimination dans le travail et le marché, les atteintes à l'environnement, la sécurité des produits et des services pour le consommateur, le respect des règles fiduciaires.

79 *Comment conduire un audit de la gestion des risques ?*

Nous l'avons vu, l'audit du programme de gestion des risques est une nécessité pour l'amélioration de la performance et le maintien de la pertinence, par-delà les évolutions de l'organisme lui-même et de son environnement physique, économique, concurrentiel, juridique, social et culturel.

La question demeure de savoir, qui est le mieux habilité pour conduire ce contrôle, de façon à ce qu'il atteigne le maximum d'efficacité.

Les risk-managers, au sein de l'entreprise, sont les responsables opérationnels, qui traduisent les instructions stratégiques contenues dans le document d'orientation approuvé par les dirigeants au niveau tactique de leur entité. Si le risk-manager, ou CRO, assiste les responsables de terrain dans la définition de leur programme en coordonnant au départ les ateliers de diagnostic, il peut aussi les assister dans l'évaluation des résultats.

L'audit doit donc comprendre la vérification des référentiels de résultats et d'activité (voir questions 76 et 77). Mais pour évaluer la résilience de l'organisme, il faut valider régulièrement les outils qui vont la permettre. Ces outils sont les plans de continuité d'activité, adaptés aux périls les plus lourds pesant sur l'entité, qui peuvent s'étendre à des plans de retrait pour les produits de consommation et des communications exceptionnelles dans les situations où l'information du public s'impose.

L'audit de gestion des risques ne peut donc pas se faire uniquement sur documents, ni même sur une simple visite des lieux. Il impose la réalisation d'exercices pour valider l'efficacité des instruments de résilience. Par exemple, les hôpitaux doivent être équipés de sources électriques de secours. Il ne suffit pas de valider leur fonctionnement pour garantir leur mise en œuvre automatique en cas d'arrêt d'alimentation externe, il faut encore vérifier leur asservissement en créant une panne réelle (en mettant une dérivation en place). Une solution de *back-up* informatique doit aussi être testée en présence d'un contrôle extérieur à l'entité.

Le constat est que l'audit de la gestion des risques ne peut pas être confié à des personnes non formées dans la discipline. Parallèlement, on peut estimer que le risk-manager est juge et partie, puisque c'est lui qui conseille et défend l'ensemble des programmes de gestion des risques devant la direction générale.

C’est pourquoi il faut sans doute envisager un audit conjoint : par les auditeurs internes pour relever les divergences par rapport aux référentiels et par le risk-manager pour participer aux exercices et à la définition des actions correctrices nécessaires.

Si une part du bonus accordé aux opérationnels est liée à leur performance gestion des risques, son évaluation relève de l’audit interne comme l’ensemble des autres domaines de performance. En revanche, la présence d’un « avocat compétent », le risk-manager, facilite l’amélioration de la performance future et contribue à la résilience globale de l’organisme.

80 *L'audit interne et la gestion de risques, sont-ils alliés ou concurrents ?*

Les limites de l'autorité directe du gestionnaire de risques pour imposer la mise en œuvre des programmes de réduction des risques, sa capacité à imposer des sanctions à ceux qui ne respecteraient pas les consignes sont très variables d'un organisme à un autre.

Dans quelques cas, l'ensemble des moyens de réduction des risques est placé sous l'autorité directe du gestionnaire de risques. Le plus souvent, la responsabilité est partagée entre les différents responsables opérationnels. Par exemple, le directeur d'usine et le directeur des ressources humaines suivent les questions d'accidents du travail et d'hygiène, le directeur technique suit les questions de qualité, le directeur juridique est le premier conseil de l'entreprise en matière légale. Fréquemment, le gestionnaire de risques est en position de consultant interne (audit et conseil) pour l'ensemble des responsables opérationnels et fonctionnels.

Dans la mesure où un certain nombre de responsabilités, en matière de réduction des risques, se sont greffées autour de la sécurité du travail, le gestionnaire de risques va se trouver face à des « forteresses sécurité ». Les responsables abandonneront difficilement leurs prérogatives. Ces responsables sécurité ayant, vraisemblablement, acquis une expertise importante par l'expérience, et du fait qu'aucun programme n'est efficace sans leur support actif, il est plus judicieux pour le gestionnaire de risques de ne pas revendiquer une autorité suprême, mais plutôt de travailler en étroite coopération avec eux. Les résultats atteints seront meilleurs, cela rejaillira sur l'appréciation de sa performance par les dirigeants. C'est d'autant plus important que la continuité se joue effectivement au niveau opérationnel.

Lorsque la fonction « gestion des risques » est créée au sein d'un organisme, elle doit trouver un appui auprès de l'audit interne, qui en connaît déjà l'ensemble de l'organisation et tous les responsables auprès desquels il a déjà une légitimité.

La question devient plus délicate lorsque, s'appuyant sur les conformités résultant des nouvelles législations (Sarbanes-Oxley aux États-Unis, NRE et LSF en France), l'audit interne s'efforce de récupérer l'ensemble de la gestion des risques, au nom de la mise en place de la gouvernance d'entreprise.

En effet, l'audit est une méthode qui repose sur la définition de mesures et la comparaison entre l'objectif et le réalisé, tandis que la gestion des risques comprend une dimension d'imagination et de création, totalement étrangère au principe de la qualité d'audit.

Par ailleurs, le service central de gestion des risques doit faire l'objet d'un audit, comme tous les services, pour valider son mode de fonctionnement et sa gestion interne. Cet audit relève naturellement de l'audit interne.

En revanche, le service d'audit interne est une source de risques significatifs pour l'entreprise. Les actionnaires et les salariés d'Enron l'ont appris à leurs dépens, les uns par la perte de leur investissement, les autres par celle de leur fonds de pension : il faut donc que l'audit interne développe son propre programme de gestion de risques avec l'aide du risk-manager.

Finalement, la gestion des risques et l'audit sont des alliés naturels, dont les actions conjuguées et la fertilisation croisée contribuent à l'excellence de la gestion de l'organisme. Toutefois elle n'est efficace que pour autant que chacune œuvre effectivement dans son domaine en indépendance et complémentarité.

La bonne gouvernance, dans les institutions financières, implique même, la création d'un troisième pilier à l'édifice de contrôle, avec le « *compliance officer* » ou directeur de conformité. Pour être efficace, le trio devra travailler en harmonie et disposer d'une autorité de sanction. Sera-t-il possible que l'un au moins tienne sa légitimité du conseil d'administration ?

V
Questions d'actualité de la gestion des risques

11
L'évolution de l'environnement de la gestion des risques

81 *La question des risques peut-elle être standardisée ?*

La question de la mise au point d'un « standard international » de gestion des risques s'est posée pendant un quart de siècle. Certains des principales associations de risk-managers, tant en Europe qu'aux États-Unis, s'y sont longtemps opposées. Mais elles ont accepté, dans un premier temps, de participer à l'élaboration de la terminologie pour le risque présentée par l'ISO (International Organization for Standardization) dans son document ISO/IEC Guide 73:2002 *Management du risque — Vocabulaire — Principes directeurs pour l'utilisation dans les normes* en version bilingue. Elles ont pris le train en marche courant 2008 alors que la norme était presque finalisée.

Il est vrai que la gestion des risques est une discipline encore en pleine évolution, et les praticiens et les universitaires véhiculent des idées divergentes sur ce que la gestion des risques implique pour un organisme ou un État, comment elle devrait être mise en place et développée, et même sur son périmètre d'action.

Dans le contexte actuel d'exigence de transparence et d'éthique dans la gouvernance des entreprises, où la gestion des risques joue un rôle primordial, à défaut de norme stricte, il faudra bien mettre en forme un consensus sur des points essentiels, tels que :

- Les objectifs de la gestion des risques en termes déclinables pour toutes les sortes d'organismes.
- Les processus de gestion des risques efficaces et efficients.
- Le fonctionnement de la gestion des risques à l'intérieur de l'organisme.
- Les facteurs permettant une évaluation objective de la qualité de la gestion des risques d'un organisme donné.
- Un glossaire pratique de référence de gestion des risques, précisant les concepts fondamentaux de la discipline.

Bien que le terme « risque » soit perçu, aujourd'hui, plus comme associé aux menaces, avec leur cortège d'impacts négatifs, la gestion des risques ne vise plus à éliminer les risques, mais au contraire à conserver un portefeuille de risques efficient, par un équilibre harmonieux entre les opportunités indispensables pour la rentabilité et les menaces acceptées ou subies, pouvant déboucher sur des sinistres. C'est pour cela que la norme ISO 31000:2010 a défini le risque comme l'impact de l'incertitude

sur les objectifs de l'organisme, c'est-à-dire que la définition inclut toutes les déviations significatives par rapport au plan ou aux attentes des parties prenantes.

Tous les spécialistes de la gestion des risques, universitaires comme praticiens, s'accordent sur certains principes de base qui sont repris dans la norme. La gestion des risques :

- est devenue une composante de toute gestion d'entreprise et elle fait partie intégrante de la gouvernance ;
- est un processus itératif découpé en plusieurs étapes à effectuer en séquence pour permettre une amélioration continue des décisions et des performances de l'entité ;
- s'appuie sur une infrastructure et une culture propre à l'entité concernée ;
- implique la mise en œuvre d'une approche méthodique, logique et systémique visant à :
  - dresser un diagnostic (identification, analyse, évaluation des vulnérabilités) ;
  - traiter les risques (réduction et financement) ;
  - auditer les processus et les mesures de gestion des risques mis en place ;
  - déboucher sur une communication interne et externe cohérente et transparente ;
  - concerner l'ensemble des risques liés aux activités, fonctions et processus (leur gestion intégrée doit permettre à l'organisme tout à la fois de maximiser ses gains et de minimiser ses pertes).

Actuellement, il existe de nombreux standards. Toutefois, si l'ISO 31000:2010 est en train de devenir la référence dans le domaine, deux standards semblent avoir une place spéciale : celui, succinct, développé en Grande-Bretagne par les associations de risk-managers et reconnu par l'ensemble des associations professionnelles européennes regroupées au sein de FERMA ; et une version plus détaillée, le COSO 3, proposée pour répondre aux exigences de la loi Sarbanes-Oxley. Quoi qu'il en soit, le groupe d'experts qui a développé la norme ISO 31000:2010 est déjà au travail pour publier une version révisée à l'horizon 2016.

82 *Qu'entend-on par gestion « holistique » des risques ?*

La gestion des risques devient une discipline du management à part entière. Elle a fait une percée au cours des dix dernières années. Les directeurs financiers et les trésoriers ont compris ce qu'ils pouvaient retirer de la quantification et du traitement d'un éventail de plus en plus vaste de risques, en explosant leur domaine traditionnel des risques financiers (risque de change, risque de taux, risques clients…) pour s'intéresser aux risques technologiques majeurs (nuages toxiques, incendies, explosion) et aux risques opérationnels (continuité de production, service informatique). Ils ont découvert les compétences et les trousses à outils de leurs risk-managers.

Dans le même temps, les rapports Turnbull et Viénot en Grande-Bretagne et en France, et King en Afrique du Sud ont donné un sens et un contenu à la gouvernance d'entreprise (voir question 87) et ont imposé la gestion des risques dans les ordres du jour des conseils d'administration.

Plus récemment, avec l'impact de la Bourse de New York, la loi Sarbanes-Oxley, avec son exigence de gouvernance fiduciaire, a étendu cette pratique à toutes les grandes entreprises cotées.

Pour rendre compte de ce nouveau concept qui doit englober tous les risques divers, différentes appellations ont été utilisées avec des succès variés :

- ***Gestion intégrée des risques :*** terme d'origine britannique pour marquer l'implication nécessaire de tous au sein des organismes.
- ***Gestion globale des risques :*** terme à double sens visant la gestion étendue à tous les risques, mais souvent entendue aux États-Unis, comme étendue à toutes les installations d'un organisme dans le monde entier.
- ***Gestion « holistique » des risques :*** le terme, forgé en France, est peu usité en dehors de l'Hexagone. L'adjectif est dérivé du grec « *holos* » qui veut dire tout. L'expression souligne la nécessité d'éliminer les « silos » pour obtenir une prise en compte optimale des risques.
- ***Gestion des risques étendue à l'entreprise :*** *Enterprise-wide risk-management* (ERM) est le terme américain trop souvent traduit comme un faux ami par « gestion des risques d'entreprise ». En français, le terme « risques d'entreprise » est synonyme de risques spéculatifs.

La traduction proposée souligne bien la notion fondamentale de création d'une culture de gestion des risques.

- ***Gestion stratégique des risques :*** le terme souligne que la gestion des risques, c'est-à-dire l'incertitude, est bien la prise en compte dans la stratégie de l'organisme. Plus récemment (en avril 2005), la *Harvard Business review* a évoqué la nécessité de gérer les risques stratégiques, mais cela revient à recréer un nouveau silo.

Il est clair aujourd'hui que, de tous ces acronymes, c'est aujourd'hui celui d'ERM qui émerge comme le vainqueur. Mais quel que soit l'acronyme, il est peut-être plus simple de revenir à la définition de Félix Kloman qui est alignée sur la définition du risque dans l'ISO 31000:2010, « *risk-management is a discipline for dealing with uncertainty* » (la gestion des risques est la discipline visant à traiter l'incertitude). Bien entendu, il va de soi que, suivant les impacts, certains risques relèvent de la gestion de terrain dans le cadre d'une politique globale tandis que d'autres, par l'ampleur de leurs conséquences, relèvent d'une approche stratégique au niveau du conseil d'administration.

C'est justement à propos de la prise en compte de l'incertitude que Peter Bernstein, auteur de l'ouvrage de référence *Against the Gods : The Remarkable Story of Risk*, donne quatre conseils de bon sens, qui renversent des lieux communs :

- Tout peut arriver. Nous ne pouvons pas connaître le futur.
- Prendre un risque ne doit pas s'appuyer, uniquement, sur votre probabilité d'avoir raison, mais également sur les conséquences d'avoir tort.
- L'instant de plus haut risque est quand vous avez raison.
- Si vous êtes à l'aise avec votre patrimoine, vous n'êtes pas diversifié. La diversification est la reconnaissance implicite de votre ignorance.

83 *La gestion des risques et la qualité, sont-elles complémentaires ou redondantes ?*

L'*European Foundation for Quality Management* (EFQM) et le DNV Consulting viennent de développer un modèle d'excellence, qui vise à proposer aux entreprises un cadre pour les aider à gérer leurs risques et à coordonner l'amélioration de leur gestion. Le modèle se veut un outil pour l'excellence en risk-management qui vise cinq objectifs traditionnels de la gestion des risques :

- Autoévaluation.
- Comparaison avec d'autres organismes (*benchmarking*).
- Identification des aspects à améliorer.
- Glossaire de base et pensée commune.
- Cadre de développement d'une gestion systémique des risques.
- Doit-on voir là, une préemption de la qualité sur la gestion des risques ?

La cohabitation entre sécurité et qualité est déjà ancienne. Lorsque les premières méthodes de qualité sont arrivées en France, avec l'importation des cercles de qualité dans les années 1970-1980, les salariés les ont souvent utilisées en priorité pour améliorer leur sécurité au travail.

Par ailleurs, au niveau de l'entreprise, il est clair que les sinistres de fréquence relèvent souvent d'actions correctrices visant à modifier le comportement des acteurs et à les encadrer dans des processus qui s'apparentent à la qualité. La dérive de la sinistralité d'une flotte automobile, par exemple, peut trouver sa source dans des erreurs de conduite, mais aussi dans des difficultés d'itinéraires, des ennuis mécaniques… Pour le transporteur public de marchandises, il s'agit bien de non-qualités, qui peuvent être corrigées par des mécanismes faisant partie de l'approche dite TQM (*Total Qualité Management*).

Au niveau des unités opérationnelles, pour l'implantation de la culture de gestion des risques, l'ingénieur qualité semble l'interlocuteur privilégié avec l'ingénieur hygiène et sécurité, d'autant qu'ils ont parfois déjà essayé de développer un système intégré sous le nom HSE (Hygiène-Sécurité-Environnement), voire QHSE en intégrant la qualité. La limite de l'exercice est qu'ils pourraient ne s'intéresser qu'aux risques dûment recensés et se prêtant à des procédures strictes, sans laisser de place pour la réflexion au niveau stratégique et aux retombées des événements extérieurs, hormis ceux qui ont des conséquences sur la santé des hommes.

Ces approches, de type OSHA par exemple, invitent à la quantification des risques, qui fait encore défaut dans beaucoup de modèles de gestion des risques pour lesquels elle est toujours un chantier en cours (lorsque les méthodes statistiques ne sont pas utilisables par manque d'échantillons suffisants, la plupart des risk-managers sont ramenés à une évaluation « qualitative »).

En revanche, pour les risques peu vraisemblables mais de gravité exceptionnelle, ces modèles ne sont pas adaptés, car ils supposent de développer des scénarios pour lesquels l'imagination est essentielle (voir question 70).

Qualité et gestion de risques doivent donc travailler en coopération dans tout organisme.

La situation se présente différemment dans le secteur des PME/PMI de la sous-traitance qui ont investi dans le recrutement d'un ingénieur qualité pour obtenir la qualification ISO exigée par leurs donneurs d'ordre pour la poursuite de leur collaboration. Leur taille ne leur permettra pas de répéter l'opération pour la gestion des risques, et l'externalisation totale est difficile (voir question 75). Or, pour la mise en place de la démarche qualité, l'ingénieur, chef de projet, a dû s'impliquer dans tous les processus de l'entreprise et se faire accepter sur le terrain. On notera que se pose aujourd'hui la question de l'inclusion de la gestion des risques dans toutes les normes ISO.

Pour résoudre la question de la gestion des risques dans les PME/PMI, il est sans doute possible d'envisager de former à cette nouvelle discipline les ingénieurs qualité. C'est certainement pour eux un moyen d'échapper à l'enfermement dans un métier très technique et d'aborder leur entreprise par le biais de la vision globale et de la stratégie. Et ce, en intégrant l'ensemble des obligations et en capitalisant sur le document unique de l'analyse des risques professionnels par poste, pour déboucher sur cette approche globale et stratégique de la gestion des risques.

84 *La gestion des risques pour un projet est-elle spécifique ?*

Les organismes sont de plus en plus engagés dans des développements en mode projet. Les entreprises les plus innovantes sont construites comme une flottille de projets, autour d'un vaisseau amiral qui se contenterait de fonctionner comme un pilote de stratégie, un chasseur de talents, une banque d'affaires et un pôle de gouvernance et de gestion des risques.

Dans ces conditions, les managers opérationnels ne sont plus en charge d'un centre de profit pour un mandat limité, mais des chefs de projet, c'est-à-dire des patrons d'entreprise provisoires, dont le voilier mené à bon port sera remis dans d'autres mains. La gestion des risques liés à cette opération est donc au cœur du processus, et certains en viennent même à suggérer que le diagnostic des risques pourrait servir de grille de référence pour la prise des décisions tactiques, pendant toute la durée du projet.

En réalité, la gestion de projet est bien un métier spécifique, mais la gestion du risque projet vient éclairer et donner un sens aux arbitrages successifs qui doivent conduire au succès final ou à l'arrêt rapide, si l'échec est perçu comme inéluctable dans des entreprises par nature « à haut risque ». Comme les échecs ou les dérives de projets d'informatisation l'ont montré, trois éléments viennent modifier le schéma traditionnel de la gestion des risques par rapport aux entreprises en croisière :

- ***Définition précise de la mission ou de l'objectif :*** beaucoup de projets se perdent dans les sables, parce que l'équipe n'a pas défini avec précision l'objectif poursuivi. Dans le cas des projets informatiques, trop souvent, les attentes des utilisateurs finaux sont modifiées en cours de route. C'est-à-dire que le cahier des charges n'a pas été défini sur la base d'une assez large consultation des personnes concernées, mais a été établi par les consultants informatiques internes ou externes.
- ***Respect des délais :*** il passe par l'établissement d'un PERT, une approche traditionnelle de recherche opérationnelle qui permet de découper le projet en étapes élémentaires. En tenant compte des antécédents, on construit un schéma représentant le projet et donnant un « chemin critique », c'est-à-dire l'ensemble des opérations ou des étapes qui déterminent la durée du projet. La mise à jour régulière du schéma donne une liste de priorités pour le suivi du projet et des risques à soigner sans retard.

On connaît les projets d'informatisation qui doivent être opérationnels en six mois et qui ne fonctionnent pas encore au bout de deux ans, par manque d'attention sur l'essentiel.

- ***Respect du budget :*** la rentabilité d'un projet s'appuie sur les retombées qu'il doit générer (l'analyse des flux de trésorerie générés sur une durée relativement courte, de six à soixante mois, par exemple). Une dérive significative dans les dépenses initiales peut détruire la rentabilité du projet, même s'il est mené à bien. La mise en péril de PME/PMI pour lesquelles le projet d'informatisation s'éternise et dépasse largement le budget initial n'est pas une légende, sans parler des projets publics de ponts ou de tunnels rendus célèbres par leur facture finale !

Attention, comme il a été souligné pour la gestion des risques en général, le risk-manager du projet est le chef de projet. Le gestionnaire des risques de l'entreprise doit rester à sa place de consultant interne et ne pas se substituer à celui qui connaît les techniques et les enjeux du projet.

Toutefois, le projet avec un seul mandant est relativement rare en ces temps où la coopération, voire la « coopétition » devient la règle pour des investissements lourds qui dépassent les capacités financières et les compétences d'un seul organisme. Les projets collectifs posent des questions spécifiques.

La gestion des risques devra faire partie des éléments du contrat signé entre les partenaires, ainsi que les conditions de sous-traitance éventuelle, car les philosophies, cultures et appétits de risques des différentes entités peuvent être divergents. Elles doivent s'entendre, en particulier pour que le « pilote » soit protégé contre les réclamations ultérieures de ses partenaires. En cas de coopération avec un concurrent, de « coopétition » (comme celle entre deux laboratoires pharmaceutiques pour développer en commun une molécule), il faut être vigilant pour assurer l'étanchéité des équipes, afin que le projet ne devienne pas un « nid d'espions ».

85 *Peut-on se protéger contre le terrorisme ?*

Le terrorisme n'est pas nouveau, la Grande-Bretagne avec l'IRA et l'Espagne avec l'ETA, y sont confrontées depuis des années. La France n'oublie pas les attentats de 1995 et le détournement du vol Alger-Paris, sans parler de la disparition du vol UTA au-dessus du désert du Sahara. De plus, la menace terroriste a de toute évidence pris une nouvelle dimension avec les attentats du 11 septembre à New York et Washington, entretenue avec ceux de Madrid en 2004 et de Londres en 2005.

L'objectif du terrorisme se distingue dans son nom même. Il vise à paralyser ses adversaires en suscitant la terreur dans les populations pour faire avancer ses options politiques ou religieuses. C'est pourquoi le choix des cibles et les modes d'actions sont dictés par des considérations d'une nature autre qu'économique.

Certains spécialistes essaient de développer des modèles d'action et des profils psychologiques, qui puisent une partie de leur réflexion sur les nihilistes et les anarchistes du passé, mais doivent prendre en compte l'impact des communications modernes qui amplifient les actes, et facilitent leur « délocalisation ». Ils permettent aux gouvernements de chercher des parades, mais la lutte contre le terrorisme relève d'une politique internationale concertée, plutôt que de l'action d'un acteur économique individuel.

Alors, les organismes privés sont-ils totalement impuissants devant les actes terroristes ? Pratiquement, comme dans le cas des événements naturels, elles n'ont aucun moyen de les empêcher. Il n'y a donc pas de prévention possible au niveau des acteurs individuels.

En revanche, s'ils acceptent de ne pas essayer de mesurer un rendement sur investissement, car la quantification d'un risque non modélisable est pratiquement impossible, la mise en place de mesures de prévention et de protection pour réduire l'impact d'un attentat est réalisable, et peut se traduire par :

- Ne pas être une cible appétissante : puisque les terroristes cherchent un maximum de publicité, ils s'attaquent de préférence à des marques globales, bien connues, plutôt que des marques locales limitées. Mais on l'a vu, bâtir des marques globales fortes est un objectif central des entreprises multinationales.

- Éviter les enseignes trop voyantes dans les pays à risques, car les terroristes peuvent souhaiter que les caméras de télévision soient en mesure de les montrer au monde entier.
- Ne pas prendre de position politique « implicite » : par exemple, éviter de s'installer dans les pays en but à des organismes terroristes, ou d'apparaître comme des soutiens.
- Limiter les déplacements d'affaires dans les zones à risques : certains pays sont le siège d'enlèvements à but terroriste. Il faut donc limiter les séjours de cadres ou de dirigeants dans ces pays et les relever régulièrement de façon à ne pas expatrier les familles.
- Être mobile et éviter les habitudes : cela s'applique aux locaux professionnels, aux hôtels, voire aux horaires de déplacements des dirigeants.
- Protéger les données et les circuits informatiques (ceci est à rapprocher de la question 33).
- Protéger médicaments et aliments contre les risques de contamination (en particulier en les protégeant par des emballages adéquats).
- Protéger et surveiller les sites névralgiques avec une enquête sur les visiteurs et le repérage des mouvements suspects.
- Gérer le personnel dans les sites névralgiques et coopérer avec les forces de l'ordre dans toute l'étendue des limites autorisées par la loi.
- Mettre en place des plans de secours et de gestion des crises pour permettre une évacuation rapide en cas d'attentat.

Au bout du compte, on s'aperçoit que l'impact financier potentiellement catastrophique des attentats fait que le recours à l'assurance est pratiquement incontournable.

La difficulté de modéliser, évoquée plus haut, fait que l'offre privée d'assurance est limitée. Les principaux pays développés ont mis en place des mécanismes, plus ou moins efficaces, soutenus par les États : c'est cas en France.

Toutefois, le Congrès des États-Unis remet régulièrement en cause le sien, basé sur la loi « *Terrorism Risk Insurance Act* » (TRIA) entrée en vigueur le 26 novembre 2002, au lendemain des événements du 11 septembre. Ce mécanisme d'assurance (système TRIA), mis en place pour une durée de trois ans, s'est achevé en 2005 et a été régulièrement reconduit depuis, avec de plus en plus de difficultés : le marché privé de l'assurance ne semble pas avoir un appétit féroce pour la couverture de ce risque.

86 *L'externalisation a-t-elle un impact sur la gestion des risques ?*

Le principal objectif de la gestion des risques est de garantir la continuité des opérations, en toutes circonstances. Dans la mesure où il maîtrise l'ensemble du processus de fabrication et de distribution de ses biens et services, un organisme peut mettre en place les processus de gestion des risques qu'il souhaite et veiller à sécuriser sa chaîne logistique de bout en bout.

La tendance actuelle, pour chaque entité, est de concentrer ses efforts sur son cœur de métier et d'externaliser les opérations qui peuvent être réalisées plus économiquement par des partenaires, amont et aval, en leur confiant la sous-traitance de parties ou de pièces. Par exemple, en aval, en confiant le transport et la vente des produits finis à des transporteurs et à des distributeurs indépendants (voir questions 5, 30 et 36).

Bien entendu, en transférant la réalisation des opérations à un tiers, l'organisme transfert la gestion des risques associés, dont il n'est plus directement responsable, mais également, dont il n'a plus la maîtrise (voir question 45). En fait, comme nous l'avons déjà souligné, en matière de « réputation », qui est l'actif immatériel le plus important de la plupart des organismes, la clé est la confiance des parties prenantes, le risque ne se compartimente pas et c'est la réputation entière qui peut être compromise, si un partenaire ne respecte pas les règles éthiques, légales ou non, attendues de l'organisme.

Sans reprendre l'ensemble du discours, on peut donner quelques règles simples, à retenir dans le choix des partenaires lors d'un processus d'externalisation.

La règle des « trois C » se résume ainsi :

- ***Choisir :*** chaque partenaire potentiel doit être validé pour la qualité de ses produits ou services, sa solidité financière et la nature de son actionnariat, sa pérennité, la composition de sa direction. Il faut également valider sa réputation parmi ses clients actuels, ses concurrents et vérifier les risques naturels auxquels il pourrait être exposé. Enfin, il faut clairement poser des questions sur sa philosophie en matière de risques et les mesures qu'il prend dans ce domaine, ainsi qu'en matière de gouvernance. En un mot, avec les partenaires-clés, il convient de mener l'équivalent d'une « *due diligence* » en matière de rachat.

- ***Contracter :*** le contrat est le seul document qui va faire la loi des parties. Il doit contenir un maximum de provisions pour le règlement « pacifique » des litiges qui peuvent naître entre les parties dans le cours de leur « vie commune ». À chaque fois qu'une question conduit à la réponse « cela va de soi », il est temps de mettre en forme dans une clause de ce qui vient d'être débattu. Si le donneur d'ordre souhaite vérifier le travail dans les sites de production du partenaire, il faut l'inscrire dans le contrat, c'est indispensable, s'il est implanté dans un pays politiquement sensible.

  Un cas particulier : si le partenaire n'est pas équipé pour répondre efficacement aux réclamations des clients communs, ou dans le cas où sa surface financière le rend vulnérable, il peut être de bonne gestion de proposer de le protéger avec une clause de protection étendue (*Hold Harmless Clause*) par laquelle le donneur d'ordre répondra pour lui, pour toute mise en cause relevant des produits du contrat. Pour les PME/PMI ou les ETI qui approvisionnent des entreprises multinationales, ce peut être la condition de l'acceptation d'un marché, par exemple si les produits finis aboutissent sur le marché américain.

  Mais attention aux grands donneurs d'ordre américains, tentés d'imposer de telles clauses à leur profit aux partenaires en dehors des États-Unis qui n'en mesurent pas toujours la portée.
- ***Contrôler :*** tout au cours de la vie du contrat, les partenaires évoluent, les dirigeants se retirent ou démissionnent, le produit connaît des évolutions technologiques, l'actionnariat peut changer. Il est donc essentiel de vérifier que la « qualité » de la relation se maintient dans le temps.

Même si les qualifications ISO, en matière de qualité et d'environnement, ont leurs limites, leur mention dans les contrats permet tout de même de garantir, au moins, le respect de certaines normes et procédures. Aujourd'hui, malgré la référence croissante à la norme ISO 31000:2010 *Management du risque — Principes et lignes directrices*, non certifiable, il n'existe pas à ce jour d'équivalent reconnu internationalement pour la gestion des risques, c'est pourquoi la règle des « trois C » est un bon bouclier ainsi que la présence d'un risk-manager certifié ONR 49000 au sein de la direction du partenaire.

87 *Pour qui la gouvernance est-elle une sécurité ?*

Parmi les champs d'action définis par l'approche cindynique en combinant plusieurs dimensions, celui regroupant objectifs, normes et valeurs a défini le domaine de l'éthique en action.

À ne juger que par les publications et les colloques, l'éthique prend une part croissante dans toute réflexion sur la gestion des organismes, qu'il s'agisse d'entreprises du secteur privé, d'établissements de soins ou de collectivités locales, voire des États eux-mêmes. Les dirigeants, comme les élus, ne peuvent plus se contenter de gérer les moyens, sans remettre en cause les fins, c'est-à-dire qu'il leur faut réviser les objectifs, redéfinir les normes et analyser les valeurs. Cette recherche a débuté il y a une quinzaine années, et il est impossible de ne pas la rapprocher de la chute du mur de Berlin qui a marqué la fin du contremodèle, du contrepoids à l'économie de marché.

En toute hypothèse, il est clair que la définition de standards ou de recueils des bonnes pratiques ne peut pas se limiter à l'efficacité économique ou à la création de « valeur pour les actionnaires ». La responsabilité de l'affectation de ressources parfois considérables, puisque supérieures au PIB de bien des nations, exige que les détenteurs de cette autorité s'interrogent sur les fins auxquelles ces moyens sont affectés.

Donc, ceux qui dirigent de grands conglomérats, mais aussi les chefs d'entreprises plus modestes, les maires, comme les présidents et les directeurs d'hôpitaux, doivent revoir leurs objectifs, redéfinir les normes et établir les valeurs, en prenant en compte l'ensemble des composants de la « valeur pour toutes les parties prenantes ».

C'est pourquoi, pour asseoir l'avenir d'un organisme et garantir sa résilience dans la tempête, il faut que chacun repense une philosophie de l'action en reposant la question des missions de la société prise dans sa globalité. En réalité, une conduite éthique passe par la définition de valeurs claires et comprises de tous, définissant une frontière que l'on ne veut pas franchir.

Mais cette limite, au-delà de laquelle il n'existe qu'un champ de mines prêtes à exploser à tout moment, n'est pas universelle : elle varie d'une personne à l'autre, d'une entreprise à une autre, d'un État à l'autre, elle est partie intégrante de la culture.

En particulier au niveau de chaque entreprise, pour « vivre et grandir ensemble », il faut que les dirigeants donnent l'exemple et définissent ce cœur de valeurs communes qui attireront et retiendront les collaborateurs compatibles.

Vivre l'éthique au quotidien, ce n'est pas se poser la question :

- « *Pourrais-je faire cela ?* » (c'est-à-dire : est-ce légal, dans les limites des lois et règlements ?),

mais la remplacer par la question supérieure :

- « *Devrais-je agir ainsi ?* » (c'est-à-dire : est-ce en accord avec mes principes, pourrai-je me regarder demain dans un miroir, si ma décision fait la une des journaux, pourrai-je regarder en face mes collègues, mes collaborateurs, mes amis, mon conjoint, mes enfants ?).

En un mot, la question de l'éthique ne pourrait-elle pas se résumer en une nécessité vitale :

« N'est-il pas grand temps, tout simplement, de replacer l'Homme au centre de tout dispositif économique ? »

Éthique et gouvernance sont au cœur du processus de création de réputation, c'est-à-dire de l'élaboration d'une image positive, et sont un ingrédient stratégique de la résilience dans la tempête.

La confiance de l'ensemble des parties prenantes est l'outil ultime de la survie dans une société, tellement conduite par l'image !

Six principes de la bonne gouvernance résultent du nouveau code qui s'impose aux collectivités territoriales britanniques :

- Les efforts et les moyens de l'organisme doivent être engagés exclusivement pour la satisfaction des utilisateurs et des citoyens.
- Chacun doit travailler efficacement dans le cadre de missions et de rôles clairement définis.
- Les valeurs de l'organisme de bonne gouvernance doivent être affichées et appliquées dans la pratique dans l'ensemble de l'organisme.
- Les décisions doivent être prises de façon transparente et informée, en intégrant la gestion des risques impliqués.
- Développer la capacité et les compétences des dirigeants pour qu'ils soient efficients.
- Établir une communication effective avec l'ensemble des parties prenantes, et se rendre réellement compte des résultats.

Le risque de conduite ou de comportement

En lien étroit avec la gouvernance et les conformités, on notera que le « risque de conduite » ou de comportement (*conduct risk* en anglais) devient une préoccupation croissante dans les organismes soucieux de leur « image » ou de leur réputation. Ce qui génère ce risque, ce sont tous les comportements des collaborateurs au sein de l'organisme qui ne seraient pas en conformité avec la réglementation, les pratiques professionnelles et plus généralement l'éthique.

À la suite de travail des organismes de contrôle depuis le déclenchement de la crise financière et économique en 2008 (en particulier des organismes financiers), un consensus se dégage pour définir le risque de conduite comme celui associé avec la conduite des dirigeants, responsables et collaborateurs de tout niveau d'un organisme. Cela inclut la culture, la gouvernance, l'exemplarité des dirigeants, les relations avec les clients, la structure des rémunérations et comment l'organisme gère les situations de conflit d'intérêt.

Il ressort d'enquêtes récentes que la structure de rémunération est un des principaux outils d'alignement du comportement des collaborateurs sur les attentes des dirigeants, et du public (se référer au *« Thomson Reuters Conduct Risk Report 2013 »* : info.accelus.thomsonreuters.com/2013ConductRiskSurveyReport).

Bien qu'il n'y ait pas d'indice défini pour suivre ce risque dont la gestion demeure embryonnaire, l'exigence de transparence toujours plus grande du public (sous l'œil attentif des médias sociaux), implique que tous les dirigeants l'intègrent dans leur réflexion, en particulier dans les banques, les fonds de pension et les assurances.

88 *Les règles comptables ont-elles un impact sur la gestion des risques ?*

Les entreprises européennes cotées en bourse connaissent une évolution profonde, voire une révolution, dans leurs pratiques comptables. En effet, elles sont tenues d'arrêter leurs comptes consolidés dès 2004 et 2005 dans le respect des standards IAS (*International Accounting Standard*), dont on sait qu'ils sont inspirés étroitement des principes comptables des États-Unis connus sous le nom de FAS.

Les standards acceptés par l'Union européenne et qui s'imposent donc à tous les pays membres sont connus sous le nom d'IFRS (*International Financial Reporting Standards*). L'Union européenne a adopté l'essentiel des recommandations IAS, résultant de l'IFRS et de l'IFRIC (*International Financial Reporting Interpretation Committee*).

Seules huit n'ont pas encore été acceptées, et ne le seront peut-être jamais. Pour celles-ci le *statu quo* prévaut avec le maintien des règles nationales actuelles. Les lecteurs concernés sont invités à se reporter aux publications spécialisées, mais il convient de souligner que de ces huit dispositions, la plus importante est l'IAS 39 qui vise les instruments financiers.

Bien entendu, le premier risque de cette évolution du cadre de référence est qu'elle laisse des marges à de nouvelles interprétations, et modifie les conditions dans lesquelles les résultats des entreprises concernées sont calculés.

Elles ont donc entraîné des « volatilités » apparentes dans les résultats annoncés pour les exercices 2004 et 2005, et les effets négatifs sur la tenue des cours de bourse ont été effacés par les événements découlant de la crise initiée par l'affaire des *subprimes* aux États-Unis. Toutefois, il a fallu former les cadres comptables et la réforme a engendré un surcroît de travail pour remettre une courbe à jour, en réinterprétant le passé récent à la lumière des nouveaux principes comptables. Quelles sont les autres conséquences les plus significatives ? Pour revenir sur la gouvernance fiduciaire évoquée à la question précédente, il faut noter un certain nombre d'effets positifs :

- Toutes les sociétés cotées seront désormais soumises aux mêmes règles comptables, ce qui facilite une comparaison et le travail des administrateurs extérieurs qui officient dans plusieurs entreprises.

- Tous les éléments d'actif et de passif doivent figurer sur le bilan, ce qui accroît la transparence.

Mais le plus gros souci découle de la volatilité accrue des actifs qui doivent être désormais évalués en valeur de marché. Les principales préoccupations recouvrent :

- Le lissage dans le temps qui est remis en cause. C'est un problème spécifique pour les assureurs vie qui ne peuvent plus tenir compte de la congruence entre actifs et engagements à long terme (ils peuvent apparaître indûment fragiles).
- La nouvelle donne pour le choix d'achats et d'investissements pour certains produits de financement alternatif qui introduit une incertitude, même au niveau des produits à long terme en place.

Un volet particulier concerne l'IAS 39 déjà citée et non adoptée : la situation a un impact particulier sur les banques et laisse ouverte la question de la couverture en « juste valeur » du risque de taux d'intérêt d'un portefeuille.

Par-delà ces considérations générales, il faut envisager l'impact spécifique sur les instruments de financement des risques. Rappelons que les instruments financiers doivent être évalués et enregistrés chaque année à leur « valeur de marché ». Les conséquences sont les suivantes :

- Le lissage d'année en année de certains produits multiannuels est remis en cause.
- Les produits basés sur des indices créés spécifiquement et non publics (par exemple, le prix des voitures d'occasion) n'ont pas de valeur de marché. Seront-ils encore autorisés dans ce nouveau contexte comptable ?

Tous les produits traditionnellement traités « hors bilan » peuvent avoir un impact significatif non seulement sur les résultats publiés, mais même encore sur les équilibres bilanciels et, pour les assureurs, sur les ratios prudentiels.

89 *Qu'est-ce que le développement durable ?*

Le terme « développement durable » est devenu un passage obligé de tout discours politique en Europe. Il est né pratiquement avec le rapport Brundtland de 1987, lui donnant une première définition qui reste la référence : « *Un développement qui répond aux besoins du présent, sans compromettre la capacité des générations futures de répondre aux leurs.* »

Elle demeure la référence, mais sa compréhension a évolué au travers des deux dernières décennies pour toucher des domaines différents. En effet, elle est sortie du strict domaine du respect de l'environnement pour partager les différents aspects de toute vie humaine. C'est à Rio, en 1992, dans ce qui est connu sous le nom de « déclaration de Rio » que certains principes fondamentaux ont été posés, à l'issue de la conférence des Nations unies sur l'environnement et le développement.

Quatre principes émergent de cette déclaration révisée à l'occasion du second sommet en 2012 :

- ***Principe de précaution*** : lorsque des conséquences lourdes, des dommages graves ou irréversibles pour les personnes ou l'environnement, ou l'absence de certitudes scientifiques ne peut pas constituer une excuse pour ne pas adopter toute mesure visant à rendre impossible ces conséquences.
- ***Principe de prévention :*** les acteurs économiques doivent s'efforcer de réduire, voire d'éliminer, les rejets de substances potentiellement nocives et mettre en œuvre des procédés moins polluants.
- ***Principe de réparation :*** l'acteur économique à l'origine de toute pollution doit assumer le coût de la réparation des dommages provoqués, de façon à intégrer dans la transaction, l'externalité négative qui fausserait le jeu normal de la concurrence, au niveau national, comme au niveau international.
- ***Principe de solidarité :*** les échanges commerciaux et la coopération internationale doivent être basés sur la transparence, de façon à ce que tous les acteurs économiques et politiques soient pleinement conscients des risques qu'ils courent ou font courir à leurs populations, dans le but de partager les responsabilités communes face au présent et à l'avenir.

L'application de ces principes, au niveau de chaque acteur économique, fait partie aujourd'hui de la « gouvernance » et replace les décisions des dirigeants dans une perspective de plus long terme. En effet, les deux dernières décennies ont été marquées par une accélération des rythmes d'évolution dans les entreprises avec la pression des marchés financiers pour des rendements à court terme. Les grandes places financières ont pris l'habitude de lire les résultats des entreprises, non pas en termes d'année, mais de successions de trimestres, ce qui condamne les décisions d'investissement à long terme.

C'est dans le cadre du « développement durable » que l'on a vu apparaître d'autres préoccupations des investisseurs individuels. On peut soutenir que les « fonds d'investissements éthiques » et le « commerce équitable » sont la traduction pratique des principes contenus dans le concept de « développement durable ».

Parallèlement, les financiers ont pris la mesure de l'impact exponentiel de l'exigence d'un rendement sur capitaux de 15%, alors que l'analyse historique sur 150 ans tend à montrer que des rendements réels, hors inflation, supérieurs à 1% sont rares sur de longues périodes.

C'est pourquoi aujourd'hui un nouveau concept voisin prend corps sous le nom de « développement soutenable ».

Une appellation qui fait référence, non seulement aux principes évoqués ci-dessus, mais également à la capacité de soutenir un taux de croissance à long terme pour les actionnaires. Elle recentre l'action des acteurs économiques dans le cadre d'une vie humaine, considérant le développement de l'entreprise en termes de décennies, plutôt qu'en trimestres, replaçant effectivement sa croissance en ligne avec celle de la vie humaine et de la société qui l'alimente. En permettant les investissements à long terme dans la recherche et le développement, elle peut effectivement contribuer à la croissance économique, effective à long terme, apportant la satisfaction des besoins des générations présentes et futures.

Pour une approche plus précise du développement durable, le lecteur peut se référer à l'ouvrage d'Alain Jounot (voir Bibliographie).

12
Les nouveaux chantiers de la gestion des risques

90 *Hygiène, sécurité et environnement : font-ils partie de la gestion des risques ?*

Les questions touchant à l'hygiène et la sécurité sur le lieu de travail font l'objet d'un ensemble de textes législatifs et réglementaires spécifiques, relevant de droit commun comme de droits spécifiques, pour l'essentiel dans le Code du travail et dans le Code de la sécurité sociale.

Le recrutement et la mise en place d'ingénieur hygiène et sécurité a trop longtemps été considéré comme une panacée relevant des ressources humaines, avec l'implication du comité d'hygiène, de sécurité et des conditions de travail (CHSCT) dans les organismes où la loi en prévoit l'existence.

Traditionnellement, le risk-manager en France issu de l'assurance ne s'en préoccupait pas, mais il a fait irruption dans son domaine par le biais de la mise en cause de la responsabilité pénale des dirigeants, en particulier par la « mise en cause de la sécurité d'autrui ».

L'évolution législative a abouti à définir une obligation de résultat de sécurité sur le lieu de travail, dont « *il appartient au chef d'entreprise de veiller personnellement et à tout moment à leur [les dispositions du Code du travail] constante application* » (Cour de cassation, chambre criminelle, arrêt du 20 novembre 1974).

Sans aller dans le détail des conditions de « protection », il convient de rappeler que la délégation de cette responsabilité à des collaborateurs est très encadrée : il faut que la direction, ou la surveillance des services en cause, ait été déléguée à des « *préposés investis par eux et pourvus de l'autorité, de la compétence et des moyens nécessaires pour veiller efficacement […] au respect des lois et règlements* » (Cour de cassation, chambre criminelle, arrêt du 22 avril 1966).

L'extension du risk-management à la protection des dirigeants pour garantir la sérénité de leurs décisions et leur implication dans le domaine de la sécurité au travail suffirait à justifier l'intérêt du gestionnaire des risques.

Toutefois, d'autres éléments sont également à prendre en compte :

- Les accidents du travail et les maladies professionnelles sont une charge significative des entreprises, dont la plupart assume la réalité des coûts, même s'il revêt la forme de cotisations appelées par un organisme public et étalées dans le temps (site de plus de 200 salariés).

En outre, les accidents du travail se prêtent particulièrement bien aux approches de retour d'expérience et d'arbres des causes, qui permettent d'éviter que des événements similaires se renouvellent sur le site concerné comme dans l'ensemble de l'organisme avec, le plus souvent, l'identification de défauts de procédures ou de non-respects auxquels on peut remédier par l'apprentissage et la formation.

- Aujourd'hui, l'obligation d'un organisme quelle que soit sa taille, public ou privé, est de réaliser un « document unique » impliquant une réflexion globale sur les risques professionnels. Le décret du 5 novembre 2002 vise la création d'un document qui répertorie les postes de travail et indique pour chacun une évaluation des risques pour la santé et la sécurité des travailleurs. La transcription doit être faite par unités de travail, dans un document unique.
- L'intérêt est une incitation à l'amélioration de la prévention et de la protection avec le suivi annuel de l'évolution.
- Il existe une offre fournie sur le marché, pour assister les organismes à se mettre en conformité avec la loi, avec des supports informatiques pour les mises à jour ultérieures. Bien que le document soit obligatoire depuis fin 2003, il semblerait que de nombreux organismes ne soient pas à jour, en particulier dans le domaine public, mais aucune enquête fiable ne permet de corroborer ce fait. On peut dresser un décalogue des recommandations sur les qualités souhaitées pour le « document unique » :
  - être synthétique ;
  - se limiter à l'essentiel ;
  - être compréhensible par tous les salariés ;
  - démontrer la volonté de satisfaire à l'obligation de résultat de sécurité ;
  - procurer des évaluations pertinentes ;
  - proposer des pistes d'amélioration réalistes.
- Construire des solutions transdisciplinaires.
- Contenir un dispositif simple de « veille ».
- Offrir une fonctionnalité de mise à jour.
- Soutenir les politiques arrêtées par les dirigeants.

91 *Dans les établissements financiers, quelle est la différence entre Bâle 2 et la gestion des risques opérationnels ?*

Le secteur bancaire constitue un élément moteur essentiel du système économique mondial, en particulier en dynamisant l'investissement à grande échelle. Son cœur de métier est donc étroitement lié à l'analyse systématique des risques. Le secteur est soumis à nombre de réglementations nationales et internationales.

Le comité international de Bâle est à l'origine d'un ratio de la solvabilité simple (Ratio Cooke, en 1988), mais un nouveau ratio a été introduit (Ratio Mc Donough) qui prend en compte l'ensemble des grandes lignes d'activité des établissements financiers : les banques, les sociétés de gestion d'actifs, les OPCVM, les sociétés de *factoring* et les sociétés de *leasing*.

Sa mise en œuvre qui s'étend sur la période 2005 à 2007 a induit des chantiers importants dans les grands établissements financiers, visant à la mise en place d'une gestion globale des risques, dépassant les traditionnels risques financiers pour s'étendre à l'ensemble des risques opérationnels.

La réglementation, dont les textes ont été finalisés en 2004 sous le nom de Bâle 2, s'appuie sur trois piliers non remis en cause dans la nouvelle version dite Bâle 3 :

- ***Pilier 1. Niveau des fonds propres :*** en formulant des exigences quantitatives face aux risques estimées, la réforme incite à une saine gestion des risques, en les réduisant en fonction de la qualité de cette gestion.
- ***Pilier 2. Processus de surveillance prudentielle :*** la mise en place d'un système de gestion globale des risques, déclinée pour chaque métier significatif, s'accompagne de choix de niveaux d'implication qui permettent d'apprécier la qualité du dispositif et de son impact sur les exigences de fonds propres.
- ***Pilier 3. Discipline de marché :*** elle se manifeste par des exigences de diffusion par les établissements financiers d'une information transparente et claire sur la gestion de risques. La gestion des risques devient donc un élément significatif pour les structures de tutelle et les établissements de cotation.

Sans aller dans le détail, on peut rappeler les trois niveaux de gestion des risques proposés dans le cadre du nouvel accord :

- ***L'approche par indicateur de base :*** cette dernière exonère la banque d'établir un modèle de gestion des risques, mais impose ses propres limites.
- ***L'approche standardisée :*** elle correspond à une analyse par activités.
- ***L'approche par mesures internes :*** il s'agit d'une analyse en profondeur des risques qui correspond à l'approche AMA (*Advanced Measures Approach*) et qui laisse aux banques le soin de mettre en place, en interne, de nouveaux modèles qui ont été évalués à l'échéance prévue (fin 2006).

Comme nous l'avons indiqué plus haut, la principale novation est l'introduction de la notion de « risque opérationnel » dans le texte même de la « feuille de route » proposée dans le document « Saines pratiques pour la gestion et la surveillance du risque opérationnel ». Sans aller dans le détail, des dix principes cités dans le document, on peut rappeler les principaux objectifs :

- Créer un cadre général favorisant la gestion des risques et placé sous la responsabilité du conseil d'administration et de la direction générale.
- Gérer, effectivement, les risques opérationnels, en mettant en place un processus systématique pour les diagnostiquer (identification et quantification), les traiter (réduction et financement) et les piloter.
- Auditer les dispositifs mis en place et leur fonctionnement, en ayant recours aux services d'auditeurs internes indépendants des responsables de la gestion des risques.

Bien entendu, l'application de la feuille de route passe par la création d'un cadre de référence, d'un référentiel accepté par l'ensemble des intervenants. Celle proposée par le régulateur est marquée par son objectif et ne permet pas une lecture détaillée des risques liés à l'activité bancaire dans tous leurs aspects. En réalité, les banques les plus avancées dans ce chantier semblent avoir retenu l'approche des vulnérabilités en trois composantes et la grille d'identification et d'analyse proposée dans cet ouvrage, ce qui en illustre encore l'adaptabilité.

92 *Qui est en charge de la gestion des risques d'une entreprise ?*

Par-delà la nécessité de l'implication de tous dans les efforts de gestion des risques, ainsi qu'il a été souligné aux questions 67 à 69, il est indispensable qu'un membre de la direction s'implique directement dans le dossier, au besoin en acquérant des compétences spécifiques dans ce domaine. Dans les organismes dont la taille le justifie, c'est un professionnel spécialisé qui aura la responsabilité de la définition et du suivi de l'exécution de la politique de gestion des risques en délégation de la direction générale.

Toutefois, les contours et le positionnement de la gestion des risques peuvent différer assez largement d'un organisme à l'autre. Il faut, bien entendu, définir les missions du risk-manager et l'AMRAE a récemment proposé un référentiel métier pour en fixer les domaines de compétences. Il ne s'agit pas de paraphraser ce document ici, mais d'indiquer les tâches au cœur de la fonction qui ne peuvent pas être déléguées. Elles sont articulées autour de trois pôles fondamentaux.

Définition de la politique générale de gestion des risques

Le gestionnaire de risques doit avoir une compréhension solide de la stratégie de l'organisme pour développer des programmes de gestion des risques qui viendront en appui de cette stratégie. C'est donc à lui d'en définir la structure et les composantes pour atteindre effectivement les objectifs assignés par la direction. C'est pourquoi, dans sa fonction de conseil auprès de l'ensemble des dirigeants et responsables opérationnels, il doit :

- Assister les dirigeants pour l'élaboration de la politique générale en matière de risques, en liaison étroite avec la stratégie.
- Planifier, organiser, animer et contrôler les ressources du service de gestion des risques.
- Assister les responsables opérationnels dans tout l'organisme pour la mise en œuvre, dans le cadre de leurs compétences respectives, des applications de la gestion des risques comme instrument de la performance.
- Travailler avec les responsables opérationnels pour la définition des responsabilités et des actions de leurs subordonnés en la matière et participer aux efforts de motivation nécessaires.

- Répartir les coûts de la gestion des risques entre les différents centres de profit de façon juste, pour refléter les risques encourus, et incitatrice pour prendre en compte les efforts de chacun pour contenir ses risques.
- Maintenir le programme à jour, en l'adaptant aux évolutions de l'organisme, en ajustant le traitement pour prendre en compte les modifications internes et l'évolution de l'offre pour maintenir l'optimum d'efficacité économique.

Choix et mise en œuvre de la réduction des risques

Son rôle essentiel est de conseiller les dirigeants sur les instruments de la résilience de l'organisme, en particulier les réactions aux situations de perturbations importantes (plan de continuité en situation d'urgence et plan de redéploiement stratégique en situation de précrise ou de crise).

Mais il doit également au quotidien :

- Mettre l'accent sur la sécurité comme partie intégrante de l'effort de gestion des risques, sur l'encouragement et la récompense des performances des salariés en matière de sécurité, sur les corrections à apporter dans les cas où les résultats ne sont pas suffisants.
- Coordonner tous les efforts de chacun en matière de mesure et de réduction des périls pesant sur l'entreprise, et mettre à disposition les services et équipements nécessaires.
- Informer les responsables opérationnels sur leurs responsabilités en matière de sûreté et de sécurité pour les opérations qu'ils contrôlent.
- Résoudre les éventuels conflits entre responsables opérationnels sur les meilleurs instruments pour réduire les risques et expliquer la mise en œuvre des politiques arrêtées.
- Exercer effectivement l'autorité qui lui est conférée en la matière, et particulièrement dans les situations d'urgence ou de crise.
- Mesurer et contrôler le rapport coût/efficacité des différents instruments pour retenir ceux qui donnent le meilleur résultat au moindre coût.

Programmes de financement des risques

Le financement des risques est un volet essentiel de la gestion financière stratégique de l'organisme. Il intègre donc l'appétence/tolérance au risque définie par les dirigeants. Le risk-manager doit donc conseiller la

direction financière pour l'éclairer sur les limites de rétention par type de risques ainsi que les besoins en financements externes, et notamment :

- Choisir, dans les limites des grandes options définies ci-dessus, les instruments de rétention et de transfert les plus appropriés à chaque type de risques de l'entreprise.
- Négocier avec les partenaires internes et externes concernés pour la mise en place effective des financements.
- Veiller à la rentrée des fonds lorsque les financements concernés deviennent indispensables.
- Mesurer et contrôler les résultats de façon à toujours adopter le cocktail d'instruments le plus efficace au plan économique.

Cet ensemble de missions est commun à presque tous les gestionnaires de risques même si leur implication dans les tâches quotidiennes varie significativement selon la vulnérabilité traitée et la nature des instruments de traitement retenus. C'est pourquoi il serait futile de donner ici une description de fonction détaillée et la liste précise des tâches quotidiennes. Un tel inventaire pourrait se révéler très approximatif face à une réalité par nature mouvante.

En revanche, dans son rapport annuel d'activité, le gestionnaire de risques devrait articuler sa présentation autour des trois grands axes définis ci-dessus : programme général, réduction ou financement des risques. C'est d'ailleurs une base pour le rapport du directeur général dans sa présentation de la politique de gestion des risques dans l'entreprise, rendue pratiquement nécessaire par la législation en cours au sein de l'Union européenne, au moins pour les entreprises cotées en bourse (lois NRE et LSF, en France).

93 *Quel est le champ de la gestion des risques à l'hôpital ?*

Un établissement de santé est un système complexe où se croisent des mondes différents regroupés autour du malade. Le découpage en services, en métiers et en compétences complémentaires rend plus long le processus d'apprentissage collectif pour faire entrer l'ensemble des acteurs dans une démarche cohérente et efficace. Cependant, le schéma général évoqué dans le chapitre 11 rappelle des démarches existant déjà dans le cadre de l'accréditation : collecte des données en vue du bilan sécurité, autoévaluation, entretien avec les experts visiteurs, notamment. En outre, des actions spécifiques à la gestion des risques s'inspirent des méthodes évoquées précédemment.

Signaler les événements indésirables

Une modalité d'entrée dans la démarche de gestion des risques dans les établissements de santé est le signalement des événements indésirables. Cette approche a été promue par le premier manuel d'accréditation, qui en faisait une référence du chapitre qualité et prévention des risques. La portée de cette approche doit être évaluée, afin de ne pas y engloutir des moyens hors de proportion des résultats espérés.

Pour cela, les objectifs de ce signalement doivent être clairement identifiés. On peut ainsi distinguer quatre objectifs de façon non exclusive les unes des autres : la prévention des accidents, la sensibilisation des acteurs à la notion d'erreur et d'incident, la surveillance de la fiabilité du système en rapprochant les données recueillies dans le temps et la gestion des plaintes.

Pour atteindre ces objectifs, il convient de s'interroger sur la nature des événements à recueillir. La Haute Autorité de santé (HAS) souligne que s'intéresser aux événements les moins graves n'a de sens que si les événements graves sont déjà maîtrisés. La réflexion sur la gravité des événements à recueillir est donc primordiale dans une double optique : l'efficacité permettant de traiter les causes des accidents ou des presque accidents pour prévenir leur récidive, l'efficience pour concentrer des moyens précieux sur des risques graves.

Dans cette optique, se concentrer sur le signalement et le traitement des événements graves et d'événements « sentinelles » nécessitant une réponse rapide semble une recommandation raisonnable. En effet, l'analyse de

leur cause permet d'identifier des défaillances humaines, techniques et organisationnelles dont les conséquences n'auraient pas pu être mesurées, si celles-ci avaient été signalées isolément à l'occasion d'un événement de faible gravité. Cette approche recentre le traitement des vulnérabilités moyennes au niveau local et transfère aux organismes, en charge de la santé publique, l'analyse des vulnérabilités rares mais graves (vigilances).

La limite de cette approche tient à la sous-notification des événements par comparaison avec d'autres méthodes et par la sous-estimation notable des événements liés aux soins. Cela souligne l'impérieuse nécessité d'une préparation minutieuse de cette démarche de signalement pour faire évoluer les mentalités et la culture collective de sécurité et d'apprentissage à partir des erreurs. C'est en effet le système de déclaration volontaire qui permet la meilleure identification des événements indésirables. Cependant, tendre vers l'exhaustivité du recensement, notamment des événements iatrogènes graves, nécessite de croiser les approches : signalement volontaire, étude rétrospective de dossiers, surveillance prospective des patients hospitalisés, étude transversale « un jour donné ».

L'utilisation des données recueillies doit être définie préalablement en fonction des objectifs. Cette définition conditionne les modalités d'analyse et de présentation des résultats au sein de l'établissement. Cela suppose de déterminer, parmi les professionnels et avec l'aval de la direction générale de l'établissement, les personnes qui collectent les données, les rendent anonymes, conduisent l'analyse des causes racines, documentent la base de données et communiquent les résultats.

Les destinataires de cette communication doivent être l'ensemble de la communauté professionnelle, sans préjuger des dispositions réglementaires visant au signalement obligatoire. Le délai de traitement de ces signalements doit être le plus court possible, en définissant des priorités en fonction de la gravité de l'événement selon son impact : atteinte aux personnes, à l'information, aux biens, à l'organisme (mise en cause de la continuité du service), aux ressources, à l'image de l'établissement.

Cette réflexion guide la définition d'événements « sentinelles » et leur réévaluation, en fonction des événements observés. En tout état de cause, une information rapide sur le devenir du signalement est délivrée aux acteurs qui en sont à l'origine. Cette attitude est garante du maintien de la mobilisation des acteurs. Ce schéma s'intègre parfaitement dans la démarche générale de diagnostic des risques évoqué aux questions 13 et 21, tenant compte des objets de risques et des périls les menaçant.

Au travers des expériences déjà entreprises, des facteurs de succès se dessinent :

- Des incitations au recueil par :
  - l'engagement formel de la direction d'une gestion non punitive des erreurs ;
  - l'élaboration de règles de fonctionnement garantissant la confidentialité des données ;
  - la définition de stratégies pour réduire la survenue des incidents ;
  - l'engagement de tous les professionnels dans le processus de déclaration.
- Des modes opératoires précis :
  - un support de signalement simple et disponible ;
  - une aide rapide ;
  - une liste définie d'événements à relever adaptée aux secteurs d'activité.
- Une personne responsable de la coordination :
  - garante de la confidentialité ;
  - maîtrisant les méthodes d'analyse et de gestion des risques ;
  - promouvant l'intégration des stratégies de maîtrise des risques dans les pratiques ;
  - impulsant la formation des équipes (notamment médicales) et des personnels infirmiers.
- Une évaluation de l'efficacité des stratégies et des méthodes mises en œuvre.

Actuellement, le recul manque pour juger de la pertinence de ces approches, d'autant que la formation à ces approches reste dispersée. C'est le chantier qui est ouvert aujourd'hui dans les établissements de santé publics et privés.

94 *Qui est en charge de la gestion des risques à l'hôpital ?*

L'état actuel de la gestion des risques dans le monde de la santé est marqué par la fragmentation de la décision en établissement de santé évoquée plus haut et la disparité de la sensibilisation traditionnelle des métiers de la santé à la prise en compte du risque. Pour les uns, chercheurs et médecins entre autres, la prise de risque est nécessaire au progrès scientifique, mais pour les autres, patients, personnel infirmier, direction…, la prise de risque est au contraire vécue comme inacceptable. Définir une approche commune passe donc par des efforts de formation et de recherche impliquant de s'investir dans la durée.

La gestion globale des risques en établissements de santé est devenue une impérieuse nécessité. Des démarches ont été entreprises, sans coordination, par certains établissements de santé, montrant la faisabilité de la démarche générique existant dans d'autres univers professionnels. De grands hôpitaux, dans la capitale comme dans les régions, s'équipent de « risk-managers », dont les profils sont variables, mais souvent avec une formation de soignant : la définition de fonction reste encore à rédiger, et leur autorité face aux chefs de service à définir !

Un effort stratégique considérable reste à entreprendre pour généraliser ces actions, en s'appuyant sur un engagement fort : l'implication de tous les acteurs de la politique de santé. Ce n'est qu'à ce prix que la coordination efficiente d'enseignements et de recherches nécessaire à l'application d'une politique, rendant plus sûrs les établissements de santé français, pourra être entreprise. En effet, seule une recherche pluridisciplinaire permettra d'aboutir : d'où la nécessité de décloisonner les départements ministériels et les échelons administratifs. Il faut un véritable engagement sur un programme pluriannuel intégrant la recherche, la réorganisation, la formation et les financements dans un ensemble cohérent et ambitieux. Les acteurs à prendre en compte sont sans doute, outre le ministère de la Santé, le ministère de l'Éducation et de la recherche avec pour maître d'œuvre les directions régionales de la santé, en liaison étroite avec les collectivités territoriales et les acteurs locaux de la santé.

La recherche en santé s'est traditionnellement intéressée aux pratiques de soins et, plus récemment, à leurs aspects économiques. Sur le plan managérial, seule l'émergence de travaux sur la qualité laisse espérer une approche transdisciplinaire.

La complexité de tout établissement de santé, déjà soulignée plus haut, interdit d'espérer dégager des modes de compréhension et d'action à partir d'expériences individuelles fragmentaires. Pour dresser l'image complète, sur grand écran, de la panoplie des risques à l'hôpital et la trousse des instruments de traitement de ces risques, il faudra s'appuyer sur un ensemble de compétences.

Par ailleurs, cette nécessité d'une référence commune a été prise en compte, de façon très différente, dans les trois pays où la gestion des risques des établissements de santé est une réalité :

- Aux États-Unis, l'Association des risk-managers de la santé (ASHRM) s'est appuyée sur le modèle développé pour les entreprises (ARM) et s'est forgée une identité propre, en créant une qualification complémentaire spécifique délivrée par l'*American hospital association* (AHA) dont l'essentiel des membres sont des cadres infirmiers.
- En Australie, les standards de gestion de risques développés pour le domaine public, et applicables dans l'ensemble des organismes sont mis en œuvre dans les hôpitaux publics également. En Grande-Bretagne, le service public (NHS) a adopté et adapté le standard de gestion des risques australien qu'il a mis à jour avec la publication de la norme ISO 31000:2010.

En France, des références opérationnelles sont constituées par les documents de l'ANAES, relayées désormais par la Haute Autorité de santé (HAS) et de la DHOS, mais leur transposition en termes de formation nécessite la publication d'une doctrine cohérente, tant pour les professionnels de santé et leurs partenaires industriels, que pour les services de l'État. Les formations existantes comportent cependant des points communs, dont certains se retrouvent aussi dans les trois modèles nationaux évoqués. Il existe aujourd'hui de nombreux diplômes universitaires (DU) qui, le plus souvent, allient qualité et gestion des risques, attirent un public varié de soignants et d'administratifs, facilitent le dialogue interprofessionnel au sein de l'établissement de santé et autour d'un socle conceptuel commun. On peut également citer les Rencontres des métiers de la santé de Strasbourg qui font annuellement fin mai le point sur les avancées de la performance en établissement de santé.

En clair, il faut une mobilisation en hommes et en moyens : c'est à ce prix qu'une gestion globale des risques, cohérente et efficace tant au plan opérationnel qu'économique, verra le jour dans notre système de santé, appuyée sur l'ensemble des acteurs opérationnels.

95 *Où s'arrête la gestion des risques dans une collectivité territoriale ?*

La gestion des risques est, sans doute, au cœur de tout gouvernement. Les collectivités territoriales, comme tout service public, doivent veiller avant tout à la santé, à la sécurité et au bien-être des populations. Cela passe par la prise en charge des situations d'urgence et la conservation des biens publics. En ce sens, toutes les collectivités territoriales pratiquent la gestion des risques.

Pour elles, le défi actuel est de mettre en place un processus rigoureux et systémique, pour évaluer et traiter globalement leurs risques, et valider les solutions mises en œuvre, en vérifiant leur efficacité. En un mot, il s'agit de créer, au sein des élus et chez l'ensemble des fonctionnaires, une véritable culture de gestion des risques.

Si la gestion des risques comprend le suivi des engagements de responsabilité et, parfois en France, les questions d'hygiène et de sécurité sur le lieu de travail, plus récemment, les fonctionnaires et les élus de certaines collectivités ont commencé d'appréhender la complexité et la diversité des risques qui pèsent sur tous les aspects de la vie communale, départementale ou régionale. En particulier ils perçoivent bien que les risques ne sont pas limités à ceux qui sont « assurables », ni même aux accidents. Ils s'étendent également aux décisions des élus, aux choix d'investissements de la collectivité, aux variations climatiques, et même, à l'évolution des « goûts » de l'électorat.

Traditionnellement, les collectivités territoriales (les communes, en particulier) se sont protégées contre les aléas, en achetant des couvertures d'assurance. La collectivité acquitte des cotisations annuelles, et en cas de sinistre, l'assureur l'indemnise ou le tiers lésé, et assure le suivi du sinistre et sa défense, si elle est mise en cause par un tiers.

En France, les contrats d'assurance étaient de durée indéterminée, mais avec une clause permettant la résiliation annuelle par les deux parties. Cette disposition permettait donc à l'assureur d'ajuster la cotisation annuelle, sauf en cas de contrat ferme de trois ans non révisable.

Cela se rencontre parfois dans les collectivités de taille importante. De ce fait, le coût du risque comprend la cotisation et le montant des franchises restant à la charge de l'assuré en cas de sinistre.

Les marchés publics sont des contrats conclus à titre onéreux, avec des personnes publiques ou privées, par des personnes morales soumises au Code des marchés publics pour répondre à leurs besoins en matière de travaux, de fournitures ou de services. Les contrats d'assurance souscrits par des collectivités territoriales sont soumis au Code des marchés publics, dès lors que le paiement de la prime est pris en charge, totalement ou partiellement, par la collectivité publique.

Une circulaire interministérielle du 18 décembre 2001 consacrée aux marchés publics d'assurance a été publiée au *Journal officiel* du 2 février 2002 (n° 28, p. 2198). Elle précise, en détail, l'interprétation à adopter de certaines dispositions du Code des marchés publics, particulièrement peu appropriées aux marchés d'assurances, et complète l'information des personnes passant des marchés publics sur des points que le nouveau Code n'aborde pas. Bien entendu, les collectivités locales doivent respecter les principes fondamentaux applicables aux marchés publics (liberté d'accès à la commande publique, égalité de traitement des candidats, transparence des procédures, définition préalable des besoins, respect des obligations de mise en concurrence, choix de l'offre économique la plus avantageuse).

Toutefois, l'achat d'assurance ne doit plus être aujourd'hui qu'un élément d'une politique de gestion des risques, ne serait-ce que du fait de la dérive des coûts des assurances pour les collectivités qui ont laissé « filer » leur sinistralité. C'est, en effet, à une gestion globale de leurs risques que sont appelées les collectivités territoriales : elles doivent passer d'un seul saut de l'artisanat à la stratégie. Le premier volet c'est d'être « candide » avec son assureur et de lui donner les moyens de tarifer au plus juste prix. L'assureur est en effet « rassuré » par des renseignements précis et rigoureux, reflet d'une gestion rigoureuse.

La pression de l'opinion publique et les attentes des électeurs ne laissent plus le choix aux élus et aux cadres de la fonction territoriale. Ils doivent définir une politique de gestion des risques visant, au-delà des actifs de la collectivité, la sécurité de tous et des biens de chacun des habitants, personnes physiques ou morales, installés sur le territoire de la collectivité. On a pu mesurer les attentes des citoyens et les limites de l'action communale au cours des évènements de l'hiver 2014, les inondations à répétition dans certaines régions.

96 *Qui devrait être en charge de la gestion des risques d'une collectivité territoriale ?*

Étant donné la perspective et l'étendue de la gestion des risques dans une collectivité territoriale (voir question 95), l'objectif ultime est de susciter une véritable culture de gestion des risques parmi les élus, les fonctionnaires et les contractuels, mais aussi tous ceux qui vivent ou transitent sur son territoire.

L'élargissement de la gestion des risques passe aussi par la montée en puissance du responsable de la gestion des risques. Aujourd'hui, on ne peut plus se contenter d'un technicien de l'assurance, pour couvrir l'étendue de la fonction, ce dernier doit aussi bénéficier d'une vision globale sur l'ensemble des activités de la collectivité territoriale. Son autorité ne peut que découler d'une mission confiée directement par le maire, le président du conseil général ou du conseil régional, sous l'autorité directe du directeur général des services ou du cabinet.

Il ne faut pas se cacher l'ampleur de la tâche des professionnels de la gestion des risques, auxquels les collectivités territoriales feront confiance pour développer et mettre en œuvre un programme global de gestion de leurs risques. Il leur faudra faire preuve de patience et de persévérance. Il y faudra également une volonté politique sans faille des élus.

Toutefois, la réalité du terrain est que l'achat de couvertures d'assurance, plutôt que la culture de risque, reste encore l'activité principale de ceux qui occupent le poste de risk-manager : fonction nouvelle qui prend progressivement sa place dans les organigrammes des collectivités.

Les procédures d'appel d'offres ouvert, rendues obligatoires ces dernières années en application des règles édictées par l'Union européenne et transposées en droit français, ont encore alourdi la charge « assurances » dans les collectivités territoriales.

Supposons que la collectivité fasse appel à un véritable professionnel, armé des compétences listées à la question suivante, cela est-il suffisant ?

La réponse est sans équivoque « non » ! La gestion des risques est l'affaire de tous, et en particulier tous les acteurs directs de la vie municipale, départementale ou régionale, ainsi qu'énoncé d'emblée au début de la question. Pour une collectivité où il s'agit de gérer un espace, c'est encore insuffisant, car il faut que tous les acteurs du « territoire » soient impliqués

dans l'œuvre commune visant à garantir la sécurité des habitants. En clair, il faut coordonner les efforts des acteurs indépendants (entreprises, associations et commerçants) installés sur le ressort de la collectivité et assurer une concertation avec les collectivités avoisinantes.

La seule réponse est donc : « tout le monde, chacun à son niveau d'action ». En effet, s'il est indispensable que les collectivités désignent un élu responsable du suivi de la politique de gestion des risques arrêté par l'ensemble des élus, s'il faut un fonctionnaire ou un contractuel de niveau direction pour l'incarner au quotidien dans les services, tous les efforts des fonctionnaires et des contractuels seront vains, si la coopération de l'ensemble des administrés n'est pas engagée. C'est à ce prix que les électeurs, lors de la prochaine échéance électorale, bénéficieront d'une sécurité, effective et perçue, accrue grâce aux efforts du patron de l'exécutif territorial, relayé par le risk-manager.

C'est pour cela qu'au niveau des collectivités, un des instruments essentiels du traitement des risques est la communication sur les risques qui doit être un effort concerté des élus et des fonctionnaires. Mais il faut être attentif à ne pas matraquer la population à coups de communiqués internes et/ou externes. Communiquer, c'est établir un processus d'échanges et de dialogue avec l'ensemble des parties intéressées sur le sujet des risques et de leur gestion. Selon l'expression des standards australiens mis en œuvre dans l'ensemble des collectivités de ce pays : *« La communication sur le risque est un processus interactif d'échanges d'informations et d'opinions impliquant de multiples messages sur la nature des risques et de leur gestion. »*

Mais attention, les « consommateurs » et leurs relais, les médias, sont devenus exigeants. De ce fait, bien communiquer sur la gestion des risques passe par un préalable incontournable : la conception et la mise en œuvre d'une véritable gestion globale proactive des risques, dans laquelle chacun retrouve la protection de sa propre sécurité physique et économique, à long terme.

97 *Quelles sont les compétences indispensables pour les risk-managers ?*

Le professionnel de la gestion des risques est un cadre supérieur qui doit avoir une vision stratégique de l'organisme renforcée par des savoir-faire spécifiques dans son domaine.

Il doit donc connaître et pouvoir mettre en œuvre l'ensemble du processus de gestion des risques, mais aussi bien connaître l'ensemble des domaines de la gestion des organismes pour mener un « dialogue informé et intelligent » avec les dirigeants et les responsables opérationnels spécialistes de leur propre domaine.

1. Gestion générale d'entreprise

Bien entendu, le professionnel de la gestion des risques, positionné dans l'encadrement supérieur de l'organisme, doit posséder les connaissances nécessaires pour comprendre les enjeux des grandes fonctions de la gestion générale.

Cela est indispensable pour être efficace dans l'assistance aux opérationnels, pour la mise en œuvre de programme d'atténuation du risque passant par un processus continu de cartographie des risques. Ces grandes fonctions peuvent être articulées autour des cinq classes de ressources.

- **Ressources humaines**

Même si les accidents du travail, gérés au niveau national en France, ne prennent pas la place prépondérante dans la vie du risk-manager comme aux États-Unis, ils n'en demeurent pas moins une source de retour d'expérience et une nécessité d'action importante. Par ailleurs, par-delà les personnes-clés, les hommes sont une ressource vitale dans de nombreuses activités, tout particulièrement dans le secteur tertiaire.

Le « *knowledge management* » pour la stratégie à long terme — relayé aujourd'hui par la gestion des compétences ou des talents — et les régimes de retraite et de prévoyance, pour leur impact financier à moyen et long terme, demeurent des volets de concertation entre le risk-manager et le directeur des ressources humaines. Comprendre le mode de fonctionnement et les contraintes de la DRH sont donc incontournables.

- **Ressources techniques**

La production est le territoire traditionnel des assurances dommages, et des pertes d'exploitation induites par le déficit de capacités de production. Les assureurs traditionnels incendie, bris de machine et risques annexes connaissent bien les processus de fabrication et les aléas qui y sont attachés. Toutefois, tous les risques ne sont pas assurables et la dépendance envers un réseau d'acteurs impose leur prise en charge, en commun, de leur globalité. Cette question sera revue dans le cadre des partenariats amont.

- **Ressources d'information**

Quand on parle information aujourd'hui, il est indispensable de penser intelligence économique et *« big data »*.

Donc, bien au-delà des systèmes informatiques, c'est la disponibilité et la sécurité des informations que reçoit, traite et transmet l'organisme qui sont essentielles. C'est même dans certains cas, un composant important de la valeur ajoutée (SSII) ou une obligation légale pouvant déboucher sur de lourds engagements de responsabilité en cas de rupture (établissements de santé).

De ce fait, le risk-manager doit suffisamment connaître les méthodes et pratiques de l'intelligence économique, ainsi que l'informatique pour comprendre l'architecture d'un système et les interactions des bases de données internes et externes.

- **Partenaires économiques**

Cette classe s'étend à l'ensemble des partenaires de l'organisme, c'est-à-dire à toutes les entités externes sur lesquelles il s'appuie pour la continuité et l'efficacité de ses opérations, depuis les achats et les approvisionnements, jusqu'à la livraison au client final, en passant par l'ensemble des moyens logistiques.

Outre la spécificité des achats et du marketing, le risk-manager doit être suffisamment familier avec le droit des contrats, les procédures des tribunaux civils et les opérations d'arbitrage, dans l'ensemble des pays où l'organisme peut être appelé à se défendre ou à attaquer pour défendre ses intérêts.

► **Partenaires amont** (sous-traitants et fournisseurs) : c'est une des missions essentielle du directeur achat et logistique de trouver des partenaires, fournisseurs et sous-traitants, fiables et de qualité.

Pour l'assister dans la gestion des risques de « frontières », toujours fragiles, le risk-manager doit comprendre les principales composantes de l'achat et de la logistique.

- **Partenaires aval** (circuits de distribution, clients) : plan marketing, plan média, recrutement et animation d'un réseau de vente relevant des compétences du directeur marketing. Il est à l'affût des opportunités et, dans sa focalisation sur le développement, pourrait ignorer certains aléas. Il revient au risk-manager de veiller à ce que tout soit pris en compte. Encore faut-il qu'il connaisse les mécanismes du marché pour participer au processus de cartographie des risques commerciaux.

- **Ressources financières**

Tous les membres de l'encadrement doivent avoir une bonne compréhension des réalités financières, en particulier savoir interpréter la liasse fiscale (bilan, compte de résultat, tableau emplois/ressources) et la comptabilité analytique. Le risk-manager ne doit pas faire exception et doit en outre, pour défendre ses projets, connaître les choix d'investissements et de financement reposant sur l'actualisation et l'arbitrage entre risque et rendement.

2. Le processus de gestion des risques

Bien entendu, le processus de gestion des risques reste au cœur des missions du gestionnaire des risques. Ce processus en trois étapes peut être analysé par analogie avec l'acte médical : par-delà les symptômes, il convient de trouver les causes profondes pour établir un diagnostic des vulnérabilités, ensuite de rédiger une « ordonnance » (un programme de traitement des risques) et enfin de valider la démarche, en vérifiant l'efficacité des mesures préconisées (la visite de contrôle) : c'est le processus d'audit du programme de gestion des risques.

- **Diagnostic des vulnérabilités et cartographie des risques**

Le risk-manager doit être un facilitateur, qui peut assister dans le développement d'un processus de diagnostic des vulnérabilités (identification et analyse) intégrant les objectifs de l'entreprise pour déboucher sur la cartographie des risques dans l'ensemble de l'organisation.

- **Traitement des risques**

Le risk-manager doit avoir une solide maîtrise de l'ensemble des instruments de traitement des risques (réduction et financement) débouchant sur la

conception de programme de gestion des risques. L'ouverture d'esprit est essentielle pour sortir des sentiers battus et susciter l'imagination des propriétaires de risques pour qu'ils trouvent des solutions innovantes, incorporant les moyens d'une évaluation des résultats atteints.

- **Audit et évaluation (programme de gestion des risques)**

Cette évaluation ne peut pas être uniquement interne, car il faut suivre l'évolution des techniques et des instruments de gestion des risques, ainsi que de l'organisme lui-même et de son environnement. Cette démarche participe de l'amélioration constante de la sécurité pour les parties prenantes de l'entreprise.

En effet, les dirigeants de l'organisme doivent disposer d'instruments de mesure des progrès réalisés en matière d'atténuation du risque, grâce aux techniques de traitement engagées. Pour ce faire, le risk-manager doit coopérer avec l'audit interne dont il doit connaître les missions et comprendre les processus (définition de référentiels, d'activité et de résultats), garantir la validité des données recueillies, évaluer les résultats atteints et tracer les axes de corrections nécessaires.

3. Communication et animation des équipes

Il serait trop facile de ne penser ici qu'à la communication en cas de crise. Elle est, certes, un temps fort de l'organisme avec des enjeux considérables. Toutefois, si le risk-manager doit maîtriser le processus global de gestion des risques, son efficacité dépend essentiellement des efforts réalisés par les responsables opérationnels pour s'approprier et maîtriser leurs risques. C'est pourquoi le risk-manager est souvent conduit à animer une commission et un réseau de correspondants pour garantir la continuité de l'effort. Il doit donc développer des qualités de communication à l'égard de l'ensemble des parties prenantes, internes et externes, de l'organisme.

4. Connaissances sur le domaine spécifique d'activité

Ce quatrième pilier de compétences est spécifique aux différents domaines d'activités de l'organisme, au sein duquel le gestionnaire des risques opère. La liste qui suit n'est, sans doute, pas exhaustive, mais elle reprend les principaux secteurs qui supposent une application spécialisée. Bien entendu, il conviendra, à la prise de fonction ou en début de mission pour un consultant, de prendre le temps de connaître chaque nouvel organisme, sa structure, ses méthodes, ses valeurs, sa culture…

- **Collectivités locales (municipalités, départements et régions)**

Le fonctionnement de ces organismes repose sur un ensemble de lois et de réglementations qui leur sont spécifiques. Le risk-manager doit donc connaître les éléments de droit, comme tous les fonctionnaires territoriaux de cadre A. En particulier parmi les points-clés : le processus d'appel d'offres pour les marchés publics, les relations entre élus et fonctionnaires, les attentes des électeurs et autres publics.

- **Établissements de santé (hôpitaux publics et cliniques privées)**

Le patient est au cœur de tous les processus d'un centre de soin. La mission essentielle est de restaurer sa santé, dans des conditions de sécurité optimales, alors même qu'il est vulnérable. Le risk-manager de la santé doit avoir une connaissance des professions médicales et des processus inhérents aux établissements de santé.

- **Entreprises (industrielles, commerciales et financières)**

C'est le secteur où la fonction est la plus répandue à l'heure actuelle. Le risk-manager doit comprendre les principes fondamentaux de la macro et de la microéconomie, ainsi que les tendances lourdes du secteur concerné. En résumé, les facteurs déterminants pour développer et mettre en œuvre une stratégie globale incluant les risques et les opportunités.

- **Organismes à but non lucratif (associations loi de 1901 et ONG)**

Les missions d'une ONG sont la clé de son fonctionnement et justifient ses opérations de collecte de dons. Le gestionnaire des risques doit les connaître et les comprendre. De plus, la réputation est l'actif essentiel, et il faut identifier les leviers qui peuvent l'accroître ou au contraire la mettre en péril.

98 *Qui doit être formé à la gestion des risques ?*

À ce stade de la réflexion, il doit apparaître clairement que la seule réponse possible est « tout le monde ». En effet, la sécurité collective, tant physique, économique, culturelle que sociale, ne peut être maintenue que par l'addition des efforts individuels. Il faut donc que chaque maillon de la société soit formé à la gestion des risques. On pourrait même affirmer que dans une approche globale des risques, elle devrait faire partie de l'éducation civique dès l'école primaire.

Sans aller à cet extrême, aujourd'hui, il est clair que les risques résultent trop souvent d'une complexité mal maîtrisée. La création d'une véritable culture de gestion des risques passe donc sûrement par une révision des paradigmes des écoles de management et des écoles d'ingénieurs chargées de former les cadres de demain. La gestion des risques devrait faire partie des enseignements de base, comme l'informatique, perçue comme un des instruments indispensable de la panoplie de tout responsable.

Pour être transversale, la gestion des risques a besoin de spécialistes pour concevoir et administrer des processus applicables à des systèmes complexes afin d'en assurer la résilience, de la même façon qu'il faut des informaticiens, même dans une société « compétente en informatique » (*computer litterate*).

Si cette approche est la réponse pour demain, en clair : comment faire, aujourd'hui, avec un constat global que peu de nos dirigeants et cadres ont été formés à la gestion des risques. Et la question devient celle qui se pose à tout responsable d'entreprise, de collectivité, d'établissement de soin… : « Quels membres du personnel doivent être formés, aujourd'hui, à la gestion des risques ? »

Pour les grands organismes où il existe une fonction « gestion des risques » reconnue et de plein exercice, la formation des responsables opérationnels doit se faire systématiquement par le biais des exercices de diagnostic terrain.

Ces diagnostics terrain peuvent être précédés par des formations ponctuelles théoriques pour donner les fondements de la méthode et de ses objectifs. Puisque l'ensemble des responsables de chaque unité opérationnelle est impliqué dans ce processus, cela devrait régler la question de la formation de tout l'encadrement de proche en proche.

Dans ces conditions, la formation conduisant à la qualification professionnelle ONR 49000 (voir question 99), doit être réservée dans chaque division à celui qui sera le « risk-manager » de celle-ci. Le correspondant du risk-manager « siège » (ou « corporate ») au sein de la division, en lien fonctionnel avec lui, mais en lien hiérarchique avec le responsable opérationnel de la division.

Il reste la question de la sensibilisation de l'ensemble du personnel d'exécution pour lequel les organes représentatifs, en particulier le comité d'hygiène, de sécurité et des conditions de travail (CHSCT) et les outils de communication interne (journal d'entreprise, affiches, message sur écrans d'ordinateurs, bandes-annonces…) doivent être préférés à des actions de formation classique, sauf dans les industries « à risque » où ces éléments doivent faire partie de l'intégration de tous les nouveaux engagés. Ceci peut être nuancé pour des formations spécifiques, comme la formation à la conduite défensive de tous les chauffeurs (y compris les cadres qui utilisent des véhicules dans leur fonction).

La question se pose en d'autres termes dans les « organismes de taille humaine », les ETI et les PME/PMI en particulier. Il est essentiel qu'un membre de la direction prenne en charge la gestion des risques et qu'il soit formé à cette tâche. Une qualification professionnelle lourde n'est pas envisageable et s'en remettre entièrement à un consultant externe est à la fois dangereux et onéreux. L'obligation de rédiger un « document unique » en matière de risques professionnels offre sans aucun doute une opportunité pour dépasser ce cadre limité, et transformer une « corvée administrative » de plus en un exercice profitable de réflexion sur la survie à long terme de l'entité. Des formations-actions, relayées au sein de l'entité avec l'appui d'un consultant formateur devraient apporter une solution économique et efficace !

Au cours de cet ouvrage, nous avons souligné avec insistance la nécessité, pour tout organisme, de s'insérer dans un environnement « sécurisé », où l'ensemble de ses partenaires internes et externes ont mis en place des processus de gestion des risques efficaces. Nous l'avons souligné également, contrairement à la qualité, il n'existe pas aujourd'hui de référence universelle, de norme « ISO GR » à insérer dans un contrat, donc la formation devrait s'étendre à des actions communes ou partagées avec les principaux partenaires.

99 *Comment former à la gestion des risques ?*

Dans la mesure où les populations à former à la gestion des risques sont très variées, il va de soi que les formations doivent être différenciées pour répondre à des objectifs pédagogiques et des compétences initiales diverses.

Pour les professionnels de la gestion des risques, destinés à avoir un emploi à temps plein dans le domaine, au moins pour une partie significative de leur vie professionnelle, il leur faut une solide base de réflexion.

En France, il existe des organismes de formations initiales, comme l'Institut de Management des Risques (Bordeaux) et le master professionnel de gestion globale des risques de l'université Paris 1, le master spécialisé en gestion globale des risques et des crises de l'INSA Centre Val de Loire (Bourges et Blois) pour ne citer que ceux où je suis intervenu personnellement.

CARM Institute, fort de son expérience de deux décennies pour la formation professionnelle qualifiante en gestion des risques, lance dès 2014 en France et en français la qualification ONR 49000, délivrée par l'organisme suisse de certification, qui vise à mettre les qualifiés en mesure :

- d'établir le diagnostic des vulnérabilités d'un organisme ;
- de recenser les instruments de traitement des risques pertinents (réduction et financement) ;
- d'élaborer un programme de gestion des risques efficace au plan éthique et économique, et de le faire approuver par le comité de direction ;
- de coordonner la mise en œuvre du programme adopté ;
- d'auditer les résultats, et de proposer des actions correctives.

C'est une formation de huit journées, scindée en quatre séminaires résidentiels de deux jours en fin de semaine, à un mois d'intervalle. Elle est idéalement conçue pour l'ensemble des dirigeants et managers opérationnels qui ne peuvent pas consacrer trop de temps à une activité, certes importante, mais en dehors de leur cœur de métier. Le processus d'établissement d'un diagnostic des risques débouchant sur un profil

formalisé est un excellent moyen d'apprentissage (voir la méthode des centres de risques à la question 19). Mais pour être mise en œuvre efficacement, elle suppose que chaque participant ait reçu au préalable une formation, action qui peut prendre la forme d'un séminaire « intra » de deux jours, suivi par la mise en pratique par département.

Les donneurs d'ordre important ont un rôle d'éducation essentiel vis-à-vis de leurs sous-traitants : les fournisseurs-clés pourraient être invités à participer à certaines des formations internes pour les intégrer pleinement dans la sécurisation de la chaîne logistique.

Pour les ETI ou les PME/PMI, celui des dirigeants qui doit prendre en charge la coordination de la gestion des risques pourrait tirer le plus grand bénéfice de la formation ONR 49000, puisque les séminaires en groupe de taille limitée faciliteront les échanges avec des pairs venant d'horizons différents.

En outre, cette formation-action doit permettre un véritable coaching pour la mise en place effective d'une gestion globale et intégrée des risques (ERM).

Pour l'encadrement de contact (les agents de maîtrise) il faudra envisager des formations ponctuelles à l'occasion de la préparation et de la mise en place des plans de continuité d'activité, des plans de secours et des exercices d'évacuation.

Pour les collaborateurs d'exécution, il faut utiliser les moyens de communication habituels, bulletin de salaire, bandeau sur les écrans d'ordinateurs, affichage, journaux d'entreprise pour faire passer les messages essentiels.

En ce qui concerne les chauffeurs « professionnels », il faut combiner les cours théoriques et les exercices pratiques, en particulier pour la formation à la conduite défensive (un coussin d'air extérieur, respect des distances et anticipation, est plus efficace que le coussin d'air intérieur).

Enfin, pour les espaces ouverts, hôpitaux, centres commerciaux, collectivités, il faut utiliser des moyens simples, avoir recours aux pictogrammes, pour assurer la sensibilisation de tous.

Comment crée-t-on une « culture de gestion des risques » ?

Il faut donc *nicher* la gestion des risques dans tous les recoins de l'organisme et de son environnement grâce à un apprentissage continu pour que chacun soit sensibilisé au risque et capable d'alerter très en amont de sa réalisation.

En résumé, il faut développer une culture de gestion des risques chez chacun des collaborateurs pour qu'ils adhèrent pleinement aux valeurs de l'organisme et participent pleinement à leur respect et à l'atteinte de ses objectifs.

Il s'agit bien d'une greffe de compétences en gestion des risques sur la culture existante à tous les niveaux de l'organisme et chez ses principaux partenaires car c'est l'instrument de la performance au quotidien et de la résilience en temps de crise ou de mutation.

100 *Les cindyniques ouvrent-elles une nouvelle voie ?*

C'est en décembre 1987, à l'occasion d'un colloque au Palais de l'Unesco à Paris, que la démarche scientifique a pris naissance, et qui désormais connue sous le nom de cindyniques, de *kindunos*, le mot grec pour danger.

L'état de choc des industries, à la suite de la série de catastrophes (Tchernobyl, Bhopal, Challenger) offrait un terrain fertile de retours d'expérience. Le mouvement cindynique poursuit son développement avec un point fort, un colloque organisé tous les deux ans. Les efforts ont été concentrés sur l'axiologie et des essais de mesures objectives.

Les lignes qui suivent, rédigées par Georges-Yves Kervern, s'appuient sur la réflexion menée pour le dernier colloque « Cindynics 1997 » à la Sorbonne, en novembre 1997.

Concepts de base

Le premier concept est celui de situation, qui fait l'objet d'une définition formelle, sur ce que recouvre une étude de danger. Conformément à la théorie moderne de la description, pour définir une situation de danger (*situation cindynique*), il faut préciser :

- le champ de l'étude des dangers ;
- les limites de temps ;
- les limites dans l'espace ;
- les limites des réseaux d'acteurs inclus dans l'étude ;
- le « regard » porté sur cet ensemble.

Le second concept est celui d'hyperespace du danger. Il est le résultat, pour chaque acteur, de la définition de cinq dimensions :

- ***La dimension des faits*** (donnée) et celle ***des modèles*** se combinent dans le retour d'expérience (technique de base pour les gestionnaires des risques dans les grandes entreprises).
- Les trois dimensions : ***les objectifs, les normes et les valeurs*** se combinent dans le domaine de l'éthique en action.

Des travailleurs sociaux ont repéré dans ce domaine les ***fonctions d'autorité***, qui s'appuient sur les valeurs qui encadrent les objectifs, pour définir, puis défendre le respect des normes. En l'absence de ces fonctions d'autorité, le viol quotidien des règles conduira d'infractions

mineures à des violations plus graves et, dans les moyens de transport publics, par exemple, à des viols tout court !

C'est grâce à cette représentation, que l'on peut comprendre les limites des actions menées trop souvent. Pour être complète, une étude du danger (le diagnostic des vulnérabilités) doit s'étendre à l'ensemble des acteurs ou des réseaux de la situation et analyser, pour chacun d'entre eux, l'état des lieux des cinq dimensions précédentes.

Et dans la pratique

Au travers de l'analyse des différences entre les cinq axes des divers acteurs (espace) et d'un même acteur à de moments différents (temps), ainsi que les divergences entre le réel et le voulu pour chaque acteur, le modèle cindynique propose un moteur de recherche des causes profondes des dysfonctionnements passés (retour d'expérience) et prévisibles (anticipation) dans un système complexe.

On pourrait alors s'interroger sur sa valeur ajoutée par rapport aux méthodes plus traditionnelles de la sécurité de fonctionnement : l'apport fondamental du modèle cindynique est d'intégrer les valeurs et les souhaits des acteurs.

Pour résumer, la sécurité de fonctionnement traite les composants humains comme des composants physiques avec leurs taux de défaillance propres. Les cindyniques traitent les « composants humains » dans leur complexité psychologique et sociale, intègrent le fait qu'ils sont également des agents de changement et s'efforcent de canaliser cette énergie créatrice, individuelle et collective, pour améliorer la résilience à long terme de l'ensemble du système. C'est ce qui explique les développements de la recherche actuelle dans les domaines de la thérapie familiale, de la gestion des espaces urbains et de la santé publique.

Les étudiants du master professionnel gestion globale des risques et des crises de l'université Paris 1 Panthéon-Sorbonne ont utilisé ce modèle pour des projets aussi divers que la perception et l'acceptabilité sociale du risque et les médias, la réputation, le diagnostic multidimensionnel des risques.

101 *La gestion des risques est-elle une ardente obligation des organismes ?*

Pour certains universitaires et praticiens, le terme de « gestion des risques » est trop marqué par ses origines dans le monde de l'assurance. C'est pourquoi ils préfèrent un terme nouveau « la gestion stratégique des risques ».

Aux États-Unis, c'est le terme ERM (*enterprise-wide risk-management*) improprement traduit, quelquefois, par gestion des risques d'entreprises. Dans leur esprit, ce terme s'appliquerait à la gestion de l'ensemble des situations présentant un caractère aléatoire, d'avenir incertain. Les principales différences entre les deux concepts peuvent être résumées en trois points :

- ***Le champ d'étude*** de la gestion stratégique couvre la globalité des risques, purs ou spéculatifs.
- ***L'objectif*** de la gestion stratégique est l'atteinte du plein rendement de l'organisme (le maximum de l'efficacité économique) Elle ne se limite pas à la restauration du potentiel après dommages. Elle vise à la croissance et à la gestion du changement, dans une approche par essence plus positive et optimiste que la gestion des seuls risques accidentels.
- ***L'approche*** de la gestion stratégique est systémique — elle s'intéresse à l'organisme, comme un tout — et non pas analytique, puisque ne cherchant pas à identifier, individuellement, les vulnérabilités de celui-ci. Au contraire, elle envisage tous les objectifs de l'entreprise, ses forces et ses faiblesses propres, ainsi que les menaces et les opportunités offertes par son environnement. Elle doit tendre à l'optimum global du système.

Dans cette perspective, la gestion des risques (accidentels) apparaît comme une des composantes de la gestion stratégique. La gestion des risques, mieux dénommée gestion de l'incertitude, trouve des applications dans tous les domaines qui composent la gestion stratégique.

Ainsi replacée, la gestion des risques apparaît à la fois comme une discipline à part entière et partie d'un ensemble plus vaste.

Depuis trois ans, on assiste à une explosion de la fonction qui demande, à chacun des gestionnaires des risques en poste et à tous ceux qui aspirent

à le devenir, de se positionner sur un échiquier nouveau. Est-ce une des retombées des attentats du 11 septembre, sans oublier le 21 du même mois, en France, avec l'explosion de l'usine AZF à Toulouse ?

En toute hypothèse, les qualités et les compétences requises sont de plus en plus étendues. Certaines entreprises américaines, qui ont reconnu la nécessité pour ce « nouveau risk-manager » de faire partie du comité de direction, ont même forgé un nom nouveau pour le qualifier. Tous les membres de l'exécutif de l'entreprise sont des « *chief officers* ». On a donc créé le terme de CRO (*chief risk officer*).

De fait, les entrepreneurs français pourraient sourire de cette « nouvelle découverte » venue d'outre-Atlantique. En réalité, c'est Henri Fayol, chef d'entreprise et ingénieur civil des Mines, qui identifiait en 1916, parmi les six fonctions principales d'entreprises, les activités de sécurité, c'est-à-dire la protection des biens et des personnes. Il avait déjà clairement identifié le « directeur sécurité stratégie ». C'est, sans aucun doute, le précurseur du CRO. Mais il est vrai qu'il avait fallu quarante ans pour que Fayol soit traduit en américain. Il a suffi de quarante ans pour qu'ils le lisent.

Alors, reviendra-t-il maintenant à ce « nouveau risk-manager », le *chief risk officer*, de trouver un « sens » aux mots risque, sécurité, menace, opportunité ?

Pour définir la tâche exaltante qui attend ceux qui s'aventureront dans cette voie, Il est tentant de reprendre un vers de Stéphane Mallarmé. Dans son poème, intitulé « Le tombeau d'Edgar Poe », il décrit la mission du poète ainsi :

« Donner un sens plus pur aux mots de la tribu. »

C'est sans doute, également, la mission du CRO du troisième millénaire. Mais alors quand verra-t-on un risk-manager dans chaque ministère ? C'est le cas en Grande-Bretagne. À quand le risk-manager de la République ? À moins que ce soit la responsabilité ultime du chef de l'État, chef des Armées ?

Bibliographie

Albouy (François-Xavier), *Le temps des catastrophes*, Descartes & Cie, 2002

Bernstein (Peter L.), *Against the Gods — The remarkable story of risk*, John Wiley & Sons, 1998

Bichon (Benjamin), *Réussir la prévention des risques dans les PME*, AFNOR Éditions, 2005

Bland (David E.), *Treasury risk*, Witherby & Co, 2000

Bradshaw (William A.), *Learning about risk. Choices, connections and competencies*, Toronto, the Canadian Institute of Chartered Accountants, 1998 (Ce document existe également en français.)

Condamin (Laurent), Louisot (Jean-Paul) et Naïm (Patrick), *Risk Quantification — Management, Diagnosis and Hedging*, Wiley Finance, 2006

Curaba (Sandra), Jarlaud (Yannick), Curaba (Salvatore), *Évaluation des risques — Comment élaborer son document unique ?*, AFNOR Éditions, 2005

Degobert (Éric), Le Ray (Jean), *Maîtrise des risques professionnels —Mettre en œuvre une démarche d'amélioration continue*, AFNOR Éditions, 2004

Delaveaud (Marie-Claude), *Le « Risk Management » en 5 étapes*, AFNOR Éditions, 2003

Dupuy (Jean-Pierre), *Pour un catastrophisme éclairé — Quand l'impossible est certain*, Seuil, 2002

Gallet (Jean-Claude, colonel) (BSPP), Louisot (Jean-Paul) (Paris 1), *Catastrophes et risques urbains : la réponse des politiques publiques — contribution : Vers une nécessaire résilience*, Éditions Lavoisier, 2010

Gaultier-Gaillard (Sophie), Louisot (Jean-Paul), *Diagnostic des risques — Identifier, analyser et cartographier les vulnérabilités*, AFNOR Éditions, 2004

Guilhou (Xavier), Lagadec (Patrick), *La fin du risque zéro*, Éditions d'Organisation, 2002

Guinier (Daniel), *Catastrophe et management, plans d'urgence et continuité des systèmes d'information*, Dunod, 1997

Herbemont (d', Olivier), César (Bruno), *La stratégie du projet latéral*, Dunod, 1996

Jounot (Alain), *Le développement durable*, AFNOR Éditions, 2004

July (Jean-Pierre), *Évaluer les risques professionnels*, AFNOR Éditions, 2003

Kervern (Georges-Yves), *Éléments fondamentaux des cindyniques*, Économica, 1995

Kervern (Georges-Yves), *La Culture réseau* (éthique et écologie de l'entreprise), Éditions ESKA, 1993

Kervern (Georges-Yves), *Latest advances in cindynics*, Économica, 1994

Kervern (Georges-Yves), Rubise (Patrick), *L'archipel du danger. Introduction aux cindyniques*, Économica, 1991

Klewes (Joachim) et Wreschniok (Robert), éditeurs, *Reputation Capital*, PLEON, novembre 2009 (Voir les trois études de Jean-Paul Louisot « *Managing reputational risk — A cindynic approach* » ; « *Managing reputational risk — Case studies* » ; « *Managing reputational risk — From theory to practice* », p. 115-178)

Lagadec (Patrick), *États d'urgence — Défaillances technologiques et déstabilisation sociale*, Seuil, 1988

Lagadec (Patrick), *La civilisation du risque — Catastrophes technologiques et responsabilisé sociale*, Seuil, 1981

Lagadec (Patrick), *La gestion des crises — Outils de réflexion à l'usage des décideurs*, McGraw-Hill, 1991

Lagadec (Patrick), *Le risque technologique majeur — Politique, risque et processus de développement*, Pergamon Press, 1981

Lagadec (Patrick), *Ruptures créatrices*, Éditions d'Organisation, 2000

Lamère (Jean-Marc), Torly (Jean) *et alii* (Clusif), *Comment gérer les risques de l'entreprise*, Méthode AROME, Dunod, 1989

Louisot (Jean-Paul), *Le guide de gestion des risques du médecin* (adapté à partir d'un original américain de Robert Pendrak), CARM Institute, 2005

Maquet (Yves), *Des primes d'assurance au financement des risques*, Bruylant, 1991

Maquet (Yves), *Le contrôle économique des accidents dans l'entreprise*, Bruylant, 1978

Maquet (Yves), *Le risk management des PME*, Bruylant, 1994

Mareschal (de, Gilbert), *La cartographie des risques*, AFNOR Éditions, 2003

Marmuse (Christian), Montaigne (Xavier), *Management du risque*, Vuibert, 1989

Monroy (Michel), *La Violence de l'excellence (Pressions et contraintes en entreprise)*, Hommes et Perspectives, 2000

Morel (Christian), *Les décisions absurdes (sociologie des erreurs radicales et persistantes)*, Gallimard, 2002

Tixier (Maud) *et alii*, *La communication de crise — Enjeux et stratégies*, McGraw-Hill, 1991

Wybo (Jean-Luc) *et alii*, *Introduction aux cindyniques*, ESKA, 1998

Autres publications

« La gestion de crise », *La Revue Risques*, 1992, n° 9, p. 85-90

« La gestion de crise », *Les cahiers de la sécurité intérieure*, La Documentation française, 1991, n° 6

« La PME face aux risques », Travaux et recherches de l'IAE de Toulouse, 1985, n° 33

« Le droit et la sécurité des entreprises » (rédigé à partir du cours donné à l'IERSE en 2004-2005 de Jacques Lautour)

Maîtrise des risques, classeur à feuillets mobiles avec mises à jour, AFNOR Éditions

Management du risque. Approche globale, recueil de normes, AFNOR Éditions, 2002

« Maîtrise des risques — Prévention et principe de précaution », Actes du Colloque du 6 novembre 2001, INRS, 2002

« Quels avenirs pour nos villes ? », Dossier du bulletin d'information des cadres, 1996, n° 32

Risques et assurances des PME/PMI, Dunod et L'Argus, 1990

Publication Riskassur

De nombreux articles sur la gestion des risques et son évolution écrits par Jean-Paul Louisot sont publiés dans la revue hebdomadaire en ligne gratuite *Riskassur* (www.riskassur-hebdo.com).

Publications du CARM Institute

Ouvrage	Auteurs	Parution	Références
EFARM acts 2002-2003	Ouvrage collectif (en anglais)	Janvier 2004	004028
Responsabilité pénale en hygiène et sécurité du travail	Jackie Boisselier	Février 2004	550413
SIGR (système d'information pour la gestion des risques)	Ouvrage collectif sous la direction de Jean-Paul Louisot	Juillet 2004	004204
Le guide de gestion des risques du médecin	PHICO, Dr Robert Pendrak (MD), adaptation française de Jean-Paul Louisot	Janvier 2005	-
Le standard de gestion des risques Australie et Nouvelle-Zélande	Standards Australia, adaptation française de Jean-Paul Louisot	Juin 2005	-

100 Questions
POUR COMPRENDRE ET AGIR

La gestion des risques connaît une véritable révolution culturelle. Jusqu'alors fonction technique, centrée autour de l'achat de couvertures d'assurances, elle est devenue une discipline managériale et transversale : une valise d'instruments que chaque manager doit connaître et appliquer quels que soient son domaine de compétence et ses missions au sein de l'organisation.

La nouvelle édition de ces 101 questions rassemblées dans cet ouvrage prend en compte les dernières évolutions de ce domaine majeur. En plus de répondre à toutes vos interrogations, vous trouverez une méthode et des outils pour conduire le diagnostic risques avec les responsables opérationnels, les propriétaires de risques, en utilisant leur langage.

Découvrez dans cet ouvrage :

- Comment identifier les risques ?
- Comment les analyser ?
- Quels sont les objectifs de la gestion des risques ?
- Une carte des risques, pour quoi faire ?
- Pourquoi faut-il financer les risques ?
- Les entreprises ont-elles des responsabilités pénales ?
- En quoi consiste la gestion des crises ?

Ce titre va rapidement s'imposer comme le livre de chevet de tout dirigeant, en particulier dans les ETI et PME/PMI... Le complément pratique et indispensable de la norme ISO 31000 !

Pour accéder à notre boutique, scannez ce QR code avec votre smartphone.

ISBN : 978-2-12-465461-1
www.afnor.org/editions