الجمهورية الجزائرية الديمقراطية الشعبية
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة المالية
MINISTERE DES FINANCES

CTRF

CELLULE DE TRAITEMENT DU RENSEIGNEMENT FINANCIER
خلية معالجة الإستعلام المالي

خ م ا م

LETTRE D'INFORMATION : Bon à savoir

COSI (Communications Systématiques d'Informations)

Les lois N° 2013-100 du 28 janvier 2013 et N° 2013-672 du 26 juillet 2013 (loi de séparation et de régulation des activités bancaires) ont créé pour les établissements de crédit, de paiement et de monnaie électronique une obligation de communication systématique d'informations (COSI) à Tracfin (cellule antiblanchiment de Bercy) relative :

- aux opérations de transmission de fonds effectuées à partir d'un versement espèces ou au moyen de monnaies électronique dépassant 1 000 euros ou 2 000 euros cumulés par client sur un mois calendaire ;
- aux opérations financières présentant un risque élevé de blanchiment de capitaux ou de financement du terrorisme en raison du pays, de l'origine ou de la destination des fonds.

1. L'objectif de ce dispositif

La finalité est différente de celles des déclarations de soupçon. Les données issues des COSI alimentent une base documentaire et ont uniquement vocation à enrichir les investigations en cours.

2. Evolution du dispositif COSI en 2016

Le champ d'application de COSI a été élargi aux opérations importantes en espèces.

Un décret du 25 mars 2015 issu de la loi bancaire de juillet 2013 introduit à compter du 1er janvier 2016 une nouvelle obligation pour les banques et établissements de crédit :

Les opérations de dépôts et de retraits d'espèces sur les comptes de dépôts et de retraits supérieures à 10 000 euros (cumulés sur un mois) feront l'objet d'une information systématique des banques à Tracfin. La déclaration est mensuelle, au plus tard trente jours suivant le mois où le seuil cumulé a été atteint.

3. Les éléments définis par le décret

Le décret définit les informations à transmettre à Tracfin, à savoir les éléments d'identification du ou des titulaires de comptes, date, référence et montant des opérations, numéro de compte bancaire international (IBAN).

4. Exception retenue par le décret

Les opérations liées à un crédit ne sont pas soumises aux dispositions du décret.

5. Est-ce que le dispositif COSI s'intègre dans la cadre de la déclaration de soupçon ?

Non, la finalité de COSI est différente de celle des déclarations de soupçon. La COSI a un caractère systématique sans notion de soupçon. La COSI ne peut à elle seule justifier l'ouverture d'une enquête. Elle ne dispense pas les établissements de crédit et de paiement d'effectuer, pour ces mêmes flux, des déclarations de soupçon.

6. Quels sont les impacts ?

Le dispositif COSI va générer des investissements informatiques pour la mise à jour des systèmes d'information des établissements financiers.

7. Date de contrainte

1er janvier 2016

8. Qu'est qu'on attend ?

Une concertation au niveau technique est en cours entre la cellule Tracfin et la profession bancaire pour la mise en place de la nouvelle déclaration systématique d'opérations COSI. (Données à charger sur la plateforme Ermes, format fichiers, interconnexion automatique à Ermes à partir des SI).

Un document technique doit être remis à la rentrée et une réunion en septembre 2015 doit évoquer les prochaines étapes (évolutions réglementaires, mise en œuvre, calendrier

Sources : Rapport annuel d'activité de Tracfin 2014

Liens : https://www.sab2i.com/blog/fr/cosi-communications-systematiques-dinformations-kesako/

La conformité: Compliance Officer, RCSI et RCCI

Définition

La compliance, en français conformité, tire sa source de la règlementation bancaire et financière : les travaux de Bâle II repris par le Règlement 97-02 du Comité de la Règlementation Bancaire et Financière, applicable aux établissements de crédit et aux entreprises d'investissement ; les Directives européennes, dont la Directive MIF (Marchés d'Instruments Financiers) transposée par le Règlement Général de l'Autorité des Marchés Financiers (AMF).

La fonction de conformité est une fonction indépendante qui identifie, évalue, et contrôle le risque de non-conformité de l'établissement, défini comme le risque de sanction judiciaire, administrative ou disciplinaire, de perte financière significative, ou d'atteinte à la réputation, qui naît du non respect de dispositions propres aux activités bancaires et financières, qu'elles soient de nature législatives ou règlementaires, ou qu'il s'agisse de normes professionnelles et déontologiques, ou d'instructions de l'organe exécutif.

Le responsable de la conformité a également un rôle d'information, de formation et de conseil, tant vis-à-vis des collaborateurs que vis-à-vis de la direction de l'établissement.

Le champ de compétences de la conformité est donc très large.

Organisation

Dans les banques la fonction est confiée à un Directeur de la Conformité, dans les entreprises d'investissement elle est confiée à un Responsable de la Conformité des Services d'Investissement (**RCSI**) ou à un Responsable de la Conformité et du Contrôle Interne (**RCCI**) selon que l'on se trouve chez un prestataire de services d'investissement au sens large (transmission et exécution des ordres de bourse, conservation de titres, investissement pour compte propre etc…) ou bien dans une société de gestion de portefeuille.

Ces différences sémantiques qui désignent peu ou prou une même fonction et une même réalité, tiennent à la diversité tant des règlementations que des autorités de supervision bancaires et financières ainsi qu'à leur histoire.

Dans les grands établissements, aux activités souvent multiples, la fonction est remplie par un Département de la Conformité, doté d'un personnel nombreux.
Dans des établissements de plus petite dimension, elle est souvent remplie par une seule et unique personne qui cumule les fonctions de déontologue, contrôleur interne, responsable de la lutte anti blanchiment avec celle de responsable de la conformité.
Enfin dans les plus petites entités elle peut être concentrée entre les mains d'un dirigeant, qui peut en déléguer l'exécution à un prestataire externe. Cette délégation peut même, dans certains cas, être encouragée, voire imposée, par l'Autorité des Marchés Financiers, qui y voit une assurance de professionnalisme et d'indépendance. Une des activités de D2R Conseil est de prendre en charge cette fonction de conformité dans de telles entités.
Les fonctions de contrôle interne et d'audit sont très proches. Si dans bien des cas les fonctions de contrôle interne et de conformité peuvent être regroupées, il en va différemment de l'audit, ou de l'inspection, qui doivent être indépendantes, de façon à pouvoir contrôler toutes les activités de l'entreprise, y compris la conformité.
La fonction de conformité est distincte de la fonction juridique à proprement parler, en cela qu'elle traite de l'application au sein de l'établissement et dans son activité de l'ensemble de règles qui régissent la profession ; mais sans interférer dans le règlement des litiges qui peuvent opposer la société à des tiers, ni dans les différends d'ordre contractuels. Cependant il n'est pas impossible de regrouper la fonction juridique avec la conformité, bien, qu'à notre sens, cette dernière soit de nature complètement différente, en raison de sa dimension de contrôle.
Enfin la fonction de conformité est incompatible avec la réalisation d'opérations comptables, commerciales, ou financières.
En termes de hiérarchie, elle doit, lorsqu'elle n'est pas confiée à un membre de l'organe exécutif, être rattachée directement à la direction générale de l'entreprise, ou tout au moins à un niveau d'autorité suffisant pour assurer son indépendance vis-à-vis des autres services.

Le compliance officer

Le compliance officer, ou le responsable de la conformité, a non seulement un rôle d'identification de la règlementation financière, du code de bonne conduite et des bonnes pratiques professionnelles à suivre ainsi que de contrôle de leur application ; mais aussi un rôle de conseil, d'information et de formation.

Définition et application des règles

Le responsable de la conformité identifie les règles applicables et met en place les procédures visant à leur respect par l'ensemble de personnel.
Il identifie les conflits d'intérêts potentiels et met en place des règles de gestion lorsqu'ils ne peuvent pas être évités, comme la tenue d'un registre des conflits d'intérêts. Il met en place des procédures connues sous le nom de « Murailles de Chine », afin de prémunir la société contre la circulation indue d'informations confidentielles.
Bien que le terme ait disparu du vocabulaire règlementaire, il est aussi déontologue : il définit les règles déontologiques, identifie le personnel concerné et fixe les restrictions en matière de transactions personnelles.
Il dresse la liste du personnel dont les conversations téléphoniques peuvent être enregistrées et est compétent pour procéder à leur écoute.

Contrôle

Rôle de contrôle : le responsable de la conformité effectue des contrôles de second niveau, réguliers, afin d'identifier les violations des règles que nous venons de citer. Parmi ces contrôles nous pouvons citer :

- Le contrôle du respect des procédures par les services opérationnels ainsi que l'exécution des contrôles de premier niveau.
- Dans une société de gestion de portefeuilles le respect des contraintes d'investissement
- Dans une entreprise d'investissement, quelque soit son métier, le respect par le personnel, des règles de transaction pour son propre compte, et, plus généralement du code de déontologie.
- Le contrôle de la prévention des abus de marché…

Ces contrôles donnent lieu à un reporting à la Direction, mais aussi, dans certains cas comme dans celui de l'abus de marché, à l'autorité de supervision.

Information et Conseil

Il conseille la direction pour la mise en place de produits nouveaux et s'assure à cette occasion que l'ensemble des mesures destinées à prévenir le risque de non-conformité ont bien été identifiées. De façon plus générale il conseille le management de l'entreprise sur l'application de la règlementation, par exemple en cas de communication de crise.

Il informe et forme le personnel sur tous les sujets de sa compétence. Il est par exemple de bonne pratique que tout nouvel entrant dans la société se voit expliquer par le responsable de la conformité les règles déontologiques en vigueur. Cette information est renouvelée à destination de l'ensemble du personnel à chaque évolution de la règlementation.

Il est responsable de la lutte anti-blanchiment et contre le financement du terrorisme et s'assure de l'existence de procédures dans ce domaine ainsi que de leur respect.

Il est le correspondant attitré des autorités de supervision, et, à ce titre leur soumet des rapports réguliers sur son activité. En France, RCCI et RCSI se voient attribuer une carte professionnelle par l'AMF, tandis que la nomination et le départ du Directeur de la Conformité, dans les banques, doivent être notifiés à la Commission Bancaire. De même, en cas d'externalisation, l'AMF autorise le recours à un prestataire après s'être entretenu avec ce dernier et le responsable de l'entreprise, sur la nature et l'étendue de sa mission.

Il va sans dire que le Responsable de la Conformité doit disposer de moyens en rapport avec l'étendue de ses tâches. Ces moyens autonomes et suffisants incluent des outils informatiques ad-hoc.

Lorsque ces moyens sont partagés avec d'autres services, comme par exemple, le juridique ou le contrôle interne, le partage doit être clairement identifié et des mécanismes de coopération mis en place.

Il est destinataire des alertes des membres du personnel sur les éventuels dysfonctionnements dont ils peuvent être témoins. Ce dispositif, connue sous le nom de « droit d'alerte » a été mis en place dans la réglementation française à la suite de la transposition de la MIF et est inspiré du « whistle blowing » de la loi Sarbanes-Oxley (Sox).

Conclusion

Les évènements que nous avons vécus ces dernières années, comme les affaires Enron et World com ont conduit les législateurs à durcir les obligations de contrôle interne : loi Sox aux Etats-Unis et loi de Sécurité Financière (LES) en France, par exemple. Les travaux du Comité de Bâle et les Directives Européennes ont insisté sur l'obligation de mettre en place une fonction de conformité indépendante et dotée de moyens suffisants. En France, cette obligation a été transposée dans la loi (Code Monétaire et Financier) ainsi que dans la règlementation bancaire et financière (CRBF et RGAMF).

Les développements récents de l'actualité sont symptomatiques d'une absence de conformité aux règles déontologiques et aux bonnes pratiques professionnelles, comme celle qui consiste, pour une banque, à ne pas pousser ses clients emprunteurs au surendettement, ou à proposer des produits financiers complexes inadaptés aux besoins des investisseurs.
Le compliance officer est un élément essentiel de la protection de son établissement contre le risque opérationnel, il joue également un rôle dans la protection de l'intégrité des marchés et est garant de la primauté des intérêts des clients. Son autorité sortira vraisemblablement renforcée de la crise actuelle des institutions financières.
D2R Conseil, cabinet de consulting spécialisé en compliance et en contrôle interne, a mis en place une offre de conseil adaptée spécifiquement à l'asset management et à la banque d'investissement
Liens : http://www.fimarkets.com/pages/compliance_conformite.php

Gestion des processus métier : conformité et lutte contre le blanchiment et la fraude

La multiplication des canaux de télécommunications a fourni aux réseaux de criminalité financière de nouveaux vecteurs pour réinjecter des fonds illicites dans le circuit économique légal. Comment ont réagi les banques ?
L'avènement de nouveaux supports électroniques tels qu'Internet a favorisé de nouveaux types de criminalité. Le marché actuel des services financiers et bancaires est confronté, à l'instar de nombreux autres secteurs, à des pressions réglementaires tant génériques que spécifiques à leur métier visant à protéger les clients et les organismes financiers contre de telles pratiques illégales et sans scrupules.
De manière générale, on constate que les changements économiques rapides s'accompagnent d'une évolution tout aussi rapide des activités criminelles. À titre d'exemple, le boom immobilier en Europe et aux États-Unis a été suivi d'une augmentation du taux de fraude dans les domaines des prêts aux consommateurs et des prêts immobiliers.
Face aux scandales financiers et autres activités frauduleuses apparus aussi bien dans la sphère individuelle que dans le milieu des entreprises, le législateur a été contraint d'intervenir afin de mettre en place de nouveaux dispositifs visant à protéger les sociétés, les actionnaires, et les clients.
Cette situation a eu pour conséquence une augmentation des dépenses liées à la gestion du risque et un alourdissement des obligations déclaratives afin d'améliorer la transparence et le contrôle au sein des entreprises.
Disponibilité des informations
Du point de vue des métiers financiers, il a été constaté, au cours des dernières années, un certain engouement autour des notions de conformité, de blanchiment d'argent et d'autres types de risques.
De nouvelles technologies ont été développées et des solutions existantes ont été peaufinées afin d'améliorer l'identification des opérations suspectes. Les entreprises se sont ainsi souvent dotées de la capacité de repérer des activités potentiellement illicites à un niveau de précision inégalé.
Toutefois, cette première vague a donné lieu à une nouvelle problématique : comment traiter de façon efficace ces alertes identifiées sans entraver trop fortement les activités commerciales ?

À titre d'exemple, aux États-Unis, une augmentation de plus de 25 % par an du nombre d'événements potentiellement suspects identifiés au cours de la dernière décennie engendre actuellement une pression considérable sur le personnel des *back office*, de la direction des fraudes et de la lutte antiblanchiment, qui doit traiter ces alertes, puis distinguer les erreurs de filtrage des activités véritablement douteuses. Pour chaque déclaration officielle de soupçon effectuée, il peut y avoir, en amont, un volume deux à trois fois supérieur d'alertes qui auront fait l'objet d'une qualification, d'une validation et d'une décision ; chaque processus comportant un volume d'inconnues toujours supérieur au processus précédent.

En d'autres termes, même si les établissements bancaires sont de plus en plus performants à identifier le risque, celui-ci a un impact négatif sur leur capacité à optimiser la maîtrise des pertes, avec pour conséquence une dégradation de l'efficacité d'exploitation et une augmentation des coûts en *back office*.

Plus inquiétant encore : l'impact des activités de mise en conformité, de lutte contre le blanchiment d'argent et contre les pratiques frauduleuses s'étend au-delà du *back office* et touche, directement la prise de parts de marché et la conquête de nouveaux clients.

Les établissements bancaires sont de nos jours confrontés à un impératif commercial visant à conquérir de nouveaux marchés et à s'ouvrir à de nouveaux clients à un rythme accéléré. Parallèlement, le nombre de plus en plus élevé des procédures de qualification, de vérification au préalable, de contre-vérification et de validation entrave le processus d'acquisition de nouveaux clients et réduit les perspectives d'augmentation de chiffre d'affaires.

Tout en maintenant la rigueur et la cohérence nécessaires en amont pour se prémunir contre des activités potentiellement illicites, les établissements doivent impérativement améliorer leur performance pour accélérer l'augmentation de leur chiffre d'affaires.

À chaque problème sa solution

Afin de garantir la conformité et la gestion du risque, les établissements bancaires et les institutions financières se sont jusqu'alors concentrés sur les mesures de détection.

La problématique principale a consisté à identifier le problème, selon le canal, le type de produit ou le secteur d'activité en cause. En réponse à cette demande, les fournisseurs ont introduit sur le marché un savoir-faire avancé et spécialisé dans le domaine de la détection de la criminalité dans chaque secteur, en proposant des solutions essentiellement propriétaires dédiées à des détections d'activités illégales spécifiques aux virements bancaires illicites ou aux fraudes à la carte bancaire par exemple.

L'objectif fondamental de chaque solution et de chaque fournisseur s'est focalisé sur les outils d'aide à la détection. Même si ces solutions sont dotées de fonctionnalités de gestion de dossiers d'investigation, il s'agit généralement d'extensions secondaires et souvent rudimentaires du moteur spécialisé en détection de masse.

Gestion des dossiers d'investigation automatisée

Si les établissements bancaires souhaitent optimiser la rapidité, l'efficacité et la précision de l'ensemble du processus, il est nécessaire qu'ils disposent d'un système unique, centralisé et automatisé de gestion des dossiers d'investigation, qui soit capable de traiter des flux provenant de moteurs de détection spécialisés et hétérogènes.

Un tel système comprend les avantages suivants :

- Il fournit le même niveau de performance aussi bien pour la gestion des dossiers d'investigation de l'établissement bancaire que pour la détection des événements, et ce, quel que soit le canal, le produit ou le secteur d'activité ;
- Il permet d'obtenir une visibilité sur l'ensemble des événements susceptibles de survenir dans l'entreprise et de participer à l'identification ou l'analyse d'un cas.

Nous disposons à l'heure actuelle de systèmes informatiques de détection extrêmement puissants capables d'identifier les activités illicites les plus sophistiquées. Jusqu'à présent, le suivi des dossiers était beaucoup plus fragmenté et reposait essentiellement sur un fonctionnement manuel. Il est désormais possible de déployer un outil BPM de gestion des dossiers, qui pourra être rapidement adapté aux activités frauduleuses et criminelles de demain.

Les systèmes actuels sont capables d'extraire en masse les événements douteux et de les transférer vers un référentiel centralisé. Ensuite, le dispositif d'investigations de l'entreprise permet aux décideurs d'obtenir une vue d'ensemble sur les activités jugées suspectes, d'analyser les événements de façon beaucoup plus fine et de déterminer les mesures à mettre en œuvre.

L'enjeu de l'automatisation

L'un des problèmes majeurs des systèmes traditionnels de gestion des investigations en mode manuel auquel les établissements bancaires étaient confrontés concerne la définition du niveau de filtrage de la détection.

En effet, un niveau de filtrage trop faible peut apparaître comme un manquement vis-à-vis des obligations réglementaires et des procédures internes de gestion des risques. À l'inverse, un niveau de filtrage trop élevé comporte le risque de submerger les équipes d'investigation avec un nombre d'événements trop volumineux à traiter. De plus, cette situation s'amplifie dès lors que surviennent une augmentation de la cadence ou des changements trop rapides dans les procédés utilisés par les fraudeurs et les différentes activités criminelles.

Un autre problème concerne la complexité du processus d'investigation. D'abord, les événements font l'objet d'un contrôle préliminaire de premier niveau avant d'être transférés vers les responsables de l'investigation des risques, qui examinent l'historique des transactions, échangent leurs points de vue avec le responsable métier ou les services concernés, puis récupèrent des données depuis d'autres systèmes informatiques situés dans d'autres services, avant de qualifier l'incident et de déterminer les mesures à mettre en œuvre.

L'automatisation de ce processus, qui comporte plusieurs étapes de saisie longues et fastidieuses et de nombreuses étapes de recherche d'informations complémentaires, ainsi que l'utilisation de règles métier précises à chaque étape du processus décisionnel, est un atout considérable.

Il permet d'optimiser les performances de l'entreprise en générant des gains de temps précieux que les équipes d'investigation et de gestion des risques peuvent consacrer à des activités à plus forte valeur ajoutée.

Une approche pas à pas

Les meilleurs systèmes automatisés actuels sont dotés de fonctionnalités avancées conçues afin de traiter de façon optimisée chaque étape du processus de gestion des dossiers d'investigation.

D'abord, une telle solution doit être en mesure de traiter de manière événementielle l'arrivée de nouvelles informations et de générer un dossier virtuel qui, contrairement à l'approche d'une gestion documentaire, capture véritablement les données brutes en temps réel et peut les acheminer automatiquement vers le service compétent.

Ensuite, une fois l'événement traité dans le système, il peut être enrichi par des données secondaires. Le dossier virtuel d'investigation est ainsi constitué d'informations pertinentes provenant de diverses sources de données de l'entreprise.
À ce stade, les informations étant rassemblées et disponibles au sein du dossier, la décision peut être prise en conformité avec les règles établies (procédures internes, mise en conformité).
Il s'agit en l'occurrence d'un second niveau de règles métier. Grâce aux technologies de gestion des règles métier, de nombreuses décisions peuvent être automatisées afin d'éliminer des événements considérés à tord par les technologies de filtrage traditionnelles comme des détections nécessitant une analyse approfondie.
L'étape suivante du processus de gestion des dossiers d'investigation consiste à acheminer l'événement, auquel est attribué un niveau de priorité approprié, vers le responsable d'investigation adéquat.
Ainsi, un événement détecté, provenant d'un pays à haut risque ou à destination d'un client sensible sera automatiquement acheminé avec un niveau de priorité maximum, puis il sera signalé de façon appropriée et le plus visible possible s'il n'est pas traité dans un délai donné.
À ce stade, le système d'investigation assistera l'opérateur grâce à de nombreux écrans, données et fonctionnalités permettant de faciliter une analyse rapide et précise, avec des liens vers des événements susceptibles d'être rapprochés de l'événement détecté, tels qu'un pays de provenance, un client ou un type d'événement associé. L'ensemble des tâches administratives ultérieures de *back office* peuvent également faire l'objet d'un traitement automatisé et le processus de bout en bout sera conforme aux normes de qualité et d'audit à respecter.
De manière générale, les procédures d'investigation sont longues et les personnes en charge de celles-ci ont bien souvent plusieurs cas à analyser en cours de traitement. Grâce à des outils de suivi des niveaux de services (SLAs), le système de gestion de dossiers sera en mesure de gérer la charge de traitement de chaque intervenant afin de garantir un respect du calendrier des obligations déclaratives auprès de l'organisme réglementaire compétent.
Enfin, il convient d'insister sur le fait que toutes ces problématiques existent au sein d'un environnement financier en perpétuel mouvement, dans lequel la réglementation et les menaces criminelles sont en évolution constante.
En adoptant une approche adaptative « Build for Change » reposant sur la définition centralisée des règles de gestion des dossiers d'investigation, les établissements bancaires et les institutions financières conserveront une longueur d'avance dans la capacité à réagir rapidement aux évolutions futures, y-compris les facteurs externes, que ceux-ci soient connus ou non.
Dans ce domaine comme dans bien d'autres, les entreprises gagnantes sont celles qui ont une vision et se dotent des capacités pour se positionner à l'avant-garde.
Liens : http://www.journaldunet.com/solutions/expert/20537/gestion-des-processus-metier---conformite-et-lutte-contre-le-blanchiment-et-la-fraude.shtml

Développement de modèles de segmentation de scénarios et de détection des anomalies

Utilisation d'outils analytiques dans le cadre des programmes de conformité BSA (Bank Secrecy Act)/AML (anti-blanchiment)
Soumises à des pressions réglementaires de plus en plus fortes, les banques doivent constamment évaluer les risques qui pèsent sur elles.

Le secteur BSA/AML a donc décidé de miser sur les technologies analytiques/statistiques pour réduire les faux positifs, étendre le périmètre de la surveillance et limiter les coûts de gestion des programmes anti-blanchiment.
Pour mener une stratégie anti-blanchiment efficace, il est indispensable de segmenter les clients en analysant leur activité et les caractéristiques des risques. Cet article explique comment coupler des méthodes quantitatives et qualitatives pour identifier les activités les plus risquées pour la banque.
Liens : http://www.sas.com/fr_fr/whitepapers/scenario-segmentation-anomaly-detection-models-107495.html

Évolution ou révolution ?
La lutte anti-blanchiment gagne en maturité

Les pratiques de lutte contre le blanchiment d'argent et le financement du terrorisme adoptées par les plus grands établissements financiers font l'objet d'une étroite surveillance.
Tout le monde reconnaît que les méthodes de suivi et de contrôle ne suivent pas l'évolution des technologies de paiement, des réseaux terroristes et criminels de plus en plus sophistiqués et des systèmes de gestion de la réputation mondiale.
L'avenir est aux services de renseignement financier que les banques couplent à des fonctionnalités et technologies avancées pour respecter les nouvelles réglementations.
Grâce à des solutions ultra-performantes, les utilisateurs peuvent désormais effectuer des analyses complètes des Big Data pour visualiser la circulation des fonds à mesure que de nouveaux schémas se dessinent.
L'utilisation conjointe de cette nouvelle technologie et de systèmes plus anciens peut réduire les faux positifs et produire immédiatement des résultats.
Elle ouvre également la voie à une transition plus fluide entre les outils de première génération en fin de vie et les toutes dernières technologies d'analyse et de détection.
Liens : http://www.sas.com/fr_fr/whitepapers/evolution-or-revolution-107695.html

Les autorités de tutelle

A tous les niveaux (international, européen, national), les autorités de tutelle répartissent entre deux champs d'action leurs actions de surveillance et de réglementation: les activités bancaires d'une part, les marchés financiers d'autre part.
Historiquement les banques centrales jouent le rôle de « banques des banques », prêteur en dernier ressort et de banquier de l'Etat. Les banques centrales veillent à la stabilité des monnaies en ajustant l'offre de monnaie en direction des banques. Les outils d'ajustement sont les réserves obligatoires que les banques doivent déposer auprès des banques centrales et surtout la définition des taux d'intérêt des prêts offerts par la banque centrale aux banques commerciales. Cette politique monétaire est souvent menée indépendamment de l'Etat : c'est le cas dans l'Union Européenne, mais pas toujours : aux Etats-Unis la Federal Reserve fonctionne sous le contrôle du Sénat.
Tous les pays se dotent également de structures adéquates pour veiller au bon fonctionnement des marchés d'instruments financiers. Ces structures coopèrent au niveau international.

La mission des autorités de tutelle comprend également une part importante d'investigation, de recueil d'informations sur l'économie et les marchés, et de réflexion, et ce dans un but non lucratif. C'est pourquoi une visite sur les sites de ces organismes est souvent très intéressante, car ce sont des mines d'informations gratuites.

Les organismes internationaux

Il n'y pas à proprement parler d'autorité de tutelle au niveau international, mais les autorités nationales se rencontrent et se concertent au sein d'organisations dont les publications ont souvent un grand intérêt et une influence certaine sur les décisions prises au niveau local.

La Banque des règlements internationaux

La BRI (en anglais BIS, Bank for International Settlements), basée à Bâle, en Suisse, agit comme la « banque centrale des banques centrales ». Elle offre un éventail de services conçus pour leur faciliter la gestion de leurs réserves de change et d'or.

Parallèlement, la BRI coordonne et anime plusieurs forums ou comités promouvant la stabilité financière internationale. Le plus connu d'entre eux, le comité de Bâle, est à l'origine des « accords de Bâle » définissant le ratio Cooke, devenu maintenant le ratio McDonough.

La BRI ne rend pas de décisions ayant force de loi, mais la collégialité des discussions organisées sous son égide confèrent à ses propositions un poids certain.

International Organization of Securities Commissions

Le IOSCO (OICV, Organisation Internationale des Commissions de Valeurs, en français) regroupe toutes des autorités de marché du monde entier. La France y est représentée par l'AMF (Autorité des Marchés Financiers). Le IOSCO promeut l'émergence de standard dans les échanges sur les marchés internationaux, la coopération entre autorités de marché dans leurs activités de surveillance, la réflexion concertée sur le fonctionnement et la régulation des marchés.

Les autorités européennes

La Banque Centrale Européenne, l'Eurosystème et le SEBC

La banque centrale européenne (BCE en français, ECB en anglais), avec les banques centrales de chacun des pays membres de la zone Euro, constitue l'**Eurosystème**. La BCE et les banques centrales des pays membres de l'Union Européenne, y compris les pays non adhérents à l'Euro, constituent le **SEBC** (Système Européen de Banques Centrales, ESCB en anglais).

La mission principale de l'Eurosystème, comme l'ont prévu les accords de Maastricht, est de veiller à la stabilité des prix. Le conseil des gouverneurs des banques centrales de l'Eurosystème définit collégialement la politique monétaire, qui est ensuite mise en œuvre localement par chaque banque centrale. La BCE édicte des règlements concernant le fonctionnement du marché bancaire et monétaire de la zone Euro.

Committee of European Securities Regulators

Le CESR regroupe les autorités de marché des 25 pays membres ou futurs membres de l'Union Européenne (la France y est représentée par l'AMF), ainsi qu'un représentant de la commission européenne. Le CESR améliore la coordination entre les autorités de régulation locales, conseille la commission européenne pour l'élaboration de la réglementation dans le domaine des Bourses de Valeurs, veille à l'application de la réglementation dans l'ensemble de la zone européenne.

Les autorités de tutelle en France

La banque de France

Membre de l'Eurosystème, la Banque de France assure la mise en œuvre de la politique monétaire unique définie par le conseil des gouverneurs des banques

centrales de la zone Euro. Concrètement, les établissements de crédit qui souhaitent obtenir des financements auprès de la banque centrale, peuvent participer aux appels d'offres qui ont lieu chaque semaine aux conditions définies par l'Eurosystème. La Banque de France collecte les informations statistiques nécessaires à l'élaboration de la politique monétaire.
La Banque de France organise l'émission de la dette de l'Etat français pour le compte de l'agence France Trésor. La Banque de France est chargée d'émettre la monnaie fiduciaire (billets et pièces). Elle gère les réserves de change de la France. Elle établit la balance des paiements pour le compte de l'Etat. Elle centralise un certain nombre d'informations utiles au banques : le service central des risques, le FIBEN (Fichier Bancaire des Entreprises), le fichier des incidents de paiement.
La Banque de France surveille et réglemente le fonctionnement du marché bancaire. Cette mission est menée à bien plus spécialement au sein de différents comités fonctionnant sous son égide : le comité de la réglementation bancaire et financière (CRBF), le comité des établissements de crédit et des entreprises d'investissement (CECEI), la commission bancaire, aujourd'hui fusionnée avec l'ACAM, Autorité de Contrôle des Assurances et Mutuelles, pour former l'ACP, Autorité de Contrôle Prudentiel, le conseil national du crédit et du titre (CNCT) et le comité consultatif.

L'Autorité des Marchés Financiers

L'AMF est issue de la fusion de la COB (Commision des Opérations de Bourse) et du CMF (Conseil des Marchés Financiers), regroupés dans un souci de rationalisation. L'AMF a pour mission de veiller à la protection de l'épargne investie dans les instruments financiers, à l'information des investisseurs et au bon fonctionnement des marchés d'instruments financiers.
L'AMF réglemente et contrôle l'ensemble des opérations financières portant sur les sociétés cotées. Elle autorise la création de SICAV et de FCP, agrée les sociétes de gestion lors de leur création. Elle définit le cadre réglementaire de fonctionnement des entreprises de marché (Bourses, systèmes de règlement-livraison) et des entreprises d'investissement et plus généralement des professionnels des services d'investissement.
L'AMF peut procéder à des contrôles ou à des enquêtes et éventuellement sanctionner les contrevenants.

Les autorités de tutelle aux Etats Unis

Aux Etats-Unis, la Federal Reserve supervise les Federal Reserve Banks, au nombre de 12, qui détiennent les réserves obligatoires des banques. La direction de la Fed (le Board of Governors) est nommée par le président et confirmée par le Sénat. La Fed met en œuvre la politique monétaire, supervise le système bancaire, maintient la stabilité du système financier et fournit un certain nombre de services, dont la gestion du système de transfert de fonds Fedwire.
La SEC, Securities and Exchange Commission, veille à la transparence des marchés financiers, surveille l'activité des acteurs des marchés, et sanctionne les manquements à la réglementation.

Les autorités de tutelle en Grande Bretagne

En Grande Bretagne, la Bank of England veille à l'intégrité et la stabilité de la monnaie, à la stabilité du système financier et à l'efficacité des services financiers. La FSA (Financial Services Authority) autorise les acteurs ayant accès au marché, réglemente le fonctionnement des marchés et protège l'investisseur final.

Liens : http://www.fimarkets.com/pages/autorites_tutelle.php

La sécurité financière

La conformité a pour objectif principal de définir le champ d'application des différentes obligations réglementaires en regard de l'éthique et de la déontologie de l'établissement de crédit. La conformité définit les règles et les procédures à appliquer, préconise une organisation à mettre en place et s'assure de l'efficacité des contrôles.

La conformité est régulièrement en relation avec le régulateur local du pays dans lequel l'établissement de crédit exerce son activité.

La sécurité financière est une fonction qui est généralement rattachée, dans l'organigramme des établissements de crédit, au département conformité, aux côtés des fonctions risques et contrôle permanent, la fonction conformité étant elle-même rattachée à la direction générale.

La sécurité financière regroupe les programmes suivants :

- Lutte contre le blanchiment des capitaux (AML/LAB)
- Lutte contre le financement du terrorisme (CFT)
- Respect des embargos commerciaux et financiers
- Surveillance des opérations de marché

La sécurité financière repose sur un socle réglementaire, qui définit les obligations dans chacun des domaines concernés.

Le socle réglementaire

Le socle réglementaire s'apparente à un mille feuilles : différentes recommandations ou réglementations à des niveaux différents : communauté internationale, Union Européenne, Pays, etc.

Au niveau international, l'organisme de référence est le GAFI.

Les composantes d'un programme AML

Le respect des embargos commerciaux et financiers

La communauté internationale, au travers de l'Organisation des Nations Unies (ONU), s'est dotée d'un arsenal juridique pour permettre le contrôle des flux monétaires. Parmi certaines mesures figure l'embargo commercial. Un embargo (généralement partiel), vise à restreindre les relations des pays membres avec le pays concerné et à encadrer strictement ce qu'il est permis de faire ou non en matière de commerce et d'échange. Les embargos se traduisent généralement par des mesures d'interdiction de certains types d'opérations, comme par exemple l'interdiction de commercer sur du matériel d'origine nucléaire ou militaire, ou encore l'interdiction d'exporter les ressources pétrolières d'un pays sous embargo.

Un embargo peut être bilatéral ou international. C'est donc l'étude à la fois du droit international et du droit national qui permet d'identifier les restrictions d'activité financière et commerciale d'un pays avec les autres nations de la communauté internationale.

Le respect des embargos regroupe l'ensemble des mesures à mettre en œuvre pour s'assurer que les différentes transactions transitant par les établissements de crédit ne vont pas à l'encontre des restrictions relatives aux embargos en vigueur.

La surveillance des opérations de marché

La surveillance des marchés est une obligation de conformité qui vise à s'assurer que l'établissement de crédit n'utilise pas son accès privilégié aux marchés financiers pour en tirer profit au détriment de ses clients.

Mise en œuvre d'un programme de conformité

Après avoir détaillé ci-dessus les composantes d'un programme AML, nous allons analyser les moyens à mettre en œuvre au sein des établissements de crédit pour appliquer de manière opérationnelle les recommandations du GAFI et se conformer ainsi aux réglementations en vigueur (ordonnance 2009-104, code monétaire et financier).

La mise en œuvre des recommandations dans les banques se traduit par :

- Un processus approfondi de connaissance et de suivi des clients,
- Le contrôle et la surveillance des transactions.

Si l'on voulait faire une analogie entre un établissement de crédit et une entreprise marchande, on pourrait comparer le client à un stock et la transaction à un flux. Lorsque l'entreprise marchande contrôle ses stocks et ses flux, l'établissement de crédit contrôlera ses clients et ses transactions.

Le processus de connaissance et de suivi des clients

Le KYC (Know Your Customers) désigne l'ensemble des processus que l'établissement de crédit met en œuvre pour assurer à la fois une connaissance approfondie de ses clients, mais également un suivi régulier de la clientèle car l'établissement de crédit dispose, par nature, d'une clientèle habituelle.

A l'opposé, une clientèle occasionnelle définit toute personne qui ne rentre en contact avec un fournisseur que dans le cadre d'une transaction isolée (même si la personne effectuera d'autres transactions dans le futur). La relation cesse dès l'achèvement de la transaction.

Les obligations de conformité envers les clients bancaires peuvent se scinder en deux (2) groupes, selon que l'on se place dans le temps au cours de la relation commerciale :

- Le processus de connaissance des clients lors de l'entrée en relation,
- Le suivi régulier des clients pendant toute la durée de la relation commerciale.

Le processus de connaissance des clients lors de l'entrée en relation

Lors de l'entrée en relation, l'établissement de crédit va procéder à un certain nombre de tâches qui permettent à la fois de recueillir les informations ayant trait au client, mais également de contrôler ces mêmes informations pour vérifier leur véracité.

Les différentes obligations de conformité concernant l'entrée en relation des nouveaux clients sont listées ci-dessous :

- Identification des clients,
- Contrôle des informations d'identification des clients,
- Contrôle des clients par rapport aux listes de sanction,
- Qualification du risque de blanchiment des clients,
- Consignation des pièces d'identification des clients,
- Production des preuves des contrôles opérés en cas d'audit du régulateur,
- Déclaration aux autorités compétentes en cas de soupçon.

Identification des clients

Tout d'abord, l'établissement de crédit va identifier son client. Les informations personnelles (dites « bio data ») tel que nom, prénoms, sexe, date de naissance, lieu de naissance, situation maritale, adresse, etc. seront demandées et enregistrées dans la « fiche client ».

La deuxième étape consiste à compléter la fiche client par les informations relatives à la relation commerciale. Par exemple, pour une banque privée, on va demander de manière formelle au client quelle est la politique de gestion de patrimoine qu'il veut se voir offrir (accès direct à la table de négociation, transferts d'ordre vers son attaché de

compte ou GSM (gestion sous mandat)), sa sensibilité au risque financier (ce qui va conditionner la constitution de son portefeuille dans le cas d'une GSM), etc.
La dernière étape concerne peu la Sécurité Financière. Elle consiste à enregistrer les informations propres au contrat souscrit ou au produit acheté par le client. Les différents contrôles effectués à cette occasion (scoring client, contrôle auprès de la Banque de France, ...) ne rentrent pas dans le cadre de la Sécurité Financière, mais dans celui de la « gestion des risques client ».

Le contrôle de l'identification des clients

Après l'acquisition des informations personnelles, un contrôle est effectué au niveau des informations d'identité déclinées par le client. L'identité va être contrôlée par rapport à une pièce d'identité officielle : carte nationale d'identité, passeport en cours de validité, carte de séjour, … Dans le cas d'une ouverture de compte en présence du client, le chargé de clientèle pourra effectuer un contrôle visuel de la personne par rapport à la photo, le sexe et l'âge du client présents sur la pièce d'identité.
Le contrôle des informations d'adresse nécessitera la fourniture par le client d'une pièce probante (facture d'eau, de téléphonie fixe, etc.). L'établissement de crédit pourra également adresser un courrier de bienvenue au client et vérifier que le courrier ne revient pas en NPAI.

Le contrôle des clients par rapport aux listes de sanction

Lors de l'entrée en relation, l'établissement de crédit contrôle la présence éventuelle de son client sur une ou plusieurs listes de sanction, selon la réglementation en vigueur dans le pays. Les autorités officielles (nationales ou supranationales comme l'ONU ou l'Union Européenne) ont établi des listes de personnes sous sanction. Elles regroupent toutes les personnes physiques et morales qui sont frappées d'une mesure nationale ou internationale et avec lesquelles toute transaction est interdite. A l'origine les listes étaient constituées de personnalités liées au trafic de stupéfiants. Au fil du temps, compte tenu de leur activité, des individus ou des groupes ont été frappés de mesure d'embargo nominative : personnalités politiques de pays sous embargo, militaires poursuivis pour crime de guerre, trafiquants d'armes, etc.
De plus, il est demandé de procéder au blocage des fonds et au gel des avoirs lorsque ces personnes ou organisations ont été identifiées au sein de l'établissement de crédit, soit à l'entrée en relation, soit dans le cadre d'une transaction financière. Nous développerons la partie contrôle par filtrage lors de l'étude des obligations de conformité concernant les transactions.

Qualification du risque de blanchiment

Le contrôle par filtrage a été effectué lors de l'étape précédente. Il a été fait mention d'un contrôle par rapport aux listes de sanction officielles et publiques. Elles sont publiées par les états et les organismes supra nationaux. Il existe pour autant d'autres listes, qui ne sont pas d'ordre public. L'établissement de crédit pourra utiliser les outils de rapprochement pour élargir le champ des listes à analyser. En effet, tous les outils de contrôle par filtrage déployés dans les établissements de crédit sont capables d'intégrer des listes publiques mais également des listes privées ou « maison ». L'établissement de crédit peut, par exemple, effectuer un contrôle par rapport à une liste interne de fraudeurs, avec lesquels elle se trouve souvent confrontée, ou une liste « d'indésirables » car en opposition avec la déontologie et les valeurs que l'établissement de crédit veut appliquer.
La 3ème directive Européenne a repris les recommandations formulées par le GAFI concernant la surveillance des personnes exposées politiquement (PEP). Un PEP a été ainsi considéré comme une personne « à risque » du point de vue du blanchiment de capitaux et les établissements de crédit sont tenus d'identifier les PEP parmi leur

clientèle dès l'ouverture de compte. Pour ce faire, il existe 2 méthodes d'identification :

- Méthode déclarative : Les établissements de crédit modifient les formulaires que doit remplir tout nouveau client lors d'une ouverture de compte, pour faire figurer des questions portant par exemple sur la détention d'un mandat politique, ou l'exercice d'une fonction judiciaire. C'est sur la base de ces informations que l'établissement de crédit qualifie le client comme PEP ou non.
- Méthode interrogative : Les établissements de crédit souscrivent un abonnement spécifique auprès d'un fournisseur de listes PEP. Ces listes sont intégrées dans les dispositifs de contrôle par filtrage et génèrent des alertes lors de rapprochement avec les clients de l'établissement de crédit.

D'une manière générale, l'établissement de crédit doit, au regard des contrôles qu'il a réalisés, qualifier le client en terme de risque lié au blanchiment. Cette qualification « risque » prend 3 valeurs : faible, normal ou élevé. Cette opération s'appelle « le profilage » du client. Des outils spécifiques existent pour aider les opérateurs à déterminer, de manière automatisée, le risque conformité d'un client donné. Le profilage, réalisé dans un premier temps lors de l'entrée en relation, est ensuite mis à jour par un processus continu qui fait partie des obligations de conformité relatives au suivi de la clientèle.

Consignation des pièces client

Après la phase d'identification du client et de son contrôle, l'établissement de crédit doit enregistrer les preuves d'identification du client et les archiver pendant une période fixée à 5 ans par le législateur. Cette consignation se fait par le biais de la numérisation des pièces apportées par le client pour attester de son identité (CNI, passeport, etc.). Les pièces numérisées constituent ainsi le dossier électronique du client.

Généralement, en parallèle du processus de numérisation, les établissements de crédit constituent un dossier physique avec les photocopies des pièces d'identité.

De la même manière l'établissement de crédit doit consigner les preuves qu'il a effectué les contrôles par rapport aux listes de sanction qui attestent que la relation d'affaires ainsi nouée est « conforme » à la réglementation.

Obligation de moyens

Les obligations réglementaires auxquelles les établissements de crédit sont assujettis sont de l'ordre de l'obligation de moyens. L'établissement de crédit est tenu de prendre en compte ses obligations de conformité et de prouver qu'il a mis en place des systèmes, des procédures, une organisation et des contrôles pour lutter efficacement contre le blanchiment de capitaux, le financement du terrorisme et le respect des embargos.

L'établissement de crédit doit apporter la preuve qu'il s'est doté de moyens pour mettre en œuvre un dispositif conforme aux obligations réglementaires et en adéquation avec le niveau de risque lié à son activité. Le régulateur a été amené à prononcer des sanctions contre un organisme financier, non pas parce que les clients utilisaient ses produits pour blanchir des fonds illicites, mais uniquement parce qu'il n'avait pas mis en place de système opérationnel pour appréhender l'ensemble de ces risques.

L'obligation de moyens est considérée au sens large du terme. Outre le déploiement d'un système informatique, l'existence d'un service spécialisé et le contrôle des procédures, la formation des salariés de l'établissement de crédit aux problématiques de lutte contre le blanchiment doit être assurée à leur prise de fonction et

régulièrement mise à jour. De plus, les procédures sur les sujets concernés (LAB, FT, embargos, KYC) doivent être rédigées et enregistrées dans un livre spécifique, puis diffusées et revues périodiquement.

La déclaration de soupçons

Dernière étape du processus de lutte contre le blanchiment de capitaux, l'établissement de crédit est tenu de déclarer les opérations susceptibles de provenir de fonds illicites ou destinés à financer des entités terroristes ou interdites. Cette déclaration de soupçon est effectuée à TRACFIN, organisme dépendant du ministère de l'économie et des finances. Après enquête, TRACFIN transmet, le cas échéant, le dossier au procureur de la république pour ouverture d'une procédure judiciaire.

Outre l'obligation de déclaration en cas de soupçon, l'établissement de crédit est tenu de ne pas divulguer au client ou à quiconque la déclaration ainsi établie. Cette obligation doit être respectée sous peine d'annulation de la procédure judiciaire envers la personne incriminée, même en cas de fait avéré. L'établissement de crédit est également tenu de fournir tout élément complémentaire que TRACFIN serait amené à lui demander dans le cadre de son enquête.

Le processus de suivi de la clientèle

Après que le client ait été identifié, puis contrôlé pendant la phase d'entrée en relation, il doit être suivi de manière régulière pendant toute la durée de la relation commerciale.

Les obligations de suivi de la clientèle reprennent et étendent celles concernant l'entrée en relation. Les obligations spécifiques de conformité sont les suivantes :

- Balayage des bases clients,
- Profilage des clients et des comptes,
- Surveillance des opérations à risque.

Balayage des bases client

Le contrôle par rapport aux listes de sanction a été effectué lors de l'entrée en relation. A cette occasion, l'établissement de crédit a vérifié que son client n'était pas présent sur une liste de sanction.

Toutefois, un client peut apparaitre sur une liste de sanction au cours de la relation commerciale. Il y a donc lieu de vérifier l'intégralité de la base clients par rapport aux listes de sanctions de façon régulière. Il est généralement pratiqué dans les établissements de crédits une fréquence de balayage de 1 fois tous les 3 mois. L'établissement de crédit est seul responsable du choix de la fréquence.

Le balayage des bases clients peut s'étendre aux listes de Personnes Exposées Politiquement (PEP). L'évaluation du risque de conformité des clients passe par un contrôle avec ce type de listes. En effet, la méthode déclarative n'est pas efficace dans la mesure où le client peut ne pas informer l'établissement de crédit d'un changement d'activité professionnelle comme par exemple l'exercice d'un mandat politique.

Il y a 3 facteurs de déclenchement d'un contrôle de base client :

- Lors de la mise à jour des listes de sanction ou de PEP. Les listes officielles de sanctions ou de PEP évoluent de manière aléatoire. Elles peuvent faire l'objet de plusieurs modifications par semaine comme ne pas évoluer pendant un mois. La moyenne se situe aux environs d'une mise à jour par semaine.
- A fréquence régulière, en fonction de la sensibilité de l'établissement de crédit à la problématique d'identification du risque de blanchiment de capitaux,
- A l'initiative de l'établissement de crédit, lors d'un audit ou pour préparer la visite du régulateur, par exemple.

Le balayage périodique est à même de modifier le « score » conformité du client en fonction des résultats des rapprochements opérés. Il est d'ailleurs à noter que le score

peut évoluer à la hausse ou à la baisse. En effet, les mesures d'embargo nominatif frappant une personne peuvent être levées et donc « améliorer » le score conformité du client.

Profilage des clients

Le balayage, s'il s'avère indispensable pour s'assurer de manière continue que les clients ne sont pas frappés de mesures de sanction, n'est cependant pas suffisant. Il faut, en complément, identifier les risques de blanchiment au travers des opérations qu'effectue la clientèle.

Suite aux orientations de la 3ème directive Européenne, le législateur a introduit une nouvelle notion pour définir le profil du client : l'approche par les risques.

Le principe consiste à déléguer entièrement à l'établissement de crédit l'identification préalable du risque de conformité (blanchiment des capitaux) et d'adapter les contrôles en fonction de ce risque. Compte tenu des masses importantes de données à traiter et du fait qu'une très large majorité de la clientèle utilise les instruments bancaires et financiers de manière parfaitement « normale », l'établissement de crédit est autorisé à ne surveiller attentivement qu'un nombre réduit de clients et de comptes. La concentration des moyens et des efforts à été préférée à un contrôle systématique et donc moins efficace.

C'est dans ce cadre que le profilage de client s'avère indispensable. Les informations client, recueillies pendant la phase d'entrée en relation, vont permettre de calculer un score. Les informations qui participent au calcul du score conformité sont les suivantes : origine des fonds, pays de résidence du client, pays de résidence fiscale, nature et montant des opérations, zones géographiques dans lesquelles le client est amené à commercer, ordre de grandeur des actifs, nature des sous jacents, etc.

L'opération de scoring ainsi décrite reste statique. Mais le profilage client peut également s'appuyer sur des données dynamiques. En effet, l'utilisation réelle des comptes par les clients ainsi que les opérations effectuées peuvent amener à modifier le score au cours du temps. On surveillera en particulier le nombre de comptes d'un même client, le nombre de changements d'adresse effectués dans l'année, etc. Le changement de score d'un client peut automatiquement le faire changer de catégorie de risque et donc amener à une surveillance accrue de ses opérations.

La surveillance des opérations

Ce point sera abordé en détail dans le chapitre suivant. Il complète les obligations de conformité de suivi de la clientèle dans la mesure où les opérations effectuées par les clients sont susceptibles de modifier le risque client et donc d'impacter le système de profilage. Les alertes qui vont être générées et transmises aux opérateurs de conformité pour investigation peuvent être regroupées en 2 catégories :

- Les alertes indiquant une différence entre l'utilisation prévue d'un compte et l'utilisation réelle de ce même compte,
- Les alertes indiquant une possible opération de blanchiment par rapport à des motifs connus.

Les alertes indiquant une différence entre l'utilisation prévue et réelle sont généralement basées sur les faits suivants : commerce avec des pays sensibles, augmentation du nombre de transactions, augmentation du montant unitaire des transactions, utilisation de devises, types d'opérations nouveaux, etc. Lors d'une opération d'un montant anormalement important, l'établissement de crédit se renseignera sur l'origine des fonds ainsi que sur la nature de l'opération. Toutes les opérations atypiques doivent être détectées et alerter l'établissement de crédit pour qu'il y porte une attention particulière.

Certaines opérations constituent des situations identifiées comme révélatrices de tentative de blanchiment : opérations de fractionnement (systématiquement en dessous des seuils de contrôle), dépôts espèces en nombre important, utilisation de comptes dormants, utilisation de comptes taxis (comptes avec une multiplicité d'ordres de virement et avec des soldes faibles),… et génèrent des alertes qui sont transmises aux opérateurs de conformité. Ces alertes méritent une attention particulière qui peut déboucher sur une déclaration de soupçons à TRACFIN.

Le contrôle et la surveillance des transactions

Le contrôle et la surveillance des transactions désignent l'ensemble des processus que l'établissement de crédit met en œuvre pour s'assurer que les transactions effectuées soit pour le compte de leur clientèle, soit en nom propre, sont conformes à la fois aux obligations réglementaires et au code de déontologie qu'il a établi en interne.
Le terme de transaction désigne tout type d'opération quel qu'en soit :

- la portée : domestique, intra-européenne, internationale,
- le sous jacent : paiement, opération titre, crédit documentaire, confirmation, etc.
- le réseau utilisé : SIT, SWIFT, SEPA, etc.

La conformité des transactions concerne donc l'ensemble des activités bancaires au sens large : banque de détail, gestion d'actifs, banque de financement et d'investissement, banque privée, etc.
Les obligations de conformité envers les transactions bancaires sont de 3 natures différentes :

- Contrôle du donneur d'ordre,
- Filtrage en temps réel des transactions,
- Monitoring des transactions.

Le contrôle du donneur d'ordre (GAFI SR7)

Le GAFI a émis 40 recommandations et 9 recommandations spéciales. Parmi ces dernières, la SR n° 7, spécifie l'obligation pour les établissements de crédit de faire figurer explicitement le donneur d'ordre des transactions. Cette recommandation a été transcrite par l'Union Européenne sous la forme d'un règlement (règlement EU 1781). Les établissements de crédits sont donc tenus d'appliquer ce règlement, et de faire figurer les informations relatives au donneur d'ordre : nom et prénom, adresse, numéro de compte. Cette obligation rend ainsi possible d'opérer des contrôles de type filtrage (voir ci-dessous) sur le donneur d'ordre. D'autres pays ont également transcrit la recommandation GAFI SR7 dans leur droit national.

Le filtrage des transactions

Pour effectuer les contrôles relatifs aux embargos et à la lutte contre le financement du terrorisme, les organismes officiels ont publié des listes accessibles au public. Ce sont les mêmes listes que celles déjà mentionnées au chapitre précédent.
Le filtrage des transactions s'opère en temps réel de manière à ne pas faire transiter sur le réseau bancaire utilisé (SWIFT, SEPA, SIT) une transaction qui aurait alors valeur d'acceptation tacite (acceptation voulant dire responsabilité en cas de contrevenance aux lois en vigueur concernant la lutte anti- blanchiment, la lutte contre le financement du terrorisme et le respect des embargos). Ce processus s'appelle : filtrage en temps réel, filtrage à priori ou filtrage au fil de l'eau (before the fact). Pour être efficace, les contrôles par filtrage doivent être opérés en temps réel.
L'identification des entités (personnes physiques, personnes morales, organisations, pays, …) sous sanction s'opère généralement avec des outils automatisés de filtrage.
Ces outils sont associés aux systèmes de gestion des transactions. Ils filtrent le contenu de tous les flux interceptés à la recherche d'une entité sous sanction présente

dans les listes mentionnées. Le rapprochement se fait de manière élaborée, c'est-à-dire que ces filtres effectuent non pas des recherches exactes, mais des recherches approchées en tenant compte d'un certain nombre de différences potentielles : interversions de mots, répétition ou omission de lettres, gestion des abréviations et mots-clés, ressemblance phonétique, etc.
Lorsque les moteurs de filtrage ont identifié des ressemblances, les transactions, ainsi que les entités pour lesquelles le moteur a trouvé une correspondance, sont présentées à des opérateurs. Ces derniers ont pour rôle de décider de l'action à mener sur la transaction après une éventuelle investigation : libérer la transaction, ce qui a valeur d'acceptation, ou au contraire bloquer la transaction et éventuellement effectuer la déclaration de soupçon à l'autorité compétente.

Le monitoring des transactions

Pour lutter efficacement contre le blanchiment des capitaux, les établissements de crédit mettent en place des systèmes qui analysent les transactions en tenant compte d'un historique, et en compilant les données de provenance et de nature diverse : comptes bancaires, clients, transactions, etc.
L'utilisation de solutions logicielles spécialisées est nécessaire eu égard au nombre important de transactions opérées par les établissements de crédit et de par l'impossibilité d'une surveillance manuelle des transactions. Il faut traiter des centaines de milliers, et plus souvent des millions d'enregistrements sur lesquels ont été ajoutées des données issues de calculs d'agrégats. Un système de monitoring de transactions opère généralement en plusieurs phases :

- **Phase d'intégration de données** :
  Les fichiers concernant les clients, les comptes et les transactions sont générés en sortie des applications de gestion, contrôlés, puis intégrés dans la base de données de l'outil de monitoring,
- **Phase d'enrichissement** :
  Les agrégats et cumuls sont calculés puis ajoutés aux données existantes venant ainsi compléter les informations disponibles dans le référentiel de l'outil de monitoring. Les scores des clients et des comptes sont également recalculés en fonction de l'activité réelle issue des nouvelles transactions,
- **Phase de génération des alertes** :
  Des scénarios de blanchiment et de surveillance sont préalablement établis, codés puis exécutés sur les nouvelles données, afin de faire ressortir les opérations, les comptes et les clients qui nécessitent une investigation spécifique. Le but d'un outil de monitoring est de faire émerger d'une masse de données, les quelques opérations qui doivent alerter les opérationnels,
- **Phase d'investigation et de déclaration** :
  Suite à l'exécution des scénarios de blanchiment, le département conformité va investiguer sur les alertes générées par le système et recueillir des informations complémentaires auprès des chargés de compte. Cette investigation donnera lieu à un « classement sans suite », ou éventuellement à une déclaration de soupçon à TRACFIN.
  De par les volumes importants de données à traiter, les systèmes de monitoring n'opèrent pas en temps réel mais en différé. Les processus d'intégration, de contrôle, de calcul d'agrégat et d'exécution de scénarios sont planifiés pour être lancés à heure fixe, et permettre de générer les alertes et le reporting dans les 24 heures suivant l'exécution des transactions.

Conclusion

Les obligations réglementaires de plus en plus nombreuses auxquelles doivent faire face les établissements de crédit nécessitent la mise en œuvre de véritables projets de mise en conformité incluant :

- La mise en place de multiples outils professionnels (filtrage, abonnements aux listes de sanction et PEP, etc.)
- l'établissement de procédures spécifiques adaptées aux obligations réglementaires, au risque encouru, aux dispositifs déployés et à la culture de l'entreprise,
- des procédures et des moyens permettant d'atteindre les objectifs mentionnés et attestant d'une prise en compte réelle des problématiques de sécurité financière vis-à-vis du régulateur.

Les investissements en matière de Sécurité Financière ne trouvent leur point de retour sur investissement que sur le long terme. Il est vraisemblable que le contexte de la crise financière que nous traversons sera générateur de davantage de régulation en matière de contrôle des activités des établissements de crédit. Ces derniers pourront mettre à profit les investissements en matière de conformité et de Sécurité Financière qu'elles auront réalisé, pour transmettre et communiquer sur leurs valeurs et sur leur éthique. A n'en pas douter, cette attitude leur ouvrira de nouveaux horizons et de nouveaux marchés.

Liens : http://www.fimarkets.com/pages/securite_financiere.php

Traite des personnes et trafic de migrants

Traite des personnes

Qu'est ce que la traite des personnes ?

L'Article 3 du Protocole visant à prévenir, réprimer et punir la traite des personnes, « l'expression "traite des personnes" désigne le recrutement, le transport, le transfert, l'hébergement ou l'accueil de personnes, par la menace de recours ou le recours à la force ou à d'autres formes de contrainte, par enlèvement, fraude, tromperie, abus d'autorité ou d'une situation de vulnérabilité, ou par l'offre ou l'acceptation de paiements ou d'avantages pour obtenir le consentement d'une personne ayant autorité sur une autre aux fins d'exploitation. L'exploitation comprend, au minimum, l'exploitation de la prostitution d'autrui ou d'autres formes d'exploitation sexuelle, le travail ou les services forcés, l'esclavage ou les pratiques analogues à l'esclavage, la servitude ou le prélèvement d'organes ».

Chaque année, des milliers d'hommes, de femmes et d'enfants sont victimes de la traite des personnes dans leur pays ou à l'étranger. Par la contrainte, la duperie ou la force, ils sont exploités pour leur force de travail, pour le sexe ou pour leurs organes. Presque tous les Etats sont touchés par ce crime contre l'humanité, comme pays d'origine, de transit ou de destination des victimes. La traite des êtres humains peut être une entreprise lucrative et les responsables sont souvent liés à la criminalité organisée. Pourtant, la traite affectant généralement des individus en marge de la société, peu de ces trafiquants sont jugés et la plupart des victimes ne seront probablement jamais identifiées et aidées.

ONUDC agit pour que cela change. Nous aidons les Etats à lutter contre la traite des personnes, à protéger les victimes et à poursuivre les coupables en justice, en accord avec le Protocole visant à prévenir, réprimer et punir la traite des personnes, en

particulier des femmes et des enfants, additionnel à la Convention des Nations Unies contre la criminalité transnationale organisée.
ONUDC aide les Etats dans la production de lois et de stratégies intégrales contre la traite et les assiste dans leur mise en œuvre. Nous offrons une assistance spécialisée, incluant le développement de capacités et d'expertise locales, et les outils pour encourager la coopération internationale dans les investigations et les poursuites. ONUDC rassemble également l'opposition internationale à la traite des personnes dans le secteur privé, la société civile, les médias et l'opinion publique grâce à l'Initiative globale pour combattre la traite des êtres humains (UN.GIFT) et la Campagne Cœur bleu. ONUDC joue aussi le rôle de secrétariat pour le Groupe de coopération inter-agences contre la traite des personnes, réunissant plusieurs entités onusiennes ainsi que d'autres organisations internationales.
En 2009, ONUDC développa, en collaboration avec UN.GIFT, un modèle de loi pouvant aider les Etats-membres dans la rédaction de leur législations nationales contre la traite des personnes. Le modèle de loi s'adapte aux besoins de chaque Etat quel que soit sa tradition juridique et ses conditions sociales, économiques, culturelles et géographiques. Il recouvre non seulement la criminalisation de la traite des personnes, mais aussi les différents aspects de l'assistance aux victimes et l'établissement d'une véritable coopération entre les Etats et les organisations non gouvernementales (ONG).

Trafic de migrants

Qu'est-ce que le trafic de migrants ?
Le Protocole contre le trafic illicite de migrants par terre, mer et air indique que « L'expression "trafic illicite de migrants" désigne le fait d'assurer, afin d'en tirer, directement ou indirectement, un avantage financier ou un autre avantage matériel, l'entrée illégale dans un État Partie d'une personne qui n'est ni un ressortissant ni un résident permanent de cet État ».
Le trafic de migrants est un crime qui implique l'assistance à l'entrée illégale d'une personne sur le territoire d'un Etat duquel cette personne n'est ni un ressortissant ni un résident, en vue d'obtenir une contrepartie financière ou tout autre bénéfice matériel. Le trafic de migrants touche presque tous les pays du monde. Il sape l'intégrité des Etats et des communautés, et coute la vie à plusieurs milliers d'individus tous les ans. ONUDC, en tant que gardien de la Convention des Nations unies contre la criminalité transnationale organisée, dite de Palerme, et des protocoles s'y rapportant, encourage sa ratification universelle et assiste les Etats dans leur efforts en vue de la mise en œuvre du Protocole contre le trafic illicite de migrants par terre, mer et air.
En vue de respecter le Protocole sur le trafic de migrants, l'Article 6 exige des Etats qu'ils criminalisent le trafic de migrants, la production de faux papiers et le fait de permettre le séjour illégal des personnes sur le territoire, et qu'ils confèrent le caractère de circonstances aggravantes au fait de mettre en danger ou de risquer de mettre en danger la vie ou la sécurité des migrants concernés et au traitement inhumain ou dégradant de ces migrants.
En 2006, l'ONUDC a publié un rapport intitulé Criminalité organisée et migration irrégulière d'Afrique vers l'Europe, retraçant les liens entre ces migrations illégales et les réseaux de la criminalité organisée et évaluant le marché que représente le trafic de migrants, les routes et modus operandi.
En collaboration avec ses partenaires, l'ONUDC participe activement à I-Map, un programme créé pour faciliter les échanges d'informations et d'analyses portant sur les flux migratoires, dans le but de soutenir les efforts de lutte contre le trafic de migrants

aux niveaux international, régional et sous-régional en Afrique, au Proche-Orient et en Europe.
L'ONUDC soutient également les Etats en Afrique de l'Ouest et du Nord dans leur mise en œuvre du Protocole sur le trafic de migrant, grace au Programme Impact.
L'ONUDC, en collaboration avec Interpol et Europol et avec un financement promenant de l'Union Européenne, élabore des modules d'entrainement dans le domaine de la prévention et de la lutte contre le trafic des migrants, à travers une série de réunions de groupes d'experts rassemblant des personnes changées de l'application de la loi et des procureurs
Liens : http://www.unodc.org/unodc/fr/human-trafficking/