GESTION DES RISQUES

Méthode à l'usage des *managers*

Fabrice Constantin

Intervenant
HEC et CNAM*

La gestion des risques interfère de plus en plus avec les autres domaines de responsabilités des *managers*. L'utilisation d'une méthode accessible à tous est utile aussi bien pour prendre les décisions appropriées que pour constituer un langage commun dans l'entreprise. Celle proposée trouve ses origines dans l'aéronautique et le nucléaire, mais a été adaptée par l'auteur au tertiaire.

La manière d'aborder les risques bancaires a évolué ces dernières années vers une approche plus globale, avec les règles Bâle II et la prise en compte des risques opérationnels, financiers ou de contreparties... En parallèle, les *managers* ou les responsables de projets ont besoin de se faire rapidement une idée des risques clés. Et si la mise en œuvre des règles est nécessaire, elle ne dispense pas pour autant d'un travail de réflexion transversal. Cet exposé propose une boîte à outils utilisable dans divers domaines par les *managers* non spécialistes du *risk management*. La méthode, qui repose principalement sur trois tableaux et quelques définitions, constitue un fil conducteur lors de l'analyse d'un dossier ou de la conduite de réunions.

LA PRISE EN COMPTE DES RISQUES

L'identification des types de risques constitue l'étape de départ : risques systémiques (système bancaire), risques contextuels (conjonction de certains facteurs), risques ponctuels (liés à une situation temporaire)... Dans les banques, les directions des risques ont en général réparti leurs domaines d'investigation selon une typologie assez détaillée. Revenons aux fondamentaux.

Un risque est une grandeur à deux dimensions. Il est caractérisé par sa gravité (G) et sa probabilité d'occurrence (P). La gestion des risques se ramène en fait à une recherche d'équilibre entre ces deux variables G et P (*tableau 1*). Plus la gravité d'un risque est élevée, plus on cherche à ce que sa probabilité d'occurrence soit faible. Réciproquement, on fait en sorte de limiter les conséquences des risques lorsqu'ils se produisent. Dans le domaine bancaire, Bâle II suit cette logique préventive. Mais il introduit également les notions de test et de *back testing* dans une optique de rétroaction.

Certaines situations favorisent l'apparition de risques et sont donc plus dangereuses que d'autres. On cherche à mettre en évidence ces phénomènes de concomitance à l'aide de tableaux croisés situations/risques. Parmi les perturbations qui peuvent favoriser la survenue d'un risque, se distinguent :

- les événements normaux, face auxquels le système doit être qualifié et fonctionner normalement ;
- les événements anormaux, peu fréquents, qui ne doivent pas affecter de manière significative l'activité, ni entraîner de pertes importantes ;
- les événements accidentels, qui ont une faible probabilité d'occurrence mais vis-à-vis desquels on admet des pertes.

LA MISE EN ŒUVRE DE BARRIÈRES FACE AU RISQUE

Les barrières s'opposent par définition aux événements susceptibles d'aboutir à des risques (*tableau 2*), qu'elles soient immatérielles (procédures, consignes, affichages, documentation, encadrement) ou matérielles (informatiques, physiques, passives, actives...). Selon les cas, elles ont un rôle de prévention ou de protection, d'insensibilisation aux perturbations, de détection d'ano-

*Consultant en organisation et en sécurité systémique, avant d'entrer au Crédit Agricole.

TABLEAU 1

Grille des objectifs généraux de sécurité

Probabilité (P) / Gravité (G)	Peu fréquent	Rare	Extrêmement rare	Extrêmement improbable
Mineure	*	concevable	concevable	concevable
Significative	interdit	**	concevable	concevable
Critique	interdit	interdit	***	concevable
Majeure	interdit	interdit	interdit	****

Les objectifs de sécurité se trouvent sur la diagonale principale : les mesures prises pour gérer le risque sont optimisées par rapport à sa probabilité.
La partie située au-dessus de cette diagonale correspond à une "sur-sécurisation" des risques.
La partie située en dessous de cette diagonale correspond à une "sous-sécurisation".

malies et parfois même de correction automatique. Le recensement des barrières et l'évaluation de leur poids face à un risque font l'objet d'une recherche appelée "démonstration de la sécurité" (*tableau 3*).
Ainsi, une procédure de sécurité, dans la mesure où elle a été formalisée et qualifiée, constitue une barrière immatérielle à condition que le personnel ait été formé, que des contrôles soient en place, puis qu'une actualisation des documents et des connaissances soit opérationnelle. Une telle barrière est de toute façon beaucoup moins fiable qu'une barrière informatique car le niveau de stress, la motivation ou les intentions vont directement influer sur les comportements. De plus, des mesures ont montré qu'après une émotion, la probabilité pour qu'un opérateur fasse une erreur pouvait passer de 1/100, référence normale, à 1/10, voire ½. Il y a dans ce cas des mécanismes de régression temporaire. Tout ceci justifie les contrôles redondants.
Lorsque plusieurs barrières se trouvent sur le même chemin d'un risque, leurs effets se cumulent à condition qu'elles soient indépendantes, voire de nature différente. Par exemple, pour fiabiliser une procédure manuelle, on peut rajouter une barrière matérielle ou logicielle. Dans le cas où plusieurs chemins peuvent aboutir à un risque, c'est le maillon faible qui impose sa loi, c'est-à-dire celui dont la probabilité d'occurrence est la plus élevée.

« L'objectif est de mettre en œuvre des barrières indépendantes les unes des autres face au risque. »

LES DÉPENDANCES ENTRE BARRIÈRES

Par ailleurs, l'impact des phénomènes de dépendance entre barrières est régulièrement sous-estimé. Ces dépendances peuvent être de natures diverses.
Le lieu ou l'implantation géographique : les relations de liaisons possibles sont mises en évidence par une "analyse des zones", tel qu'un incendie détruisant des sauvegardes stockées en un lieu unique.
Le fonctionnel : il s'agit de défaillances en modes communs, issues d'une même chaîne fonctionnelle. Ce serait le cas d'un programme informatique regroupant plusieurs sécurités, et modifié par le même opérateur, si celui-ci n'était pas contrôlé à son tour une fois son travail terminé.
Les événements indésirables ou incidents qui sont susceptibles d'affecter simultanément plusieurs organes.
Les relations entre des entités (information, environnement, etc.).

L'ÉVALUATION GLOBALE DE LA SÉCURITÉ

On est ici au cœur du sujet et on parle de "démonstration de la sécurité". Celle-ci peut se faire à l'aide d'une matrice à trois dimensions : l'événement inducteur du risque, le risque lui-même et les barrières qui lui font face (*tableau 3*). Cet outil, qui aboutit à un bilan et des recommandations, est assez facile à utiliser. Le principe est simple : face à chaque risque, il s'agit de comptabiliser le niveau de sécurité obtenu et de mettre en évidence les maillons faibles.

EXEMPLES

Application de la méthode

Dans le domaine bancaire, la méthode peut être appliquée pour évaluer puis améliorer la sécurité de processus.
Un processus bancaire type comporte en général des séquences avec des procédures manuelles, des échanges d'information, des traitements informatiques, des résultats. Face à un risque de fraude interne, on va rencontrer des barrières immatérielles (consignes ; efficacité *), des sécurités logicielles (codes confidentiels et contrôles automatiques ; efficacité ** à ***), des sécurités physiques (portes d'accès, alarmes ; efficacité **).
Si on construit l'arbre généalogique du risque en faisant apparaître tous les types de combinaisons possibles (chemins) et en précisant les situations (travaux préparatoires, prises de décision, traitement des opérations, *reporting*, contrôles...), un premier constat important peut être établi :
toutes les barrières ne sont pas disposées sur les mêmes chemins ;
dans certaines situations, et en fonction des circonstances, certaines barrières sont inopérantes si elles ont été levées dans des séquences antérieures ;
le cumul de barrières peut aboutir sur une somme de * insuffisante par rapport au risque considéré.
En utilisant le *tableau 3*, des points névralgiques vont donc apparaître, ce qui va donner lieu à des rééquilibrages.
Si, dans une situation donnée, toute la sécurité reposait sur une seule barrière, il serait nécessaire de considérer que la défaillance de cette barrière constituerait un risque à analyser, et il faudrait appliquer la méthode de manière itérative.
Ce serait notamment utile pour renforcer les mesures préventives et de détection, si les barrières logicielles ou matérielles pouvaient être neutralisées par une personne (efficacité réelle réduite à * ou nulle, au lieu de ** ou *** attendues).

L'estimation de la sécurité obtenue grâce aux dispositions initialement prévues est comparée à l'objectif de sécurité de manière à identifier les points faibles et à les localiser. En fonction du résultat, on rajoutera des barrières, en précisant au passage si elles ont un rôle de prévention, de protection, de détection, ou de correction de manière à les répartir de manière équilibrée sur le chemin d'un risque.

RÉDUIRE LES ÉCARTS DE TRAJECTOIRE

En situation de changement ou en environnement interculturel, la méthode peut être étendue aux risques relatifs à la gouvernance d'une entité ou

TABLEAU 2

Évaluation des objectifs de sécurité

Gravité d'un risque	Objectifs de sécurité	Échelle de valeur de l'efficacité d'une barrière
(dommage potentiel)	(atteindre le niveau de sécurité requis par le jeu du "poids" et/ou du cumul de barrières indépendantes)	
MINEURE : dysfonctionnement n'affectant pas la mission de l'organisme	* - 1 barrière d'efficacité *	* procédure manuelle (ou automatisée mais dépendante d'une action manuelle)
SIGNIFICATIVE : dysfonctionnement gênant le déroulement de la mission de l'organisme, mais ayant des conséquences directes ou indirectes limitées	** - 1 barrière d'efficacité ** (mécanique ou automatisée et protégée vis-à-vis d'actions malencontreuses) ou - 2 barrières d'efficacité* et indépendantes	** barrière automatisée et protégée vis-à-vis d'une action humaine ou barrière automatisée et protégée physiquement ou barrière mécanique
CRITIQUE : événement indésirable pouvant se traduire soit par des pertes financières directes ou indirectes importantes, soit par des dommages corporels, soit par des sanctions graves	*** - 1 barrière d'efficacité *** ou - 2 barrières d'efficacité * et ** indépendantes ou - 3 barrières d'efficacité * indépendantes	*** barrière entièrement automatisée et totalement protégée vis-à-vis d'actions extérieures. Ce type de barrière multifonctions est capable de prévenir, de détecter des anomalies et éventuellement d'en assurer la correction avec information des personnes habilitées. Ensemble modulaire
MAJEURE : événement indésirable se traduisant par des pertes financières directes ou indirectes (image commerciale, manque à gagner, pertes d'exploitations, dommages corporels) très importantes. La pérennité de l'organisme pourrait être mise en péril.	**** - 2 barrières d'efficacité ** indépendantes ou * et *** ou ** et * et * ou * et * et * et *	**** il n'y a pas de barrières de sécurité uniques d'efficacité ****. Ce niveau ne peut en général être atteint que par un cumul de barrières indépendantes de niveau inférieur.

Les * sont utilisés à la fois pour représenter :
- la gravité du risque : * pour un risque mineur ; ** pour un risque significatif, etc.
- l'efficacité des barrières placées face aux risques : * pour une efficacité faible, ** pour une efficacité moyenne…

- les * étant des probabilités d'occurrence inférieures à 1, elles correspondent dans les modèles à des puissances négatives de 10.

La logique provient des opérateurs exponentiels, ce qui explique les résultats d'addition et de multiplication :

dans le cas où plusieurs chemins aboutissent à un risque, la probabilité la plus forte d'occurrence est retenue : ** + *** = **
Une barrière d'efficacité * couplée avec une barrière d'efficacité ** permet d'obtenir un niveau de sécurité ***.

TABLEAU 3

Évaluation de la sécurité : matrice (événement inducteur de risque / risque / barrière)

Événement inducteur de risque (perturbation, contrainte)	Risque induit	Gravité	Objectif de sécurité	Recensement des barrières prévues	Prévention	Rôles Détection	Correction	Barrières supplémentaires recommandées pour atteindre l'objectif 4*
E1	R1	Majeure	****	B1 (*)				B2 (**)
								B3 (*)

Les événements inducteurs de risques peuvent être de toute nature (organisationnels, humains, informatiques, électriques, incendies, climatiques, etc.) et d'origine interne ou externe à l'organisme étudié.

Ils sont à prendre en compte dès les phases de conception, au niveau du cahier des charges. Comme pour les situations, on élaborera des matrices événements/risques Ei.Rj permettant

d'identifier les relations de cause à effet.
On procédera ensuite au recensement des barrières s'opposant à l'action de chaque événement.

d'une activité. Imaginer le changement revient d'abord à imaginer une nouvelle trajectoire pour l'entreprise, puis ensuite à la suivre pour réduire les écarts. En faisant la comparaison avec un objet en mouvement, il est naturel de s'intéresser à la "pilotabilité" de l'entreprise, à sa manœuvrabilité, puis à sa sensibilité aux différentes perturbations possibles. Utiliser notre méthode revient dans ce cas à mettre en place des indicateurs d'alerte et des barrières face aux différentes sources de perturbation.
Par exemple dans le cas d'une acquisition ou d'une fusion, s'interroger sur la "pilotabilité" de la nouvelle structure reviendrait à examiner à la fois la possibilité de trouver un pilote qualifié pour la situation, mais aussi la pertinence du tableau de bord et la qualité de tout le dispositif opérationnel qui permettrait ce pilotage de manière réactive...

« La méthode peut être étendue aux risques relatifs à la gouvernance d'une entité ou d'une activité. »

En ce qui concerne la manœuvrabilité, celle-ci peut se définir de la manière suivante : la capacité d'une structure à mettre en œuvre de manière opérationnelle les changements décidés, dans des conditions d'efficacité, de délais et de coûts, face à un environnement donné. Qu'est-ce qui pourrait limiter la manœuvrabilité ? Différents facteurs : culturels, référentiels ou interprétations divergents, organes de *management* et de transmission, climat social et conflits, spécificités de la réglementation locale, état de l'appareil de production, effets de taille...

UN DOMAINE PROCHE DES SCIENCES HUMAINES

Tous ces points sont sujets à des investigations et ouvrent de nouvelles perspectives à la gestion des risques en environnement incertain, laquelle boucle alors sur des questions de communication, de management, de prise de décision et de gouvernance.
Dans ce domaine proche des sciences humaines, la méthode peut également permettre de clarifier les actions et fiabiliser l'organisation grâce au recours systématique à des critères objectifs. ■