

## **Quels modèles pour la gestion des risques ? Assemblée Générale de la FANAF, Bamako, 26 février 2008.**

Patrick Naïm

Ecole Centrale de Paris (84), Associate in Risk Management (ARM)

Président de la société Elseware, Paris.

Vice-Président du CARM (Cercle des Associés en Risk Management), Paris

Membre de Risk Manager Sans Frontière, Paris

Coauteur avec Laurent Condamine et Jean-Paul Louisot de « Risk Quantification, Management, Diagnosis and Hedging », Wiley 2006

### **Préambule**

Cet article aborde le rôle de la modélisation en matière de gestion globale des risques pour les entreprises, et en particulier sa contribution à l'évaluation et à la réduction effective des risques.

S'il fallait la résumer en une phrase, la position défendue ici est que la modélisation des risques ne se réduit pas à l'analyse statistique, mais doit procéder d'un travail de connaissance des risques.

Nous tenterons de le démontrer en quatre étapes.

Tout d'abord nous discuterons de la nécessité de la quantification des risques pour une approche rationnelle de leur gestion.

Ensuite nous examinerons comment cette nécessité a été prise en compte pour deux contextes et à deux époques différentes.

Nous en déduisons que la modélisation quantitative des risques se caractérise et se distingue par la connaissance que l'on a pu construire sur les phénomènes.

Enfin, nous discuterons de la coopération du risk manager et de l'assureur dans cette démarche de connaissance.

### **Introduction – Le risque, préoccupation d'un monde qui change**

Le nombre de références au mot « risk » sur Google est aujourd'hui près de 400 millions, ce qui en fait l'un des mots les plus cités sur le moteur de recherche le plus utilisé au monde, et ce nombre va sans cesse croissant. Si besoin était, ce simple chiffre montre que le risque est une préoccupation centrale et sans cesse croissante pour les humains, et en particulier pour les sociétés développées.

C'est bien sûr la perception générale du **changement** des équilibres du monde, sur les plans politique, économique, et même naturels qui est sans nul doute l'origine de cette préoccupation, le changement étant source **d'incertitude**, c'est-à-dire de **risque**.

Dans ce contexte, la gestion des risques devient une préoccupation majeure pour les gouvernements et les entreprises, donnant lieu à des tentatives de « cadrage » des risques à tous les niveaux, depuis l'inscription du principe de précaution dans la Constitution Française, jusqu'aux lois Sarbanes Oxley ou NRE en France, ou aux efforts de normalisation de l'ISO sur le risk management.

Or, par définition, les risques semblent mal se prêter au cadrage et à la réglementation. Dès qu'on parle de risque, on parle d'événement aléatoire, c'est-à-dire qui échappe à la prévision, au déterminisme. Les *événements aléatoires fréquents* présentent néanmoins des propriétés organisées, dont la science des assurances a depuis longtemps tiré avantage : « *C'est sur la régularité des résultats moyens des événements considérés en grand nombre, que reposent divers établissements, tels que les rentes viagères, les tontines, les assurances, etc.* » (Pierre-Simon de Laplace, Théorie analytique des probabilités 1812-1820). Mais évidemment les risques majeurs, ou les nouveaux risques, ou les *risques de risques*, supposés évités par le principe de précaution, n'étant pas fréquents (et heureusement) ne peuvent pas être abordés *directement* par les lois de probabilité classiques.

## **La quantification pour une gestion rationnelle des risques**

Comment donc peut-on poser la problème de la gestion des risques de façon rationnelle, c'est-à-dire comment peut-on chercher à prévoir et réduire les risques ?

Tout d'abord, il nous semble nécessaire de considérer que la quantification est la base d'une approche rationnelle. S'agissant d'événements rares et graves, comme les pandémies, les attaques terroristes, les changements climatiques majeurs, on ne les envisage que pour s'y préparer, et se protéger de leurs conséquences éventuelles. Cette préparation a un coût, et on ne peut se préparer à tout. La quantification des risques, c'est-à-dire l'évaluation de leur probabilité de survenance et de la gravité de leurs conséquences, est donc nécessaire pour les *hiérarchiser*. Pour être sérieuse, et opposable à des tiers, cette évaluation quantitative suppose une analyse détaillée, qui va nécessairement conduire à une meilleure prise de conscience des vulnérabilités et de leurs causes. Au-delà de la prise de conscience, la connaissance des points de faiblesse permet d'envisager des améliorations, autrement dit des actions en réduction. Si l'évaluation quantitative peut être effectuée dans l'état initial, c'est-à-dire avant les actions en réduction, elle peut aussi l'être après. Il en résulte qu'une analyse détaillée des risques permet d'évaluer le bénéfice des politiques de réduction des risques, et donc de justifier économiquement celles-ci.

La quantification des risques est le fondement de deux réglementations de nature et de portée différentes, qui, à quelque 30 ans d'écart, nous semblent montrer une évolution dans l'attitude face aux risques, même si, encore une fois, les risques envisagés sont très différents.

La NRC (Nuclear Regulatory Commission) a créé dans les années 1970 les niveaux de sécurité exigibles pour les centrales nucléaires américaines. Ces niveaux fixent aujourd'hui à  $5.10^{-7}$  la probabilité maximum acceptable de décès pour un individu pour cause d'accident nucléaire.

On considère que cette exigence a été l'un des moteurs du développement de la technique dite de PRA (Probabilistic Risk Assessment), ou autrement dit des techniques de sûreté de fonctionnement utilisées dans toute l'industrie. La mise en œuvre de ces techniques nécessite une analyse détaillée des systèmes en place, et des conséquences éventuelles d'une défaillance, pour des risques évidemment et heureusement très rares.

Quelque 30 ans plus tard, au début des années 2000, le Comité de Bâle demande pour la première fois aux banques de prendre en compte dans leurs fonds propres les risques opérationnels, c'est-à-dire le *risque de pertes provenant de processus internes inadéquats ou défaillants, de personnes et systèmes ou d'événements externes*. Le périmètre couvert est très large, puisqu'il recouvre les événements naturels, les fraudes interne ou externe, la responsabilité civile, la sécurité du travail, les défaillances des systèmes, notamment informatiques.

La demande du Comité de Bâle est formulée en termes également quantitatifs : l'établissement doit couvrir par des fonds propres tous les événements ou combinaisons d'événements de risque opérationnel dont la probabilité de survenance dans l'année est supérieure à 1 pour 1000.

Ces deux approches partagent un point de vue quantitatif, puisque l'exigence est, dans les deux cas, de garantir un niveau de garantie acceptable. Dans le cas de la NRC, l'exigence exprime le fait que le risque de décès du au nucléaire doit être rendu négligeable par rapport à d'autres causes de décès, et donc finalement acceptable. Dans le cas des accords de Bâle, l'exigence exprime le fait qu'un établissement bancaire fera face dans 99.9% des cas à toutes les situations adverses qu'il pourrait rencontrer. Elle contribue donc à garantir la stabilité du système bancaire.

Mais les contexte d'applications sont très différents et peuvent conduire à des approches différentes.

En effet, dans le domaine de la sûreté nucléaire ou plus généralement industrielle, les accidents, mêmes mineurs sont heureusement très rares. Il n'est donc pas possible d'aborder le problème par une approche statistique, en extrapolant les incidents ou accidents habituels pour évaluer la probabilité et les conséquences d'un éventuel accident

grave. L'exigence se traduit nécessairement en nécessité d'analyse et de décomposition du problème, autrement dit en démarche de *connaissance*.

D'un autre côté, le périmètre du problème est fermé, puisqu'il s'agit d'un système bien délimité, quelle que soit sa complexité par ailleurs. Une démarche analytique de connaissance semble alors possible, même si elle est difficile.

Le domaine des risques opérationnels diffère sur les deux aspects. De nombreux sinistres de risque opérationnel existent, que ce soit pour la banque considérée, ou pour des établissements concurrents. Par ailleurs, le périmètre est beaucoup plus ouvert puisque les vulnérabilités internes ou externes sont très nombreuses : rappelons que des pandémies aux risques juridiques, en passant par les attaques informatiques externes, tous les risques doivent être couverts.

Dans ces conditions, on peut être tenté d'adopter une approche par les données, c'est-à-dire basée sur l'ajustement de lois statistiques sur les sinistres constatés. Ce faisant, on calque l'approche des risques opérationnels sur celle des risques de marché. En effet, dans le domaine de la finance, les risques de marché présentent des caractéristiques apparemment similaires : des données en grand nombre, et des causes de variation des prix très nombreuses. En 1900, dans sa thèse sur la « Théorie de la Spéculation », Louis Bachelier a construit les bases de la théorie des marchés financiers sur la simple hypothèse que les prix de marché étaient imprévisibles – donc purement aléatoires, parce que les facteurs influençant les investisseurs étaient innombrables. Cette hypothèse, dite des marchés efficients, reste à la base de la modélisation des risques sur les marchés financiers. Malheureusement, cette approche purement statistique n'est pas applicable aux risques opérationnels, et plus généralement aux risques d'entreprise. Elle est inadaptée en termes statistiques, et elle est inadaptée en termes d'approche, dans la mesure où elle suppose de renoncer à la compréhension des phénomènes impliqués dans la survenance et le déroulement des sinistres.

La gestion globale des risques, au niveau d'une entreprise ou d'un Etat, ne peut se contenter d'une approche analytique des risques considérant le système comme « fermé ». Qui ne se souvient des batteries de missiles protégeant les centrales nucléaires françaises après le 11 septembre ? Elle ne peut non plus se satisfaire d'une approche simplement statistique qui considère que l'analyse est impuissante devant la multiplicité des causes, car cette approche est celle du renoncement.

## **Modéliser les risques, c'est acquérir des connaissances**

Quels modèles peut-on alors envisager pour la gestion globale des risques ?

Les risques sont les événements adverses qui peuvent ralentir ou empêcher l'atteinte des objectifs d'une entreprise ou d'une collectivité, territoriale ou nationale.

La poursuite de ces objectifs, dans un environnement ouvert, ne peut se faire sans embûches. Pour un gestionnaire de risque, il ne peut s'agir que de baliser et de sécuriser autant que faire se peut, le parcours.

Cela suppose une démarche de connaissance, qui, n'est finalement que le contraire du risque, ou de l'incertitude. Admettre la coexistence de la connaissance et de l'incertitude semble la seule approche rationnelle. Cette coexistence n'est pas réductible, car l'apparition de nouvelles connaissances engendre de nouveaux risques, et l'investigation de ces nouveaux risques engendre de nouvelles connaissances. Cette recherche de connaissance doit également être guidée par les enjeux, et en cela la quantification des risques est essentielle.

Cette approche de l'incertitude comme liée à la connaissance n'est pas nouvelle. Elle remonte aux pères fondateurs des probabilités.

Citons à nouveau Pierre-Simon de Laplace dans sa *Théorie Analytique des Probabilités* (1812-1820) : *En faisant, par exemple, remonter la plus ancienne époque de l'histoire à 5000 ans, ou 1826213 jours, et le Soleil s'étant levé constamment, dans cet intervalle, à chaque révolution de vingt-quatre heures, il y a 1826214 à parier contre un qu'il se lèvera encore demain. Mais ce nombre est incomparablement plus fort pour celui qui, connaissant par l'ensemble des phénomènes le principe régulateur des jours et des saisons, voit que rien dans le moment actuel ne peut en arrêter le cours.*

Ce que nous dit ici Laplace est simplement que celui qui *connaît* les lois de la mécanique céleste est incomparablement plus assuré dans son analyse des probabilités que celui qui ne connaît que les fréquences.

Dans son essai historique publié à titre posthume (*Essay Towards Solving a Problem in the Doctrine of Chances*, 1763), Thomas Bayes définit la notion de probabilité conditionnelle, mettant en évidence le fait que la probabilité d'un événement à venir et incertain dépend du niveau d'information dont on dispose avant la survenue de cet événement. Cette notion est fondamentale car elle exprime le fait que l'incertitude est spécifique à chacun en fonction de son niveau de connaissance, et est donc plus proche d'une « croyance » (*belief* en anglais) que d'une fréquence.

Ce que formalise de son côté Thomas Bayes est le lien intuitif entre « information » et « probabilité », ou autrement dit entre « connaissance » et « non-connaissance ». Il pose ainsi les bases de toute théorie de la décision. La décision rationnelle est celle qui recherche toute l'information disponible – *décider en connaissance de cause*.

La quantification des risques ne saurait donc se réduire à la modélisation statistique de la sinistralité passée. Modéliser les risques, ce n'est pas modéliser les sinistres, mais modéliser les connaissances, même si, bien sûr les données de sinistres sont une part significative de la connaissance disponible.

Comment alors aborder concrètement la quantification en gestion globale des risques alors même que les historiques de sinistres sont inexistants, ou très partiels ? Tout simplement en utilisant les avantages des deux approches mentionnées plus haut, c'est-à-dire la recherche d'exhaustivité du diagnostic des risques inspirée de l'approche Bâle 2, et la rigueur analytique de recherche des causes et des conséquences inspirée de la démarche PRA.

Il serait trop long ici de détailler ce type de méthodologie, dont la mise en œuvre est en cours dans plusieurs organisations. Nous n'avons pas cité Thomas Bayes par hasard : l'une des technologies à l'œuvre dans ce type de démarche s'appelle les réseaux bayésiens, et permet de construire des modèles probabilistes en combinant les évaluations d'expert et des données historiques.

### **La coopération du risk manager et de l'assureur**

La coopération entre le risk manager et l'assureur va de soi : le financement des risques est la troisième étape de la gestion des risques, une fois que la quantification initiale a été faite, et que tous les efforts raisonnables pour réduire cette quantification auront été entrepris.

Le financement des risques, plus encore que le diagnostic ou la réduction, va bénéficier d'une quantification précise des risques. Combien faut-il transférer ou conserver en rétention ? sont des questions dont les réponses seront d'autant plus solides qu'elles seront quantifiées.

Les primes d'assurance sont basées sur des modèles quantitatifs créés par les actuaires des compagnies d'assurance et de réassurance. Les compagnies – ou les courtiers - ont donc une vision quantitative, mais externe, et donc nécessairement « moyennée » des risques de chaque entreprise, basée sur la connaissance d'un périmètre plus large. A cette connaissance générale, un risk manager doit pouvoir confronter la sienne, plus détaillée, interne, des propres risques de son entreprise.

De cette confrontation naîtra la négociation, dont l'objectif n'est pas seulement – même si celui-ci est important – de fixer le bon niveau de la prime d'assurance. De cette confrontation naîtra aussi un renforcement réciproque des connaissances, des meilleures pratiques des entreprises de chaque secteur.

### **Conclusion**

Le risk management est aujourd'hui en plein développement dans le monde entier. C'est un besoin en réponse aux changements du monde. Les entreprises et les collectivités territoriales et nationales se dotent progressivement d'une fonction de risk management.

En dernier ressort, le rôle du risk manager est de distinguer, parmi les vulnérabilités identifiées, celles qu'il peut réduire et celles qu'il doit transférer aux assureurs. Ce travail de réduction doit s'appuyer sur une quantification, et cette quantification, sur une démarche de connaissance, qui va au-delà de l'analyse statistique.

Tous les risk managers n'ont pas aujourd'hui les moyens de construire des modèles de leurs risques : moyens méthodologiques ou connaissances à disposition. Mais nous pensons que la profession au sens large, des législateurs et des régulateurs aux entreprises, en passant par les assureurs et les courtiers, prendra sa part à cette rationalisation de l'approche des risques, dont le but n'est finalement que de libérer de la capacité à prendre « les bons risques », ceux qui permettent d'assurer le développement.