EN DEUX MOTS **Responsables de la conformité, des contrôles permanents, de la sécurité des systèmes d'information, de la sécurité économique, des risques opérationnels... comment organiser ce foisonnement de fonctions ? Dominique Garabiol, du groupe Caisse d'Épargne, puis Pierre Sarton du Jonchay, de la Caisse d'Épargne du Pays du Hainaut, répondent à cette question.**

ORGANISATION

Harmoniser contrôle permanent, conformité et risques opérationnels

Dominique Garabiol

Directeur
de la déontologie
et de la conformité
Groupe Caisse d'Épargne

Une structuration des dispositifs de maîtrise des risques pourrait reposer sur la distinction entre risques bancaires et financiers, matière première des activités génératrices de produit net bancaire d'une part, et risques opérationnels communs à toutes les entreprises industrielles et commerciales.

La dernière modification du règlement CRBF n° 97-02 a surtout frappé par l'introduction de la fonction conformité parmi l'arsenal de maîtrise des risques exigé par le régulateur. Mais cette modification introduit aussi la notion de responsabilité des contrôles permanents, dissociée de celle des contrôles périodiques. Destinée à éviter les conflits d'intérêts, elle n'a guère fait débat. Elle fait pourtant, elle aussi, l'objet d'interrogations sur sa nature même. Sans doute faudra-t-il faire preuve de patience pour mesurer l'impact réel de ces nouvelles obligations, d'autant plus qu'elles s'ajoutent aux avancées du Comité de Bâle sur les risques opérationnels. La matière permet quand même d'anticiper un certain nombre d'évolutions structurelles possibles.

L'INTERDÉPENDANCE DES RISQUES OPÉRATIONNELS

Le dictionnaire de l'Académie française propose deux synonymes à "contrôle" : "maîtrise" et "vérification". Le contrôle permanent renvoie aux dispositifs de maîtrise des risques, ce qui suppose une immersion dans l'opérationnalité. La vérification nécessite une approche extérieure à l'opérationnalité : c'est le contrôle périodique.

La fonction conformité s'insère dans les contrôles permanents. Sa proximité avec la gestion des modes opératoires permet de la distinguer de la fonction juridique. Tandis que cette dernière est par nature normative et participe directement au support opérationnel, la fonction conformité s'attache à la pertinence des procédures. Elle veille à la transcription des règles professionnelles dans les procédures opérationnelles et aux contrôles qui accompagnent le traitement des opérations [1].

Parallèlement, le contrôle permanent concerne tous les risques : le risque de non-conformité, bien sûr, mais aussi les risques bancaires et financiers, les risques juridiques et comptables, les risques sur les systèmes d'information, les risques opérationnels... Une énumération qui est le fruit des prises de conscience successives de la profession et des régulateurs.

Il en découle une organisation en râteau, à la gestion délicate, des dispositifs de maîtrise de ces risques. Cette situation ne paraît pas stable car elle s'accommode d'un risque opérationnel pesant sur la fiabilité même du contrôle interne.

Cette organisation se heurte, en premier lieu, aux interférences étroites des risques opérationnels les uns avec les autres. La conformité en est un bon exemple. D'abord si la fonction conformité est distincte de la fonction juridique, le risque de non-conformité est bien *in fine* un risque

> *« Pas moins de trois unités devraient intervenir pour la maîtrise d'un risque opérationnel : l'unité spécialisée, la conformité et les risques Bâle II. »*

ORGANISATION

Deux pôles de contrôle permanent

Risques bancaires et financiers	Risques d'entreprise
• Crédit	• Risques opérationnels - Bâle II
• Marché	• Conformité professionnelle
• Taux d'intérêt global	• Sécurité des systèmes d'information
• Liquidité - Transformation	• Sécurité économique - Fraude
• Règlement-Livraison	• Sécurité physique
• Interdermédiation	• Juridique
	• Comptabilité - Information financière
	• Fiscalité
	• Ressources humaines

juridique. Ensuite, les différentes catégories de risques opérationnels étant encadrées réglementairement, elles relèvent aussi la fonction conformité. Environ la moitié des risques opérationnels répertoriés dans les cartographies sont précisément des risques de non-conformité. Un quart additionnel peut provenir de défaillances de conformité ou avoir un impact en termes de conformité [2]. *Last but not least*, le contrôle permanent répondant lui-même à des exigences réglementaires, il paraît inclus dans le champ de la conformité alors qu'il l'englobe fonctionnellement. Idem pour les risques opérationnels.

En second lieu, la définition bâloise des risques opérationnels fait précisément naître des redondances. Les risques opérationnels définis par le comité de Bâle s'articulent autour de quatre grands thèmes : les défaillances humaines ou de procédures, la fraude et la sécurité, les systèmes d'information, le juridique qui comprend pour l'occasion la conformité. La maîtrise de ces risques est assurée par des unités spécialisées. Ces dernières ont la responsabilité des dispositifs de maîtrise "opérationnelle" de ces risques selon la logique de règlement CRBF n° 97-02. De tels dispositifs sont inconcevables sans une bonne compréhension des risques, ce qui suppose leur identification et leur mesure préalables.

Mais une unité est aussi en charge des risques opérationnels au sens du comité de Bâle, en superposition. Cette dernière identifie elle aussi les risques opérationnels au moyen de cartographies et les mesure dans le cadre de Bâle II. D'où une adjonction de cartographies à l'intérêt incertain ou plus encore un risque de dilution des responsabilités.

En fin de compte, pas moins de trois unités devraient intervenir pour la maîtrise d'un risque opérationnel : l'unité spécialisée, la conformité et les risques Bâle II. Les risques opérationnels apparaissent bien comme un tout indissociable.

QUALITÉ ET RISQUES OPÉRATIONNELS D'ENTREPRISE

Une organisation selon la typologie des risques serait ainsi une source de déperdition de ressources et de faiblesse du dispositif de contrôle interne. Un comité de contrôle interne rassemblant tous ces acteurs et appelé à être animé par un responsable des contrôles permanents, peut tenter de canaliser les risques de redondance, d'incohérence ou d'absence de complétude les plus criants du dispositif. Mais il ne peut pas effacer les effets d'une organisation en râteau avec la parcellisation des responsabilités qu'elle implique et les risques qu'elle génère. Une structuration des dispositifs de maîtrise des risques pourrait reposer sur la distinction entre risques bancaires et financiers d'une part, et risques opérationnels d'entreprise, d'autre part. S'agissant de la gouvernance, le gouverneur de la Banque de France insistait récemment sur les spécificités des entreprises que sont les banques [3]. Elles n'en sont pas moins des entreprises. C'est aussi vrai en matière de risques.

Les risques bancaires et financiers sont la matière première des activités génératrices de produit net bancaire. Ils participent aux spécificités de ce secteur. Ils sont au cœur des métiers. Leur exercice n'est pas concevable sans appétence pour ces risques. Le dispositif de maîtrise des risques n'est pas destiné à les éliminer mais à s'assurer de leur bonne compréhension, à borner cette appétence et à la structurer au travers de politiques d'allocation de fonds propres.

Les risques opérationnels sont des risques communs à toutes les entreprises industrielles et commerciales. Ils ne sont pas producteurs de chiffre d'affaires. Ils sont subis. L'appétence pour ces risques est nulle. Seul le calcul économique de la rentabilité de leur prévention en limite l'aversion. Le dispositif de maîtrise de ces risques vise à les éliminer. L'objectif est le zéro défaut et s'insère dans les perspectives de politiques qualité.

Les directions qualité et risques des entreprises industrielles et commerciales pourraient servir d'ai-

[1] Vivien Levy-Garboua, "De nouveau défi à relever", Revue Banque n° 671, juil.-août 2005.
[2] Le quart restant a trait aux domaines finalement écartés de la conformité "professionnelle" par le régulateur : droit du travail, droit fiscal…
[3] Christian Noyer, "Corporate governance et banque : les banques se gouvernent-elles comme d'autres entreprises", séminaire de la Cour de cassation, 10 octobre 2005.

« La distinction des deux univers de risques, les risques spécifiques au secteur et les risques communs à toutes les entreprises, permettrait de fiabiliser le dispositif de contrôle permanent. »

guillon à la structuration en deux pôles risques cohérents au sein du secteur bancaire (*encadré*).

DEUX UNIVERS DE RISQUES

Il s'agit bien de deux univers de risques. Sur le plan qualitatif, les dispositifs de maîtrise des risques bancaires et financiers reposent sur des prescriptions professionnelles spécifiques au secteur et auxquelles les régulateurs contribuent substantiellement. Pour les risques opérationnels d'entreprise, les références qui inspirent les professionnels ou les régulateurs découlent des processus de certification qui relèvent d'une normalisation commune.

Sur le plan quantitatif, cette différence est aussi notable. Sous l'hypothèse, audacieuse il est vrai, d'une distribution gaussienne des pertes, le seuil admis pour les risques bancaires et financiers est de 3 écarts type. Ceci correspond à l'anticipation d'une occurrence de risque d'environ une fois sur 1 000. Pour les risques opérationnels, le seuil de référence commun est de 6 écarts type, correspondant à une occurrence du risque d'une fois sur 300 000 environ. L'aversion aux risques opérationnels est 300 fois supérieure à l'aversion aux risques bancaires et financiers.

La distinction des deux univers de risques, les risques spécifiques au secteur et les risques communs à toutes les entreprises, permettrait de faire jouer les synergies de compétences et de fiabiliser le dispositif de contrôle permanent. Le règlement CRBF n° 97-02 offre une flexibilité qui préserve cette voie. Ses prescriptions en matière d'organisation permettent, en effet, la désignation de plusieurs responsables des contrôles permanents dont les attributions respectives restent à la discrétion des établissements.

RISQUES OPÉRATIONNELS ET CONFORMITÉ
Tirer parti des réformes réglementaires

Pierre Sarton du Jonchay

Directeur des contrôles permanents
Caisse d'Épargne des Pays du Hainaut

Les contrôles permanents des risques opérationnels et ceux de la conformité se rejoignent par leur approche méthodologique et par leurs effets sur l'organisation interne des banques.

Les dernières modifications réglementaires sur la couverture des risques opérationnels par les fonds propres ou sur l'instauration d'une fonction de conformité et de supervision des contrôles permanents constituent des réformes dont la mise en œuvre est lourde. Il est certain qu'elles vont entraîner une profonde évolution conduite par les établissements qui auront su adapter leur organisation pour en tirer le meilleur parti.

CONVERGENCE MÉTHODOLOGIQUE

Les régulateurs ont pris acte que les risques ont tout autant pour origine les contrats de crédit ou d'opérations financières effectivement négociés que la logistique organisationnelle et opérationnelle nécessaire à leur gestion. L'introduction d'un volet "risques opérationnels" dans Bâle II et des volets "risques de conformité" et "contrôle permanent" dans le règlement CRBF n° 97-02 en témoigne. Leur juxtaposition fait apparaître des convergences méthodologiques porteuses de synergies.

L'appréciation quantitative des risques opérationnels conduit à une problématique nouvelle de définition et de délimitation de ce que l'on mesure. Une organisation, des règles ou une articulation d'étapes et de moyens sont beaucoup plus abstraites qu'un contrat, une somme d'argent ou un prix. Elles ne sont pas en elles-mêmes spécifiées par des quantités. À la différence des risques de marché ou de crédit, la mesure des risques opérationnels passe par une étape supplémentaire d'identification de spécifications quantifiables des phénomènes à risque.

Il s'agit de compter des "incidents" et de leur attribuer des coûts, effectifs ou potentiels. Il faut définir des incidents non par rapport à des opérations, mais par rapport aux moyens de toute nature nécessaires à leur réalisation ; il faut également que la survenance de ces incidents ne résulte pas d'opérations précises individualisables, mais des processus qui conduisent à leur réalisation.

L'identification des processus débouchant sur la conclusion des opérations est un préalable incontournable à la gestion quantitative du risque opérationnel. Cette même description est aussi un but et un moyen des fonctions de conformité et de coordination des contrôles permanents.

Le contrôle permanent est une démarche de management visant à réduire les risques de toutes natures. Le bon manager contrôle pour garantir la réalisation de ses objectifs. Le régulateur instaure l'obligation du contrôle permanent pour minimiser la probabilité que la rentabilité effective des opérations ne s'écarte trop de leur rentabilité attendue. Le contrôle n'est plus seulement une obligation fonctionnelle, mais devient dans le nouveau règlement une obligation organique.

La spécification dans l'organigramme des acteurs dédiés au contrôle accentue la question de leur dimensionnement et de leur positionnement. L'explicitation du coût de contrôle rend nécessaire celle de son rendement. Les coordinateurs du contrôle permanent ne peuvent plus raisonner sans localiser les contrôles dans les processus et sans valoriser, même approximativement, des incidents minimisés ou évités.

REPÈRES

Des concepts communs dans toutes les politiques de risques et de contrôle

Risque	Tout élément du processus de création de valeur dont la contribution au résultat économique est incertaine.
Structure	Elément de l'organigramme disposant d'une autonomie décisionnelle et d'action ; centre de responsabilité à qui est confiée la gestion d'un ou plusieurs risques.
Activité	Ensemble de tâches ayant la même finalité, concourant à la maîtrise d'un même risque, avec les mêmes outils.
Tâche	Ensemble d'actions concrètes visant un objectif unique : décision opérationnelle, analyse de risque, traitement d'informations…
Procédure	Formalisation d'un enchaînement d'activités ou de tâches visant des objectifs communs. La procédure décrit le contexte et les moyens de cet enchaînement.
Contrôle	Action associée à une tâche visant à identifier une défaillance, à en mesurer sa probabilité d'occurrence ou de perte afin d'en limiter les effets.

Parallèlement, la fonction conformité nécessite aussi la description des processus pour structurer le contrôle. La fonction conformité vise, préalablement à toute opération, à garantir la conformité à la réglementation et aux bonnes pratiques. Il convient d'identifier les produits, les clients, les outils, les étapes techniques, les responsabilités internes successivement engagées. Chacune de ces dimensions qualifie le risque de non-conformité et détermine la cible des contrôles à réaliser.

UN MANAGEMENT PAR LES PROCESSUS

L'obligation réglementaire de formalisation et de documentation des dispositifs de gestion et de contrôle conforte la nécessité d'un management par les processus. Il n'est plus simplement question de produire des manuels spécialisés pour chacun des acteurs de l'entreprise. La démonstration doit être donnée en permanence de la cohérence d'ensemble de l'organisation. Or, ce qui permet d'établir un lien entre la mesure d'un risque, un contrôle, une norme, un contrat, une écriture comptable, une déclaration réglementaire, une donnée informatique et un dispositif de sécurité physique, ce sont bien les étapes et les résultats d'un processus.

« La démultiplication réglementaire des fonctions dédiées au contrôle et au management des risques suscite une inflation des effectifs et des coûts. »

Les derniers développements réglementaires posent ainsi le défi d'un langage commun à toutes les fonctions de la banque. Les concepts du risque et du contrôle doivent rester univoques et recouvrir toutes les disciplines. Ils doivent être intuitifs afin de parler à tous les métiers. Au-delà des mots employés, qui sont adaptables selon les cultures d'entreprise, les mêmes concepts se retrouvent dans toutes les politiques de risque et de contrôle (*encadré*).

LE PILOTAGE DES DIFFÉRENTES FONCTIONS

La définition des concepts de la maîtrise des risques et du contrôle débouche sur une attribution des responsabilités fonctionnelles. Chaque fonction utilise l'ensemble des concepts, mais s'organise et se spé-

cifie sur l'un d'entre eux selon des termes largement issus du règlement CRBF n° 97-02. La formalisation des concepts crée un espace de coordination nécessaire entre les fonctions risques, conformité et contrôle permanent.

La fonction risques renvoie à l'identification et la mesure des risques. Elle détermine des limites d'exposition adaptées aux allocations de fonds propres. Elle catégorise les risques, répertorie et définie les défaillances. Elle délimite et renseigne les paramètres de segmentation risques, puis les attribue à des activités. Enfin, elle évalue la contribution de chaque élément de l'environnement de gestion à la maîtrise du risque.

La fonction conformité est responsable de la traduction en normes intégrées aux processus internes des obligations et de leur contrôle. L'application des procédures doit minimiser le risque de mise en cause de la responsabilité de l'établissement. À partir des règles et bonnes pratiques, la fonction conformité répertorie et renseigne les normes professionnelles puis les relie aux activités auxquelles elles s'appliquent. Elle identifie, en coordination avec les risques, les principales défaillances qui peuvent surgir de l'application de la norme et détermine les contrôles nécessaires au niveau opérationnel et fonctionnel.

La fonction contrôle permanent veille à ce que le dispositif de contrôle couvre tous les risques et que chaque risque s'inscrive dans une chaîne de gestion et de responsabilités dotée de moyens appropriés. La coordination des contrôles permanents permet de rapprocher ces contrôles des défaillances visées. Elle permet aussi de vérifier que l'activité génératrice du contrôle est bien en relation avec l'activité soumise à la défaillance.

La complémentarité des contrôles suppose l'adoption d'un référentiel commun. L'attribution des activités aux structures décisionnelles de l'entreprise passe par une modélisation par une fonction "organisation et méthodes". Cette modélisation gagnerait à être validée par l'organe dirigeant sur avis des fonctions risques, conformité et contrôle permanent. Le contrôle périodique aurait, entre autres, à vérifier la sincérité et l'exhaustivité de la modélisation et sa bonne interprétation par le management.

La démultiplication réglementaire des fonctions dédiées au contrôle et au management des risques suscite une inflation des effectifs et des coûts. Ce surcoût se justifie par la conduite du changement dans une organisation en mode projet. Il devra en sortir de nouveaux modes de fonctionnement dans un cadre restructuré sur une nouvelle allocation des compétences et des responsabilités. Au final, il faudra produire plus et mieux avec autant ou moins de personnes.

Une telle avancée est impossible sans une refonte des systèmes d'information où le pilotage et la gestion s'intègrent à la production. Les données de pilotage et de gestion doivent être traitées avec la même attention que les données de production sur une infrastructure informatique urbanisée. Si la technique le permet de plus en plus, il faut que les hommes suivent. Ils doivent partager les informations et assumer leurs responsabilités en tenant compte des contraintes qui peuvent s'imposer aux autres. ■

« À la différence des risques de marché ou de crédit, la mesure des risques opérationnels passe par une étape supplémentaire d'identification de spécifications quantifiables des phénomènes à risque. »