RISK MANAGEMENT

Directive européenne antiblanchiment : vers une culture de vigilance

Alors que le France a été rappelée à l'ordre en juin pour la seconde fois en raison de son retard, la troisième directive antiblanchiment sera transposée par ordonnance. L'approche fondée sur l'analyse des risques qu'introduit cette directive implique le renforcement de la culture de vigilance dans la conception et le suivi de nouveaux dispositifs.

Emmanuel Saillard
Senior Consultant

Stéphane Germain
Consultant Manager
VBF Consulting

Le rôle des banques dans la lutte antiblanchiment et contre le financement du terrorisme (LAB/CFT) a longtemps fait débat. Elles collaborent avec la justice, mais sont mises en cause, comme les fraudeurs, sciemment à l'origine des opérations. La complexité de cette mission a déjà été démontrée en France par l'affaire du Sentier qui a incriminé le système de gestion des chèques. À ce sujet, Daniel Bouton déclarait, en juin dernier devant le tribunal correctionnel de Paris, qu'il était "idiot" et inefficace de contrôler systématiquement les milliards de chèques passant chaque année par les guichets, plaidant pour un contrôle par sondage lorsqu'un événement anormal était détecté dans la vie d'un compte.

La troisième directive européenne, adoptée en 2005 (2005/60/CE), répond à cette inquiétude de la profession en préconisant une approche basée sur l'évaluation des risques. L'amendement 517, visant à habiliter le gouvernement à la transposer par ordonnance, a été adopté le 11 juin 2008 à l'Assemblée nationale. Les banques, traditionnelles "acheteuses de risques", vont devoir encore plus mobiliser leurs compétences. Cette réforme de fond – qui s'inscrit dans l'esprit de Bâle II – amène en effet à concevoir et mettre en œuvre des dispositifs adaptés à chaque établissement, plutôt qu'à appliquer des méthodes uniformes.

UNE DÉMARCHE MÉTIER

L'impact sur les organisations et les systèmes s'annonce particulièrement fort. En complément de la nouvelle approche, les régulateurs nationaux ont énoncé des recommandations générales pour les banques, qui doivent déployer des systèmes transverses capables de relever les alertes, et de stocker les informations pertinentes pour décider.

> *« Les synergies entre démarches KYC (know your client) et activité commerciale doivent être explorées pour que les investissements trouvent un intérêt métier. C'est la meilleure garantie que le dispositif reste opérationnel jour après jour. »*

Pour les banques de détail qui brassent des masses considérables d'opérations industrialisées, sur des produits banalisés et avec une clientèle souvent locale, le *monitoring* des transactions permet de profiler des comportements types pour déceler les opérations anormales. Toutes les synergies entre démarches KYC (*know your client*) et activité commerciale doivent être explorées pour que les investissements trouvent un intérêt vis-à-vis du métier. L'analyse comportementale, fondée sur les études statistiques et l'intelligence artificielle, trouve tout son sens si elle est ainsi mutualisée avec le CRM. C'est la meilleure garantie pour que le dispositif reste opérationnel jour après jour. Les outils doivent aussi être étalonnés en permanence pour s'adapter aux évolutions réglementaires, aux nouveaux produits, aux habitudes des clients et au contexte international. Surtout, leur effica-

cité dépend de leur mise en commun sur l'ensemble du périmètre d'activité de l'établissement.
Pour les banques de financement et d'investissement, le problème est sensiblement différent dans la mesure où les transactions peuvent être financièrement et juridiquement complexes, impliquer de multiples acteurs – potentiellement étrangers – et restent spécifiques.
L'analyse doit donc être guidée par des filtres sur des critères croisés d'attention tels que les montants ou les natures de transaction. Le défi majeur réside dans la capacité à faire le lien entre les informations et à leur donner sens. Les outils, figure imposée par les régulateurs, doivent faciliter l'identification des cas qui nécessitent une attention particulière et le recours aux ressources compétentes. L'écueil majeur consisterait à utiliser les avancées technologiques uniquement pour collecter et entreposer des quantités de données croissantes, qui s'avéreraient impossibles à traiter et à analyser à temps. Le passé prouve que ces contrôles systématiques demeurent coûteux et inefficaces.
D'où l'importance de ressources bien formées et suffisantes pour traiter la multitude de données éclatées et parcellaires. C'est tout le paradoxe de la société de l'information, dont ont déjà été victimes les services de renseignement américains, qui possédaient de nombreux éléments sur la préparation des attentats du 11-Septembre mais "ne savaient pas ce qu'ils savaient".
Les experts doivent comprendre ce qui se trame, sans préjuger de la nature des menaces réelles, c'est-à-dire sans chercher systématiquement à prédire l'avenir en prolongeant des courbes dans des schémas préexistants.

« Cette directive permet de cibler davantage les ressources et ainsi de les utiliser plus efficacement. »

DES BASES CONCEPTUELLES RENOUVELÉES

L'approche fondée sur l'analyse des risques doit permettre de déterminer l'appartenance à des catégories de risques, et ainsi d'adapter le niveau de contrôle. Mais pour maîtriser ses risques, encore faut-il les connaître. Ceci semble irréalisable sans une démarche globale et continue d'évaluation des risques liés aux activités des établissements.
L'évolution de la société précédant toujours le droit, se borner au strict respect des lois revient à ignorer les risques présents. Voilà pourquoi une acceptation restrictive des concepts de *compliance* et de *due diligence*, se traduisant par le respect formel de normes qui s'imposent à tous, ne peut suffire dans la construction d'un dispositif LAB/CFT.
Une telle démarche réactive est valide dans un monde figé, mais les échanges financiers sont internationaux et quasi immédiats, et surtout les menaces terroristes mais aussi criminelles évoluent sans cesse. Des listes de personnes et des procédures figées ne peuvent pas être efficaces aujourd'hui. À peine publiées, elles deviennent périmées et, de fait, inutiles contre les vrais dangers. La compilation de listes officielles et de nouvelles plus ou moins à jour en provenance de sources ouvertes se réfère systématiquement aux précédents. Elle ne permet aucune anticipation.

UNE CULTURE DE VIGILANCE RENFORCÉE

La culture globale de soumission aux normes et procédures, qui domine depuis le Sarbanes-Oxley Act dans l'univers juridique et comptable international, pourrait conduire les banques à se contenter d'acquérir des outils et à plaquer un organigramme dédié. Ce traitement formel serait cependant inadapté à l'obligation de résultat qui pèse sur les banques concernant la lutte contre le financement du terrorisme. L'esprit de la troisième directive recourt à la *soft law*, ensemble de normes impliquant les professionnels dès la construction d'une "co-réglementation", mieux adaptée aux évolutions et aux disparités nationales de l'économie mondiale. Elle vise une réglementation proche des métiers et fondée sur des principes plutôt que sur des règles. Cela présuppose une évaluation "proactive" et exhaustive des risques, comprise par les organes dirigeants des établissements qui assument une responsabilité accrue.
Cette directive permet de cibler davantage les ressources et ainsi de les utiliser plus efficacement. Elle contribue au renforcement de la culture d'entreprise et à la convergence en stimulant les échanges entre professionnels sur les critères et modalités de contrôle les plus adaptés aux spécificités de leurs activités. Chaque établissement doit fixer son niveau d'exigence, selon les moyens consentis, en arbitrant entre les standards requis, peut-être suffisants pour les classes les moins risquées, et les meilleures pratiques constatées dans les cas suspects. ■