

RISQUES OPERATIONNELS DE LA CONFORMITÉ À LA PERFORMANCE



Thiébaud Viel

Associé fondateur
Horisis

Les établissements bancaires, pour appliquer la réglementation bâloise en matière de gestion du risque opérationnel, peuvent et doivent intégrer dans leurs modèles des méthodes issues du secteur industriel.



Patrice Grosjean

Consultant risques
Aedian
Consulting

Comment la mise en place d'un dispositif de management effectif des risques opérationnels peut être un véritable levier de performance pour l'entreprise? Après avoir mis en évidence le lien entre management des risques et performance, un parallèle avec le milieu industriel est possible ainsi qu'avec certaines approches déployées, en particulier pour la sûreté de ses procédés et la sécurité de ses personnels.

RISQUES OPÉRATIONNELS: GÉRER OU MANAGER?

Les sinistres que bien des industriels ont rencontrés ont souvent pris une dimension dramatique (Minamata, Three mile Island, Tokaimura, Ceveso, Bohpal, AZE, Tchernobyl). L'expérience qu'ils ont acquise en matière d'évaluation des risques peut être partagée avec les entreprises du secteur tertiaire.

Dans la banque les exemples sont tout aussi abondants : Sumimoto,

1995, 1,8 milliard de dollars, *rogue trading*; Orange County, 1994, 1,6 milliards de dollars, *rogue trading*; Metallgesellschaft, 1993, 1,3 milliard de dollars, dérivés climatiques; Barings, 1995, 1,2 milliard de dollars, Bank of America & FleetBoston Financial Corp, 2004, 675 millions de dollars, actionnaires lésés; pour ne parler que des cas plus célèbres. Au total, de 1980 à 2000, 200 milliards de dollars, de pertes ont été générés par le risque opérationnel dans le secteur bancaire. Le rapport entre les pertes liées au risque opérationnel et le PNB des banques atteint 3,5 %, en moyenne. Partant de ce constat, comment appréhender les risques opérationnels?

Le schéma 1 présente une matrice où sont positionnés les risques en fonction de leur nombre (fréquences, probabilité) et de leur impact (niveau de pertes). Il illustre tout à la fois le lien existant et la difficulté à actionner le levier management des risques pour bénéficier de gains de performance. En effet, dans les zones 1 (zone sanctuaire) et 2 (zone

de transfert) sont présents des risques qui peuvent menacer la pérennité de l'organisation. Leur couverture n'améliore pas significativement sa productivité. Dans la zone 3 (zone des risques courants), sont par contre présents des risques qui bien que d'impacts réduits n'en sont pas moins très présents. Leur fréquence d'apparition fait que ce sont ceux que l'on rencontre véritablement dans l'organisation. Ce sont donc aussi ceux dont le traitement effectif influence les résultats financiers.

Cette vision répond à une réalité concrète. De nombreux risques opérationnels recensés dans les bases de données des banques entrent dans cette catégorie. C'est le cas pour les catégories de risques bâloises telles que "Exécution, production et gestion des processus" (36 % des événements en nombre, et 20 % en montant de pertes) ou "Fraude externe" (42 % des événements en nombre, et 35 % en montant de pertes) (schéma 2).

Si la gestion des risques des zones 1 et 2 peut-elle être concentrée dans quelques petites équipes spécialisées (service assurances ou cellule PCA), en revanche le management des risques de la zone 3 exige l'implication de l'ensemble du personnel d'une ligne de métier, parfois disséminé dans de nombreux sites. Il sera donc plus aisé pour l'entreprise de gérer les premiers, quoique parfois fort coûteux, que de manager les seconds.

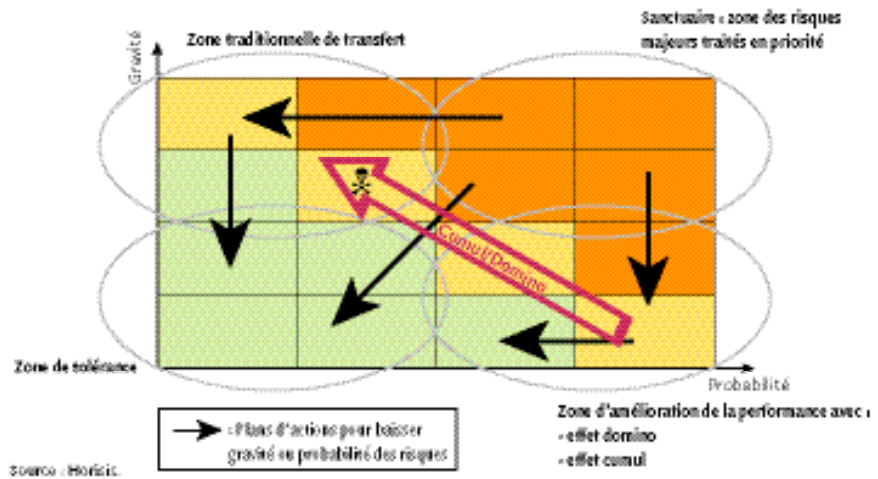
« Les industriels ont veillé à créer une culture du risque, former et informer les collaborateurs, définir des fonctions de gestion du risque. Les risques ne sont pas restés une affaire de spécialistes. »

L'APPROCHE INDUSTRIELLE : SYSTEME & MANAGEMENT

Fortement confrontées pour des raisons évidentes de sécurité du personnel et des populations à des exigences sans cesse croissantes de sûreté, les industries (énergie, chimie, industries lourdes) ou les transports (notamment transports publics) ont développé des approches de management des risques qui apportent aussi des éléments de réponse à des questions que se pose aujourd'hui le milieu bancaire :

- quel niveau de risque (notamment perte) doit être traité?
- à quel niveau de granularité s'arrêter?
- comment évaluer les risques, les mesures d'atténuation ou de maîtrise?
- quelle stratégie de gestion des risques adopter (activités, risques à privilégier, appétence aux risques, réponses à apporter)?

1. TYPOLOGIE DES RISQUES OPÉRATIONNELS



- quels chantiers mener en priorité?
- comment prendre en charges les nouveaux risques?

Au-delà de ces questions, fondamentales mais théoriques, les industriels ont veillé à créer une culture

du risque, former et informer les collaborateurs, définir des fonctions de gestion du risque. Les niveaux de ressources attribués à ces fonctions prennent explicitement en compte les problématiques de gestion du

1. MAÎTRISE DU RISQUE OPÉRATIONNEL

Exemple de déploiement

■ Les cartes bancaires

La sécurisation du processus "traitement" des Cartes Bleues est un exemple significatif de traitement du risque opérationnel. Ici le système d'information ne peut être incriminé. Il est plutôt dans la nature du support d'exposer les banques à des événements tels que vol, perte, falsification, contrefaçon, usurpation de numéro de carte, usage abusif. Le risk driver (facteur de risque) peut être le nombre de cartes émises, ou l'évolution du profil des porteurs. L'indicateur de risque peut être le montant unitaire des opérations ou le nombre d'opérations sur

une période donnée. L'événement de risque peut être une transaction frauduleuse. La perte brute est le montant de la transaction. La perte résiduelle est le montant non recouvré. La mesure d'atténuation du risque vise à réduire le risque – en termes de fréquence ou d'impact. Il peut s'agir de mettre en place un dispositif capable d'identifier en temps réel des comportements atypiques – relativement au profil du client et à l'analyse statistique de ses comportements. Ce dispositif conduit le système d'information à générer des alertes occasionnant le blocage de la carte en cause ou

une prise de contact avec le porteur (par texto ou par téléphone) afin de s'assurer de la validité de la transaction. Résultat : La mise en œuvre de telles solutions a pu permettre de réduire le niveau de perte de l'ordre de 60 % d'une année sur l'autre, tout en évitant de trop pénaliser les porteurs et les commerçants. Elles mettent en jeu à la fois l'organisation de la banque, le système d'information, les statistiques, le traitement des opérations, la gestion des risques, le commercial.

■ **Dans l'industrie :** projet de maîtrise du risque opérationnel sur le

processus de réapprovisionnement d'un magasin : Le projet a été mené en deux étapes :

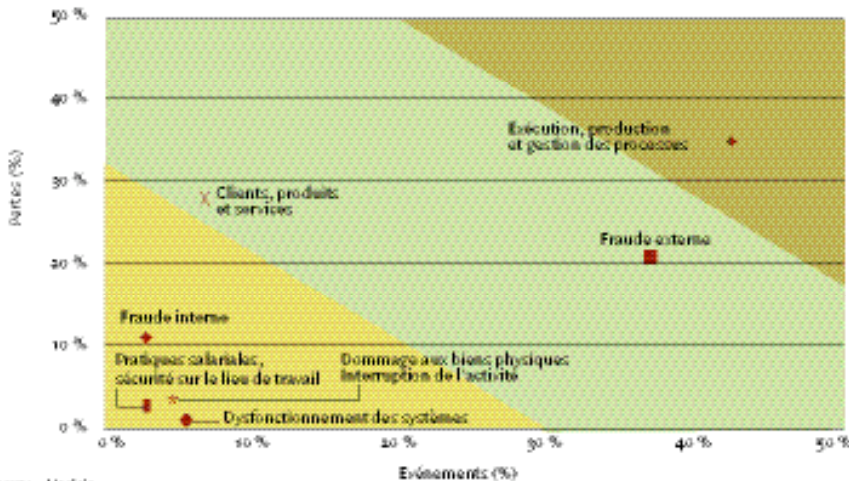
- Identification de 15 vulnérabilités majeures de l'organisation achat/ approvisionnement / stockage/ sortie du magasin, au nombre desquelles : non-maîtrise des procédures douanières, défauts de traçabilité des stocks, absence de contrôle sur les procédures de réapprovisionnement "urgent", mauvais transfert d'information entre acheteur et utilisateur, etc.
- Mise en œuvre d'un plan de conduite du changement :

- Analyse des pratiques externes
- reengineering du processus
- mécanismes de couverture contractuels et opérationnels des risques de rupture d'approvisionnement
- optimisation des niveaux de stocks
- formation des personnels
- déploiement

Résultat : le retour sur investissement de la démarche a été de 3,3 pour un, soit 2 millions d'euros d'économie en année pleine pour un coût de mise en œuvre ponctuel de 600 000 euros.

2. RÉPARTITION DES RISQUES OPÉRATIONNELS

Schéma inspiré des réponses apportées aux questionnaires soumis aux établissements bancaires dès 2001 par le comité de Bâle.



source : Heficis

risque opérationnel. Dans le secteur industriel, les risques ne sont pas restés une affaire de spécialistes. L'accidentologie du travail constitue une première approche de management des risques. Il s'agit de la "détection des situations dangereuses" ou DSD (schéma 3). Elle démonte les méca-

nismes qui font qu'une situation à risque dégénère en accident, et montre ainsi que les possibilités d'action sont multiples antérieurement à l'accident. Notons qu'un facteur 10 existe à chaque étape. Plus l'incident est identifié et traité en amont, plus on limite le risque d'accident. Au pire, on limite

les pertes matérielles et financières. En revanche, traiter toutes les situations à risque aboutit à des résultats non optimisés et coûteux.

L'approche qui prévaut alors repose sur deux leviers : système et management.

En partant du principe que le bon timing consiste à intervenir lorsqu'une situation à risque commence à devenir périlleuse, il faut pouvoir détecter la phase de transition. C'est le rôle du levier "système", c'est-à-dire le dispositif de gestion du risque opérationnel (facteurs, indicateurs, pilotage, reporting).

Pour que l'action soit efficace, il faut que le système soit piloté – par les risk managers, les responsables opérationnels et la direction de l'entreprise – et le personnel sensibilisé et formé. C'est le rôle du levier "management".

En pratique, cette approche, appliquée par exemple à la logistique, peut permettre d'optimiser un niveau de stock tampon en logistique, dont la fonction est de couvrir le risque de rupture des approvisionnements : doit-il être de 12 h, 24 h, de 48 h ? Dans le domaine des systèmes d'information, elle peut conduire à spécifier l'engagement de service : performance, perte de données acceptée, durée d'indisponibilité maximale. Concernant l'activité de gestion, elle amène à définir les stocks d'opérations à traiter, les délais de traitement, le volume des suspens, le taux d'erreurs acceptable, etc.

Dans chacun de ces exemples, le niveau d'exigence souhaité découle de la stratégie de l'entreprise et des objectifs qu'elle s'est fixés. Par la suite, le respect de ces objectifs dépend de la qualité du système et du management, de sa capacité à détecter, voire anticiper une rupture d'approvisionnement, une indisponibilité du système d'information ou un saut dans les stocks d'opérations à traiter et de sa réactivité.

2. TECHNOLOGIE

Des solutions informatiques pour la gouvernance, la maîtrise des risques, la conformité, est-ce possible ?



Daniel Delpuech

Directeur général
Keyword

■ De la même façon que les systèmes informatiques de gestion se sont progressivement intégrés en 20 ans, les systèmes informatiques de gestion des risques (SIGR) sont déjà en voie d'intégration (référentiels, cartographie, collecte, évaluation, statistiques modélisation, calcul des fonds propres, reporting...). Il est important pour celui qui cherche une solution

d'inscrire cette préoccupation dans son cahier des charges, sinon il sera confronté à un assemblage de solutions hétérogènes et globalement incompatibles. Aujourd'hui deux types d'outils tendent à converger : ■ Des outils connus du marché qui répondent traditionnellement à des problématiques associées au risque de marché ou au risque de crédit (traitement

statistique modélisation), de modélisation des processus ou de collecte des pertes. ■ Des outils internes (parfois bureautiques) construits en vue de cartographier les risques et de collecter les premières pertes. L'objectif est d'élaborer en interne ou avec l'aide d'éditeurs des outils permettant de répondre à l'ensemble des fonctionnalités attendues.

Opérationnellement et financièrement, l'impact peut être important. Dans l'approche Bâle II, la problématique est similaire : après la constitution de la base de données d'incidents, la collecte des événements et des pertes, la mise en œuvre d'outils de pilotage (permettant de suivre les facteurs et indicateurs de risques), la question qui vient est : quelles actions mener ? Quels impacts ces actions ont-elles, non seulement d'un point de vue réglementaire, mais également sur la performance globale de l'organisation ? La contribution première attendue est généralement la réduction des fonds propres nécessaires pour couvrir les risques, avec un objectif affiché de l'ordre de 2 à 4 %.

La mise en œuvre d'une démarche de management du risque opérationnel a également un impact positif sur l'ensemble des dysfonctionnements de l'organisation susceptibles de générer des pertes : sur le plan financier (allocations en fonds propres, notation auprès des agences, valorisation des actifs, capitalisation boursière), mais également en termes de qualité de service et de performance organisationnelle.

Cet impact est plus important encore, si l'on prend en compte les événements qui ne font pas partie des incidents déclarés au sens réglementaire, mais qui de par leur effet volume ont, malgré tout, un impact significatif sur le résultat opérationnel. Ces éléments doivent être pris en compte dans le calcul du retour sur investissement de tels projets.

ANALYSE ET CONDUITE DU CHANGEMENT

Cependant, le déploiement sur l'ensemble de l'organisation de dispositifs de grande ampleur serait lourd et mettrait en cause le retour sur investissement espéré. De plus, les ressources que l'entreprise est susceptible d'y consacrer restent limitées. Il convient de privilégier les chantiers les plus profitables et de procéder au préalable à une analyse des types de risques, des lignes d'activité, des entités ou des implantations sur lesquels il serait le plus pertinent d'intervenir, au regard de la stratégie et de l'appétence au risque de l'entreprise. Cette analyse cherche à quantifier le niveau de maturité de l'organisation (système et management) en matière de gestion des risques.

Gérer ou Manager ?

■ Gérer = Administrer

On gère les risques que l'on peut administrer, donc dont la couverture peut passer par un contrat (d'assurance, d'externalisation) ou relève de l'expertise technique d'une équipe dédiée (incendie, marché).

■ Manager = Diriger, Organiser

Il faut manager les risques dont la couverture demande des modifications de

comportement et de l'organisation : application généralisée de procédures et de contrôles. Cela passe par l'expression de ce que l'on veut, de ce que l'on ne veut pas et de ce que l'on ne veut plus, le respect et l'application des responsabilités et de la ligne hiérarchique. La plupart des risques de non-performance sont de cette nature.

« Dans l'industrie, sur les opérations de mise en œuvre du dispositif de gestion du risque opérationnel dans l'industrie, les bénéfices obtenus par rapport aux investissements sont de deux à trois pour un dans les douze mois qui suivent le projet. »

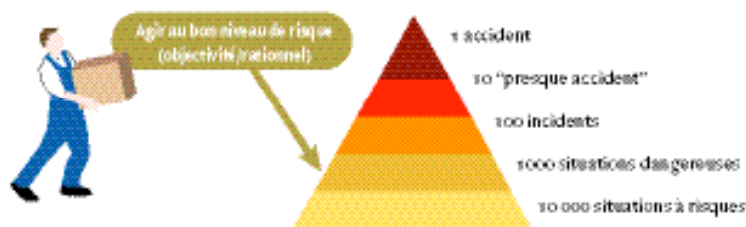
Cela conduit à évaluer les enjeux pour chacun des métiers inclus dans le périmètre de l'analyse (couverture en fonds propres ou tout autre retour sur investissement), identifier les meilleures pratiques internes et/ou en externes (benchmark) et à mesurer l'ampleur des améliorations à apporter. Cela passe par la conception d'un schéma cible d'organisation et l'élaboration d'un plan d'actions :

- principes d'organisation ;
- outils à déployer ;
- plan de mise en œuvre et processus de conduite du changement.

Le schéma cible défini est d'abord déployé sur un périmètre limité (entités pilotes), alliant à la fois une exposition significative au risque, une faisabilité acceptable et un retour sur investissement facilement identifiable, avant d'être généralisé. Ces dispositifs mis en place, les processus d'amélioration deviennent permanents et doivent être pérennisés. Quel est, au final, le retour sur investissement que l'on peut espérer de la mise en œuvre du dispositif de gestion du risque opérationnel ? Sur les opérations de cette nature menées dans l'industrie, les bénéfices obtenus par rapport aux investissements sont de deux à trois pour un dans les douze mois qui suivent le projet. Dans le secteur bancaire, les économies relativement aux pertes peuvent être de l'ordre de 60 %. En matière de qualité, des projets de type Six sigma conduisent à réaliser 50 % des gains espérés sous 6 mois. Ces chiffres confirment que management du risque opérationnel est autant synonyme d'opportunités de gains que de contrainte réglementaire. ■

3. ACCIDENTOLOGIE DU TRAVAIL

Maîtrise des risques = approche systématique au bon niveau



source : Moric.