

Cette publication est éditée par la société Optimind, 46 rue La Boétie, 75008 Paris.

Également disponible sur :
www.optimind.fr

Risques opérationnels

Quelles réponses face à un risque difficile à appréhender ?



Les risques opérationnels sont considérés comme nouveaux. Pourtant, bien qu'isolés récemment des autres risques par les réglementations des banques et assureurs, ils ont souvent fait la une de la presse - la faillite de la Barings en témoigne. Ainsi, derrière chaque événement ayant ébranlé fortement des entreprises se cachent des risques opérationnels. C'est d'ailleurs surtout lorsqu'ils sont associés à d'autres types de risques qu'ils sont susceptibles de prendre une ampleur significative.

Sommaire

| | |
|---|----|
| Introduction | 1 |
| Risques opérationnels : définition et enjeux | 2 |
| Quels dispositifs pour gérer les risques opérationnels | 5 |
| Quel pilotage mettre en œuvre ? .. | 10 |
| Conclusion | 12 |

C'est pour ces raisons que l'on cherche, depuis une dizaine d'années, à mieux les appréhender et à évaluer plus finement leurs impacts. En effet, l'environnement nouveau des entreprises accentue fortement leur exposition aux risques opérationnels avec notamment : une concentration des acteurs qui amène à des volumétries et montants en jeu plus importants, une internationalisation des activités avec une multiplication des interconnexions, une sophistication des techniques financières, une sensibilité plus grande aux systèmes d'information, une inventivité des fraudes ou encore une judiciarisation progressive qui conduit de plus en plus les acteurs à être assignés en responsabilité.

Quels sont les enjeux liés à ces risques ? Comment mettre en place les dispositifs permettant d'innover l'organisation, sensibiliser les acteurs, gérer et piloter judicieusement ces risques ? Quels sont les leviers à notre disposition pour y faire face ? Autant de questions auxquelles ce dossier technique tend à apporter un éclairage.

Dan Chelly - Directeur métier

Dossier réalisé par Benjamin Nahoumovitch et Fabien Tannhof, consultants, Emmanuel Berthelé, Thibaud Hager, Vincent Meister, Gildas Robert et Magali Roujas, actuaires consultants.

Risques opérationnels : définition et enjeux

Définition du risque opérationnel

De quoi s'agit-il ?

Le jeudi 6 mai 2010, les marchés américains connaissent quelques minutes d'une intense panique, provoquée par la chute brutale de 37 % du cours de l'action Procter & Gamble, et celle de l'indice Dow Jones, qui perd 9 %. Fort heureusement, l'erreur est vite détectée, et les ordres passés dans l'intervalle sont annulés.

Quelle a été la cause de cette défaillance aussi soudaine que passagère ? Selon certaines rumeurs, il s'agirait d'un trader ayant malencontreusement confondu milliards et millions. Selon d'autres sources, un dysfonctionnement informatique serait la cause du problème. Une fraude a également été évoquée. Qu'importe : dans un cas comme dans l'autre, il s'agit de la survenance d'un risque opérationnel dont les impacts, loin d'être négligeables, peuvent venir ébranler fortement une entreprise. Les événements majeurs marquent souvent de ce fait les mémoires et le marché sur le long terme. Ainsi, tout le monde a en tête l'exemple d'une filiale américaine d'un important groupe d'assurances qui a détecté, en juin 2009, une erreur de programmation dans le calcul des risques associés à ses portefeuilles d'actifs l'ayant conduit récemment à verser plus de 240 M\$ pour solder le litige avec l'autorité américaine des marchés.

Ces deux exemples illustrent bien l'importance qu'il faut donner aux risques opérationnels, qui prennent d'ailleurs toute leur ampleur lorsqu'ils sont associés à d'autres natures de risques. En effet, parce qu'ils sont diffus et difficiles à appréhender - leurs impacts étant de natures variées, et souvent étalés dans le temps - ils sont parfois sous-estimés dans le dispositif global de gestion des risques. Mais qu'entend-on exactement par risque opérationnel ?

Banque/Assurance : des définitions très proches

Les réglementations de la banque comme de l'assurance donnent chacune une définition du risque opérationnel :

Ces deux définitions sont très proches et sont appelées à confluer du fait des convergences des réglementations prudentielles de la banque et de l'assurance. Elles assignent au risque opérationnel les mêmes provenances, réparties en deux catégories : celles qui viennent d'éléments internes à l'entreprise, comme ses procédures, son personnel ou ses systèmes ; et celles provenant d'éléments extérieurs. Sont écartés de ces définitions, les risques stratégiques - puisque par définition les risques opérationnels sont subis et sans espérance de gain - et les risques de réputation qui sont eux difficilement quantifiables et souvent indirects.

Comment appréhender les risques opérationnels ?

Les différentes approches

Deux approches très complémentaires pour appréhender les risques opérationnels peuvent être distinguées : une approche via les processus et une approche davantage causale.

Approche par les processus

L'approche par les processus permet de prendre en compte les spécificités de l'entreprise et ses métiers multiples. On cherche alors à rattacher les risques aux processus principaux, sources de valeur ajoutée, et permettant de délivrer au client le produit ou le service correspondant à sa sollicitation initiale.

On distingue habituellement trois catégories de processus :

- les processus opérationnels au cœur de l'activité, vente, souscription, gestion sinistres, etc. ;
- les processus de management ou de pilotage, dont la finalité est de fixer des orientations, d'évaluer la situation et de décider d'actions correctives si nécessaire ;
- les processus supports au cœur de l'activité - juridique et fiscal, informatique, logistique, etc.

DÉFINITION DE L'ARRÊTÉ DU 20 FÉVRIER 2007 [BANQUE]

Le risque de pertes résultant d'une inadaptation ou d'une défaillance imputable à des procédures, personnels et systèmes internes, ou à des événements extérieurs, y compris les événements de faible probabilité d'occurrence, mais à risque de perte élevée.

DÉFINITION DE LA DIRECTIVE SOLVABILITÉ II [ASSURANCE]

Le risque de perte résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'événements extérieurs.

Il est souvent omis de compléter ce découpage par la définition de processus transverses et multiactivité. Or, certains risques s'attaquent par exemple aux immeubles, quelles que soient les activités qui y sont logées, alors que les conséquences sont justement fortement liées aux activités abritées.

Approche causale

L'approche causale consiste, quant à elle, à analyser le risque en l'encadrant, d'une part de la cause première qui lui a donné naissance et, d'autre part, des conséquences et effets qu'il engendre.

Cette approche, très orientée risk management permet d'identifier plus facilement les causes sur lesquelles il faut agir pour en limiter les occurrences - et intervenir ainsi sur la fréquence - et les actions à mettre en œuvre pour en limiter les effets/conséquences.

Les typologies de risques opérationnels

Les référentiels existants

Fondés sur les définitions réglementaires, des référentiels de typologies de risques opérationnels ont été créés dans les mondes bancaire et de l'assurance.

Le référentiel le plus utilisé est celui proposé par le dispositif prudentiel bancaire de Bâle II. Il a contribué le premier à mieux cerner la notion de risque opérationnel, et sert régulièrement de niveau 1 pour les compagnies d'assurance qui souhaitent définir une arborescence à plusieurs niveaux de leurs propres risques opérationnels.

Le référentiel de Bâle est présenté selon trois niveaux de granularité, dont le premier est constitué des sept familles de risques suivantes :

1. fraude interne impliquant au moins un membre de l'entreprise ;
2. fraude externe ;
3. insuffisance des pratiques internes concernant les ressources humaines et la sécurité du lieu de travail ;
4. clients, produits et pratiques commerciales : manquement, délibéré ou non, à une obligation professionnelle envers un client, à la nature ou aux caractéristiques d'un produit ;
5. dommages aux actifs physiques ;
6. interruption d'activité et dysfonctionnement des systèmes ;
7. dysfonctionnement des processus de traitement - exécution, passation d'ordre, livraison, gestion des processus intégrant les relations avec les contreparties commerciales et les fournisseurs.

Un groupe de travail de l'IFACI, Institut Français d'Audit et de Contrôle Internes a, quant à lui, élaboré une nomenclature des risques pour les entreprises d'assurance. Le référentiel proposé est constitué de trois niveaux :

1. le premier niveau concerne les grandes familles de risques, dont le risque opérationnel ;
2. le deuxième niveau précise la catégorie de risque

dans laquelle on se situe au sein d'une même famille : production, humain, commercial, organisation, système d'information, logistique hors SI ou relation avec les tiers ;

3. le troisième niveau offre un degré de détail supplémentaire au sein de ces catégories.

Quels que soient les choix en matière de structuration du référentiel de risques, l'objectif est que ces risques puissent être clairement définis, compréhensibles par tous, et d'un nombre limité pour éviter les redondances et faciliter la classification et l'analyse agrégée des pertes.

Les natures d'impacts

De par leur définition, les risques opérationnels sont vus comme entraînant uniquement des pertes financières. Néanmoins, s'ils sont bien réels, les impacts qui découlent de la survenance d'un risque opérationnel ne transparaissent pas toujours dans les comptes. Il s'agit notamment de manques à gagner :

- les coûts d'opportunité - non-placement de sommes importantes sur x jours ;
- les pertes de revenus non récupérables - fermeture d'agence suite à un sinistre.

D'autres n'ont pas d'effet négatif. Ainsi, des événements de risques opérationnels peuvent ne pas causer une perte mais au contraire un gain. Par exemple, une erreur de saisie lors du passage d'un ordre sur les marchés financiers est un risque opérationnel qui peut entraîner un gain au moment du débouclage favorable de la position liée à l'évolution du marché.

Il est également important de tenir compte des événements qui ont un coût nul pour l'entreprise, appelés *near misses* ou quasi-pertes, car même si dans ce cas, la défaillance ne produit pas de perte, il est souhaitable de les appréhender pour des questions de gestion des risques. Elles peuvent souligner un réel dysfonctionnement, susceptible de se reproduire, avec cette fois un impact financier réel.

L'impact en termes d'image ou de réputation est lui aussi souvent retenu car l'image d'une entreprise grand public a une valeur inestimable et une dégradation peut occasionner des manques à gagner directs et nécessiter des campagnes de communication coûteuses pour « effacer le passé » - le Crédit Lyonnais devenu LCL en est un bon exemple.

Les risques « frontières »

Les risques opérationnels peuvent survenir seuls ou bien être associés à d'autres risques. Étant donnée la nature des risques opérationnels, ces liens sont parfois difficiles à distinguer, ceci pouvant conduire à la classification incorrecte d'un événement de perte.

“ Certains risques plus complexes nécessitent la définition de règles bien précises pour les appréhender : les pertes de revenus, les litiges juridiques ou fiscaux, les indisponibilités informatiques, etc. ”

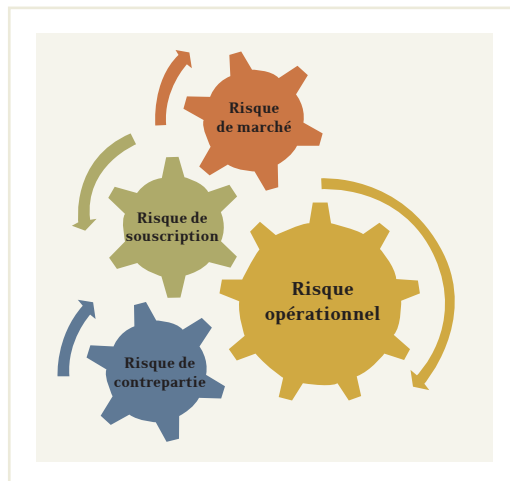
Il en découle que le niveau de fonds propres alloués aux risques opérationnels - qu'il ne s'agit pas d'augmenter pour autant - ne reflète pas toujours la réalité des enjeux.

À ce titre, le Comité européen des superviseurs bancaires, CEBS, soulignait en octobre 2010, que « certains établissements se sont concentrés sur les risques de marché sans reconnaître suffisamment l'importance d'une gestion appropriée des risques opérationnels » or, « les événements passés et plus récents montrent que [...] la sévérité des risques opérationnels associés aux risques de marché peut être très élevée, grevant les profits, l'existence de lignes d'activités ou encore l'existence de l'entreprise tout entière. »

En effet, par définition, les risques de marché correspondent à l'évolution défavorable de la valeur d'un portefeuille ou d'une position. C'est pourquoi ils constituent souvent des circonstances aggravantes de risques opérationnels plutôt que l'origine première du dysfonctionnement. On peut ainsi identifier les pertes dues à :

- la dissimulation intentionnelle d'opérations, *rogue trading* du cas Kerviel ou de la Barings ;
- des erreurs opérationnelles telles que l'erreur de saisie d'un ordre ;
- une mauvaise sélection ou compréhension de modèle de valorisation du produit et/ou du risque ;
- une mauvaise conception, implémentation ou un mauvais paramétrage d'un modèle.

Le risque de souscription des assureurs qui englobe les risques propres à la sinistralité des produits d'assurance, découle régulièrement d'un risque opérationnel.



Source : Optimind

C'est par exemple le cas si, lors de la tarification d'un produit de prévoyance une erreur est commise sur le choix de la table de mortalité ou encore sur la saisie des coefficients de surprime en fonction de l'état de santé. Les pertes financières induites doivent ainsi être imputées au risque opérationnel si les hypothèses utilisées dans les modèles ne correspondent pas aux hypothèses validées en raison d'une erreur humaine ou informatique.

Pour sa part, le risque de contrepartie - risque qu'une contrepartie n'honore pas ses engagements financiers - est régulièrement associé au risque opérationnel lorsqu'une opération se constitue sur la base de faux documents, fraude externe, ou lorsqu'une garantie devient inapplicable suite à des dysfonctionnements.

On le voit, seuls ou associés à d'autres risques, les risques opérationnels peuvent venir impacter l'atteinte des objectifs d'une entreprise, voire mettre en question sa survie. Les enjeux liés à la maîtrise des risques opérationnels sont donc bien réels.

Le facteur humain dans la gestion des risques opérationnels

Une étude menée en 2008 par la BRI, Banque de Règlements Internationaux, a révélé que la plupart des cas de réalisation du risque opérationnel sont liés à une erreur d'exécution et que leurs impacts sont supérieurs à ceux du risque de fraude.

Dans un monde financier porté par l'informatique et l'être humain, l'homme s'avère être facilement le « maillon faible » expliquant les dysfonctionnements d'une activité. Cela peut paraître évident en matière de défauts de conseil, fautes, erreurs ou omissions mais c'est également le cas en matière de systèmes d'information régulièrement fragilisés par des erreurs humaines.

Ce n'est pas pour autant une fatalité car un top management et des collaborateurs sensibilisés disposeront des outils de gouvernance appropriés et des nécessaires réflexes en matière d'identification des risques et de gestion des alertes. En effet, on ne voit souvent que ce que l'on a appris à voir.

Les enjeux liés aux risques opérationnels

Ces enjeux sont de différents ordres :

- sécuriser le compte de résultat ;
- optimiser l'allocation des fonds propres, dans le cadre de l'utilisation d'un modèle interne dédié ;
- sécuriser le cours de bourse et la réputation de la société : on observe régulièrement l'incidence négative des sinistres majeurs sur les cours de bourse, autant pour des raisons financières que d'image. La fuite sur la plateforme BP au cours de l'été 2010 en est une bonne illustration ;
- améliorer ou conserver le rating fourni par les agences de notation, qui définit notamment le coût du refinancement sur les marchés lors d'émissions d'emprunts ;
- améliorer les organisations et réduire les risques ;
- se conformer à la réglementation de la profession et éviter ainsi les sanctions, voire les retraits d'agrément ou assimilés, tels que celui prononcé à l'encontre d'*Ennery Balance - Universal Assurances*, le 28 février 2011, invoquant l'interdiction de pratiquer l'activité d'intermédiation d'assurance pendant 10 ans.

Quels dispositifs pour gérer les risques opérationnels ?

La mise en œuvre de la gestion des risques opérationnels constitue un véritable projet d'entreprise et de conduite du changement. Ce projet nécessite le concours de l'ensemble du personnel et il convient de l'accompagner dans le cadre de son déploiement. Des changements sont à opérer pour prévoir, définir et mettre en œuvre une véritable démarche de pilotage de ces risques.

Un tel projet poursuit la démarche suivante :

❖ La mise en place d'approches qualitatives d'identification et d'évaluation des risques opérationnels, qui permettent simultanément de sensibiliser et de responsabiliser les agents opérationnels sur la gestion des risques.

❖ L'élaboration d'approches quantitatives consistant à :

- mettre en évidence le coût des risques opérationnels ;
- identifier les expositions aux risques et donc la consommation de fonds propres.

Dans ce cadre, il est nécessaire de combiner à la fois l'expérience du passé avec une vision prospective du futur proche tout en disposant au quotidien d'outils d'alertes.

Apprendre à tirer les leçons du passé

Toute organisation se doit d'apprendre de ses expériences ou incidents passés, afin de capitaliser, éviter et mieux gérer les incidents.

Une approche disciplinée et structurée de collecte des incidents contribue à l'établissement de la culture du risque dans l'entreprise. Cette démarche joue en effet un rôle important au niveau de la vigilance des acteurs, de gestion des incidents, du traitement des alertes, de la conduite et du suivi des plans d'actions.

Par ailleurs, pour les risques dits « de fréquence », l'analyse des incidents avérés permet d'objectiver l'évaluation des risques potentiels propre à la cartographie.

Base interne de collecte des incidents

La mise en œuvre d'une base incident nécessite de :

- organiser la base de collecte des données d'incidents en définissant les rôles et responsabilités dans la détection et caractérisation des incidents ;
- définir le périmètre de la notion d'incidents
 - seuil de collecte, quasi-pertes, manques à gagner, etc. ;
- proposer des méthodes d'évaluation des impacts et de prise en compte des incidents « complexes ».

Dans le cadre d'une bonne gouvernance, il est nécessaire de définir une procédure d'escalade qui permette la remontée des alertes pour gestion selon leur criticité.

Bases externes

Les entreprises sont forcément également exposées à des événements extrêmes et particulièrement

rare. Or, elles ne disposent « heureusement » pas dans leur base incident de l'ensemble de ces événements. C'est pourquoi l'utilisation de bases de données externes offre une réelle valeur ajoutée pour appréhender ces risques rares, en s'appuyant sur l'expérience des « autres » entreprises. Aussi, il existe en la matière :

- des bases de données commerciales qui utilisent des données publiques collectées à partir de différentes sources issues de la presse, de régulateurs, ou encore de rapports annuels ;
- des consortiums de banques internationales, tel ORX ou d'assureurs, tel ORIC, dans lesquels les données anonymisées sont collectées auprès des membres, selon un processus normé.

Vivre au présent : détecter les sources de dysfonctionnement ou de modification du profil de risque

Les indicateurs de risque - KRI

Les indicateurs de risque, ou KRI - *Key Risk Indicators* - mettent en évidence l'évolution de l'exposition d'une entreprise à un risque. Ils permettent d'anticiper la réalisation d'un risque par le biais du système d'alerte associé. Pouvant être de deux natures, ils offrent une évaluation régulière de l'évolution du risque lui-même ou encore de l'environnement de prévention et de contrôle. Ils permettent ainsi de détecter une situation anormale avant qu'un incident ne survienne.

En assurance, un taux important de réclamations-client peut indiquer une défaillance au niveau de la gestion des contrats ou un défaut dans la conception du produit nécessitant une réaction rapide de l'assureur via éventuellement une revue des conditions générales.

Des tableaux de bord d'indicateurs permettent ensuite l'exploitation des résultats, tant par les acteurs métier, qui peuvent trouver ainsi un moyen d'objectiver leurs décisions, que par le responsable des risques opérationnels.

“

La mise en place en mode projet du dispositif rejoint rapidement la gestion au quotidien, l'animation de la filière puis le pilotage global du risque.

”

Afin de garantir la pertinence et l'efficacité de ce type d'outil, le responsable des risques opérationnels doit s'assurer que :

- les indicateurs de risques reflètent réellement et significativement l'exposition au risque des métiers concernés ;
- les indicateurs de risques sont fondés sur des données fiables ;
- la fréquence de rafraîchissement est suffisamment élevée et adaptée pour garantir une information fluide, permettant de prendre rapidement des décisions ;
- les indicateurs sont compréhensibles et pertinents pour ceux qui les exploitent.

Le dispositif de contrôle

Le dispositif de contrôle est composé de l'ensemble des opérations de contrôle effectuées par l'entreprise. Ces opérations sont de différentes natures, telles qu'indiquées dans le schéma ci-dessous.

Ainsi, ces contrôles remplissent notamment les missions suivantes de sécurisation de l'activité :

- exercer un rôle d'alerte en détectant la survenance d'anomalies à un taux anormal, afin d'enrayer cette survenance et diminuer ainsi la fréquence des incidents ;
- garantir l'intégrité de l'organisation, en assurant par exemple la séparation des fonctions ;
- sécuriser l'activité ;
- mesurer l'efficacité du dispositif de maîtrise du risque opérationnel, afin de l'optimiser.

Le dernier objectif joue en quelque sorte un rôle de garde-fou, lorsque les indicateurs de risque, qui sont nécessairement en nombre limité, n'ont pas ou peu joué leur rôle d'alerte préalable.

Ces contrôles s'intègrent dans un processus itératif et dynamique de gestion des risques visant une amélioration en continu de l'organisation et sa sécurisation.

Anticiper l'avenir : l'approche prospective

Les seules pertes internes ne suffisent pas à parfaitement appréhender les risques opérationnels. La cartographie et les scénarios permettent d'apporter une vision complémentaire et prospective sur les risques potentiels auxquels l'organisation est exposée.

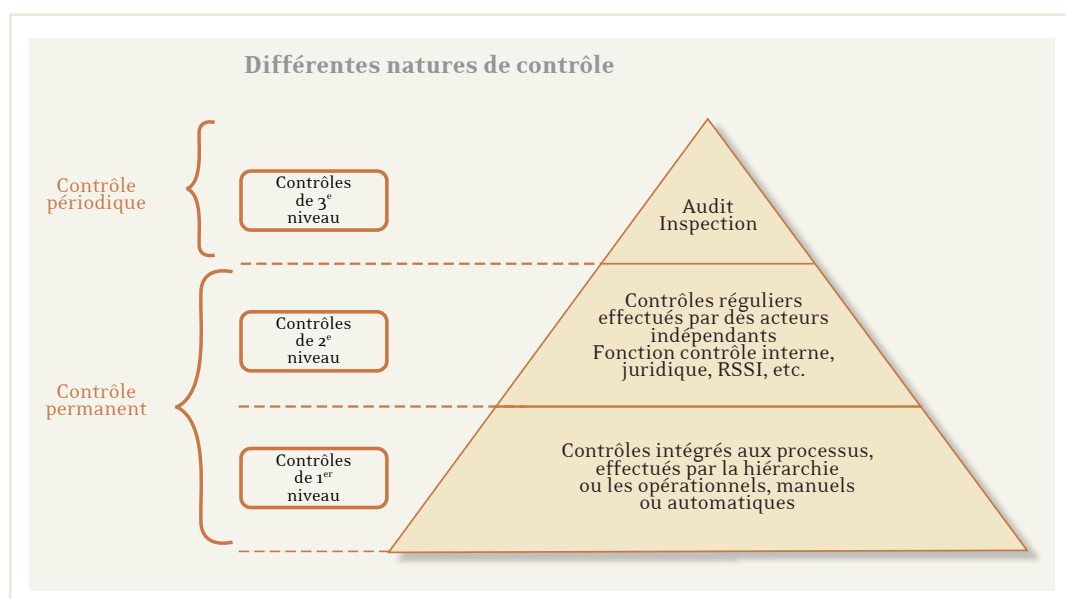
La cartographie des risques

La cartographie des risques constitue un processus vivant d'identification, d'évaluation et de hiérarchisation des risques opérationnels susceptibles d'avoir un impact sur un processus ou une ligne métier. À ce titre, cet outil constitue un élément fondamental du dispositif de gestion des risques et de contrôle interne de l'entreprise. La cartographie contient l'ensemble des informations nécessaires, permettant de prendre des décisions en termes d'actions correctrices par rapport à des expositions aux risques trop importantes ou insuffisamment maîtrisées.

L'appréciation de l'exposition aux risques repose sur l'évaluation de la fréquence de survenance des risques et de l'impact financier au regard du dispositif de maîtrise mis en œuvre.

De ce fait, l'évaluation des risques débute souvent par celle des risques bruts, ou intrinsèques, qui sont les risques qui pèsent sur l'activité, abstraction faite de tout dispositif de maîtrise existant. La prise en considération des dispositifs de maîtrise conduit ensuite à réévaluer ces risques, que l'on appelle alors les risques nets, ou risques résiduels.

La périodicité de revue des évaluations se fait le plus souvent annuellement. Pour autant, la mise à jour de la cartographie des risques peut être anticipée lors de la survenance d'événements considérés comme remarquables, dès lors qu'ils sont susceptibles de



Source : Optimind

modifier le profil de risque de l'entreprise. Parmi ces événements, on peut citer l'évolution substantielle de la législation applicable à l'entreprise - intégration en France par exemple de *class actions* - ou la modification du fonctionnement interne de l'entreprise telle que l'automatisation d'un processus à l'aide d'un système d'information.

Les axes d'analyse des résultats issus de la cartographie des risques conduisent notamment à étudier au cas par cas si le risque résiduel qui subsiste est acceptable ou non. Les approches de classification des risques alors mises en œuvre, permettent de déterminer les priorités afin d'améliorer le dispositif existant via l'élaboration de plans d'actions.

La cartographie, schéma A, fait ressortir majoritairement :

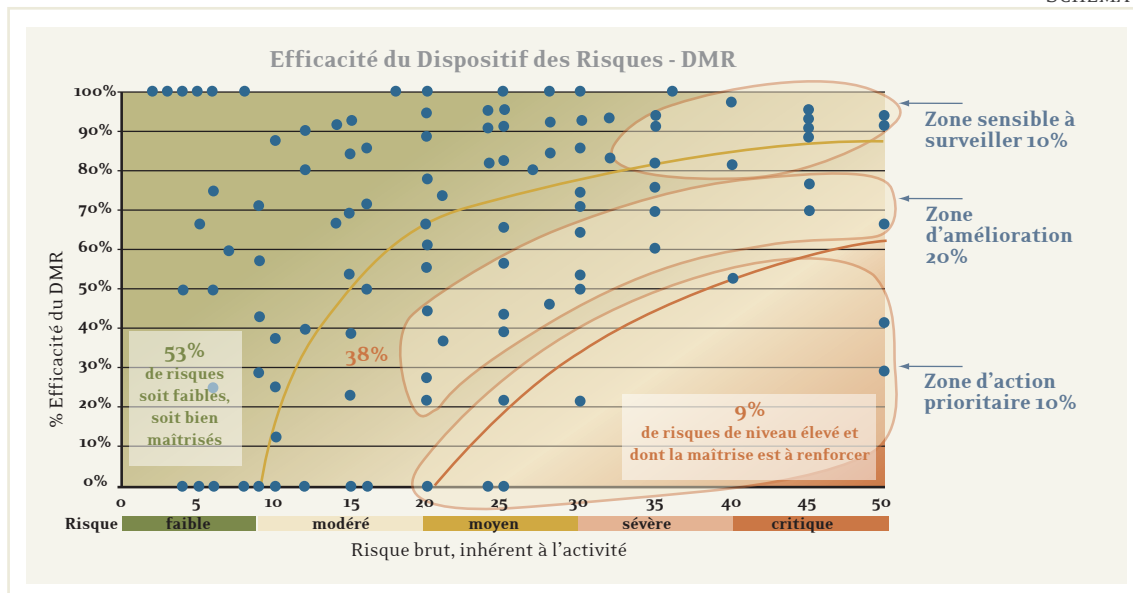
- les risques exogènes, rares et à fort impact pour lesquels l'entreprise n'a pas la maîtrise sur l'occurrence

de l'événement mais peut en limiter l'impact avec notamment un plan de continuité de l'activité, PCA ;

- les risques au cœur de l'activité dont l'impact peut être fort et pour lesquels une bonne maîtrise est nécessaire au quotidien. Il s'agit alors, avec la mise en place d'indicateurs d'alerte, de s'assurer que ce dispositif reste à tout moment opérationnel et sans défaillance.

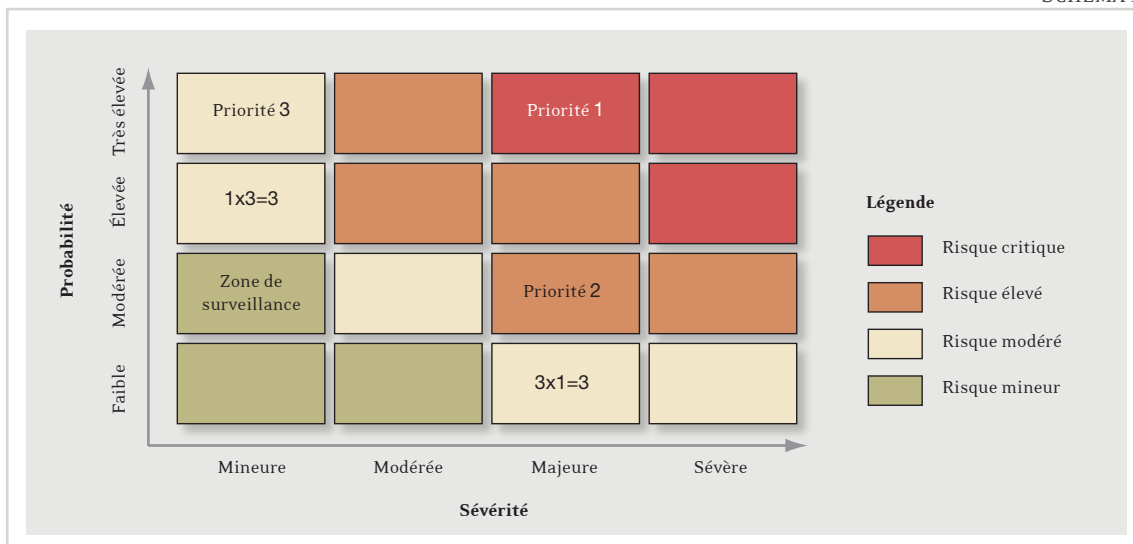
Il est à noter que certaines démarches de restitution introduisent des biais d'analyse non négligeables s'appuyant sur des matrices dites « de chaleur » mal conçues et aboutissant à une analyse erronée des risques, matrice 4 par 4 de fréquences et sévérités, scores issus de formules non justifiées, etc. La matrice ci-dessous, schéma B, est l'exemple même de ce qu'il vaut mieux éviter de réaliser.

SCHÉMA A



Source : Optimind

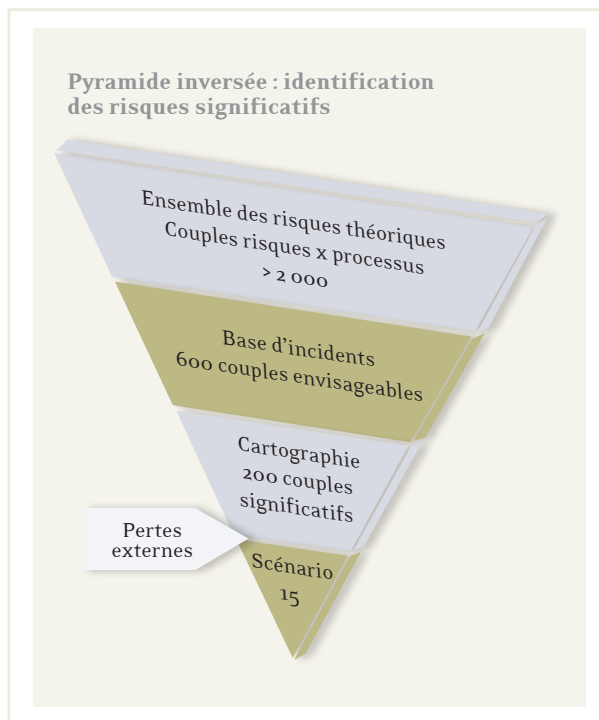
SCHÉMA B



Source : Optimind

Les analyses de scénarios sur les risques significatifs :

Comme l'indique la pyramide inversée ci-après, l'analyse de scénarios constitue le « filtre » ultime d'approfondissement des risques identifiés par l'entreprise.



Source : Optimind

Les analyses de scénarios sur les risques significatifs s'inscrivent donc dans la finalité de cette démarche itérative de risk management. Elles doivent permettre d'identifier les cheminements possibles du risque, les facteurs d'amplification éventuels et ainsi optimiser les leviers de réduction.

“ Le risk manager se doit de rester vigilant et de réagir face à l'évolution ou à l'émergence de risques opérationnels. Ces éléments nouveaux sont à évoquer en Comité RO. ”

Dans leur mise en œuvre, les analyses de scénarios impliquent donc de forts niveaux d'expertises nécessitant, comme dans l'analyse de tout système complexe, l'association de compétences internes - voire externes - très différentes dans le cadre d'ateliers bien structurés.

Les scénarios sont souvent associés au modèle interne sur les risques forfaitaires opérationnels. Or, compléter une démarche par l'utilisation de scénarios, s'avère être réellement pertinent.

Quelle mesure/quantification du risque opérationnel ?

Les difficultés d'évaluation du risque opérationnel

En termes d'évaluation des risques opérationnels, deux catégories de risques peuvent être distinguées :

- les risques opérationnels récurrents - fréquents - peuvent être évalués par une approche « fréquence × coût » classique en assurance, réalisée sur la base incidents et les historiques. Cette approche nécessite d'accorder une importance particulière à la profondeur de l'historique, la survenance d'un incident devant alors être tracée et qualifiée convenablement ;
- les risques extrêmes constituent la deuxième catégorie. Ils prennent une part essentielle lorsque l'on s'intéresse à la solvabilité. Il s'agit des risques majeurs comme par exemple les catastrophes naturelles, les risques industriels, les fraudes de grande ampleur, les indisponibilités majeures et durables du système d'information ou encore les risques frontières. Pour ces risques, très peu d'historiques sont disponibles. Il est donc indispensable de recourir à des expertises ou des modèles très complexes qui nécessitent, de plus, de disposer d'une très bonne visibilité sur son exposition.

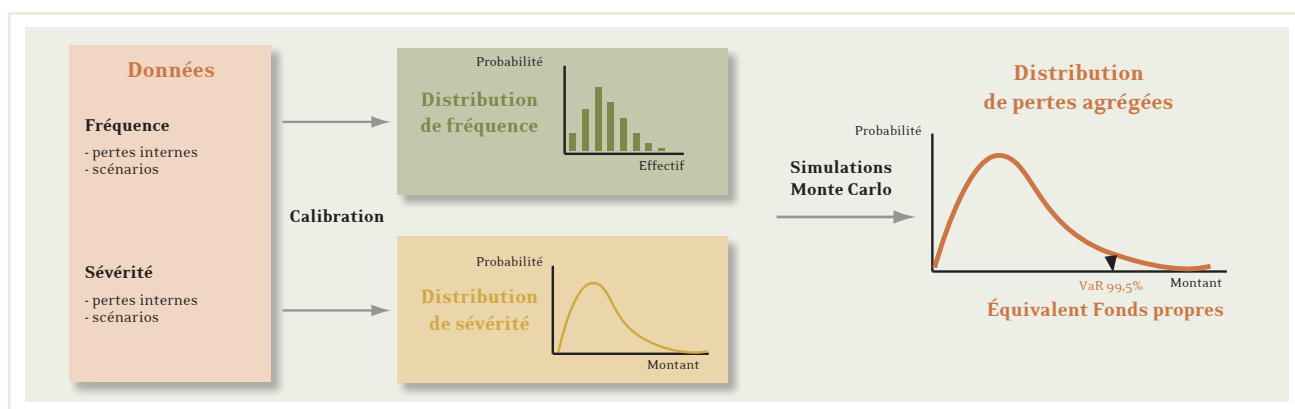
Dans tous les cas, le caractère diffus des risques opérationnels, lié à leur nature en lien étroit avec l'organisation de la société, aura des conséquences fortes sur les modèles d'évaluation. Les difficultés d'identification de l'ensemble des coûts les rendent également complexes à appréhender : les impacts peuvent être étalés dans le temps, en cas de contentieux client par exemple, l'impact financier peut survenir longtemps après le fait générateur. Enfin, les nécessaires approches par auto-déclaration et auto-évaluation sont susceptibles d'être à l'origine de biais dans les évaluations, même si des démarches existent pour les fiabiliser au mieux.

Les modèles d'évaluation

L'approche LDA - *Loss Distribution Approach* - est l'approche statistique la plus fréquemment utilisée pour l'agrégation de distributions de pertes. Concernant les risques opérationnels, elle s'appuie sur la base incidents contenant les données des pertes collectées au sein de l'entreprise.

L'approche consiste à établir, pour chaque ligne métier et chaque type d'événement de pertes, la courbe de distribution des montants de pertes et la courbe de distribution des fréquences sur un intervalle de temps donné. Les modélisateurs cherchent ensuite à ajuster une loi de probabilité sur chaque distribution obtenue en utilisant des tests d'adéquation statistique. Ces deux distributions sont ensuite combinées grâce à un algorithme numérique tel que les simulations de Monte-Carlo, l'approche récursive de Panjer ou encore en inversant la fonction caractéristique, car il n'existe en général pas d'expression analytique de la distribution composée.

Le montant des fonds propres recherché correspond alors à la *Value at Risk* à un quantile donné - VaR99,5% pour l'assurance, VaR99,9% pour la banque - sur un horizon d'un an.



Source : d'après *Risques opérationnels - De la mise en place du dispositif à son audit*, C. Jimenez, P. Merlier et D. Chelly, 2008.

Bien qu'elle soit la méthode la plus communément utilisée par les établissements bancaires et les organismes assureurs pour modéliser les risques opérationnels, cette approche renferme plusieurs inconvénients :

- l'hypothèse de pertes indépendantes et identiquement distribuées, imposée par cette méthode implique que la VaR soit calculée sur un périmètre représenté par l'intersection d'une ligne métier et d'un type de risque ;
- en considérant les incidents comme complètement indépendants, on ne tient pas compte des éventuelles corrélations ou liens de cause à effet qui pourraient entraîner un effet cumulatif ou atténuateur ;
- ces calculs sont réalisés sur des données historiques qui non seulement sont des données d'échantillonnage et peuvent être rares, dispersées et soumises à nombre d'appréciations subjectives mais de plus, ces données historiques ne permettent pas d'intégrer les changements dans le profil de risque de l'entreprise suite à la survenance d'un incident.

Pour pallier à certains de ces inconvénients, l'approche LDA sur les pertes internes est souvent combinée à des modèles quantifiés de scénarios. Une autre alternative est la méthode des *scorecards* qui s'appuie non pas sur des données de pertes effectivement constatées, mais sur des indicateurs de

risque, qui incorporent donc une vision « a priori » des risques opérationnels.

Dans tous les cas, les modèles d'évaluation des risques opérationnels intégreront toujours des limites, qu'il faut garder à l'esprit.

En premier lieu, les modèles utilisant des lois statistiques présupposent indirectement que les événements et comportements futurs peuvent être globalement déduits des événements et comportements passés. Bien sûr, une utilisation de choc, y compris fictif, permet de limiter cette insuffisance conceptuelle. Toutefois, le modèle se trouve limité à la seule vision de son créateur.

D'autre part, quels que soient les éléments modélisés, il convient de se placer à un niveau de granularité et de sophistication adaptés. En effet, la sophistication excessive d'un modèle engendre généralement un besoin important en termes d'hypothèses associées naturellement à un manque de robustesse potentiel du modèle. Il est donc important de se baser au niveau de granularité suffisant permettant une modélisation fiable et réaliste de l'activité et de tester la capacité prédictive du modèle, ou mieux, de ses différentes composantes.

Le choix entre la formule standard et le modèle interne en assurance

Dans Solvabilité II, les assureurs ont le choix entre la formule standard et le modèle interne pour calculer leur capital réglementaire. L'approche modèle interne comporte l'inconvénient majeur d'être beaucoup plus coûteuse : d'une part la formule standard devra également être mise en œuvre, mais d'autre part le modèle interne comporte des exigences de validation et de maintenance très fortes. Toutefois, sur les risques opérationnels, la formule standard a retenu à ce stade une approche très forfaitaire éloignée de la réalité des risques sous-jacents : des facteurs par secteur d'activité sont appliqués aux encours et aux primes. L'approche par modèle interne permettra alors :

- d'économiser des capitaux réglementaires : cet intérêt n'est bien entendu pas acquis car il dépend des risques réels de l'assureur et dans tous les cas ne peut pas constituer l'unique argument pour un assureur.
- d'améliorer la connaissance des risques, et donc de permettre le lancement de plans d'actions en vue de la réduction et de la maîtrise des risques opérationnels. Cet avantage apparaît à la fois sur les risques fréquents de faible impact, par exemple par la modification des processus ou la mise en place de contrôles adaptés. Il s'inscrit également sur les risques extrêmes du fait de l'analyse poussée qui en est faite lors de la construction du modèle.
- de bénéficier d'avantages concurrentiels, notamment en termes de communication sur le marché. En particulier, les modèles internes sont pris en compte par les agences de notation.

Quel pilotage mettre en œuvre ?

L'insertion opérationnelle

Le day to day management

Loin de n'être qu'une exigence réglementaire, la gestion des risques opérationnels peut constituer un véritable levier de management. C'est tout l'enjeu d'un pilotage quotidien de la gestion des risques opérationnels, qui doit s'insérer de façon harmonieuse dans les activités opérationnelles. On parle alors de mode de management par les risques, c'est-à-dire intégrant ce prisme dans les prises de décision importantes.

“
Le paramétrage et le
déploiement d'une solution
GRC qui vient innover
l'organisation doivent
s'accompagner d'une réelle
gestion du changement :
communication, formation,
etc.

”
Pour autant, la complète insertion de la gestion des risques opérationnels dans l'activité quotidienne ne doit pas devenir une routine, ou encore donner un sentiment de fausse sécurité, au point de faire oublier d'exercer une vigilance accrue dans les situations qui le nécessitent. Il ne suffit pas en effet de s'appuyer sur le dispositif existant, mais l'adapter aux évolutions de l'entreprise. C'est pourquoi il convient d'intégrer « l'aspect risque opérationnel » dans les prises de décision porteuses de risques telles que le lancement d'un nouveau produit, la création d'une nouvelle activité ou encore l'automatisation d'un processus. Le risk manager exerce alors un rôle de conseil en analysant les risques avant la prise de décision, afin de garantir, non pas la suppression totale du risque, mais l'identification et la prise en compte de ces risques dans les arbitrages qui sont opérés.

L'intérêt de l'outil GRC pour piloter au quotidien

Pour garantir la fluidité du dispositif de gestion et de pilotage du risque opérationnel, un système d'information spécifique s'avère souvent indispensable. Un système d'information efficace permet de structurer et d'agréger aisément les données pour analyser les informations sous différents angles. Or, depuis plusieurs années, de nombreux éditeurs proposent des systèmes d'information de gestion des risques - SIGR - plus couramment appelés outils GRC - gouvernance, risques et contrôles. Ils permettent, comme indiqué sur le schéma C ci-dessous, de déployer et de piloter l'ensemble du dispositif de gestion des risques opérationnels et de contrôle interne.

Le pilotage

Les tableaux de bord

Les tableaux de bord constituent des outils indispensables au suivi des risques. En fournissant une vision globale, synthétique et agrégée, ils permettent au top management d'assurer des prises de décision adaptées dans une logique de bonne gouvernance des risques.

La définition et la sélection des informations et indicateurs constituent les phases critiques de réalisation de ces tableaux de bord : ils doivent à la fois correspondre aux besoins de l'organe dirigeant qui devra se les approprier parfaitement, et être suffisamment pragmatique afin que leur alimentation puisse être réalisée de manière récurrente sans impacter trop fortement l'activité opérationnelle. Enfin, ils doivent posséder une certaine souplesse pour s'adapter au caractère changeant du risque et permettre d'identifier les risques émergents.

Ils peuvent également avoir vocation à être transmis en externe, au régulateur et aux auditeurs, notamment afin de justifier de l'existence des processus de suivi des risques, conformément à l'ORSA dans le cadre de Solvabilité II.

Ils doivent s'appuyer sur une définition de seuils de significativité adaptés aux enjeux, c'est-à-dire à la taille et à la complexité de l'entreprise.

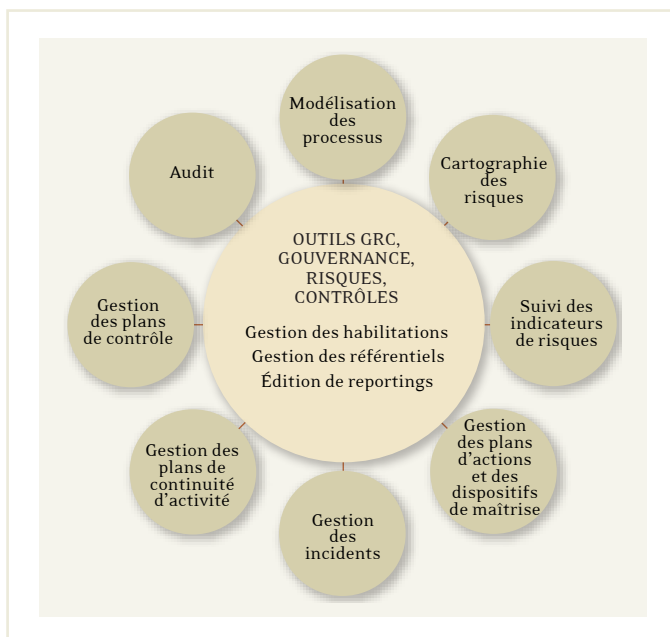
Le suivi des plans d'actions

Chaque élément du dispositif peut souligner des points à améliorer et donc amener à proposer des plans d'actions. Cela peut intervenir à la suite :

- d'un risque majeur résiduel issu de la cartographie ;
- d'un incident avéré susceptible de se répéter ;
- de la dégradation soudaine d'un indicateur de risque ;
- de la découverte d'une mauvaise adéquation de certains contrôles.

Un comité risques opérationnels doit alors assurer notamment un suivi de ces plans d'actions et observer l'évolution des risques liés.

SCHÉMA C



Source : Optimind

Les leviers complémentaires face aux risques opérationnels

L'Enterprise Risk Management

Le risque opérationnel étant aux confins d'autres risques, il s'inscrit idéalement dans une démarche plus globale dite d'ERM, *Enterprise Risk Management*. Cette démarche consiste en un ensemble de processus conduisant à identifier, quantifier et gérer les risques auxquels est exposée l'entreprise, qui peuvent mettre en péril l'atteinte de ses objectifs stratégiques. Il s'agit alors de construire une véritable politique de gestion des risques sur tous les risques significatifs. L'objectif de l'ERM n'est pas forcément de réduire le risque au minimum mais de le contenir au mieux afin d'optimiser le coût du risque, et ce, toujours en lien avec la stratégie de l'entreprise qui oblige à prendre en compte, certes les pertes, mais également le coût des mesures de prévention, de protection et de financement du risque.

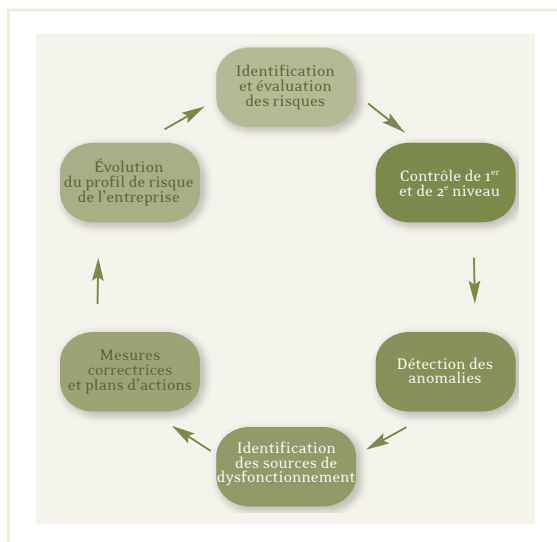
La liste des risques entrant dans le périmètre du risk management n'est évidemment jamais fermée. Une bonne démarche ERM doit aussi et surtout déterminer le plus tôt possible tous les nouveaux risques pouvant influencer, à plus ou moins long terme, l'atteinte des objectifs stratégiques.

L'ajustement du dispositif de contrôle

Parmi les différents moyens de maîtrise à disposition des risk managers, il faut citer la mise en place de points de contrôle complémentaires ou réajustés. Ainsi, en réponse à certains risques, il est possible de décider d'assurer :

- la validation systématique par le département juridique de la plaquette commerciale d'un nouveau produit avant son lancement ;
- le blocage automatique de la saisie sur le système d'information pour éviter le dépassement d'un seuil de montant pour une transaction.

Le processus de mise en place des points de contrôle est un processus itératif d'amélioration.



Source : Optimind

Le Plan de Continuité d'Activité, PCA

Les entreprises ne peuvent empêcher la survenance de certains risques exogènes, tels que la crue d'un fleuve, mais elles peuvent à défaut en limiter les impacts. C'est alors qu'intervient notamment le plan de continuité d'activité.

En effet, quels que soient les événements et leurs niveaux de gravité, l'entreprise doit être en mesure d'assurer au mieux les prestations de services attendus par les acteurs du marché, que ce soient ces clients, actionnaires, investisseurs ou encore les autorités de tutelle.

Dans le cas particulier des banquiers et assureurs, il est impératif d'assurer à tout moment le maintien en condition opérationnelle, via des tests, de la continuité des activités dites « critiques ». Ces dernières devront être préalablement identifiées, pour définir les besoins de continuité et les ressources nécessaires à leur fonctionnement.

L'assurance

La souscription de polices d'assurance permet d'assurer le financement d'une perte par un tiers assureur. Elle constitue donc également un levier de maîtrise du risque opérationnel avec notamment l'utilisation de polices d'assurance responsabilités civiles professionnelle, exploitation ou mandataires sociaux, fraude, perte d'exploitation ou de revenu, et dommages aux biens et personnes.

La plupart de ces polices d'assurance couvrent des risques opérationnels purs ou liés à d'autres risques. Tous les risques ne sont cependant pas assurables, ils doivent vérifier les conditions classiques des risques d'assurance, à savoir, être issus d'événements aléatoires, futurs, licites et dont la survenance est indépendante de la volonté de l'assuré. À noter que le fait d'assurer un risque ne dédouane pas l'entreprise de mettre en œuvre une gestion des risques et un contrôle interne efficaces permettant de prévenir la survenance du risque opérationnel.

Enfin, les risques doivent être raisonnablement assurables compte tenu de la prime et de la franchise eu égard au niveau de couverture. Ainsi, à chaque exercice, l'entreprise évalue son appétence au risque et peut envisager un transfert des risques qu'elle ne parvient pas elle-même à mutualiser ou dont la survenance aurait des conséquences trop importantes sur son résultat ou sa solvabilité. Elle considère alors le profil de chacun des risques afin de définir une limite de risque acceptable.

Dans le cadre des banques en approche avancée - AMA -, il est possible de diminuer les fonds propres réglementaires alloués au titre des risques opérationnels à hauteur de 20 %, si les polices répondent à des critères d'éligibilité, notamment le *rating* de l'assureur. En effet, externalisé via une police d'assurance, le financement d'un risque opérationnel transforme une grande part de ce risque en risque de contrepartie, défaillance de l'assureur, refus d'indemnisation, etc.

“

Une direction générale doit pouvoir rapidement visualiser les risques significatifs susceptibles d'ébranler l'entreprise et prendre les décisions qui s'imposent, y compris d'accepter le risque en l'état.

”

Conclusion

Les risques opérationnels peuvent à la fois survenir au quotidien dans le cadre d'une activité commune mais également intervenir très ponctuellement et de façon dévastatrice dans des cas extrêmes. Face à cette diversité de manifestation du risque opérationnel, les dispositifs présentés dans ce dossier technique offrent un panorama complet permettant de les appréhender et de les réduire.

Pour pouvoir les apprécier finement, il est absolument nécessaire d'en comprendre les contours et donc de disposer de formation ou de sensibilisation ciblée c'est-à-dire adaptée aux métiers concernés. Bien sûr, ces dispositifs, bien que réglementaires, dépassent largement les seuls objectifs de conformité ou de calcul des fonds propres et s'inscrivent davantage dans une réelle dynamique de sécurisation de l'activité. C'est là, tout l'enjeu d'une démarche de gestion et de pilotage des risques opérationnels.

Dans le monde des assurances, la directive Solvabilité II n'est pas encore très précise sur ces attentes en matière de risque opérationnel. Les mesures d'exécution de niveau 2 et 3 devraient y remédier. Dans cette attente, la majorité des organismes assureurs se sont appuyés sur les textes et les expériences de leurs homologues bancaires pour mettre en place les différentes approches et déployer leurs dispositifs. Le monde bancaire continue d'ailleurs lui-même à ajuster ses attentes au regard des années d'expérience. Les *consultative papers* très riches et précis publiés par le Comité de Bâle en décembre 2010 le confirment. Les démarches risques opérationnels mûrissent et évoluent donc au fil du temps. Les assureurs, de plus en plus actifs, s'inscrivent en ordre de marche pour relever ce nouveau défi. En effet, 2013 n'est qu'un premier jalon pour une démarche pérenne qui va bien au-delà du projet Solvabilité II.

optimind. ::

Qui sommes-nous ?

Société de conseil en actuariat et gestion des risques, OPTIMIND est un interlocuteur de référence pour les assureurs, mutuelles, banques et grandes entreprises qui souhaitent un partenaire métier les accompagnant dans leurs projets. Éthique, déontologie, expertise, méthode, pragmatisme et investissement sont les valeurs clefs qui animent les soixante-quinze consultants, actuaires et experts métier d'OPTIMIND. Nos clients bénéficient ainsi d'une prestation de qualité associée à la signature d'une société de conseil reconnue.

OPTIMIND s'organise autour des métiers suivants :

- > Actuariat Conseil
- > Actuariat Entreprise
- > Projets & Maîtrise d'Ouvrage
- > Risk Management
- > Audit & Contrôle interne

Concepteur de valeur ajoutée
Actuariat, Risk Management,
Conformité & Projets

Optimind

46 rue La Boétie
75008 Paris
T / 01.48.01.91.66
F / 01.48.01.08.82

www.optimind.fr

