



Association Luxembourgeoise
des Compliance Officers
du Secteur Financier

Le Bulletin d'informations

N°21

JANVIER 2011

Editorial



Chers membres de l'ALCO, chers amis lecteurs,

En ce tout début 2011, permettez-moi d'abord de vous adresser au nom du Conseil d'Administration nos meilleurs vœux pour une année remplie de satisfactions professionnelles et privées. Qu'elle vous apporte les réponses à vos attentes et la sérénité dans votre activité. 2011 est, comme vous le savez, l'occasion de fêter le 10^{ème} anniversaire de notre association. Nous vous attendons tous le 20 janvier au Conservatoire de Musique de la ville de Luxembourg pour marquer dignement cette étape. N'oubliez pas de vous inscrire auprès du secrétariat de l'ALCO.

Le 21^{ème} bulletin de l'ALCO s'inscrit bien dans cette rentrée annuelle. Le rendez-vous avec Gérard Lommel, patron de la CNPD rappelle les principales missions de l'autorité administrative indépendante chargée de la protection des personnes à l'égard du traitement des données à caractère personnel. Un dialogue ouvert aborde les sujets essentiels et notamment le rôle du Compliance Officer en ce domaine, rôle qui varie d'une institution et d'un PSF à l'autre.

Sans pratiquer non plus la langue de bois, Catherine Bourin, qui représente l'ABBL auprès de l'ALCO, porte un regard réaliste sur le nouveau dispositif anti-blanchiment mis en place au Luxembourg après la sévère évaluation du GAFI. La loi du 27 octobre 2010 et les autres dispositions légales en la matière souffrent de cet objectif univoque mais apparaissent inévitables. Nous attendons maintenant le règlement de la CSSF pour compléter le dispositif.

Le Bulletin

L'article suivant, traitant des risques de blanchiment dans le commerce électronique illustre quant à lui des chemins nouveaux en matière de blanchiment, chemins qui échappent largement aux contrôles des Compliance Officers des banques et autres institutions financières.

L'approche risque en matière d'acceptation et de suivi des clients a fait l'objet de deux tables rondes tenues successivement en anglais et en français. Si l'approche risque est maintenant présente dans toutes les institutions concernées, elle prend logiquement des formes et des mises en œuvre variées correspondant précisément aux risques spécifiques à chaque professionnel du secteur financier.

Bonne lecture à toutes et tous.

Jean Noël Lequeue
Président de l'ALCO

* *

Interview

Rencontre avec Monsieur Gérard LOMMEL, Président de la Commission Nationale pour la Protection des Données

Question 1 : moyens à disposition de la CNPD

Gérard Lommel : (avec un large sourire) – fait part qu’il y a consensus parmi les membres du groupe de travail de l’Article 29 (v. à ce sujet « infra », question 6) de ne pas faire de déclaration dans le sens que les moyens à disposition sont suffisants ; plus sérieusement, il aborde ensuite le cahier des charges de la Commission et détaille ses pouvoirs et moyens à disposition ;

La Commission nationale pour la protection des données (Commission nationale), est une autorité administrative indépendante instaurée par la loi du 2 août 2002 entrée en vigueur le 01.12.2002 relative à la protection des personnes à l’égard du traitement des données à caractère personnel. La Commission nationale a pour mission essentielle de contrôler et de vérifier la légalité des traitements de données à caractère personnel et d’assurer le respect des libertés et droits fondamentaux des personnes en matière de protection des données.

Parmi ses principales missions, figurent notamment :

- La vérification de la légalité de la collecte et de l'utilisation des données soumises à un traitement, notamment à travers l'autorisation préalable ou des contrôles à posteriori ;
- Guider et informer les responsables du traitement quant à leurs obligations;
- La sensibilisation au respect des libertés et droits fondamentaux des personnes, notamment au respect de la vie privée, et l'information du public sur les droits des personnes concernées;
- l'examen des plaintes et demandes de vérification de la licéité des traitements;
- l'activité de conseil au Gouvernement en la matière.

La Commission nationale est également chargée d’assurer l’application des dispositions de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et de ses règlements d’exécution.

Parmi ses prérogatives, elle dispose d’un pouvoir d’investigation qui lui confère un droit d’accès direct aux locaux autres que les locaux d’habitation où a lieu le traitement ainsi qu’aux données faisant l’objet du traitement et procède aux vérifications nécessaires.

Elle a également la possibilité (guère encore utilisée que quelque fois jusqu’ici) de prendre différentes sanctions disciplinaires susceptibles d’un recours en réformation.

Après des débuts rendus difficiles tant par les ressources limitées à disposition que du nombre des dossiers soumis à traiter, la Commission a trouvé aujourd’hui son rythme de croisière – elle compte à l’heure actuelle un effectif de 10 personnes (Collège compris) dont 6 juristes et un ingénieur-informaticien .

Question 2 : Rôle joué par le Compliance Officer au sein des entités financières:

- a. Traitement des données ?
- b. Protection des données ?

Gérard Lommel : La loi modifiée du 2 août 2002 traduit en son article 4 la démarche de responsabilisation résultant de la directive 95/46/CE en ce qu'elle dispose que « le responsable du traitement doit s'assurer que les données à caractère personnel qu'il traite le sont loyalement et licitement. » Alors que le responsable du traitement est, aux termes de l'article 2, littéra **n** de la loi du 02 août 2002 telle que modifiée « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui détermine les finalités et les moyens du traitement de données à caractère personnel », l'article 40 de la même loi offre la possibilité à tout responsable de désigner un chargé de la protection des données, dont il communique l'identité à la Commission nationale. Sa mission consiste à conseiller (étant familier des processus internes ou consultant externe proche) l'entreprise qui l'a mandaté quant aux obligations en matière de protection des données en même temps que de surveiller le respect de la loi. Il est en liaison directe avec la CNPD pour s'accorder avec quant à l'interprétation des textes et constitue en quelque sorte son correspondant sur place qui assure un rôle de médiateur face aux réclamations et décharge cette dernière de l'examen en premier ressort des plaintes et vérifications de licéité.

Notre interlocuteur se dit d'emblée déçu par le peu d'engouement que la possibilité de pouvoir désigner leur « Compliance Officer » comme chargé de la protection a trouvé auprès des banques; à l'heure actuelle, seule une vingtaine d'instituts bancaires ont utilisé cette possibilité, ce qui est décevant alors qu'il s'agit pourtant d'un rôle naturel pour le « Compliance officer » et que des démarches dans ce sens avaient été faites notamment auprès de l'ABBL. Les banques allemandes semblent être parmi les plus favorables à la désignation du responsable « Compliance » comme chargé de la protection – ce dernier doit jouir d'une indépendance certaine et occuper un rang élevé dans l'organisation – son rôle ne doit d'ailleurs pas être vu comme étant celui d'un « policier » ou « espion » à l'intérieur de l'organisation; il s'agit plutôt pour le Président de la CNPD d'un interlocuteur privilégié qui parle le même langage que la CNPD qui s'impose également - lorsqu'un tel chargé de la protection est nommé - une certaine retenue -a priori pas de contrôle sur place pour les instituts disposant d'un chargé de la protection des données.

Question 3 : D'une façon générale, êtes-vous satisfait de l'attitude des entités sous votre surveillance vis-à-vis des directives de la CNPD ?

Gérard Lommel : Spécialement concernant le secteur bancaire, la collaboration peut être qualifiée de très bonne. Le Président de la CNPD cherche à avoir une attitude commerciale à ce niveau et de prêcher la bonne parole à chaque fois que l'opportunité se présente – encore récemment a-t-il ainsi participé à une réunion d'un groupe de travail des banques allemandes et il entend dorénavant encore renforcer son rôle de sensibilisation à tous les niveaux d'intervention. R. Diligent, le Président de la CNIL (homologue français) lui semble à ce niveau l'exemple à suivre – il le qualifie comme « bête de la communication » qui a grandement renforcé la visibilité de la CNIL en France.

A Luxembourg, ce n'est pas le secteur bancaire qui cause souci et il est toujours délicat de donner des exemples concrets de problèmes si ce n'est ceux qui ont déjà été amplement commentés dans les médias comme l'affaire de la Vidéo-surveillance du centre Aldringen, du Domaine Thermal de Mondorf, Auchan, Google, etc.

Au fond, la courte histoire de la CNPD peut se résumer en trois phases :

- dans une première phase elle a cherché à faire connaître la loi,
- la phase deux a consisté dans la mise en place du traitement des plaintes,

Le Bulletin

- aujourd'hui, la CNPD est en transition vers une phase trois qui va consister à accroître et améliorer la « guidance ».

Question 4 : Certaines entités considèrent que les restrictions imposées par la CNPD à l'enregistrement des communications téléphoniques, nuisent à leur sécurité.

Gérard Lommel : Il est vrai que la loi luxembourgeoise renferme des dispositions et procédures plus élaborées que celles de la plupart des autres Etats membres pour protéger l'employé. L'article 11 de la loi a d'ailleurs été intégré dans le Code du travail et le point de vue des syndicats a été largement pris en compte. Les cas d'ouverture sont énumérés limitativement et traduisent de façon un peu rigide les principes de nécessité, loyauté et proportionnalité prévus dans la directive pour la mise en balance des intérêts respectifs.

Si certains pensent que la loi est trop stricte, elle a quand même permis d'autoriser l'enregistrement des courriels, celui des communications téléphoniques (pour autant que cela soit motivé par des besoins de preuve).

Pour ce qui concerne la vidéo-surveillance, elle ne peut s'exercer en permanence sur le poste de travail des employés, mais elle est néanmoins autorisée dans les lieux à risque, entrées, sorties, passages et zones à risques,, etc...

Question 5 : Coordination de la CNPD et de la CSSF.

Gérard Lommel : Cette coordination a toujours été recherchée dans l'action de la CNPD mais il faut bien avouer que la perspective est parfois différente, compte tenu de la législation spécifique. Il arrive à chacune des deux Autorités de développer un point de vue qui lui est propre. La CSSF s'est montrée récemment plus ouverte à l'organisation du stockage de données dans les pays tiers.

Question 6 : Position relative de la CNPD avec ses homologues des pays européens (CNIL).

Gérard Lommel : La Directive Européenne n° 95/46 du 24 octobre 1995 organise dans son article 29 « un groupe de protection des personnes à l'égard du traitement des données à caractère personnel ». Ce groupe se compose d'un représentant de l'Autorité désigné par chaque Etat membre, ainsi que de représentants des institutions et organismes communautaires.

Ce groupe fonctionne de façon régulière et les différentes autorités nationales échangent leurs expériences et développent des positions communes favorisant l'application homogène de la directive à travers l'UE. Toutefois, certaines d'entre elles - on peut penser à la CNIL, par exemple - ont réussi à établir une visibilité qui renforce leur influence.

La coopération entre les autorités de protection des données des différents Etats membres a gagné de façon spectaculaire en importance ces dernières années avec la mondialisation et l'évolution technologique. Les difficultés de détermination de la loi applicable augmentent en parallèle avec celles de la détermination du lieu réel de traitement de l'information). En effet, il est bien difficile dans un réseau informatique de déterminer le « lieu » du traitement d'une information (prenez l'exemple du « cloud computing » ou simplement celui de sous-traitances en cascades. Ce problème est d'autant plus crucial que des pays tiers peuvent être concernés.

Enfin, d'une façon générale, les positions des différentes Commissions de protection des données des Etats membres sont très proches les unes des autres. On notera cependant des nuances

Le Bulletin

marquées entre certains pays d'Europe du Nord, le Royaume-Uni et la pratique dans certains domaines par rapport au reste de l'Union.

Rien que pour la notion de données à caractère personnel : la conception anglo-saxonne est cantonnée de façon plus restrictive à celle de données nominatives alors que nous retenons toute information susceptible d'être rattachée à une personne identifiable. Nous pensons cependant être capable aussi bien qu'eux de pragmatisme et d'attitude « business friendly » dès lors qu'il y a une réelle volonté de rechercher des solutions équilibrées tenant compte des attentes légitimes de respect de la vie privée des personnes.

Propos recueillis par Patrick Schott et Jean-Marie Legendre

Articles

Le nouveau dispositif anti-blanchiment « post-évaluation » du GAFI ou « la raison du plus fort est toujours la meilleure »¹

En mai 2009, une délégation du GAFI venait visiter le Luxembourg en vue d'évaluer son dispositif anti-blanchiment et d'en apprécier la conformité aux recommandations de cet organisme intergouvernemental. Le rapport qui en a résulté, publié en février 2010, a été assez médiocre, donnant des notes peu honorables : 9 « *non conforme* » et 30 « *partiellement conforme* », pour seulement 9 « *largement conforme* » et 1 « *conforme* ».

Compte tenu de la menace planant sur le Luxembourg d'une classification sur « liste grise » et des répercussions extrêmement néfastes d'une telle classification pour la place financière, le gouvernement luxembourgeois a déposé au mois d'août 2010 un projet de loi qui fut voté dès le 13 octobre 2010 par la Chambre des Députés. La loi du 27 octobre 2010 portant renforcement du cadre légal en matière de lutte contre le blanchiment et contre le financement du terrorisme a ainsi pour (unique) objectif de répondre aux critiques du GAFI. Il s'agit d'intégrer au dispositif luxembourgeois un ensemble d'amendements affectant pas moins de 21 lois différentes, aussi diverses que la loi du 7 mars 1980 sur l'organisation judiciaire, la loi modifiée du 31 janvier 1948 relative à la réglementation de la navigation aérienne, ou la loi modifiée du 20 avril 1977 relative à l'exploitation des jeux de hasard et des paris relatifs aux épreuves sportives.

1. Un texte mosaïque à visée cosmétique

Si le langage juridique paraît obscur à plus d'un, la lecture de la loi du 27 octobre 2010 n'y fait pas défaut. Elle apparaît comme un modèle de complexité, usant à souhait de renvois et de formules énigmatiques pour un non-initié. A titre d'exemple, l'article 5 de cette loi dispose : « *Dans le point 3) de l'article 8-1 de la loi précitée du 19 février 1973, la référence à « l'article 8 sous a) et b) » est remplacée par une référence à « l'article 8, paragraphe 1, a) et b) »* ». Le texte est en effet constitué d'une mosaïque de modifications sporadiques et en devient pratiquement illisible et incompréhensible pour le néophyte.

Cette curieuse technique législative tient en réalité à l'objectif avoué de cette loi, qui vise uniquement à adapter le dispositif législatif luxembourgeois en matière de lutte contre le blanchiment et le financement du terrorisme aux exigences du GAFI. Il suffit pour s'en convaincre de relever, dans le commentaire des articles du projet de loi, le nombre de dispositions dont la justification est : « *...vise à répondre aux critiques résultant des paragraphes [x,y,z] du rapport d'évaluation mutuelle* ».

Uniquement motivée par ce souci, cette loi n'apporte parfois rien au droit luxembourgeois. Il en est notamment ainsi lorsqu'elle se contente de donner un caractère légal à certaines positions jurisprudentielles bien établies. Ainsi, en vertu du nouvel article 506-8 du Code pénal, « *les infractions visées à l'article 506-1 sont punissables indépendamment de toutes poursuites ou condamnations pour une des infractions primaires de l'article 506-1* ». Il a pourtant toujours été clair selon les autorités et la jurisprudence luxembourgeoises que la preuve de l'infraction primaire

¹ Les opinions exprimées dans cet article sont personnelles et n'engagent que son auteur.

ne dépend pas d'une condamnation préalable et que l'infraction de blanchiment est bien une infraction autonome².

Pour citer un autre exemple, l'article 506-1 (2) du Code pénal est complété par une référence au «*déguisement*», de sorte que l'infraction de blanchiment est également celle par laquelle une personne apporte sciemment son concours à une «*opération de placement, de dissimulation, de déguisement, de transfert ou de conversion*» de biens, alors même que la notion de «*dissimulation*» recouvre logiquement celle de «*déguisement*».

Par ailleurs, pour ce qui concerne l'identification du bénéficiaire effectif, la loi requiert que les professionnels prennent des mesures «*raisonnables*» et non plus des «*mesures adéquates et adaptées au risque*» (article 4, point 8, de la loi du 27 octobre 2010). Citons encore le fait que les déclarations d'opérations suspectes doivent désormais être faites «*sans délai*» au lieu d'être faites «*promptement*» (article 4 point 20). Ces modifications purement cosmétiques n'auront en fait qu'un impact limité sur les pratiques des professionnels.

2. Confusion et incohérences

A l'heure de la simplification réglementaire, la loi du 27 octobre 2010 risque d'apporter confusion et incohérence à notre droit. Citons quelques exemples.

En premier lieu, le souci de satisfaire le GAFI conduit à des redondances entre lois différentes. Il est ainsi précisé que le secret professionnel n'est pas applicable à l'égard de la Cellule de renseignement financier (CRF) (nouvel article 5-4 de la loi modifiée du 12 novembre 2004). Cette disposition vise à souligner qu'aucun obstacle légal n'empêche les professionnels d'effectuer des déclarations d'opérations suspectes à la CRF. Or, en matière de coopération avec les autorités, le secret professionnel tombe en vertu de l'article 41(2) de la loi du 5 avril 1993 sur le secteur financier. Cette même précision est encore reprise à l'article 39 de la même loi afin de spécifier que la règle du secret professionnel tombe également lorsque les demandes des autorités portent sur «*les informations accompagnant les virements de fonds et les informations conservées correspondantes*». Nous retrouvons ainsi à trois endroits différents (dont deux fois dans la même loi) la règle selon laquelle les professionnels ne peuvent opposer leur secret professionnel aux autorités. Si cela devrait désormais paraître clair au GAFI, cela était néanmoins déjà une évidence pour les professionnels de la place.

En second lieu, une curieuse technique législative a conduit à faire modifier une même loi par deux textes différents. L'article 10 de la loi du 27 octobre 2010 vise à modifier l'article 3 de la loi du 8 août 2000 relative à l'entraide judiciaire de sorte que cette disposition vise les affaires qui sont exclusivement fiscales. Parallèlement, le même jour, la loi du 27 octobre 2010 en matière d'entraide judiciaire internationale en matière pénale réforme certaines dispositions de la loi du 8 août 2000, et en particulier ce même article 3, sans cependant que le mot «*exclusivement*» ne soit repris dans le texte. Il s'ensuit que nous sommes en présence d'un conflit de lois, deux lois datées du même jour changeant le contenu d'une même loi.

Par ailleurs, la technique législative utilisée par la loi du 27 octobre 2010 est assez surprenante et crée une nouveauté : la loi «*poupée-russe*». En effet, les articles 24 et 25 de cette loi institue ... deux nouvelles lois, celle du 27 octobre 2010 portant organisation des contrôles du transport physique de l'argent liquide entrant au, transitant par le ou sortant du Grand-Duché de Luxembourg, et celle relative à la mise en œuvre de résolutions du Conseil de Sécurité des Nations Unies et d'actes adoptés par l'Union européenne comportant des interdictions et mesures restrictives en matière financière à l'encontre de personnes, entités et groupes dans le cadre de la lutte contre le financement du terrorisme. Plutôt que de disposer de plusieurs lois distinctes et autonomes, nous sommes en présence de deux textes de loi imbriqués dans une troisième, la loi anti-blanchiment. Pourtant, ces textes forment un tout homogène et auraient pu être adoptés distinctement.

² Un arrêt de la Cour d'appel du 3 juin 2009 précise : «*...il n'est toutefois pas requis que l'auteur de l'infraction primaire ait fait l'objet de poursuites ou qu'il ait fait l'objet d'une condamnation identifiant le crime ou le délit à l'aide duquel les avantages patrimoniaux ont été obtenus*».

La loi du 27 octobre 2010, instituée par l'article 24 cité ci-dessus, vise à introduire des contrôles des mouvements d'argent liquide aux frontières du Luxembourg. Le règlement (CE) n° 1889/2005, considérant le territoire européen comme un ensemble, avait introduit ces contrôles aux frontières de l'Union européenne. La loi du 27 octobre 2010 est ainsi la négation même d'un espace commun européen, comme elle est aussi la négation du processus de Schengen et du principe de libre circulation des capitaux inscrit dans les traités fondateurs. Le GAFI oblige les Etats européens à revenir sur le processus engagé depuis des dizaines d'années et visant à créer un marché unique. Le GAFI se base à cet égard sur les faibles résultats des contrôles du trafic en provenance des Etats tiers : *« De juillet 2008 à mai 2009, seules 12 déclarations ont été enregistrées alors que plus de 1800 vols en provenance de pays tiers à l'Union européenne arrivent tous les ans au Luxembourg. Aucun cas de non-déclaration ou de fausse déclaration n'a été détecté et aucune saisie n'a été effectuée. Le nombre de déclarations étant particulièrement faible, l'équipe d'évaluation s'interroge sur la qualité de la mise en œuvre du dispositif et des contrôles réalisés afin de s'assurer du respect de l'obligation de déclaration ».*

3. Oserions-nous être « politiquement incorrect » ?

D'un point de vue strictement juridique, les normes édictées par le GAFI n'ont aucune valeur obligatoire en tant que telles, ni aucun effet direct. Elles ne trouvent pas leur place dans la hiérarchie des normes. Il s'agit de recommandations qui s'adressent aux Gouvernements. Ces recommandations ne s'adressent pas aux professionnels qui ne sont aucunement tenus par elles. Elles n'ont de valeur juridique que ce que les Etats veulent bien en faire, c'est-à-dire les transposer ou non dans leur droit interne. Toutefois, en raison des possibles sanctions assorties au défaut de prise en compte des règles du GAFI, les Etats ont tout intérêt à procéder à l'intégration des normes du GAFI dans leur ordre juridique interne. Précisons que la lutte contre le blanchiment et contre le financement du terrorisme en tant que telles ne sont nullement en cause ici, les professionnels ayant depuis fort longtemps introduit dans leurs procédures internes les moyens de prévention de la lutte contre ces fléaux.

Les conséquences économiques d'une non-conformité aux conclusions du rapport adopté en février 2010 par le GAFI sur le Luxembourg pourraient être dramatiques pour la Place financière. Pourtant, l'état du dispositif législatif luxembourgeois était en parfaite conformité avec la troisième directive européenne en matière de lutte contre le blanchiment et le financement du terrorisme (directive 2005/60/CE). En réalité, les textes communautaires apparaissent en décalage avec les normes du GAFI. A titre d'exemple, la troisième directive permet l'application de mesures simplifiées de vigilance dans certains cas particuliers. C'est ainsi que les établissements de crédit et établissements financiers situés dans les pays de l'Union européenne ou de l'Espace économique européen bénéficient d'un régime allégé. Le GAFI, considérant qu'il s'agit purement et simplement d'une exonération totale des obligations de vigilance, a estimé que ces règles ne sont pas en conformité avec celles du GAFI. Le rapport d'évaluation note que *« l'ensemble de ces dispositions envisage l'équivalence aux obligations en matière de lutte contre le blanchiment de capitaux et contre le financement du terrorisme du Luxembourg issues de la Directive communautaire. Elles ne visent pas les recommandations du GAFI qui constituent un standard plus élevé ».*

Précisons encore que ce ne sont pas uniquement les textes qui ont été évalués par le GAFI, mais également l'efficacité du système mis en place. Celle-ci est appréciée au regard d'un critère majeur : l'importance de la Place financière comparativement aux statistiques qui lui ont été présentées par les autorités. Le rapport relève en effet que *« compte tenu de l'importance de la place financière, l'absence de condamnations significatives au Luxembourg du chef de blanchiment est un élément non dissuasif pour les criminels ».* De même, en matière de lutte contre le terrorisme, le rapport note que *« l'efficacité du système n'a pu être testée en l'absence de poursuites du chef de financement du terrorisme ».* L'argument selon lequel le Luxembourg étant une place financière internationale, il n'existe pas d'affaire purement luxembourgeoise, mais uniquement des affaires forcément connectées à d'autres Etats, n'a pas pu convaincre le GAFI, ni l'argument selon lequel c'est grâce à une entraide judiciaire efficace et une coopération entre

Le Bulletin

autorités de différents Etats que certaines affaires ont pu être jugées ... mais dans un autre Etat que le Luxembourg.

Pour conclure, la loi du 27 octobre 2010 n'a pas révolutionné le dispositif législatif anti-blanchiment du Luxembourg. En réalité, le GAFI a essentiellement critiqué l'absence de preuve de l'efficacité des mécanismes de prévention du blanchiment au Luxembourg. Il s'est basé pour cela notamment sur le faible nombre de déclarations d'opérations suspectes effectuées par rapport au nombre d'institutions financières établies au Luxembourg.

Il importe d'être conscient que le GAFI s'attachera essentiellement à vérifier l'évolution par rapport à ces remarques, lors de la prochaine évaluation du Luxembourg dans le cadre du 4^{ème} Round d'évaluations mutuelles, qui devrait débiter en 2012. Le Luxembourg devra alors, avant toute autre chose, faire état de l'efficacité de son dispositif, si évaluation il doit y avoir... Pour rappel, le GAFI est un organisme intergouvernemental, créé par une déclaration économique du G7, et non par une Convention internationale liant des Etats entre eux. Son existence repose sur un mandat temporaire, d'une durée de 8 ans, qui expirera en 2012. *« Le plus fort n'est jamais assez fort pour être toujours le maître, s'il ne transforme sa force en droit, et l'obéissance en devoir »*, comme le disait Jean-Jacques Rousseau³.

Catherine BOURIN

Docteur en Droit

³ « Du Contrat social ».

Les risques de blanchiment dans le commerce électronique : quelques nouvelles techniques de blanchiment

De nos jours, les risques de blanchiment ne sont plus là où tout le monde les attend même si les secteurs les plus risqués restent les vendeurs automobiles, le secteur de la plaisance et de la navigation, de l'immobilier, les loteries et les jeux de hasard, les courses de chevaux et les casinos. Néanmoins, en parallèle de ces secteurs dits « traditionnels », il existe aussi de nombreux cas de blanchiment sur Internet. Le rapport d'activités 2007 de la Cellule de Renseignement Financier de Luxembourg cite parmi d'autres le cas d'une banque de la place dont l'activité principale est le paiement électronique : *« Dans les six derniers mois de l'année 2007, une banque a opéré quelques 112 déclarations à la CRF. Ce chiffre s'explique par l'activité particulière de cet établissement qui se déploie principalement dans les opérations financières liées au commerce électronique entre particuliers, et qui permet à ce professionnel d'avoir accès directement à des informations concernant l'opération sous-jacente à la transaction financière. Cet avantage est cependant mitigé par les difficultés existantes dans l'identification (même simplifiée) des acteurs au-delà du lien qui peut être établi entre un acteur et la carte bancaire utilisée pour l'opération ».*

Au-delà de la banque sur Internet et du porte-monnaie électronique, on a pu noter que le développement de la banque par téléphone et des casinos sur Internet pouvait faciliter les opérations de blanchiment. L'usage intensif des services bancaires téléphoniques 24 heures sur 24 crée un obstacle significatif pour les enquêtes en matière de blanchiment et de financement du terrorisme. En Asie, il est désormais possible de régler ses dépenses à l'aide de son téléphone portable soit en lecture optique soit en envoyant un SMS. Cette possibilité de paiement et donc de transaction financière peut être facilement exploitée par les réseaux criminels qui souhaiteraient blanchir de l'argent puisque la plupart des téléphones mobiles peuvent être rechargés par l'achat d'une carte de téléphone que l'on peut trouver quasiment partout, supermarché, station essence, librairie, etc. La transaction passe bien par le réseau de l'opérateur téléphonique mais l'achat de la carte elle-même peut être réglé en espèces à la caisse du magasin sachant qu'aucune identification préalable d'un tel type de téléphone n'est requise. En effet, il suffit de s'acheter un téléphone portable dans un supermarché et de se procurer une puce rechargeable à la caisse de ce même supermarché où personne ne vous demandera de vous identifier.

La banque directe implique l'installation d'une distance entre le banquier et son client, qui provoque une atténuation, voire même la disparition du contact physique entre eux sur lequel reposait la conception traditionnelle de l'identification et la connaissance du client. Si il est évident que ces services présentent des avantages pratiques pour les clients en terme de flexibilité, ils rendent plus difficile la détection des activités de blanchiment en l'absence d'application des méthodes de contrôle traditionnel. Au regard des informations disponibles sur Internet, des casinos de plusieurs pays proposent un anonymat complet aux joueurs potentiels, ces derniers effectuant leur mise grâce à leur carte de crédit. Le risque de blanchiment est encore plus patent si les casinos en question gèrent également les comptes de leurs clients ayant joué via Internet.

Les casinos et le secteur des jeux en général peuvent constituer un véritable sujet de préoccupation pour les autorités, car il s'agit d'un secteur en expansion qui est au centre du développement de l'industrie touristique dans de nombreux pays. Cependant, les conséquences de la multiplication des jeux hors casinos, et notamment leur développement sur Internet (comme le "Bingonet", par exemple) devraient faire l'objet d'analyses bien plus détaillées puisque la plupart

Le Bulletin

des casinos physiques sont eux, fortement règlementés⁴. Il en va de même pour les opérations commerciales qui sont effectuées sur Internet.

En effet, Internet peut favoriser l'anonymat de ses utilisateurs puisque dans certains cas, il suffit pour s'enregistrer de fournir une adresse électronique, celle-ci, ne garantissant pas du tout l'identité de l'utilisateur. Dès lors, chaque transaction qui aura lieu à l'aide de cette adresse sera complètement anonyme.

Les transactions électroniques les plus risquées sont celles qui seront directement effectuées entre utilisateurs notamment lorsque le vendeur et l'acheteur opèrent sur un site commercial électronique où il n'existe pas de dispositif de contrôle interne permettant de prévenir un risque de blanchiment d'argent ou de financement du terrorisme⁵.

Les méthodes de paiement les plus risquées qui sont actuellement utilisées sont les cartes de paiement prépayées offertes par de grands noms ou les chèques ou cartes cadeaux puisque ces méthodes offrent l'anonymat le plus complet à son utilisateur sachant que l'on peut se les procurer quasiment n'importe où et les régler en espèces. Il est important de noter que les sociétés qui offrent des services de paiement électroniques ont parfois des difficultés à distinguer une carte de paiement émise par une institution bancaire et une carte de paiement prépayée puisque les sociétés qui émettent des cartes de paiement utilisent souvent les mêmes numéros de cartes⁶.

Les sites commerciaux sur Internet ainsi que les moyens de paiement électroniques peuvent être utilisés pour vendre ou acheter des produits illicites comme de la drogue ou des articles de contrefaçon mais aussi pour éviter de payer des taxes (TVA ou impôt sur le revenu). Ils peuvent faciliter également la dissolution de l'argent collecté de manière illicite et ainsi faciliter le transfert des fonds vers un autre compte ou un autre pays ou tout simplement en procédant à d'autres achats sur Internet.

Les criminels peuvent aussi ouvrir leur propre site commercial sur Internet afin d'y vendre des produits illicites et utiliser un fournisseur de paiement électronique pour réaliser leurs transactions. Une autre possibilité consisterait à effectuer des opérations commerciales fictives entre deux sites commerciaux sur Internet sachant qu'il n'est pas obligatoire d'utiliser les services d'un fournisseur de paiement électronique pour ce faire, puisqu'il suffit simplement de lier un compte bancaire ou même de se faire payer par virement postal pour recevoir le paiement d'articles ou de produits fictifs qui ne seraient jamais livrés à leur acheteur. Il n'y aurait aucune plainte émanant de la partie acheteuse puisqu'il y a collusion entre les deux parties. Le bénéficiaire n'a pas de problème à expliquer la provenance des fonds reçus puisqu'ils proviennent d'une vente et l'acheteur justifie la dépense par un achat. Les sites commerciaux sur Internet autorisent des transactions pour des articles de grande valeur ce qui permet aux criminels de blanchir de fortes sommes d'argent rapidement. Ces mêmes criminels sont parfois même disposés à perdre un peu d'argent à des fins de blanchiment notamment en envoyant des émissaires acheter des produits de luxe payés en espèces qui seront ensuite revendus sur un site Internet à un prix très attractif pour faciliter l'écoulement de la marchandise.

Les exemples précédents permettent de démontrer qu'il est possible de blanchir des avoirs d'origine criminels sans nécessairement devoir passer par un établissement de crédit ou un professionnel du secteur financier. Les évolutions technologiques croissantes augmentent les possibilités de blanchiment pour les réseaux criminels qui souvent s'allient à des spécialistes de

⁴ Vulnerabilities of Casinos and Gaming Sector, March 2009, FATF Report

⁵ Money laundering & terrorist financing vulnerabilities of commercial websites and internet payment systems, FATF report

⁶ Money laundering & terrorist financing vulnerabilities of commercial websites and internet payment systems, FATF report

Le Bulletin

tous les domaines d'activités afin d'arriver à leurs fins et qui possèdent également de gros moyens financiers.

Sundhevy Goïot
May Controls Solutions S.A.
Sundhevy.goiot@maycoso.lu

Résumé des Tables Rondes

NOUVEAUX PRODUITS : Processus d'acceptation

Présents : 14 membres de l'ALCO

Référent : Tim Geyens, Head of Compliance Advice KBL & Group

Pour le GT 34 :

- Jean-Michel Righi, Société Générale, modérateur
- Charles van Doorslaer, KBL European Private Bankers, secrétaire

Introduction

Pour cette 3^e table ronde thématique de l'année 2010, 21 membres ont marqué leur intérêt et 14 d'entre eux se sont retrouvés pour aborder les problématiques liées au processus d'acceptation des nouveaux produits. Le panel était constitué de banquiers, asset managers, spécialistes fonds et assurances. La synthèse proposée vise à rappeler les principaux échanges.

Synthèse des réponses au questionnaire

Un questionnaire a été envoyé à tous les membres de l'ALCO en précisant que les réponses fournies serviraient de base à la discussion de la Table Ronde du 29 juin. Une synthèse des réponses aux 11 questionnaires qui ont été renvoyés complétés est mise à votre disposition ci-dessous. Les quelques grandes lignes qui ont pu en être dégagées ont été incluses dans le compte rendu. Certains éléments, tels que des exemples de définitions du concept 'nouveau produit/service' sont repris en annexe.

Pourquoi un Comité d'acceptation des Nouveaux Produits/services (CNP) ?

Le CNP est vu comme un **outil** fondamental pour la **gestion du risque**. Il peut être lié à l'ensemble du processus ICAAP⁷. C'est aussi et surtout un outil **de sensibilisation et de décision**, un forum qui permet aux intervenants de compétences variées de s'exprimer pour mieux expliquer et comprendre les approches et contraintes de chacun des services ou départements concernés. C'est aussi grâce à l'implication des participants à ce type de comité que s'instaure progressivement un climat de bonne coopération et de confiance entre les différents services ou départements concernés par de nouveaux produits/services.

C'est souvent à l'initiative de la maison mère qu'un process de CNP est mis en place, dans le cadre d'une politique de groupe.

Plusieurs participants confirment que dans leur établissement, ce type de comités est de création récente (moins de 2 ans). C'est souvent la crise financière, voire même un accident lié à un produit bien précis qui déclenche le besoin de créer un CNP ou de redonner vie à un comité ou un processus devenu une pure formalité, voire hélas tombé dans l'oubli. Dans bien des cas, ce CNP est une émanation du Comité de Direction, qui délègue à ce comité, constitué d'experts métiers, le pouvoir de valider ou non des nouveaux produits ou services. En cas de désaccord au sein du CNP, la décision pourra être 'escaladée' au Comité de Direction.

⁷ Internal Capital Adequacy Assessment Process (*Basel II*)

S'agit-il d'une instance formalisée au sein de l'établissement ? Une procédure spécifique encadre-t-elle son fonctionnement ? Timing ? Risques ?

La réponse est clairement « **oui !** » pour la grande majorité des participants. Toutefois, certains participent à la table ronde justement parce que la mise en place ou la formalisation d'un tel comité fait partie de leurs projets.

Généralement, l'initiative de présentation du produit/service est entre les mains de celui qui le crée. Le passage au CNP doit se faire le plus tôt possible dans le processus, avant la commercialisation. Cela permet d'améliorer le produit et/ou la façon dont il est décrit, grâce aux apports et questionnements d'autres départements. Des réticences peuvent exister. En effet, les créateurs peuvent craindre que soumettre un projet pour avis à un stade précoce augmente les critiques et ralentira le processus. Lorsqu'un produit très abouti est présenté au comité, cela peut permettre d'obtenir une décision plus rapide, voire de forcer celle-ci (« c'est à prendre ou à laisser ! », « Ce projet est le fruit de nombreuses heures de travail, alors... ne venez pas nous mettre des bâtons dans les roues avec des critiques qui ne sont pas 'vitales' ! »...)

Il s'agit donc de trouver le délicat équilibre entre la présentation d'un projet déjà suffisamment avancé que pour ne pas trop prêter le flanc à la critique et celle d'un produit pas encore finalisé, de sorte que des suggestions d'amélioration puissent encore être prises en compte.

Lorsque, dans certains cas, le processus de validation se clôture alors que la commercialisation du produit a déjà été lancée, le passage au CNP a surtout pour but de s'accorder sur un document final, comprenant non seulement les descriptions détaillées du produit et des documents commerciaux, mais aussi les diverses analyses de risque.

Quel est l'objet du CNP? Comment appréhender le concept 'nouveau produit/service'?

Les définitions et approches sont forcément différentes d'une entreprise à l'autre. Les réponses peuvent, en effet, varier considérablement en fonction de l'activité ou de la culture d'entreprise. Pour des exemples de **définitions** du concept, nous renvoyons le lecteur à l'annexe. Parmi les propositions, une définition très large est susceptible de contenter le plus grand nombre : « Tout produit ou service pour lequel une analyse de risque n'a pas encore été effectuée ou validée ».

Les **banquiers et gestionnaires** de fonds ont pour objectif de bien anticiper tous les risques que pourraient comporter les nouveaux produits et services qu'ils ont élaborés ou sélectionnés.

Les **assureurs** cherchent aussi (et surtout) à bien comprendre et cataloguer des produits existants, élaborés par leurs contreparties bancaires et autres. Il semblerait que c'est dans **l'activité OPC** que nous retrouvons la plus longue expérience, voire la meilleure organisation, en matière de processus d'acceptation. Du côté de la **clientèle privée**, les concepteurs et distributeurs de nouveaux produits et services semblent moins enclins à soumettre leurs créations au jugement de collègues d'autres entités.

Il est également intéressant de constater que, indépendamment du métier, **l'approche** peut être orientée « commercialisation » ou, inversement, « traitement opérationnel ». En effet, certaines institutions ressentent prioritairement le besoin d'être rassuré sur le fait qu'un produit et sa commercialisation ne risquent pas d'être critiqués, voire entraîner des plaintes auprès des autorités ou des condamnations devant les tribunaux. D'autres sont d'abord attentifs aux risques opérationnels : les systèmes, chaînes de traitements, l'infrastructure et le know how parviendront-ils à bien assumer le suivi de ces nouveaux produits/services. En effet, dans certains cas, ce ne sont pas tant les produits eux-mêmes qui engendrent un risque mais davantage la capacité qu'on a ou non à les traiter. Néanmoins, dans les deux cas, l'approche ne semble pas se limiter à une analyse '**technique**', mais semble toujours être voulue de façon '**globale**' ?

Les acteurs

Le responsable de **l'introduction d'un dossier** au CNP est en principe le métier concerné. Dans certains cas, c'est un département bien précis qui est désigné comme responsable du processus, par exemple le Marketing, la Compliance, le Risk Management, voire un service dédié.

La **composition des membres du CNP** peut être variable, en fonction des dossiers d'approbation qui sont à l'ordre du jour. Parmi les membres permanents, l'enquête indique clairement le Risk Management, le Juridique et la Compliance comme faisant partie du noyau dur. Ensuite nous retrouvons, dans la grande majorité des cas, la Direction, les 'opérationnels' (BO et MO) et l'IT.

La non-implication de la Compliance est, pour la plupart des établissements, une erreur du passé qu'il a fallu corriger. Il semble désormais acquis que la Compliance doit être intégrée au processus de façon permanente.

Qui en assure le secrétariat? Là aussi, les approches varient : un secrétariat permanent dédié au CNP dans un cas, une tournante parmi l'ensemble des participants dans un second cas, divers départements désignés (dont la Compliance, le Risk Management ou le Marketing) pour les autres.

Un des défis est la rapidité du processus de validation

Il peut être envisagé de créer **2 processus** différents : une validation **en séance plénière** (processus pouvant prendre du temps) ou une validation **rapide**, par voie circulaire.

Ce dernier procédé pourra permettre l'acceptation de plusieurs nouveaux produits par jour, grâce à l'utilisation de l'e-mail permettant une communication entre l'ensemble des membres du CNP. Elle est surtout utilisée dans l'hypothèse où le nouveau produit/service est proche d'un produit qui a déjà fait l'objet d'une validation, où il fait partie d'une famille existante de produits déjà passés en CNP. Le principal risque réside alors dans la modification d'un élément qui paraîtrait anodin de prime abord, mais qui pourrait néanmoins être un motif de refus.

A titre d'exemple, citons le cas d'un changement d'émetteur pour un sous-jacent inchangé. Si le rating et la réputation du nouvel émetteur sont bons, une acceptation sera obtenue sans difficultés. Par contre, s'il s'avère que le nouvel émetteur du produit structuré est aussi par exemple l'émetteur du sous-jacent, un conflit d'intérêt peut être invoqué pour refuser la modification.

Pour une prise de décision rapide et efficace, des **guidelines** peuvent être établies afin de faciliter la détection de cas 'borderline' pour lesquels la consultation préalable des membres du CNP est indispensable. Certaines règles de base peuvent être établies, comme par exemple faire un principe que l'émetteur du sous-jacent d'un produit ne puisse être le même que celui du produit lui-même, ou bien une règle qui exige que les produits dont les 'term sheets' sont difficiles à comprendre pour des professionnels ne puissent être commercialisés à des clients privés, ou encore, que les produits de type 'loterie' ne sont pas acceptés...

Certains évoquent aussi la possibilité d'un CNP très formaliste, ne se réunissant qu'une fois par trimestre. Pour satisfaire au besoin de rapidité et d'efficacité, d'autres démarches et réunions permettant des validations partielles devront alors être organisées entre les séances formelles. La réunion trimestrielle sert dans ce cas principalement à formaliser l'ensemble du processus, à ratifier les décisions (partielles) déjà prise en engageant la responsabilité du comité de direction.

Certains CNP se sont vu, à l'occasion de la crise, attribuer la tâche de passer **en revue la totalité des produits existants** (c.-à-d. encore présents dans les portefeuilles de clients) afin de réexaminer leur risque à la lumière des événements et problèmes mis à jour à l'occasion de la crise.

Processus décisionnel et formalisation

En général, les décisions sont prises à l'unanimité. Tous les participants doivent signer pour accord. Dans certains cas, l'accord peut être conditionné à l'une ou l'autre condition. Si l'unanimité ne peut être atteinte, il y a alors lieu d'escalader le dossier, soit au(x) responsable(s)

des participants qui ne parviennent pas à ce mettre d'accord, soit à la direction, ou encore auprès du CNP de la maison mère.

La prise de décision du CNP peut être formalisée de différentes façons et organisée par une procédure plus ou moins détaillée. Souvent la signature de l'ensemble des participants, voire des membres du CNP doit être apposée sur les documents descriptifs. Ensuite la décision est distribuée par e-mail aux membres du CNP ainsi qu'aux personnes concernées (p.ex. le comité de direction). Ces destinataires peuvent ensuite, à leur tour transmettre les décisions aux personnes intéressés. Quant au formalisme du document de décision lui même, chaque banque semble avoir ses propres habitudes en matière de structure, de forme et de contenu

Quel est le rôle du Compliance officer dans ce processus décisionnel?

Dans certains CNP, chaque participant est appelé à analyser, commenter le nouveau produit en se limitant à son strict périmètre. Dans d'autres, au contraire, chacun est amené à s'exprimer librement sur l'ensemble des aspects et des risques.

Il semble acquis que **le rôle principal de la Compliance** est d'analyser les risques de protection de l'investisseur (adéquation, suitability (caractère approprié), best execution, conflits d'intérêts...), de vérifier si la documentation destinée au client est compréhensible et transparente et respecte bien toutes les règles de présentation (en fonction des établissements, ce rôle peut être partagé avec le département juridique). La Compliance est aussi tenue de vérifier si le nom du produit ou sa description ne peut pas induire en erreur le client ou prêter à confusion et si, au niveau de l'éthique, des éventuels reproches ne peuvent engendrer un risque de réputation. Tant l'aspect réglementaire que le risque de réputation font donc partie des points sur lesquels le Compliance Officer est amené à s'exprimer.

Le Compliance Officer est-il aussi appelé à intervenir lorsque l'établissement agit pour son propre compte ? C'est beaucoup moins fréquent. Pourtant, ce pourrait être une plus-value certaine, surtout en matière de conflits d'intérêts, d'éthique, de réputation. Quelques grandes institutions financières prises dans les turbulences de la crise le regrettent probablement aujourd'hui.

Indicateurs de risque et classification du risque lié au Nouveaux Produits

A défaut d'une classification européenne unique, les produits sont classés en fonction de la zone géographique où ils sont distribués ou, à défaut, selon la classification utilisée par la maison mère. Les aspects suivants sont soulevés:

- Les indicateurs de risques les plus utilisés sont le niveau de protection du capital, le caractère complexe et le niveau de risque interne.
- « Le CNP doit-il se limiter à une approche purement technique du produit/service, ou doit-il avoir une approche globale »

D'un point de vue efficacité, ceci devrait être une approche globale mais trop souvent, l'approche est centralisée et puis « adaptée à la sauce locale ». Ceci peut entraîner l'apparition de nouveaux éléments de risques non-identifiés en amont.

- Le risque de réputation fait-il aussi l'objet d'une analyse par le CNP ?

Ce risque de réputation est particulièrement difficile à appréhender, à mesurer.

Un des participants mentionne un système de scoring qui permettrait d'évaluer le risque sur base des réponses à 6 ou 7 questions objectives (taille de l'émission, type de sous-jacent, émetteur, endroit de la commercialisation...).

D'autres évoquent une approche plus subjective, pouvant toutefois aussi aboutir en un critère d'élimination.

Perspective ‘Groupe’

Dans certains Groupes, le Comité Nouveaux Produits & Services a aussi pour tâche, de coordonner, voire diriger, la validation de nouveaux produits ou services des filiales/succursales. Les Chief Investments Officers des différentes entités du groupe sont alors amenés à participer au CNP et en tout cas à recevoir les ordres du jour et les PV/minutes afin d’être bien informés des débats et des orientations prises par le groupe. Les difficultés liées aux contraintes et spécificités locales restent le principal défi à relever.

Conclusion

Malgré le peu de réglementation en la matière, la plupart des participants ont confirmé qu’un CNP dument formalisé fonctionne bel et bien dans leur établissement. Toutefois certains d'entre eux sont justement présents parce que la mise en place ou la formalisation d’un tel comité fait partie de leurs projets. La table ronde constitue pour eux une occasion de glaner des idées et de mettre à profit l’expérience des institutions qui ont déjà mis en place un processus formalisé de CNP.

Pour bon nombre d’établissements, la non-implication de la Compliance dans le processus de validation est une erreur du passé qui a été corrigée. Il semble désormais acquis que la Compliance, au même titre que le ‘Risk Management’ et le département juridique, soit devenue incontournable dans ce processus.

La Compliance (ainsi que le juridique) qui pouvait dans le passé être parfois comme un "deal killer", n'est plus considérée comme tel aujourd'hui. Progressivement, un modus operandi satisfaisant s’est mis en place entre les départements commerciaux et de support. Au fil du temps, la preuve a pu être apportée que les questions soulevées par la Compliance ainsi que l’exigence d’une description plus détaillée et plus transparente des nouveaux produits n’en rendait pas la commercialisation plus difficile, bien au contraire. C’est souvent tout bénéfice pour le client, ainsi que ... pour le vendeur !

Les participants à la table ronde ont apprécié l’occasion de partager leurs questions, expériences et éléments de réponses avec des confrères. Nous tenons à les remercier pour les discussions ouvertes et leur participation active. Nous adressons un remerciement tout particulier à Monsieur Tim Geyens, qui, en tant que référent technique de nos discussions, a contribué à élever le débat et à l’agrémenter de nombreux exemples.

Au plaisir de vous retrouver nombreux à l’occasion de la prochaine table ronde !

Pour le GT 34 ‘Tables Rondes’, Charles van Doorslaer & Jean-Michel Righi

TABLE RONDE ALCO DU 29/06/2010 PROCESSUS D'ACCEPTATION DES NOUVEAUX PRODUITS

REponses AU QUESTIONNAIRE				
BANQUE	GESTION D'ACTIFS	ADM. DE FONDS	ASSURANCE	AUTRES
31,82%	27,27%	22,73%	9,09%	9,09%

EXISTENCE DU CNP	Oui
• Le concept de nouveau produit/service fait-il l'objet d'une approche structurée au sein de votre établissement?	90,9%
• L'acceptation en vue de commercialisation d'un nouveau produit/service fait-elle faire l'objet d'une validation formalisée selon une procédure bien établie?	90,9%
• Cette validation se fait-elle via un comité 'nouveaux produits/services' (CNP)?	81,8%
• Votre Direction supporte-t-elle l'analyse et le principe des CNP?	63,6%

FONCTIONNEMENT DU CNP	Oui
• Si un CNP est mis en place, quels en sont les membres permanents	
O Expert marchés	22,2%
O Commerciaux Banque privée	22,2%
O Gestion d'actifs	44,4%
O Marketing	22,2%
O Juridique	100,0%
O Risques	88,9%
O Compliance	100,0%
O Fiscaliste	33,3%
O middle/back office – operations	66,7%
O IT	77,8%
O Direction	66,7%
• Quels sont les produits/services nécessitant validation CNP?	
O Tous	55,6%
O Seuls ceux d'un nouveau genre	44,4%
• Quel est le rôle de la Compliance dans le CNP?	
O Donne son avis	77,8%
O Bénéficie d'un droit de veto	22,2%
O Peut déclencher procédure d'escalade	66,7%
• Le CNP se limite-t-il à une approche technique du produit/service, ou a-t-il une approche globale sur	
O Commercialisation cross-border ? Règles spécifiques ?	66,7%
O Conflits d'intérêts, rétrocessions, inducements ?	77,8%
O Offre publique vs offre privée?	44,4%
O Publication des Term Sheets sur internet, disponibilité libre en agence?	33,3%
O Analyse du marché secondaire, des possibilités de rachats ?	33,3%
O Suivi du produit pendant sa vie?	66,7%
O Y a-t-il un indicateur de risque sur les produits? Is there a risk indicator/ranking of the product?	66,7%
O Compatibilité avec les autres stratégies développées par la Banque (Gestion discrétionnaire, conseil?)	33,3%
O Ethique?	44,4%
O Analyse des émetteurs et contreparties??	66,7%
O Nom du produit, Qualité et transparence de l'information client?	88,9%
• Quels indicateurs de risques utilisez vous?	
O Niveau de protection du capital	55,6%
O Indicateur de risque interne	55,6%
O Volatilité	44,4%
O Liquidité	55,6%
O Classification complexe ou non complexe	55,6%
O Maturité	25,0%
• Qui est en charge de la préparation d'un dossier en vue de passage au CNP?	
O Métier concerné	62,5%
O Marketing	12,5%
O Compliance	12,5%
• Qui est en charge du secrétariat du CNP?	
O Compliance	25,0%
O Juridique	12,5%
O Risques	12,5%
O Autres (Métier concerné, Etudes et développement, Marketing...)	25,0%
• Les décisions des CNP sont-elles facilement disponibles à l'ensemble des départements/Services?	
O Oui	44,4%
O Non	33,3%
O Sur demande	22,2%

Scope d'un Comité Nouveau Produits - définition du concept « nouveau produit/service » Exemples de définitions puisés dans les questionnaires et illustrant la variété des approches

1. Pour les banquiers ou asset managers :

- concept très vaste, comprenant tout nouveau instrument ('dérivé', 'OPC' ou autre), stratégie d'investissement ou tout changement opérationnel significatif sur des produits existant...
- tous produits ou services qui élargissent la gamme existante ou qui feront l'objet d'opérations de marketing, de nouveaux contrats, de nouvelles facturations.
- tout produit ou service dont l'introduction entraîne un changement substantiel dans une chaîne.
- tout nouveau produit/service qui n'est pas dans le scope des activités habituelles
- tout produit ou service dont l'introduction entraîne un changement substantiel dans une chaîne de traitement (BO, IT, risk) ou dans le profil de risque du produit (complexité, risque financier...)
- tout instrument financier qui ne peut être considéré comme 'simple', c'est-à-dire les produits dérivés et/ou structurés (via OPC ou autres structures)

2. Pour les assureurs :

- produits et services et autres nouveautés en matière d'expertises de gestion, localisations, technologies, risques...
- nouvelles structures & produits d'assurance vie : comment les qualifier par rapport aux règles du CAA et éviter les différences d'interprétation entre acteurs bancaires et assurances. Par exemple, les ETF et ETC (Exchange Traded Funds, resp. Certificates). En cas d'une différence de point de vue entre banquier et assureur, comment concilier les deux visions dans le cadre des contrôles à mettre en place pour le respect des restrictions d'investissement ?

Exemples d'appellations d'organes qui valident les nouveaux produits et services :

- New Business Committee
- Comité de Construction de Produits et Services
- Comité pour l'Autorisation et la Supervision des Instruments Financiers⁸
- New Product Approval Committee
- Comité nouveaux Produits (éventuellement doublé d'un comité 'produits' plus formel et moins fréquent)

Exemple de questions qui se sont posées concernant les nouveaux produits et services

- Pouvons-nous donner à certains clients sélectionnés un accès aux travaux du département 'Recherche Financière Groupe' ?
- Pouvons-nous accepter de commercialiser en OTC⁸ des produits structurés à de clients privés ? Les contrats ISDA peuvent-ils s'appliquer à nos clients privés ?
- Pouvons-nous élargir la zone de distribution en incluant d'autres pays, le cas échéant hors Union Européenne ?

⁸ Over-The-Counter, c'est-à-dire négocié sur une base bilatérale avec des contreparties professionnelles ; en opposition avec ce qui est 'standardisé', coté en bourse 'exchange-traded'.

Mise en œuvre de l'approche risque en matière d'acceptation et de suivi des clients

Présents : 30 membres de l'ALCO, représentant tant les banques que les compagnies d'assurances ou les sociétés de gestion, répartis sur deux sessions.

Référent des 2 sessions : Patrick Schott que nous tenons à remercier tout particulièrement.

Pour le WG 34 :

- Pierre Hennericy, Banque Pictet & Cie
- Xavier Leydier, Banque Havilland
- Charles Van Doorslaer, KBL European Private Bankers
- Mike Sommer, Franklin Templeton

Rappelons que ce résumé des discussions n'a pas pour but de refléter des points de vue, mais seulement la teneur des discussions de compliance officers provenant de différentes professions du secteur financier.

Évolution de la législation luxembourgeoise

Depuis la première loi ayant traité de la lutte contre le blanchiment à Luxembourg en 1989, jusqu'à la loi du 27 octobre 2010, en passant par la loi du 12 novembre 2004⁹, la matière n'a cessé d'évoluer. Rappelons que la circulaire IML 89/57, introduisait déjà une petite révolution dans le monde financier luxembourgeois : elle obligeait notamment les institutions financières d'identifier leurs clients. Ensuite, après la création du GAFI à Paris en 1989 à l'initiative du G8, le monde financier n'a eu de cesse d'améliorer son arsenal réglementaire en matière de lutte contre le blanchiment. La dernière étape fut la 3^{ème} Directive de l'Union européenne n° 2005-60 transposée en droit luxembourgeois par la loi du 17 juillet 2008 et par la circulaire CSSF 08/387. La 3^{ème} Directive impose le critère de risque comme base de toute approche KYC et KYT¹⁰ et traite spécifiquement des Personnes Exposées Politiquement et de l'Ayant Droit Économique.

Dans son rapport sur le Luxembourg au printemps 2010, le GAFI déclare le Luxembourg comme non conforme en ce qui concerne l'application des 40 recommandations puisque seule une est reconnue comme entièrement remplie, 30 le sont partiellement et 9 ne le sont pas du tout. Afin d'éviter que des mesures ou sanctions soient prises à son encontre, le Luxembourg a adapté sa législation au pas de course, tout au long de l'année 2010.

Un règlement grand-ducal du 1^{er} février 2010 vise à renforcer et préciser certaines mesures existantes en matière d'**obligations incombant aux professionnels**, notamment concernant la surveillance transactionnelle et les mesures de vigilance à respecter;

La Loi du 3 mars 2010 introduit la **responsabilité pénale des personnes morales** et permet d'imposer des sanctions notamment aux sociétés, en cas d'infractions ;

La Loi du 27 octobre 2010 (et son Règlement d'exécution) rappelle l'obligation de respect des dispositions des Nations Unies et de l'UE en matière de mesures restrictives adoptées dans le cadre de la **lutte contre le financement du terrorisme** (gel des fonds, interdiction ou restriction des services financiers...).

⁹ <http://www.alco.lu/docs/docmembres/version coordonnée de la loi modifiée du 12 novembre 2004.pdf>

¹⁰ Know your customer & Know Your Transaction

Le Bulletin

La Loi du 27 octobre 2010 renforçant la **lutte contre le blanchiment** modifie 21 textes légaux. Elle s'articule principalement autour de dispositions d'ordre pénal et judiciaire (entraide, méthodes d'instruction...).

La nouvelle loi prévoit aussi de renforcer et de préciser les compétences des ordres professionnels, en tant qu'instances d'autorégulation (Chambre des notaires, Ordre des avocats, Ordre des experts-comptables, Institut des réviseurs d'entreprises). D'autres règles concernent l'introduction d'une obligation de déclaration de l'argent liquide entrant, transitant ou sortant du Luxembourg dès €10.000.

Le nouvel article 506-8 du Code pénal consacre le principe, d'ores et déjà acquis en jurisprudence, qu'une condamnation pour blanchiment ne requiert pas une condamnation ou des poursuites préalables pour l'infraction primaire dont proviennent les avoirs blanchis.

La nouvelle loi crée une obligation de poursuite et introduit la notion de « mini » instruction, une instruction qui doit allier rapidité et célérité par opposition à la lenteur de la traditionnelle instruction à charge et à décharge.

La CSSF peut désormais infliger des amendes administratives jusqu'à €250.000 en sus des éventuelles sanctions pénales. Les Douanes et Accises ont la responsabilité du contrôle des marchandises de grande valeur. La Cellule de Renseignement Financier (CRF) reste sous l'autorité du Parquet mais avec des moyens renforcés en personnel et avec une plus grande autonomie fonctionnelle.

En ce qui concerne l'Approche Risque, il n'y a pas de grande évolution dans cette dernière loi. Les PEP sont mieux définis notamment en ce qui concerne les liens familiaux à prendre en considération. La loi précise qu'il n'existe pas d'Approche Risque en matière de déclaration de soupçons. Les professionnels du Secteur Financier ont l'obligation de déclarer tout soupçon auprès de la CRF.

Par contre, la nouvelle loi demande une définition des risques en fonction du Business Model du Professionnel en fixant des critères quantitatif, géographique, pour les PEP ou encore pour les banques correspondantes (on notera ici que c'est une notion parfaitement théorique car aucune banque luxembourgeoise ne travaille avec des « Shell Banks »).

Tour de table et discussions

Un tour de table est organisé sur la base d'une série de quinze questions remise aux participants avant la Table Ronde (en annexe). Il est à signaler que le taux de retour fut particulièrement élevé. Nous remercions tous ceux qui se sont prêtés à l'exercice.

Les obligations AML incombant aux professionnels sont des obligations de moyen. Ceci implique que le professionnel doit pouvoir apporter la preuve d'avoir fait le nécessaire pour la mise en œuvre de ses obligations. Le régulateur doit quant à lui se donner les moyens de vérifier que les professionnels ont bien mis en place une organisation adaptée permettant de remplir l'ensemble de ses obligations (par exemple en matière de formation et de sensibilisation, de contrôles, de procédures, du système informatique....)

En matière d'AML, les compagnies d'assurances se retrouvent sur la même ligne que les banques. Elles se réfèrent à des circulaires CAA dont les textes sont similaires aux circulaires CSSF.

Pour les OPC, un problème particulier se pose lorsqu'ils font face à des nommées et plus particulièrement des nommées se trouvant dans des pays exotiques.

Le GAFI a rappelé qu'il n'est pas favorable à une liste des pays pratiquant des règles AML équivalentes. En effet, une telle liste peut créer une présomption de « good standing ». En conséquence, le Règlement Grand-ducal traitant de l'équivalence de contrôle a été abrogé et la circulaire CSSF 10/476 supprime l'équivalence de plein droit. Les pays de l'Espace Économique Européen sont quant à eux toujours considérés comme des pays à législation équivalente. Pour les autres pays, il y a donc lieu de procéder à un Risk Assessment et de pouvoir démontrer, dans ce

Le Bulletin

domaine aussi, le fait d'avoir rempli son obligation de moyen. La circulaire CSSF 10/469 donne, quant à elle, la liste des pays ne remplissant pas les obligations en matière de lutte contre le blanchiment dans laquelle figure la Grèce au côté de l'Angola, entre autres.

Mise en place d'une approche risque

L'intégralité des professionnels présents à la TR ont mis en œuvre une Approche Risque pour leurs nouveaux clients. Cette approche générale est malgré tout très diversifiée dans la pratique :

- Pour certains, il existe une exclusion d'office de certaines catégories de clients en fonction des lignes métiers exercées par le professionnel ;
- Pour d'autres, le profil attribué au client lors de l'entrée en relation est revu à la lumière des premières transactions effectuées auprès du professionnel ;
- Pour d'autres encore, le principe d'égalité de traitement est mis en œuvre et tous les prospects suivent le même circuit d'approbation pour devenir clients ;
- On va aussi trouver des compromis entre les exigences groupe et les exigences locales avec par exemple, la notion de risque 'pays' déterminée et gérée au niveau de la maison-mère et le risque 'activité' étant géré au niveau des filiales ;
- Certains professionnels doivent faire face aux exigences de leur maison-mère et se doivent de négocier pour mettre en œuvre des critères locaux qui peuvent être requis en fonction des différents métiers exercés par la filiale luxembourgeoise.

Exclusion – Refus de nouveaux clients

La question est de savoir sur quelle base refuser de nouveaux clients dans un contexte de plus en plus difficile. Soit on se limite aux marchés traditionnels, soit on s'ouvre aux nouveaux marchés que sont les pays émergents, l'Asie, la Russie,...

Dés lors, pour une ouverture aux nouveaux marchés, différentes questions se posent :

- Comment gérer les risques inhérents à la langue (lorsque les documents reçus ne sont pas dans une langue connue du professionnel), à l'activité (la distance permet-elle de vérifier l'activité ?), aux pratiques locales ?
- Comment gérer les moyens : qui récolte les informations ? Il s'agit d'un problème structurel. Le Front Office veut vendre, poussant les Middle Offices / Back Offices à affirmer leur rôle tout en leur demandant toujours plus d'implication dans les processus de Due Diligence.
- Comment éviter de trop avoir recours au « profilage » qui facilite l'analyse du prospect mais qui ne permet pas une analyse spécifique ?
- Le Compliance Officer peut-il suppléer aux Middle Office / Back Office pour assumer l'obligation de moyens ?
- Qui assure les suivis des contrôles afin de se préparer aux visites de la CSSF ?

L'utilisation d'une check-list servant de base pour une prise de décision quant à l'acceptation du prospect est abordée. Le danger de ce type de liste survient lorsqu'elle son utilisation devient trop automatique, trop routinière. Dans ce cas là, on pourrait avoir tendance à ne voir que ce qui figure sur la liste. Ce type de révision est différent d'un risk assessment qui se veut plus une « attitude » à avoir en fonction du cas présenté. Les dangers d'utiliser des outils non mis à jour sont aussi soulignés. Cela a pour conséquence d'induire en erreur l'utilisateur. La définition de l'activité du prospect est importante afin de pouvoir affiner l'activité du compte auprès du professionnel de façon à être en conformité avec la législation.

On souligne aussi le manque de recul et donc, le manque de repères historiques vis-à-vis des pays émergents ou vis-à-vis de pays dits « exotiques ». On constate qu'il n'existe pas de liste d'exclusion pour ces juridictions. L'approche risque se doit donc d'être une approche au cas par cas, dans la ligne de la politique du professionnel.

Comité d'acceptation

Le Bulletin

La notion de comité d'acceptation (CA) semble être un fait acquis pour la quasi-totalité des professionnels avec pour l'immense majorité des réunions physiques. Uniquement des dossiers complets semblent être soumis à la décision d'approbation.

Les petites structures, principalement des PSF, reconnaissent qu'un CA a souvent tendance à prendre ses décisions par la voie « circulaire ». La séparation des tâches telle qu'exigée par le régulateur n'est pas toujours aisée à respecter au sein des plus petites structures bénéficiant d'un agrément.

Le débat se porte aussi sur la participation ou non de la Compliance dans les CA et quel doit être la nature de son droit de vote. Le Compliance Officer doit-il bénéficier d'un droit de veto au sein des CA ? Différentes écoles sont représentées autour de la table :

- Des Compliance Officers disposant d'un droit de veto ; dans certains cas, on remarque que l'évolution vers le droit de veto du Compliance Officer se fait naturellement, en fonction des expériences passées vécues par le professionnel ;
- Des Compliance Officers ne disposant pas d'un droit de veto mais pour qui le mode de scrutin du CA exigeant une acceptation à l'unanimité lui accorde de facto un droit de veto, sauf lorsqu'il est absent et non représenté ; souvent si l'unanimité ne peut être atteinte, la décision est 'escaladée' à la direction
- Des Compliance Officers disposant d'un droit d'abstention noté au PV de la réunion du CA ;
- Des Compliance Officers disposant d'un « avis de réserve » ayant une valeur informative pour autres membres du CA ;

L'industrie des fonds d'investissement doit faire face à la problématique de la succession d'intermédiaire ou le changement d'intermédiaire. De plus, les critères nationaux locaux qui peuvent être différents des critères luxembourgeois rendent l'acceptation du client plus complexe. Les définitions des mots « apporteurs d'affaires » ou « intermédiaires » dans certains pays par exemple sont parfois non compatibles avec les définitions locales. Pour le professionnel, la question des limites de la délégation en matière d'identification se posent alors. Les participants reconnaissent que la nécessité d'avoir un contrat avec le tiers introducteur couvrant les questions d'AML y compris l'analyse de risque, s'impose à eux.

La notion de l'existence des comptes de passage

Cette notion semble en voie de disparition. La plupart des professionnels interdisent totalement leur utilisation pour la clientèle privée. L'utilisation de ces comptes se doit d'être documentée de façon exhaustive avec un vrai dossier de Due Diligence et d'analyse de risque et doit revêtir un caractère exceptionnel.

Analyse des Comptes dormants

Cette analyse est rendue difficile par l'absence de définition du terme « compte dormant ». Chaque professionnel choisit la durée qu'il estime convenir pour entrer dans sa définition du compte « dormant », souvent entre 6 et 24 mois, suivant la composition du portefeuille ou l'activité du client. Certains professionnels exigent de leur Front Office au minimum un contact direct avec le client durant l'année. D'autres demandent aux clients une certification des soldes sur base annuelle.

L'analyse des comptes dormants va de pair avec l'analyse des comptes ouverts et fermés dans le courant de l'année ou dans les 12 mois qui suivent leur ouverture.

Révision périodique des dossiers clients

Cette révision comprend habituellement non seulement l'examen de la documentation, mais aussi celui des transactions. Cet examen doit être effectué de manière plus ou moins poussée, conformément aux résultats de l'analyse de risque effectuée lors de l'entrée en relation avec le client. L'analyse des réponses du questionnaire a montré une grande disparité dans la fréquence des revues des comptes clients. En fait, tout dépend de la nature de l'activité du professionnel

(assurance, banque, PSF, société de gestion...) et du risque généré par l'activité du client. La revue se fait:

- sur la documentation fournie par le client / le gestionnaire au moment de l'entrée en relation ;
- sur l'adéquation de l'activité du client pendant une période donnée par rapport avec l'activité annoncée, décrite au moment de l'ouverture du compte.

Certains professionnels représentés à la Table Ronde ont déjà, pour faire face à l'urgence ou à l'ampleur de la tâche, opté pour une externalisation du travail de révision.

Certains professionnels disposent de logiciels générant des rappels, bloquants ou non, pour signaler la nécessité de la revue ou les documents à réactualiser.

Les PSF peuvent éprouver des difficultés à effectuer un suivi des transactions de leurs clients car elles n'ont pas autant de moyens que les banques. Les PSF se sentent parfois comme étant là pour documenter les banques et leurs Compliance Officers doivent sans cesse relever le défi de la charge de travail accrue qui leur est demandée.

La révision des dossiers conduit naturellement à la question du maintien de la relation client, en particulier dans le cas d'un changement d'activité brusque et sans rapport entre l'ancienne et la nouvelle, d'un profil non en adéquation avec le profil initial, d'une activité figurant sur une liste d'exclusion du professionnel... Les participants reconnaissent qu'une telle décision est du ressort du comité d'acceptation qui se doit alors de prendre position sur la poursuite ou non de la relation professionnelle.

Conclusion

Cette table ronde met en évidence que la notion de risque est une notion parfaitement intégrée dans notre métier. Il n'y a pas de réponse standard aux problématiques soulevées lors de cette table ronde, puisque la notion de risque est définie par chaque professionnel de la place en fonction de son métier, sa culture ou de son acceptation du risque. Les Compliance Officers reconnaissent leur rôle dans la mise en place de cette approche afin de remplir au mieux l'obligation de moyens qui s'impose aux professionnels.

La réunion a été appréciée pour avoir permis de confronter les points de vue et de mieux partager les interprétations et pistes de solutions, ce type d'exercice permettant à chacun de se « benchmarker » par rapport à la pratique professionnelle de la place.

© Groupe de Travail 34 « Tables rondes »¹¹

¹¹ Xavier Leydier, Charles van Doorslaer, Pierre Hennericy, Vincent Salzinger, Jean-Michel Righi, Eef Liesens, Mike Sommer,

Le Bulletin

Type d'institution :

Bank 11 Insurance Co. 2 Asset Mgt Company 7
Fund Administration Company 4 Other 4

Risk based approach : How is it implemented ?

Has you institution implemented a risk based approach process for accepting new

Yes 28 No 0

If yes, and should your institution belong to an international group, is a local process applicable?

Yes 16 No 12

Do you have to implement "group" critererias?:

Yes 16 No 12

Has your institution been granted with flexibility in the implementation of the

Yes 10 No 18

Is your risk based approach process

Yes 16 No 12

Static (independent criteria):

Yes 14 No 14

Matric (criteria having influence one to the other and to which some weighting

Does your institution apply for exclusion criteria to some potential new clients?

Yes 23 No 5

If yes, on which basis :

Geographical

Yes 20 No 8

Business/ occupation

Yes 11 No 17

Predicted activities with the institution

Yes 15 No 13

Origin of funds

Yes 20 No 8

Legal structure of the owner of the account

Yes 10 No 18

Other

Does your institution apply for a specific additional process to the potential new PEP clients at the time of entering into business relationship or specific regular controls to existing PEP clients?

Yes 25 No 3

Has a new client acceptance committee been implemented within your

Yes 20 No 15

If yes, what are the rules of such committee?:

Veto

Yes 10 No 18

Requirement of the unanimity of the committee members

Yes 7 No 21

Circular resolution

Yes 4 No 24

Resolution in formal meetings

Yes 15 No 13

Other

Yes 2 No 26

Are the following business lines part of the acceptance process?

Front

Yes 15 No 13

Executive Committee

Yes 24 No 4

Compliance

Yes 25 No 3

Other

Yes 7 No 21

In which way?

Are risk criteria applied in the review of the following accounts?:

Dormant accounts

Yes 16 No 12

Hold mail accounts

Yes 5 No 23

Pseudonyms' / numbered accounts

Yes 7 No 21

Transitory account (internal & external)

Yes 8 No 20

Are risk criteria applied to the documentation on which a decision is taken (Client Due diligence documentation)?

Yes 16 No 12

Type of criteria: authenticity, origin, language...

Is the review of the client files based on:

Geographical

Yes 18 No 10

Type of Business of the Ultimate Beneficila Owner / Client

Yes 18 No 10

Type of clients (individual, Corporation, trust, etc)

Yes 19 No 9

Type of transactions

Yes 14 No 14

Threshold of transactions

Yes 13 No 15

Mix of above

Yes 14 No 14

Vie associative

VIE ASSOCIATIVE

GROUPES DE TRAVAIL ACTUELS

Groupe de travail 11

Site Internet

Responsable Olivier GILSON
Téléphone +352 48 48 80 51 08
olivier.gilson@efa.eu

Groupe de travail 16

Commission permanente juridique et relations publiques

Responsables Claudine FRUTSAERT
Téléphone +352 44 24 24 43 15
claudine.frutsaert@axa.lu

Jean-Marie

LEGENDRE

Téléphone +352 24 67 26 07
Jean-Marie.LEGENDRE@ca-luxembourg.com

Groupe de travail 20

Funds practices and recommendations AML

Responsable Patrick Watelet
Téléphone +352 45-14-14-231
patrick.watelet@citi.com

Groupe de travail 21

Interprétation pratique des restrictions d'investissements de fonds

Responsable Tim WINFIELD
Téléphone +352 34 10 23 85
tim.winfield@jpmorgan.com

Groupe de travail 27

Formations IFBL

Coordinateur Sundhevy GOÏOT
Téléphone +352 621 30 23 63
sundhevy.goiot@maycoso.lu

Groupe de travail 29

Abus de marché

Coordinateur Cyril MATHIEU
Téléphone +352 40 46 46 400
cyrilmathieu@lu.hsbc.com

Groupe de travail 30

Domiciliation de société

ASSOCIATION ACTIVITIES

CURRENT WORKING GROUPS

Working group 11

Website

Owner Olivier GILSON
Phone +352 48 48 80 51 08
olivier.gilson@efa.eu

Working group 16

Legal and public relations

Owners Claudine FRUTSAERT
Phone +352 44 24 24 43 15
claudine.frutsaert@axa.lu

Jean-Marie

LEGENDRE

Phone +352 24 67 26 07
Jean-Marie.LEGENDRE@ca-luxembourg.com

Working group 20

Funds practices and recommendations AML

Owner Patrick Watelet
Phone +352 45-14-14-231
patrick.watelet@citi.com

Working group 21

Practical interpretation of fund investment restrictions

Owner Tim WINFIELD
Phone +352 34 10 23 85
tim.winfield@jpmorgan.com

Working group 27

Training IFBL

Coordinator Sundhevy GOÏOT
Phone +352 621 30 23 63
sundhevy.goiot@maycoso.lu

Working group 29

Market abuse

Coordinator Cyril MATHIEU
Phone +352 40 46 46 400
cyrilmathieu@lu.hsbc.com

Working group 30

Domiciliary agent

Le Bulletin

Coordinateur Sophie RASE
Téléphone +352 40 25 05 408
sophie.rase@maitlandgroup.com

Coordinator Sophie RASE
Phone +352 40 25 05 408
sophie.rase@maitlandgroup.com

Coordinateur Marie-Hélène CLAUDE
Téléphone +352 48 18 28 39 03
marie-helene.claude@alterdomus.lu

Coordinateur Marie-Hélène CLAUDE
Téléphone +352 48 18 28 39 03
marie-helene.claude@alterdomus.lu

Groupe de travail 33

Working group 33

Réponses aux questions des membres

Answers to questions of members

Coordinateur Carine VAN MULDER
Téléphone +352 47 97 28 15797 2815
CARINE.VAN-MULDER@kbl-bank.com

Coordinator Vincent WILLEM
Phone +352 49 924 3956
CARINE.VAN-MULDER@kbl-bank.com

Groupe de travail 34

Tables rondes

Working group 34

Round tables

Coordinateur Charles VAN DOORSLAER
Téléphone +352 47 97 39 09
charles.van-doorslaer@kbl-bank.com

Coordinator Charles VAN DOORSLAER
Phone +352 47 97 39 09
charles.van-doorslaer@kbl-bank.com

Groupe de travail 35

Doctrine

Working group 35

Doctrine

Coordinateur Guillaume BEGUE
Téléphone +352 26 96 22 31
guillaume.begue@bnpparibas.com

Coordinator Guillaume BEGUE
Phone +352 26 96 22 31
guillaume.begue@bnpparibas.com

MEMBRES ET VIE ASSOCIATIVE

MEMBERS AND ASSOCIATION ACTIVITIES

Nombre de membres (au 30/09/2010):

Banques	222
Fonds	93
Fonds / Banques	28
Assurances	58
Consultants / Réviseurs	35
Admin. et domiciliation de sociétés	17
Avocats	8
PSF	48
Gestion de fortune	22
Autres	14
Effectif total:	545

Number of members (as per 30/09/2010):

Banking sector	222
Funds sector	93
Funds / Banking sector	28
Insurance sector	58
Consultants / Auditors	35
Admin. and company domiciliation	17
Law firms	8
SFP	48
Asset management	22
Other	14
Total number:	545

Membres effectifs 440

Active members 440

Le Bulletin

Membres d'honneur	<u>105</u>	Honorary members	<u>105</u>
Effectif total:	545	Total number:	545
Réunions et activités:		Meetings and activities:	
Mensuellement	Réunions du conseil d'administration	Monthly	Board meetings
1 / 2 x par an	Réunions plénières	1 / 2 x per year	Plenary assemblies
2 / 3 x par an	Rencontres informelles autour d'un thème	2 / 3 x per year	Informal meetings on a subject

– Conseil d'administration:

Jean-Noël LEQUEUE	Président
Claudine FRUTSAERT	Vice-Président, section assurances
Patrick WATELET	Vice-Président, section fonds
Vincent SALZINGER	Vice-Président, section banques
Marie-Hélène CLAUDE	Trésorière
Guillaume BEGUE	Administrateur
Sundhevy GOÏOT	Administrateur
Jean-Marie LEGENDRE	Administrateur, Président honoraire
Custodio PORTASIO	Administrateur
Thierry GROSJEAN	Administrateur
Patrick SCHOTT	Administrateur
Olivier GILSON	Conseiller
Patrick CHILLET	Conseiller
Tim WINFIELD	Conseiller
Karine VILRET-HUOT	Conseiller
Benoît MARTIN	Conseiller
Rob Sonnenschein	Conseiller

– Secrétariat de l'ALCO:

Emilie Schmitt
secretariat@alco.lu
2 rue de l'Eau
L-1449 Luxembourg
Tél: 26-63-86-25

– Secrétariat du Bulletin:

Emilie Schmitt
secretariat@alco.lu

– Comité de rédaction:

Claudine FRUTSAERT (responsable), Patrick SCHOTT, Jean-Marie LEGENDRE, Julie BECKER, Leen BOM, Stefano PIERANTOZZI, Olivier GILSON, Jean-François PEMMERS, Sandra SIMON, Ingrid MALMEDY, Sundhevy GOÏOT, Karine VILRET-HUOT, Jean Noël LEQUEUE, les membres du GT 33 et du GT34

Le Bulletin

VISITEZ NOTRE SITE WEB : www.alco.lu