De l'achat des assurances à l'Enterprise risk management

Des événements spectaculaires ont marqué les deux dernières décennies du XXe siècle alimentant la « peur de l'an 2000 » : catastrophes de Tchernobyl, de Bhopâl, de l'Exxon Valdez, effondrement de la Barings pour n'en citer que quelques-uns. Les médias ont saisi l'occasion pour fustiger les méfaits de la globalisation, les fragilités du système socio-économique mondial. Il est vrai que les relations entre les divers acteurs de ce système deviennent de plus en plus complexes, leurs interdépendances croissantes. Cette situation invite à approcher la situation à l'aide de la théorie du chaos.

Le dernier millénaire s'est achevé sur la campagne de prévention du bug de l'an 2000. Or, il ne s'est rien passé de grave le 1er janvier 2000 à minuit. En réalité, les professionnels du risque y ont vu une illustration d'un paradoxe du métier : la catastrophe annoncée a été évitée, et le succès même de la gestion de ce risque emporte sa disparition, jusque dans la mémoire des acteurs. En effet, le « bug » a entraîné des investissements considérables, en recherche et développement et en matériel informatique, consentis pour gérer pro-activement la situation ; ils ont eu des retombées majeures :

- soutien du développement de l'économie mondiale ;
- mise en place de systèmes informatiques plus performants.

Le troisième millénaire, le nouveau siècle s'est ouvert sur les attentats du 11 septembre 2001, suivis de l'explosion AZF 10 jours plus tard. Par ailleurs, les catastrophes financières, en particulier l'affaire ENRON quelques semaines plus tôt, le Tsunami en Asie du sud-est en décembre 2004 et l'année 2005 record pour les cyclones dans le Golfe du Mexique. Plus près de nous, nous vivons encore les suites de la crise financière déclenchée par les « sub-primes » qui s'est transformée en crise économique « à queue longue », sans parler des effets du réchauffement de la planète qui n'est peut-être même plus un risque mais un changement à gérer.

Dès lors, il est clair que la vision traditionnelle et statique de la gestion des risques, limitée à l'achat d'assurance pour protéger le patrimoine physique d'un organisme, est devenue obsolète. Elle doit faire place à une vision globale et dynamique, intégrant en particulier les risques de la sphère logistique, les risques à la réputation, en un mot l'ensemble des dangers, réels ou perçus par l'ensemble des parties prenantes, ce qui a l'avantage en outre de s'appliquer à des systèmes ouverts et à des territoires plutôt qu'à des organismes à périmètre délimité (voir ci-dessous ERM).

Pour rendre compte de ce développement, le sigle « ERM » (Entreprise-wide Risk Management) est largement employé. In fine et de manière plus globale, sont à prendre en considération l'interaction avec la stratégie de l'organisme intégrant les opportunités comme les menaces et la responsabilité individuelle des responsables opérationnels.

Une vulnérabilité masquée par les approches gestionnaires classiques

Il s'agit d'une approche globale des risques par un organisme qui doit prendre en compte les intérêts et perceptions de l'ensemble des parties prenantes. La gestion des risques ne se limite donc plus à l'achat de couvertures d'assurance, même si le rôle de l'assurance dans la gestion des risques de la plupart des organismes reste primordial, à la fois comme instrument de financement exceptionnel et comme source de méthodes de réduction de certains risques.

La gestion globale des risques doit donc s'appliquer à toute forme d'entité. Le terme générique d'organisme regroupe ici les entreprises industrielles et commerciales bien entendu, mais également les établissements de soins, les collectivités territoriales, et même les États. En effet, les États eux-mêmes doivent concevoir des politiques de sécurité interne (police, gendarmerie et sécurité civile) et externe (forces armées) et garantir le développement soutenable.

La pression de l'opinion publique, les attentes des citoyens et des consommateurs ne laissent plus le choix aux élus et aux responsables. Ils doivent définir, mettre en œuvre, et communiquer, une politique de gestion des risques visant au-delà des actifs de l'organisme lui-même, la sécurité de tous et des biens de chacun des habitants, personnes physiques ou morales, installés sur les territoires concernés par leurs décisions.

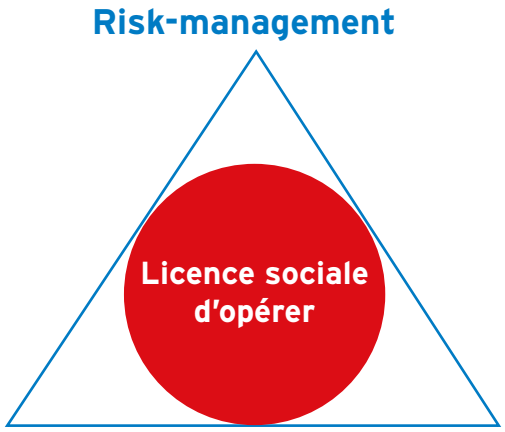
L'élargissement du champ de la gestion des risques passe aussi par la montée en puissance du responsable de la gestion des risques. Aujourd'hui, il n'est plus

possible de se contenter d'un technicien de l'assurance. Pour embrasser l'étendue de la fonction, il doit pouvoir porter un regard global sur l'ensemble des activités de l'organisme concerné, et ses interactions avec ses partenaires et les acteurs du territoire sur lequel il opère. Toutefois, l'autorité du responsable « risques » ne peut que découler d'une mission confiée directement par le principal dirigeant, président-directeur général, maire, président du conseil général ou du conseil régional, tout en rendant compte au conseil d'administration ou aux élus, sans oublier les communications avec l'ensemble des parties intéressées.

Gouvernance, risques et conformités

L'espace des vulnérabilités d'un organisme comprend un grand nombre de risques ; toutefois, seul un petit nombre de vulnérabilités peut effectivement mettre en cause l'atteinte de ses objectifs stratégiques. Certains de ces risques sont directement liés à la gouvernance.

Le triangle GRC



La philosophie de gouvernance d'un organisme, ainsi qu'il ressort de son cadre de gouvernance, de ses politiques, de ses pratiques et de la mise en œuvre de ces politiques, peut soutenir ou non l'atteinte de ses objectifs. Mais, à l'inverse, le cadre de gouvernance de l'organisme constitue également un outil de gestion des risques adopté par le conseil d'administration sous mandat des actionnaires.

Différents cadres de gouvernance permettent à tout organisme de respecter ses obligations de conformité. Il revient à chaque organisme de concevoir le cadre hybride adapté à ses besoins propres. Dans tous les cas, il devra répondre aux attentes de performance des autorités de contrôle et du marché.

Un modèle de gouvernance doit être construit sur les prémices suivantes. La gouvernance :

- n'est pas seulement un outil pour satisfaire une législation ou une réglementation, elle vise à faire ce qui est le mieux pour les actionnaires ;
- ne se limite pas à la mise en place de comités et de conseils, elle s'applique à l'ensemble de l'organisme, inclut les fonctions de contrôle interne et de conformité, en particulier la gestion des risques, l'audit interne, et l'audit externe ;
- repose sur la transparence ; une communication effective, une métrique définie et la responsabilisation des acteurs sont des composantes essentielles d'une bonne gouvernance.

Le fondement d'un modèle de gouvernance efficace pour tout organisme privé repose sur des propriétaires, ou actionnaires qui confient la gestion à des mandataires, administrateurs. Leur rôle est de veiller au bon développement de l'organisme et de nommer les dirigeants qui conçoivent les stratégies, déploient les ressources, conçoivent et contrôlent la mise en œuvre de processus, pour générer des surplus, bénéfices, et créer de la valeur pour les actionnaires. Pour les organismes publics, c'est le citoyen qui confie ce rôle aux élus par son bulletin de vote.

Les organismes, tant publics que privés, ont fait des efforts considérables pour développer une structure solide de gouvernance et de gestion des risques. Cependant, la gestion des risques ne peut influer la culture existante de l'organisme qu'en veillant à l'acquisition de compétences e gestion des risques par tous les opérationnels pour qu'ils puissent de venir véritablement des propriétaires de risques. Encore faut-il qu'ils soient en mesure d'apprécier les nouveaux processus comme des outils de leur performance.

Des instruments de mesure concrets peuvent valider cette évolution au travers des indices de risques clés (KRI - key risk indicators) et indices de performances clés (KPI - key performance indicators).

Gestion des risques et stratégie de l'organisme

Le rôle de la gestion des risques dans le processus de décision stratégique est de fournir une information de haute qualité sur l'incertitude du futur, essentielle pour la prise de décision et la survie de l'organisme.

Le processus de gestion des risques

La planification stratégique est le processus par lequel les dirigeants d'un organisme élaborent, amendent ou affinent une stratégie qui reflète leur vision du futur. Lorsqu'il s'agit d'une entreprise, doivent être pris en compte les risques qui pèsent sur lui au travers de la concurrence, de l'évolution technologique, des marchés, des attentes des consommateurs, etc. En revanche, pour les organismes publics ou les collectivités territoriales l'analyse s'ancre sur les attentes des électeurs et des habitants, sans oublier qu'il peut y avoir une réelle concurrence pour attirer les acteurs économiques. Le processus schématisé ci-dessus montre bien le lien avec l'approche SWOT au travers de l'analyse du contexte interne (forces & faiblesses) et du contexte externe (Menaces & Opportunités) qui peut bénéficier également à un exécutif élu dans une collectivité.

La formalisation de l'incertitude qui accompagne le programme de gestion des risques améliore le processus de planification stratégique :

- il permet d'envisager, et de répondre, aux menaces catastrophiques ;
- il permet de saisir les opportunités en les incorporant au business model ou en inventant un nouveau modèle pour assurer le succès futur ;
- il procure un outil pour gérer les variations non souhaitées (la volatilité) autour des issues espérées.

Le cadre organisationnel de la gestion des risques implique de mettre en œuvre un processus comprenant l'établissement de ses contextes interne et externe, l'élaboration du diagnostic de ses vulnérabilités (appréciation du risque), la sélection des traitements qui sont les plus appropriés, et ensuite l'audit (surveillance et revue) des instruments et du plan de gestion des risques. Tout au long de ce processus, l'organisme doit engager un processus d'information et de consultation avec l'ensemble de parties prenantes. L'intégration du processus de gestion des risques à l'élaboration de la stratégie accroît les chances de l'organisme de gérer efficacement les risques auxquels il est confronté.

L'apport de la norme ISO 31000:2009

En prenant pour base de discussion la norme australienne AS/NZS 4360, la norme ISO 31000:2009 a été rédigée par une trentaine d'experts d'une douzaine de pays, dont la France, avec la participation active de l'AFNOR, l'Association française de normalisation. Elle définit les lignes directrices du management des risques et les processus de mise en œuvre au niveau stratégique et opérationnel. Peut-être convient-il de rappeler ici que la notre australienne s'appliquait à l'ensemble des organismes du pays,

publics et privés, y compris les ministères fédéraux. Bien entendu, l'adoption de la nouvelle norme internationale n'a pas modifié le périmètre d'application. Donc, l'ISO 31000 peut se décliner sans grande difficulté aux administrations et collectivités, même si les parties prenantes doivent être identifiées avec rigueur et l'aspect communication et consultation peut revêtir des formes plus réglementées que dans le secteur privé.

La norme ISO 31000:2009 - Management des risques, principes et lignes directrices de mise en œuvre - a été publiée en décembre 2009 et devrait s'imposer comme le cadre de référence international en gestion des risques.

La norme ISO 31000:2009 définit le risque comme toute conséquence de l'incertitude, c'est-à-dire toute déviation par rapport au plan ou aux attentes des parties prenantes.

La norme est structurée en trois parties :

- les principes répondent à la question pourquoi faire du management des risques. Le processus d'intégration de ces principes se fait ensuite à deux niveaux : le niveau décisionnel et le niveau opérationnel ;
- le cadre organisationnel explique comment intégrer, via le processus itératif de la roue de Deming (Plan-Do-Check-Act), le management des risques dans la stratégie de l'organisme (conduite stratégique) ;
- le processus de management précise comment intégrer le management des risques au niveau opérationnel de la stratégie de l'organisme (conduite opérationnelle).

Le processus reprend les étapes traditionnelles de la gestion des risques à savoir :

- le diagnostic, ou l'appréciation du risque, scindé en trois temps : identification, analyse ou quantification du risque brut et évaluation, ou quantification du risque résiduel, débouchant sur un traitement si le risque résiduel excède la capacité d'absorption choisie par l'organisme (appétit de risque ou tolérance au risque) ;
- le traitement comprenant les deux volets traditionnels de réduction et de financement ;
- le suivi et la révision visant à s'assurer de la qualité de la mise en œuvre et la boucle de retour indispensable pour la mise à jour.

Ce processus est complété par deux éléments importants :

- l'établissement du contexte interne et externe qui assure bien la liaison avec l'élaboration de la stratégie de l'organisme ;
- la communication et la consultation de l'ensemble des parties prenantes tout au long du processus. Doit être effectivement prise en compte la perception des risques par l'ensemble des acteurs potentiellement impliqués dans la réalisation des risques de l'organisme.

La norme ne vise ni à imposer une uniformisation des pratiques, ni à mettre en place un système de management parallèle. En revanche, la norme ISO 31000:2009 propose un référentiel unique pour les organismes de tout secteur et de toute taille. Elle est adaptable et suffisamment flexible ou paramétrable pour harmoniser les processus de management de tous les types d'événements ou de circonstances faisant peser une incertitude sur l'atteinte des objectifs de l'organisme.

L'existence de ce standard international plutôt que des normes nationales, offre aux risk managers une plus grande crédibilité et une meilleure reconnaissance interne face aux autres fonctions traditionnelles dans la direction des organismes publics ou privés. La fonction devient ainsi plus structurée, renforçant son rôle de facilitateur et de communicateur, surtout au sein d'une société internationale.

Les auteurs de la norme ont pris soin de préciser que celle-ci ne se prêtera à aucune certification. Toutefois, malgré cette affirmation retranscrite dans son texte même - ne pas rendre ce standard « certifiable » -, certains pays, au contraire de la France, semblent ouverts à un tel processus à partir de la norme internationale.

Quelques points devraient évoluer à l'usage :

- la nécessité d'une communication/consultation avec l'ensemble des parties prenantes. Cet accent mis sur la perception des risques par les parties prenantes avait initialement troublé plusieurs groupes nationaux ;
- le besoin d'identifier, pour chaque risque, une seule personne comme « propriétaire du risque » (risk owner) et donc comme seul responsable du management de ce risque (v. no Erreur ! Source du renvoi introuvable.). La notion de responsabilité collective ou du « responsable, mais pas coupable » n'est pas été accueillie favorablement par les instances du groupe ISO ;

la notion « d'appétit de risque » qui a soulevé une opposition des responsables de santé et des spécialistes d'hygiène/sécurité. Le consensus s'est formé sur les risques à conséquences positives (opportunités) ou négatives (menaces), l'appétit de risque pouvant être de zéro dans certains domaines. Mais il faut garder à l'esprit également qu'en matière d'hygiène/sécurité, le risque est intrinsèquement négatif, tandis qu'en matière de santé il s'agit d'une stratégie thérapeutique arrêtée avec le patient et/ou sa famille.

La nécessité de penser « territoire »

Lorsque la norme évoque le contexte interne et externe de l'organisme, elle conduit naturellement à envisager le réseau d'approvisionnement dans une économie de plus en plus intégrée où les interdépendances sont complexes et pas toujours prises en compte. Mais le contexte, c'est aussi l'environnement physique et social de l'organisme qui vit en osmose avec les voisins et les autorités installées sur le même territoire. Il est donc essentiel d'organiser une coopération active et proactive avec l'ensemble des acteurs, publics et privés, présents sur ce territoire. En effet, en cas de situation très dégradée, pouvant conduire à une crise, la collaboration de tous sera essentielle et ne peut pas se décréter dans l'urgence.

Certes, cela fait longtemps que les entreprises sont invitées à contacter les pompiers en amont de tout incendie pour se préparer ensemble pour le cas où. Mais c'est insuffisant, et du côté public il faut aussi une coordination entre les différents services impliqués, et qu'ils commencent par utiliser un même SIG (Systèmes d'information Géographique), ou du moins des systèmes compatibles, par exemple. Nos voisins britanniques vont beaucoup plus loin et la législation en vigueur « invite » les risk-managers des territoires, villes ou comtés, à réunir autour d'eux l'ensemble des risk-managers du public et du privé pour une concertation sur l'ensemble des risques auxquels ils sont exposés en communs , risques systémiques ou territoriaux.

En France, c'est ce qui a poussé les pouvoirs publics à s'impliquer dans les PCA et la gestion des crises. Toutefois, il ne faudrait pas que toute situation d'urgence soit considérée comme une crise, il conviendra donc bien définir une hiérarchie partagée par tous les acteurs pour que la coordination soit efficace et efficiente. La résilience sociétale est à ce prix.

En conclusion, et en matière de gestion des risques elle est toujours par essence provisoire, pour autant qu'elle soit prise en compte dans le processus d'élaboration de la stratégie, l'intégration de la gestion des risques contribue au renforcement de ses chances de survie et de succès d'un organisme public ou privé, c'est-à-dire à sa résilience, et par-delà même à la résilience sociétale pour autant que cette rigueur de gestion des risques soient étendues à tous les acteurs présents sur un territoire donné. C'est pour cela que la coordination devient essentielle en particulier lorsque sont en jeu la sécurité et la santé des personnes, la continuité de l'état et des fonctions régaliennes.

Professeur Jean-Paul Louisot
Anc. Université Paris 1 Panthéon-Sorbonne
Institut Catholique de Lille
Directeur Pédagogique de CARM_Institute

IFRASEC
Institut français de sécurité civile
32 rue Bréguet
75011 Paris
www.ifrasec.org