

Bulletin d'informations ALCO



Editorial par Jean-Marie Legendre, Président de l'ALCO

N°6 Oct. 05

La bonne santé du bulletin de l'ALCO ne se dément pas. Le nombre de visiteurs du site www.alco.lu qui viennent consulter le bulletin est resté élevé, y compris pendant les mois d'été. Aussi souhaitons-nous maintenir le rythme d'édition du bulletin à au moins trois numéros dans l'année.

Ce bulletin n° 6 comporte deux volets principaux :

Tout d'abord, Patrick Gouden de l'équipe Compliance de la KBL met en exergue les principaux points de la troisième Directive européenne sur la lutte anti-blanchiment. On voit que les textes luxembourgeois ont déjà bien anticipé, à différents égards, les dispositions de cette directive, même s'ils n'échapperont pas à un certain nombre d'ajustements.

A ce propos, signalons un événement réglementaire important dans le domaine de la lutte anti-blanchiment à Luxembourg avec la préparation d'une circulaire « coordonnée » de la CSSF.

Il s'agira d'une circulaire globale sur la lutte anti-blanchiment qui va rassembler les données aujourd'hui dispersées dans une vingtaine de circulaires émises sur le sujet. Ce sera un grand progrès pour les Compliance Officers qui sont chargés d'appliquer ces règles sur le terrain, et qui vont ainsi disposer d'une « bible » réglementaire sur ce qui est aujourd'hui leur premier domaine d'intervention.

Cette circulaire est conçue sur une base modulaire qui permettra sa mise à jour en continu. L'ALCO a été conviée, via plusieurs de ses membres, à participer à sa mise au point.

En deuxième partie, le bulletin propose un article de Benoît Martin sur la gestion du risque de réputation, sujet essentiel tant pour les différents acteurs du secteur financier, que pour la Place elle-même. Si le coût lié au risque de réputation n'est plus à démontrer, il reste nécessaire de réaffirmer qu'une bonne gestion de ce risque crée un cercle vertueux, « une force motrice majeure ».

Quelques nouvelles de l'activité de l'ALCO :

- *le Groupe de Travail 23 vient de publier son rapport sur la politique de compliance, document requis par la Circulaire CSSF 04/155. Gageons que ce texte fort intéressant, sera très utile aux Compliance Officers, et vient compléter les recommandations de l'ALCO après la publication du rapport sur la charte de compliance.*
- *Le Groupe de Travail 25 prépare une analyse comparative des fonctions de compliance, d'audit interne et de risk management. Un rapport sera publié, et une conférence organisée conjointement avec IACI et PRIM, si possible d'ici la fin de l'année.*
- *Le temps passe, et l'ALCO va célébrer son cinquième anniversaire. Retenez bien la date du 31 janvier 2006 pour cet événement !*

A bientôt, donc.

EN BREF

Actualités législatives

ACTUALITES DE DROIT COMMUNAUTAIRE

Le projet de troisième directive européenne relative à la prévention de l'utilisation du système financier aux fins de blanchiment de capitaux a été adopté le 7 juin dernier à Bruxelles, puis avalisé définitivement par le Conseil le 20 septembre dernier.

Cette directive, non encore publiée officiellement, vient consolider le système législatif en vigueur sur plusieurs points :

- intégration des quarante recommandations du groupe d'action financière (le GAFI) révisées en juin 2003 ;
- extension du champ d'application pour les professionnels concernés par la législation anti-blanchiment ;
- introduction d'obligations de vigilance renforcée dès lors que le risque de blanchiment est particulièrement élevé.

Le texte officieux du projet de directive peut être consulté sur le site de :

http://www.europa.eu.int/comm/internal_market/company/financial-crime

IN BRIEF

Legal Issues

AT COMMUNITARIAN LEVEL

The draft of the third EU's money laundering Directive regarding the prevention of the use of the financial system for the purposes of money laundering or terrorist financing has been adopted on June 7, 2005 in Brussels, .

This Directive, which has not been officially published yet, enhances the present legal system at several levels:

- Integration of the 40 recommendations of the Financial Action task Force (FAFT) revised June 2003;
- Extension of the scope of application for all professionals concerned by anti-money laundering laws.
- Introduction of enhanced customer due diligence measures whenever a situation presents a higher risk of money laundering

For further information, please check the unofficial version on the following website:

http://www.europa.eu.int/comm/internal_market/company/financial-crime

**Relevé des dispositions importantes
contenues dans le projet de 3^{ème}
directive européenne en matière de
lutte contre le blanchiment et le
financement du terrorisme**

1. Le financement du terrorisme est désormais visé au même titre que le blanchiment. L'activité criminelle de blanchiment comprend donc le financement du terrorisme.

2. Application à d'autres professions que les établissements financiers (*prestataires de services, sociétés et fiducies et aux intermédiaires en assurance vie, comptables, notaires, agents immobiliers, casinos, personnes négociant des biens pour un montant de plus de 15.000 € lorsque le paiement est réalisé en espèces, etc*).

3. Le blanchiment s'applique à toute participation criminelle à une infraction grave. Les infractions graves sont les suivantes : terrorisme / stupéfiants / organisation criminelle / fraude grave contre les intérêts financiers de la Communauté européenne / corruption / infractions punies d'une peine privative de liberté d'une durée maximale supérieure à 1 an, (*c'est à dire toutes les infractions sanctionnées par une peine d'emprisonnement dont le seuil maximum dépasse 1 année ; les peines dont le minimum est inférieur à une année et le maximum est 1 année ou moins ne sont pas visées*).

4. Les personnes physiques et morales qui exercent une activité financière occasionnellement ou à une échelle limitée pourront ne pas être concernées par ces dispositions si les Etats membres le décident.

5. Définition de l'ayant droit économique :

a) sociétés:

- la ou les personnes physiques qui, en dernier lieu, possèdent ou contrôlent au moins 25 % d'une entité juridique du fait qu'elles possèdent ou contrôlent directement ou indirectement un pourcentage suffisant d'actions ou de droits de vote dans cette entité juridique, y compris par le biais d'actions au porteur. Les sociétés admises à la côte officielle d'une bourse de valeurs ne sont pas concernées ;

- la ou les personnes physiques qui détiennent ou contrôlent au moins 25 % d'une des entités juridiques suivantes :

b) fondations / fiducies : dispositif juridique similaire ;

- Toute personne physique au nom de laquelle une transaction est exécutée ou une activité réalisée;

6. Les personnes politiquement exposées sont définies comme les personnes physiques qui détiennent ou se sont vues confier une fonction publique importante et qui effectuent des transactions commerciales ou financières importantes ou complexes ainsi que les membres de la famille proche ou les proches associés de telles personnes.

7. Interdiction de tenir des comptes ou des livrets anonymes ou des noms fictifs.

8. Obligation d'avoir des procédures de vigilance à l'égard de la clientèle et de les appliquer dans les situations suivantes:

a) entrée en relation d'affaires ;

b) transactions occasionnelles de 15 000 € au moins (en une fois ou sous la forme d'opérations fractionnées, mais liées);

c) lorsqu'il y a suspicion de blanchiment de capitaux ou de financement de terrorisme, indépendamment de tout seuil ;

d) lorsqu'il existe des doutes concernant la véracité ou la pertinence des données précédemment obtenues aux fins de l'identification d'un client.

9. En ce qui concerne les obligations de vigilance à l'égard de la clientèle, la directive prévoit des dispositions générales,

des dispositions simplifiées et des dispositions renforcées.

10. Obligations générales de vigilance :

- a) identifier le client et vérifier son identité,
- b) le cas échéant, identifier l'ayant droit économique et prendre des mesures adéquates et adaptées au risque pour vérifier son identité, de manière à avoir l'assurance de connaître ledit ayant droit économique. Pour les personnes morales, les fiducies et les dispositifs juridiques similaires, cela implique de prendre des mesures raisonnables pour comprendre la structure de propriété et de contrôle du client;
- c) obtenir des informations sur l'objet et la nature envisagée de la relation d'affaires;
- d) soumettre la relation d'affaires à une vigilance constante par un contrôle sur les transactions et sur l'origine des fonds, vérifier que ces transactions sont conformes à la connaissance qu'on a de son client, de ses activités commerciales et de son profil de risque, et en tenant à jour les documents, données ou informations détenues ;

Ces obligations de vigilance peuvent être ajustées selon le risque associé au type de client, de relation d'affaires, de produit ou de transaction concernés.

f) la vérification de l'identité du client et de l'ayant droit économique a lieu avant l'établissement d'une relation d'affaires ou lors de l'exécution d'une transaction ou, par dérogation, durant l'établissement d'une relation d'affaires s'il est nécessaire de ne pas interrompre l'exercice normal des activités et lorsqu'il y a un faible risque de blanchiment de capitaux ou de financement du terrorisme. Un compte bancaire peut être ouvert avant, à condition que des garanties suffisantes soient mises en place afin d'assurer que les transactions financières ne soient pas réalisées pour le client avant conformité totale avec les exigences d'identification.

g) ces procédures de vigilance s'appliquent à l'égard des nouveaux clients, mais aussi, à des moments opportuns, à la

clientèle existante en fonction de leur appréciation des risques.

11. Obligations simplifiées de vigilance à l'égard de la clientèle

a) Ces exigences ne s'appliquent pas lorsque le client est une personne ou un établissement relevant de la directive, ou lorsque le client est une personne ou un établissement établi dans un pays tiers et qui y est soumis à des obligations équivalentes à celles prévues par la directive, et dont le respect fait l'objet d'une vérification.

b) Les États membres peuvent autoriser les établissements et personnes relevant de la présente directive à ne pas appliquer les obligations de vigilance à l'égard de la clientèle aux clients représentant un faible risque de blanchiment de capitaux, tels que:

- Les établissements de crédit et autres établissements financiers des États membres ou de pays tiers soumis à des exigences de lutte anti-blanchiment ;

- Les sociétés cotées dont les valeurs sont admises à la négociation sur un marché réglementé dans un État membre ou dans un pays tiers soumis à des exigences de publicité compatibles avec la législation communautaire;

- Les ayants droit économiques de comptes groupés tenus par des notaires ou des membres d'une autre profession juridique indépendante établis dans un État membre ou un pays tiers, sous réserve qu'ils soient soumis à des exigences de lutte anti-blanchiment;

- Les polices d'assurance vie dont la prime annuelle ne dépasse pas 1000 € ou dont la prime unique ne dépasse pas 2500 €;

- Les contrats d'assurance retraite qui ne comportent pas de clause de rachat et qui ne peuvent être utilisés en garantie;

- Les régimes de retraite ou dispositifs similaires versant des prestations de retraite

aux employés, pour lesquels les cotisations se font par déduction du salaire et dont les règles ne permettent pas aux bénéficiaires de transférer leurs droits;

- La monnaie électronique : si le support ne peut pas être rechargé, la capacité maximale de chargement du support ne doit pas être supérieure à 150 EUR; si le support peut être rechargé, une limite de 2 500 EUR est fixée pour le montant total des transactions dans une année civile, sauf lorsqu'un montant d'au moins 1 000 EUR est remboursé dans la même année civile par le porteur;

L'établissement recueille en toutes circonstances des informations suffisantes pour établir si le client remplit les conditions requises pour une telle dérogation.

12. Obligations de vigilance renforcées à l'égard de la clientèle

- a) Les établissements et les personnes qui relèvent de la directive doivent appliquer, en fonction de leur appréciation du risque, des mesures de vigilance renforcées à l'égard de la clientèle, dans les situations qui par leur nature peuvent présenter un risque élevé de blanchiment et de financement du terrorisme et notamment :

- Lorsque le client n'est pas physiquement présent aux fins de l'identification, il y a lieu d'appliquer les mesures suivantes :

- l'identité du client est établie au moyen de documents, données ou informations supplémentaires;
- vérification ou certification des documents fournis ou attestation de confirmation de la part d'un établissement financier ou de crédit relevant de la directive;
- le premier paiement des opérations doit être effectué via un compte ouvert au nom du client auprès d'un établissement de crédit.

- En cas de relation transfrontalière de correspondant bancaire avec des

établissements correspondants de pays tiers, les États membres exigent de leurs établissements de crédit:

- qu'ils recueillent sur l'établissement client des informations suffisantes pour comprendre la nature de ses activités et pour apprécier, sur la base d'informations accessibles au public, sa réputation et la qualité de la surveillance dont il fait l'objet;

- qu'ils évaluent les contrôles anti-blanchiment et le financement du terrorisme mis en place par l'établissement client;

- qu'ils obtiennent l'autorisation de l'encadrement supérieur avant de nouer de nouvelles relations de correspondant bancaire;

- qu'ils précisent par écrit les responsabilités respectives de chaque établissement;

- concernant les comptes de passage, qu'ils s'assurent que l'établissement de crédit client a vérifié l'identité des clients ayant un accès direct aux comptes de l'établissement correspondant et a mis en œuvre des mesures de vigilance constante ;

- En ce qui concerne les relations d'affaires avec des personnes politiquement exposées, les États membres exigent des établissements et personnes relevant de la présente directive:

- qu'ils disposent de procédures adaptées au risque afin de déterminer si le client est une personne politiquement exposée;

- qu'ils obtiennent l'autorisation de l'encadrement supérieur avant de nouer une relation d'affaires avec de tels clients;

- qu'ils prennent toute mesure raisonnable pour établir l'origine du patrimoine et l'origine des fonds ou qu'ils assurent une surveillance continue.

Interdiction d'avoir des relations de correspondant bancaire avec une banque fictive.

13. L'exécution des obligations d'identification peut être déléguée à un tiers (établissement ou personne relevant de la directive ou établissement ou personne équivalents situés sur le territoire d'un pays tiers qui remplissent certaines conditions). La responsabilité finale de l'exécution des obligations continue cependant d'incomber au déléguant.

14. Les États membres s'informent mutuellement et informent la Commission des cas où ils estiment qu'un pays tiers remplit les conditions relatives aux obligations équivalentes.

15. Obligation d'accorder une attention particulière à toute transaction complexe ou d'un montant inhabituellement élevé, ainsi qu'à tous les types inhabituels de transactions n'ayant pas d'objet économique apparent ou d'objet licite visible.

16. Exigence de coopération avec les autorités nationales.

17. Aucune responsabilité en cas de déclaration de bonne foi d'un soupçon de blanchiment.

18. Interdiction de divulguer au client une déclaration de soupçon de blanchiment. Dissuader un client de prendre part à une activité illégale, n'est pas considéré comme une divulgation.

19. Obligation pour les établissements financiers d'avoir des systèmes permettant de répondre rapidement à une demande d'informations de la cellule de renseignements.

20. Obligation de mettre en place des mesures adéquates et appropriées en matière de vigilance à l'égard du client, de déclaration, de conservation des documents et pièces, de contrôle interne, d'évaluation et de gestion des risques et de communication, afin de prévenir et d'empêcher les opérations de blanchiment de capitaux.

21. Obligation de sensibilisation et de formation continue du personnel.

22. Les établissements et les personnes visés par la directive devront avoir accès à des informations actualisées sur les pratiques de blanchiment et de financement du terrorisme. Chaque fois que possible, ils devront bénéficier en temps opportun d'un retour d'information sur l'efficacité des déclarations de soupçons et sur les suites données à celles-ci.

23. Les autorités compétentes doivent disposer de pouvoirs renforcés en matière de surveillance et notamment de la possibilité d'effectuer des inspections sur place.

24. Les États membres doivent veiller à ce que les personnes physiques et morales soumises à la directive puissent être tenues responsables des violations des dispositions nationales adoptées conformément à la directive. Une personne morale doit pouvoir être tenue pour responsable en cas de défaut de surveillance ou de contrôle de la part d'un représentant de la personne morale ou de toute autorité qui a pouvoir de décision ou de contrôle au sein de la personne morale.

25. Les États membres doivent veiller, à ce qu'une personne morale tenue pour responsable d'une infraction aux obligations en matière de conservation des documents et pièces, d'identification des clients et de déclaration des transactions suspectes soit passible de sanctions efficaces, proportionnées et dissuasives puissent être infligées.

26. Les États membres peuvent arrêter ou maintenir en vigueur des dispositions plus strictes pour empêcher le blanchiment de capitaux et le financement du terrorisme

27. La date de publication dans le JO des CE est prévue courant le dernier trimestre 2005. A partir de cette date les Etats auront deux ans pour transposer la directive dans leur droit national.

Patrick GOUDEN

**Main important measures in the
European Union's Third Money
Laundering and terrorist financing
draft Directive.**

1. Terrorist financing is included within the money laundering provisions.

2. The Directive applies also to other professions than the financial institutions (company service providers, life insurance intermediaries, companies and fiduciaries, real estate agents, casinos, persons trading in goods only to the extent that the payments are made in cash in an amount of EUR 15 000 or more)

3. Any serious crime or any participation in criminal activity shall be regarded as money laundering. Serious offences are: terrorist financing / drug offences/ criminal organisations / serious crimes against the European Community's financial interests / corruption / offences that are punishable by deprivation of liberty for a maximum of more than one year, (i.e. all offences which are punishable by deprivation of liberty the maximum of which is more than one year; offences that are punishable for a minimum of one year and for a maximum of one year or less are not concerned).

4. If the Member States decide so, legal and natural persons who engage in a financial activity on an occasional or very limited basis may not fall within the scope of the Directive,

5. Definition of the beneficial owner:

a) In the case of corporate entities

- The natural person (s) who ultimately owns or controls 25 % of a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights in that legal entity, including through bearer share holdings.

- The natural person(s) who owns or controls at least 25 % of one of the following legal entities:

b) foundations / fiducies :

- Any natural person on behalf of whom a transaction is made or an activity is performed.

6. Politically exposed persons are defined as natural persons who are or have been entrusted with prominent public functions and make either large or complex corporate of financial transactions) as well as immediate family members, or persons known to be close associates of such persons.

7. Prohibition to keep anonymous accounts or anonymous passbooks or fictitious names.

8. Mandatory customer due diligence measures in the following cases:

a) When establishing a business relationship;

b) When carrying out occasional transactions amounting to EUR 15 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

c) When there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold.

d) When there are doubts about the veracity or adequacy of previously obtained customer identification data.

9. As far as customer due diligence is concerned, the Directive foresees general provisions, simplified customer due diligence and enhanced customer due diligence.

10. Customer due diligence measures shall comprise:

a) Identifying the customer and verifying the customer's identity.

b) Identifying, where applicable, the beneficial owner and taking risk-based and adequate measures to verify his identity so that the institution or person covered by this

Directive is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts and similar legal arrangements taking risk-based and adequate measures to understand the ownership and control structure of the customer.

c) Obtaining information on the purpose and intended nature of the business relationship;

d) Conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's or person's knowledge of the customer, the business and risk profile, including, where necessary, the source of funds and ensuring that the documents, data or information held are kept up-to-date.

e) These customer due diligence requirements can be adjusted depending on risk depending on the type of customer, business relationship, product or transaction.

f) The verification of the identity of the customer and the beneficial owner takes place before the establishment of a business relationship or the carrying out of the transaction and by way of derogation during the establishment of a business relationship if this is necessary not to interrupt the normal conduct of business and where there is little risk of money laundering or terrorist financing occurring. A bank account can be opened provided that there are adequate safeguards in place to ensure that transactions are not carried out by the customer until full compliance with the identification obligations is obtained. (35)

g) These procedures apply not only to all new customers but also at appropriate times to existing customers on a risk-sensitive basis.

11. Simplified Customer due diligence

a) Those customer due diligence measures do not apply where the person is a credit or financial institution covered by this Directive, or where a credit or financial institution situated in a third country which

imposes requirements similar to those laid down in this Directive and supervised for compliance with those requirements.

b) Member States may allow the institutions and persons representing a low risk of money laundering covered by this Directive not to apply customer due diligence in respect of:

- Credit and financial institutions of Member States or of third countries that impose anti-money laundering requirements.

- Listed companies whose securities are admitted to trading on a regulated market in a Member State or in a third country which are subject to disclosure requirement consistent with Community legislation;

- Beneficial owners of pooled accounts held by notaries and other independent legal professionals from the Member States, or from third countries, provided that they are subject to requirements to combat money laundering or terrorist financing.

- Life insurance policies where the annual premium is no more than EUR 1 000 or the single premium is no more than EUR 2 500.

- Insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral.

- A pension or similar scheme that provide retirements benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme.

- Electronic money: if the device cannot be recharged, the maximum amount stored in the device is no more than EUR 150; if the device can be recharged, a limit of EUR 2 500 is imposed on the total amount transacted in a calendar year, except when an amount of EUR 1 000 or more is redeemed in that same calendar year by the bearer.

The institution gathers in any circumstances sufficient information to ensure whether the client meets the required conditions pour such derogation.

12. Enhanced customer due diligence.

a) The institutions and persons covered by this Directive have to apply on a risk-sensitive basis, enhanced customer due diligence measures, in situations which by their nature can present a higher risk of money laundering or terrorist financing.

- Where the customer has not been physically present for identification purposes, the following measures shall be applied:

- Ensuring that the customer's identity is established by additional documents, data or information ;

- Supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution covered by this Directive;

- Ensuring that the first payment of the operations is carried out through an account opened in the customer's name with a credit institution.

- In case of cross-frontier correspondent banking relationships with respondent institutions from third countries, Member States shall require the credit institutions to:

- Gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision.

- Assess the respondent institution's anti-money laundering and anti-terrorist financing controls.

- Obtain approval from senior management before establishing new correspondent banking relationships.

- Document the respective responsibilities of each institution.

- In respect of transactions or business relationships with politically exposed persons, Member states shall require those institutions and persons covered by this Directive to:

- have appropriate risk-based procedures to determine whether the customer is a politically exposed person ;

- have senior management approval for establishing business relationship with such customers ;

- take adequate measures to establish the source of wealth and source of funds that are involved in the business relationship or transaction or that they conduct ongoing monitoring of the business relationship;

e) Prohibit any correspondent banking relationship with a shell bank.

13. The customer due diligence procedures can be delegated to a third party (institution or person covered by this Directive or equivalent institutions or persons situated in a third country who meet certain requirements). The ultimate responsibility for the customer due diligence procedure remains with the institution or person to whom the customer is introduced.

14. The Member States shall inform each other and the Commission of cases where they consider that a third country meets the conditions regarding the equivalents customer due diligence measures.

15. Obligation to pay special attention to any complex or unusually large transactions and all unusual patterns of translations which have no apparent economic or visible lawful purpose.

16. Requirements to cooperate with the national authorities.

17. No liability in case of disclosure in good faith of suspicious transactions.

18. Prohibition to disclose reports of suspicions of money laundering to the client. Seeking to dissuade a client from engaging in illegal activity shall not constitute a disclosure.

19. Financial institutions are required to have systems in place that enable them to respond rapidly to requests for information from the financial intelligence unit.

20. Obligation to establish adequate and appropriate procedures of customer due diligence, risk assessment, risk management, compliance management and communication, in order to forestall and prevent operations related to money laundering or terrorist financing.

21. Obligation to conduct ongoing training programmes as regards employees to help them recognise operations which may be related to money laundering or terrorist financing.

22. The institutions and persons covered by this Directive shall have access to up-to-date information on the practices of money launders and terrorist financiers etc. Member States shall ensure that timely feedback on the effectiveness of and on follow up to reports of suspected money laundering is provided. (58)

23. Competent authorities shall have enhanced supervisory powers, notably the possibility to conduct on-site inspections.

24. Member states shall ensure to natural and legal persons covered by the Directive can be held liable for infringements of the national provisions adopted pursuant to this Directive. The Member States shall ensure that legal persons can be held liable where a lack of supervision or control by a representative of the legal person or by any authority taking decisions on behalf of the legal person or exercising control within the legal person is reported.

25. Member States shall ensure effective, proportionate and dissuasive administrative penalties are imposed to all natural person held liable for infringing customer identification obligations, record keeping requirements and suspicious transactions reporting.

26. The Member States may adopt or retain in force stricter provisions to prevent money laundering and terrorist financing.

27. Member States will have two years, from the date of official publication which is scheduled for the end of 2005, to transpose the Directive into national law.

Traduction du Bulletin ALCO

La gestion du risque de réputation

La réputation de l'entreprise est un facteur déterminant de son succès commercial. C'est un actif essentiel de toute société. Elle doit être gérée et protégée.

Les deux choses les plus importantes n'apparaissent pas au bilan de l'entreprise : sa réputation et ses hommes. Henry Ford

La Commission de Surveillance du Secteur Financier considère le Compliance Officer comme un acteur essentiel de cette gestion. Elle l'indique dans sa circulaire 2004/155, tel que ci-dessous, en incluant le risque de réputation dans la notion de risque de Compliance.

« 10. Par risque de Compliance on entend le risque de préjudices qu'un établissement peut subir suite au fait que les activités ne sont pas exercées conformément aux normes en vigueur. Il peut comporter une variété de risques tels que le risque de réputation, le risque légal, le risque de contentieux, le risque de sanctions ainsi que certains aspects du risque opérationnel, ceci en relation avec l'intégralité des activités de l'établissement. Circulaire CSSF 2004/155, page 3. »

Pour répondre à la citation d'Henry Ford ci-dessus et paraphraser cette notion, la réputation est-elle mesurable et gérable ? Quels sont les risques qui y sont attachés ?

Doit-on considérer la gestion du risque de réputation comme simple conséquence du mode de gestion ou de culture de l'entreprise ?

Comment définir ce risque à partir des informations dont nous disposons aujourd'hui ?

Nous partageons ici avec le lecteur, le fruit de notre réflexion et expérience en la

matière, en définissant ce risque, en développant une approche de mesure et de gestion, en incorporant quelques exemples pratiques ainsi qu'une valeur sûre en terme d'outil Compliance qu'est le code de conduite.

1. Définitions

Les quelques définitions suivantes permettent de préciser notre connaissance du sujet :

1. « *Risque de réputation : Le risque d'une publicité défavorable des pratiques commerciales d'un assureur, vérifiée ou non, créant une perte de confiance dans l'intégrité de l'établissement.*

Le risque de réputation peut découler d'autres risques inhérents aux activités d'une organisation. Le risque de perte de confiance des actionnaires, incluant, inter alia, les clients existants ou potentiels, les investisseurs, fournisseurs de services et autorités de contrôle¹. »

2. « *Le risque de réputation est à mettre en relation avec les aspects légaux et contractuels de la clientèle d'un établissement et la plupart du temps avec des dossiers de blanchiment d'argent et de délit d'initié en relation avec l'utilisation des services de l'établissement.*

Le risque de réputation doit aussi être associé avec l'impact actuel et potentiel sur le capital et les pertes et profits qui découlent d'une opinion publique défavorable.

Ce risque affecte la capacité de l'établissement de mettre en place de nouvelles relations ou services ou même de continuer la gestion des relations existantes. Le risque expose l'établissement à des contentieux, pertes financières, ou dégringolade de la base de données clientèle.

¹ Source : IAIS - Guidance paper on anti-money laundering and combatting the financing of terrorism, October 2004. Note: Consistent with definition in BCBS paper Customer due diligence for banks – October 2001. Traduction de l'auteur

L'exposition au risque de réputation est omniprésente dans une organisation et requiert la nécessité d'exercer une grande prudence dans la gestion des clients et de l'environnement social². »

3. « Les amendes sont souvent faibles comparées au chiffre d'affaires des compagnies, particulièrement des grands établissements financiers.

L'opinion publique a potentiellement un plus grand impact que les pénalités, par les dommages à la réputation, à la marque.

L'importance des amendes reflète le niveau de coopération de l'établissement et son aptitude à corriger une situation incorrecte.

Si l'irrégularité apparaît malgré la mise en place d'instructions claires et précises, une pénalité supérieure se justifie. ...

...Toutes ces considérations – l'accent sur les responsabilité du senior management, le niveau des amendes et la publicité pour les injonctions d'implémentation des décisions des autorités – ont le dessein d'influencer les comportements futurs : pour nous permettre d'atteindre les objectifs d'efficacité et de transparence des marchés de masse et un traitement correct de la clientèle « retail ». ³»

A partir de ces définitions, considérons :

- a. que les risques majeurs d'une entreprise sont globalement les suivants:
 - La performance financière et la rentabilité ;
 - Le gouvernement d'entreprise, la qualité du management, l'aspect social, éthique, la culture d'entreprise ; l'organisation du contrôle interne ;
 - Le Marketing, l'innovation et les relations clientèle ;
 - Les litiges et la gestion des tiers (Partenaires essentiels, fournisseurs de services) ;

- La communication et la gestion des crises.
- b. la nature abstraite et volatile de la notion de réputation.

Les caractéristiques principales de la définition du risque de réputation se résument comme suit :

Impact financier	l'impact de l'opinion publique, présent ou futur, sur les gains et le capital d'une entreprise.
Contentieux/ Non-respect des lois	Il correspond à l'exposition de l'établissement aux litiges potentiels, aux pertes financières directes ou à des pertes dans sa base de données clientèle. C'est le risque, par exemple, de publicité négative ou de rumeur, suite par exemple à la non observation des règles de protection des consommateurs.
Organisation de l'établissement	Plus généralement, le fait pour les tiers et clients que la société ne soit pas capable de se gérer en toute sécurité et de façon responsable. De même, la réputation de l'entreprise peut être impactée par des tiers. Lorsque des fournisseurs ne respectent pas les règles de protection de données des clients d'un établissement par exemple.
Caractère volatile	Le développement des technologies de communication ainsi que l'influence prépondérante des médias sur l'opinion des consommateurs en même temps que l'augmentation des normes et réglementations, accélère la volatilité du risque de réputation.

² Extraits de BIS Review 23/2003 – A G Romero – Integrity and good governance – reputation risk in the public sector and financial institutions.

³ Extraits de FSA Annual Report 2003/2204 ; page 11.

Une gestion proactive a pour objectif de protéger l'entreprise, mais aussi et surtout comme conséquence de la promouvoir sur le long terme.

2. Gérer le risque de réputation – une approche globale pour tous

Les questions clefs à se poser pour la gestion de ce risque sont les suivantes :

- Qui sont les actionnaires ?
- Leurs attentes stratégiques sont-elles réalistes ?
- Qu'attendent-ils de l'entreprise ?

Généralement, les acteurs sont invariablement toujours les mêmes, c'est-à-dire, les **clients**, les **employés** et les **investisseurs**.

On considèrera ensuite les autorités de contrôle, les partenaires stratégiques et les fournisseurs, ils ont une influence importante sur les acteurs de base qui composent l'entreprise.

Sur cette base, nous allons développer ci-après notre conception quant à la mesure et à la gestion du risque de réputation.

a. La mesure de la réputation

Le risque de réputation a détruit ou sérieusement ralenti le développement d'entreprises diversifiées ou non, de toutes tailles et dans tous les secteurs d'activité (Arthur Andersen, Worldcom, Enron, Ahold...).

Pourquoi est-il si souvent méconnu et ignoré.

Certaines recherches tendent à prouver qu'une entreprise ayant une forte réputation se relèvera mieux d'une crise boursière. La bonne réputation d'une entreprise attirera toujours les capitaux vers elle.

A cet égard, il est intéressant de citer un rapport de l'université du Kansas ayant examiné la relation entre la valeur de marché, la valeur comptable, la rentabilité et la réputation des sociétés reprises dans la cote du magazine Fortune, dans la catégorie « most admired companies » entre 1983 et 1997.

Le Rapport constate que le changement d'un point de leur réputation était corrélé à une hausse moyenne de 500 millions de \$ en valeur de marché.

Si certaines tentatives ont été expérimentées, il n'en reste pas moins difficile d'évaluer la réputation d'une entreprise. Et faute de modèle universel, elle reste une valeur non mesurable, qui n'apparaît pas au bilan de l'entreprise.

A contrario, la conséquence de la survenance de ce risque est quantifiable en terme d'impact négatif sur le chiffre d'affaire et/ou d'engagement de frais, de natures diverses, liés à ce type de situation.

b. La gestion de la réputation

Les récents changements législatifs et les nouvelles règles de Corporate Governance ont fait de la transparence et de la fiabilité la norme.

S'il n'y a pas de solution miracle pour la gestion de ce risque, certains éléments de base permettent d'en asseoir une gestion appropriée et préventive.

Ces éléments peuvent être rassemblés lorsque:

- Le conseil d'administration de l'entreprise donne le ton et définit les responsabilités et la stratégie en la matière ;
- Tous les employés se sentent concernés et gèrent ce risque au quotidien ;
- Le système de contrôle interne identifie, fixe les priorités, permet une prise de décision et la résolution adéquate des risques identifiés.

Dans le tableau ci-dessous, la gestion du risque de réputation se répartit entre 3 acteurs de base:

- les actionnaires,
- les clients,
- les employés.

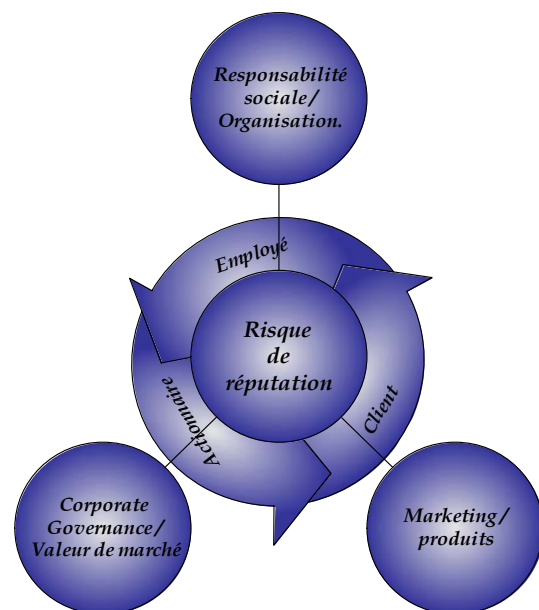
Nous décrivons ensuite les composantes de ce modèle, ainsi que ses principes de gestion.

Nota bene: On l'adapte à l'entreprise ou aux circonstances le cas échéant. Il se révèle opportun dans certaines situations d'intégrer les partenaires tiers, intermédiaires et/ou les fournisseurs de

service dans les axes de gestion. Il ne s'agit pas d'un modèle statique, bien au contraire.

Les autorités ne sont pas représentées, non pas que nous les oublions, mais elles définissent le cadre général dans lequel fonctionnent les entreprises et à cet égard, n'ont que peu d'influence.

Tableau 1 : Exemple de modèle de gestion du risque de réputation



a. Le mode de gestion applicable aux **actionnaires** se répartit entre :

- Les droits pécuniaires des actionnaires et les informations qui les accompagnent, comme les résultats actuels et prévisionnels, les comparaisons avec les concurrents, toutes types de données financières et comptables ainsi que l'image véhiculées par celles-ci.
- Le droit d'intervention dans la vie sociale de l'entreprise. La stratégie et le

contrôle des résultats, transparence des méthodes, les opportunités de marché et la vision de l'avenir de la société.

Si le premier point est habituellement bien intégré, le second moins présent se développe de plus en plus. Les interventions des actionnaires sont de plus en plus nombreuses et précises quant aux questions relatives aux choix de gestion de l'entreprise.

C'est une nouvelle donne pour le management et un nouveau défi pour le Compliance Officer.

b. L'axe **client**, se préoccupe de l'image que l'entreprise désire véhiculer d'elle-même dans le public. Les notions de qualité, d'innovation, de fiabilité, de confiance, de performance produits et/ou services, l'homogénéité de son offre.

Cette notion de confiance est primordiale dans le secteur financier. Les ratings comme le Standard & Poors, par exemple, matérialisent les effets financiers sur une entreprise du prix de la confiance du marché.

c. Les modes de suivi de gestion des **employés** :

En préambule, rappelons que le secteur financier recrute surtout un personnel qualifié qu'il n'est pas facile à trouver. Compétence et expérience vont aussi de pair, et l'axe employé revêt toute son importance.

- L'organisation interne : Les employés s'intègrent-ils facilement dans leur milieu de travail ? L'entreprise est-elle correctement organisée ? Donne-t-elle confiance à ses ressources ? Les employés sont-ils équitablement rémunérés ? L'entreprise connaît-elle les qualités de ses employés ?
- La responsabilité sociale : Comment l'entreprise s'intègre-t-elle dans le tissu socio-culturel ? S'implique-t-elle dans la vie sociale et comment ? Est-elle préoccupée par le respect de l'environnement ?

Une fois ces axes définis, ils peuvent être gérés selon les principes suivants :

Le professeur Fombrun de « The Leonard N. Stern School of Business of New York university » distingue 5 principes de gestion qui créent les meilleures réputations :

a. Spécificité – Les sociétés qui détiennent une position spécifique dans l'esprit des investisseurs.

b. Convergence – Les entreprises qui concentrent leurs actions et communications autour d'un thème unique et simple.

c. Cohérence – Les sociétés qui sont consistantes quant à leurs actions et communications, c'est-à-dire qui ne changent pas régulièrement de message. On constate souvent aujourd'hui, que la norme en cette matière est la division des tâches. Les personnes qui gèrent l'image à véhiculer aux investisseurs s'adressent aux analystes, le département marketing gère les produits et le positionnement de la marque, les ressources humaines la communication aux employés.

Cette organisation décentralisée et sans contrôle garantit une incohérence de la communication de l'entreprise.

d. Identité– Les valeurs véhiculées doivent correspondre réellement à l'identité de l'entreprise. Une manipulation de l'image au travers de la publicité et des relations publiques est un échec ou une contre performance si elle est déconnectée de la réalité des valeurs de l'entreprise.

e. Transparence – La transparence exige beaucoup de communication. On remarquera que les entreprises à forte réputation communiquent souvent plus que les autres.

Une forte réputation est le résultat d'initiatives et d'un travail sur l'image qui véhiculent des valeurs d'authenticité et de différenciation de la personnalité d'une entreprise.

Parce que la gestion de la réputation est une activité émergente, il convient d'adapter la gestion au besoin. On distingue à cet effet

le mode de gestion préventif du mode réactif.

En mode réactif, lorsque la suspicion, le sentiment d'insécurité, d'incompétence, de corruption existent à l'encontre d'une organisation, plus rien ne peut prévenir la chute de celle-ci. Le sang froid réclamé en de telles circonstances ne s'improvise pas.

Lorsqu'il s'agit d'une gestion proactive ou préventive, un spécialiste isolé ne suffit pas. La gestion de ce risque influence fortement l'ensemble des actions, comportements et standards de la société de manière cohérente.

A l'instar de la lutte contre le blanchiment, cette gestion est l'affaire de tous, pas d'une seule fonction.

3. Quelques exemples

a. La communication « génération Internet »

L'évolution technologique s'accompagne de nouveaux risques liés à la communication. Internet et la messagerie électronique ont gonflés le nombre de messages et de documents communiqués dans et entre les entreprises. Nous parlons ici uniquement des messages professionnels.

Ces messages sans contrôle peuvent créer des dommages à la réputation de la société.

Les interlocuteurs s'expriment souvent très librement dans les E-mails, qui deviennent de plus en plus un mode écrit de conversation téléphonique et revêtent un caractère moins formel que la lettre classique qu'il faut souvent contresigner. C'est oublier qu'ils peuvent être distribués de façon incontrôlée à un nombre infini de personnes.

D'un point de vue de la protection de données, envoyer un E-mail à l'extérieur de l'entreprise s'apparente à correspondre par carte postale.

On remarque que ce type de correspondance implique des comportements d'irresponsabilité entres collègues.

Dans ses procédures, le programme de communication met l'accent sur la communication interne de la société. Il prévoit une revue des données marketing ainsi que des mises en garde et autres décharges de responsabilité, pour s'assurer que les clients disposent de la bonne information, et la société de la protection adéquate vis-à-vis des informations diffusées.

Il n'est pas inutile de rappeler, le cas échéant, les valeurs de l'entreprise, afin d'éviter des comportements non désirés entre collègues liés à ce type de messagerie.

b. Le « Social Engineering »

Un autre type de risque nouveau lié à la communication est appelé « Social Engineering ».

Les auteurs de ce piratage de données se concentrent sur le point le plus faible de la chaîne de protection des données, l'homme. Souvent, ils en obtiennent toutes les données nécessaires pour entrer dans le système informatique d'une entreprise.

Les objectifs recherchés sont de commettre des fraudes, de l'espionnage industriel ou simplement nuire au bon fonctionnement du système informatique.

En outre des procédures classiques de sécurité physique, formation et information sont des outils clefs lorsqu'il s'agit de se prémunir contre ce type de fraude.

c. Gérer les plaintes et critiques ou comment apprendre des expériences négatives

Cette gestion dépend des règles de la Corporate governance dictées par les autorités.

Elles ne concernent pas uniquement les clients. Sarbanes & Oxley ouvre le principe aux employés lorsqu'ils détectent une anomalie comptable par exemple.

Une gestion réussie qui traite correctement ces informations a une influence importante sur la gestion du risque de réputation.

Elle augmente la connaissance que l'entreprise a d'elle-même et lui permet d'apporter le cas échéant des réponses

définitives à des problèmes ou des risques récurrents cachés ou ignorés.

Il est utile de tirer les enseignements de ces informations et d'installer les critères de prévention qui découlent de ces expériences.

L'entreprise doit assurer un traitement adéquat de ces plaintes. Celles-ci doivent être perçues comme des opportunités d'entrer en communication avec le plaignant.

Lorsque l'apparition d'erreur est inévitable, le suivi et l'analyse des tendances, donne d'excellentes indications sur les survenances de risques majeurs. Ceci dépend bien sûr de la qualité des indicateurs mis en place et des modèles de corrélations utilisés.

4. Le code de conduite – Une valeur sûre

Habituellement le code de conduite couvre deux volets.

- Dans un contexte économique et un environnement réglementaire évolutifs, les entreprises ressentent naturellement le besoin de créer un Code de Conduite, souvent lié au caractère international de leurs activités et à la taille de l'entreprise.

Ce document est utilisé comme cadre de référence. Il énonce une série d'engagements et les valeurs de l'entreprise. Il s'accompagne souvent par la volonté pratique mise en place par l'entreprise pour « vivre » ses valeurs.

- Il signifie aux membres de la société les comportements et les pratiques commerciales non désirés voire interdits.

La confiance est un élément crucial pour le secteur financier. Le non-respect de cette valeur entraîne des dommages de réputation importants. Ceci explique pourquoi le code de conduite couvre aussi toute une série de matières liées à la confidentialité et protection des données, aux informations conduisant à un délité d'initié, à la non discrimination etc....

En énonçant ses valeurs et en rappelant les comportements inacceptables, le code de conduite est un instrument précieux de communication et de prévention du risque de réputation.

Preuve s'il en faut, un code de conduite a été récemment utilisé dans le cadre d'un dossier de délit d'initié traité par le Financial Services Authority en Grande Bretagne. L'employeur a licencié son employé qui n'avait pas respecté les prescriptions du code acceptées lors de son engagement.

5. En conclusion

Les résultats des études des entreprises qui ont déterminé et géré ce risque, constatent que sa gestion efficace améliore les performances et les bénéfices de l'entreprise.

Les responsables de la gestion du risque de réputation disposent les composants suivants au centre de leur approche.

- Une vision et une définition claire des responsabilités ;
- Des valeurs simples, accompagnées d'un code de conduite qui explique les comportements et les standards acceptés ;
- Pour les activités importantes, les performances et les risques tolérés sont fixés par écrit.
- Une culture ouverte, des relations de confiance, une communication effective ;
- Un système de contrôle interne efficace qui prévient à temps des risques encourus ;

- Une organisation qui apprend et apporte des actions correctrices adaptées ;
- Des récompenses et des reconnaissances qui renforcent les objectifs et les valeurs de l'entreprise ;
- Une communication des valeurs aux partenaires, intermédiaires et fournisseurs.

« Dans le monde d'aujourd'hui, où les idées supplantent le matériel dans la création de la richesse, la réputation devient une force motrice majeure qui propulse l'économie en avant. »- Alan Greenspan, président de la réserve fédérale.

L'argumentation classique utilisée par les détracteurs de la gestion effective du risque de réputation, pour retarder son implantation immédiate, est de prétendre que ce risque est nul ou de penser que cela n'arrive qu'aux autres !

La capacité de gérer le risque de réputation et les risques associés font déjà partie des éléments de compétition.

La réputation est bien plus qu'un concept abstrait, c'est un atout et même un actif de la société, qui comme un aimant attire ou repousse les clients, les employés ou les investisseurs.

Benoît Martin- Compliance Officer

Luxembourg, le 20 mai 2005

VIE ASSOCIATIVE

ASSOCIATION ACTIVITIES

GROUPES DE TRAVAIL ACTUELS:

CURRENT WORKING GROUPS:

A. SECTEUR TRANSVERSAL:

A. CROSS-SECTOR:

Groupe de travail 08b

Circulaires CSSF: checklists - deuxième partie

Responsable Patrick WATELET
Téléphone (+352) 45 14 14 231
patrick.watelet@citigroup.com

Working group 08b

CSSF circulars: checklists – part 2

Owner Patrick WATELET
Telephone (+352) 45 14 14 231
patrick.watelet@citigroup.com

Groupe de travail 16

Commission permanente juridique et relations publiques / site internet

Responsable Karine VILRET-HUOT
Téléphone (+352) 26 44 14 13
kvilret@vilret-avocats.com

Working group 16

Legal and public relations / internet site

Owner Karine VILRET-HUOT
Telephone (+352) 26 44 14 13
kvilret@vilret-avocats.com

Responsable internet Olivier GILSON
Téléphone (+352) 25 04 04 22 81
olivier.gilson@fid-intl.com

Internet Owner Olivier GILSON
Telephone (+352) 25 04 04 22 81
olivier.gilson@fid-intl.com

Groupe de travail 25

Les fonctions compliance, audit interne et risk management

Coordinateur Jean-Marie LEGENDRE
Téléphone (+352) 47 67 26 07
jean-marie.legendre@cail.lu

Working group 25

The functions of compliance, internal audit and risk management

Coordinator Jean-Marie LEGENDRE
Telephone (+352) 47 67 26 07
jean-marie.legendre@cail.lu

B. SECTEUR BANCAIRE:

B. BANKING SECTOR:

Groupe de travail 04

Lutte contre le blanchiment dans le secteur de la banque privée

Responsable Patrick SCHOTT
Téléphone (+352) 46 71 71 400
pschott@pictet.com

Working group 04

Anti-money laundering in private banking

Owner Patrick SCHOTT
Telephone (+352) 46 71 71 400
pschott@pictet.com

Groupe de travail 10

Contrôles compliance

Responsable Patrick CHILLET
Téléphone (+352) 40 65 40 584
p.chillet@crediteurop.lu

Working group 10

Compliance controls

Owner Patrick CHILLET
Telephone (+352) 40 65 40 584
p.chillet@crediteurop.lu

C. SECTEUR FONDS:

Groupe de travail 18

Compliance relativement aux investissements alternatives

Responsable Jean-Marie FOURQUIN
Téléphone (+352) 26 27 16 1
jmfourquin@alternativeleaders.lu

Groupe de travail 20

Transposition de la directive anti-blanchiment (à mettre en place en coopération avec l'ALFI)

Responsable Tim WINFIELD
Téléphone (+352) 34 10 23 85
tim.winfield@jpmorganfleming.com

Groupe de travail 21

Interprétation pratique des restrictions d'investissements de fonds

Responsable Tim WINFIELD
Téléphone (+352) 34 10 23 85
tim.winfield@jpmorganfleming.com

D. SECTEUR ASSURANCE:

Groupe de travail 12

Lutte contre le blanchiment dans le secteur des assurances

Responsable Gérard ZOLT
Téléphone (+352) 22 51 51 342
gerard.zolt@kpmg.lu

Groupe de travail 13

Compliance et intermédiaires

Responsable Bruno GOSSART
Téléphone (+352) 24 18 58 5160
b.gossart@fortis.lu

Groupe de travail 14

Statut du compliance officer dans le secteur des assurances

Responsable Benoît MARTIN
Téléphone (+352) 45 67 30 49 54
benoit.martin@paneurolife.com

C. FUNDS SECTOR:

Working group 18

Compliance for alternative investments

Owner Jean-Marie FOURQUIN
Telephone (+352) 26 27 16 1
jmfourquin@alternativeleaders.lu

Working group 20

Transposition of the anti-money laundering directive (to be set up in co-operation with ALFI)

Owner Tim WINFIELD
Telephone (+352) 34 10 23 85
tim.winfield@jpmorganfleming.com

Working group 21

Practical interpretation of fund investment restrictions

Owner Tim WINFIELD
Telephone (+352) 34 10 23 85
tim.winfield@jpmorganfleming.com

D. INSURANCE SECTOR:

Working group 12

Anti-money laundering in insurance

Owner Gérard ZOLT
Telephone (+352) 22 51 51 342
gerard.zolt@kpmg.lu

Working group 13

Compliance and intermediaries

Owner Bruno GOSSART
Telephone (+352) 24 18 58 5160
b.gossart@fortis.lu

Working group 14

Status of the compliance officer in insurance

Owner Benoît MARTIN
Telephone (+352) 45 67 30 49 54
benoit.martin@paneurolife.com

MEMBRES ET VIE ASSOCIATIVE:**MEMBERS AND ASSOCIATION ACTIVITIES:****Nombre de membres (au 31/08/2005):**

Banques	85
Fonds	62
Fonds / Banques	27
Assurances	36
Consultants / Réviseurs	24
Admin. et domiciliation de sociétés	8
Autres	29

Effectif total: 271

Membres effectifs	216
Membres d'honneur	55

Effectif total: 271

Réunions et activités:

Mensuel	Réunions du conseil d'administration
Anniversaire de l'ALCO	31 janvier 2006

Number of members (as per 31/08/2005):

Banking sector	85
Funds sector	62
Funds / Banking sector	27
Insurance sector	36
Consultants / Auditors	24
Admin. and company domiciliation	8
Other	29

Total number: 271

Active members	216
Honorary members	55

Total number: 271

Meetings and activities:

Monthly	Board meetings
Birthday of ALCO	31 January 2006



Association Luxembourgeoise
des Compliance Officers
du Secteur Financier

Secrétariat de l'ALCO:

Solyane LORKOVIC	
Téléphone	(+352) 47 67 26 12
Fax	(+352) 47 67 36 12
E-mail	Solyane.LORKOVIC@ca-luxembourg.com
Adresse	B.P. 1104 L-1011 Luxembourg

Secrétariat du bulletin:

Coralie CZERWINSKI	
Téléphone	(+352) 26 44 14 13
Fax	(+352) 26 44 15 14
E-mail	cczerwinski@vilret-avocats.com

Comité de rédaction / Drafting committee:

Karine VILRET-HUOT, Jean-Marie LEGENDRE, Marie-France DE POVER, Patrick SCHOTT, Olivier GILSON, Leen BOM, Jean-Florent RICHARD, Philippe SCHNEIDER, , Viatcheslav SKRIPKINE

Visitez notre site / Visit our website: www.alco.lu