



Association Luxembourgeoise
des Compliance Officers
du Secteur Financier

Newsletter

N°23

JULY 2012

Editorial



Dear ALCO Members, dear Readers,

Summer is already here and it was time to publish the 23rd edition of the ALCO newsletter.

While increasingly developing new channels, such as roundtables and answers to questions from members, the board of directors is very keen to maintain the Newsletter as a more comprehensive means of communication, which enables us, in particular, to address subjects of general interest via a wide range of detailed articles.

In this edition the feature article focuses on exchanges of information between professionals concerning a common customer. Banking secrecy does not require each of the professionals to repeat all the customer identification processes and even allows these processes to be outsourced under strict conditions. It is also legitimate for professionals to share information on common customers to confirm or remove money laundering suspicions.

The interview focuses on an activity for which a government bill has been tabled in Luxembourg and which may have direct and indirect impact on our activities as Compliance Officers: electronic archiving. The President of FedISA Luxembourg and the chair of its scientific committee participated in a game of questions and answers.

This Newsletter also includes a document eagerly awaited by the fund industry and produced by ALCO with the support of the ABBL: the new AML LETTER. The new model letter will enable financial sector professionals in Luxembourg to provide a correct and satisfactory answer to

Newsletter

questions from foreign correspondents on anti-money laundering measures put in place in Luxembourg.

Roundtable summaries have become recurring articles in your Newsletter. The first deals with controls on Custodian Banks, a topical subject which sometimes gives rise to concerns for many of us. The second deals with the problem of “cross-border” activities, inherent in private banking and already controlled in Switzerland under the aegis of FINMA.

Finally, the Newsletter publishes two questions from members: one on exemptions from the investment restrictions imposed on SIF and the other on the applicability of banking secrecy in the area of non-life insurance.

Finally, I would like to wish you an excellent summer vacation to recharge your batteries ... for the challenges ahead of us.

I hope that you all find this newsletter both interesting and useful.

Jean Noël Lequeue
President of ALCO

* *

Article

Exchanges of information between professionals on a common customer

In order to carry out properly the delicate mission of combating money laundering and terrorist financing that the legislator has entrusted to them, the professionals concerned are required not only to apply customer due diligence measures, but also to report any suspicions of money laundering or terrorist financing. With a view to easing these two sets of professional obligations, the legislator has provided for the possibility for professionals with a common customer to share information on that customer, subject to certain conditions. Therefore, exchanges of information in the framework of the performance of the due diligence obligations are allowed pursuant to article 3-3 of the amended law of 12 November 2004 (hereinafter the “Law”), while article 5, paragraph (5) of the Law provides for the possibility of sharing information in the framework of a suspicious transaction report.

First of all, the aforementioned article 3-3 transposes into national law the provisions of section 4 of Directive 2005/60/EC of the European Council and of the Parliament on the prevention of use of the financial system for the purpose of money laundering and terrorist financing. This article authorises the professionals concerned to entrust to a third party the performance of the due diligence measures referred to in article 3, paragraph (2), points (a) to (c), of the Law. Article 3-3 of the Law provides for two possible outsourcing solutions, i.e. the use of a “third party” as defined in paragraph (1) of the said article, or the use of an “agent or an outsourcing service provider”. The latter solution is simply evoked in paragraph (5) of the same article. In fact, neither the Law nor Directive 2005/60/EC is very explicit as regards the applicable system. It is necessary therefore to refer to Circular CSSF 08/387, supplemented by Circular CSSF 10/476, to obtain more information on the provisions of article 3-3 of the Law. Circular CSSF 08/387 distinguishes between what it refers to as “the third party regime” on the one hand and “outsourcing” on the other hand. The “third party regime” referred to in Circular CSSF 08/387 corresponds to the “third parties” mentioned in the amended law of 12 November 2004 and in Directive 2005/60/EC, which also uses the term “introducer” (see recital (27)). These “third parties” are listed exhaustively in article 3-3, paragraph (1) of the Law, whose provisions are specified in points 98 to 100 of Circular CSSF 08/387, supplemented by parts I and V of Circular CSSF 10/476. In accordance with recital (27) and section 4 of Directive 2005/60/EC, the aforementioned article 3-3, paragraphs (1) to (4), refers to the use of a “third party” and defines the applicable regime. On the other hand, Directive 2005/60/EC (recital 28 and article 19) and article 3-3, paragraph (5), refer to outsourcing, but without specifying the applicable regime. These texts simply stipulate that the applicable rules where a third-party introducer is involved are different from those applicable to “outsourcing or agency relations”. The aforementioned Circular CSSF fills this void by clarifying the regime applicable to outsourcing relations.

In accordance with Circular CSSF 08/387, the third party regime applies when a professional wants to accept customers who have already been identified by one of the professionals enumerated exhaustively by the Law. Use of the third party regime is therefore intended to avoid repetition of customer identification procedures. Exchanges of information between professionals, for the purpose of combating money laundering and terrorist financing, concerning a common customer, are therefore authorised.

As regards outsourcing, Circular CSSF 08/387 specifies that this applies where a professional contractually entrusts the performance of due diligence measures to a trusted third party that is not subject to the amended law of 12 November 2004 or equivalent rules on combating money laundering and terrorist financing. The obligations of the agent or outsourcing service provider with regard to combating money laundering and terrorist financing may therefore only result from the contract and not from the amended law of 12 November 2004. Consequently, it is essential to sign a written contract whose minimum content is defined in point 103 of Circular CSSF 08/387. The outsourcing contract must thus describe in detail the due diligence measures that have to be applied by the third party to which the task is entrusted. The contract must also provide that the said third party must, if requested, transmit promptly the information and documents required to the professional that has delegated this duty.

It is reasonable to question whether the outsourcing regime can also apply to a professional using the services of a third party subject to the amended law of 12 November 2004 or to equivalent rules on combating money laundering and terrorist financing, since article 3-3, paragraph (5), of the amended law of 12 November 2004 and recital (28) of Directive 2005/60/EC are ambiguous on this point, insofar as neither of these two texts expressly excludes the hypothesis of an outsourcing relation where the third party is subject to the amended law of 2004 or to equivalent rules. Point 102 of Circular CSSF 08/387 clarifies this point. Thus, according to the provisions of point 102, outsourcing concerns “the situation where professionals outsource or delegate certain duties by way of contract to other trusted persons not subject to the law of 12 November 2004 as amended or to equivalent regulation concerning the fight against money laundering and terrorist financing”. Consequently, application of the third party regime implies that the third party is either subject to the amended law of 2004 or to equivalent regulation. On the other hand, an agency or outsourcing contractual relationship implies that the third party is not subject to the Law or equivalent regulation.

As noted previously, professionals also have the possibility to share information on a common customer, pursuant to articles 28 and 29 of Directive 2005/60/EC, whose provisions have been transposed into national law by article 5, paragraph (5) of the Law. This article 5, relative to obligations to cooperate with authorities, enshrines the principle whereby professionals are prohibited from disclosing to the customer concerned and/or to third parties that information and/or documents have been transmitted to the Financial Intelligence Unit (the FIU). The confidential nature of the procedure for reporting suspicious transactions concerns not only the existence and content of the actual report (article 5 (5)), but also the identity of the reporting party (article 5 (1)). There are however exemptions to the confidential nature of the suspicious transaction report provided for in paragraph (5) of the Law, with regard to certain professionals, since the disclosure of information is authorised exclusively for the purpose of combating money laundering and terrorist financing, subject to certain conditions intended to reconcile respect for professional secrecy, private life and fundamental rights of customers. Accordingly, the communication of information is authorised between the establishments of Member States or third countries provided that they satisfy the conditions specified in article 3-1 paragraph (1) and belong to the same group within the meaning of article 51-9 paragraph (15) of the amended law of 5 April 1993 on the financial sector or of article 79-9 paragraph (15) of the amended law of 6 December 1991 on the insurance sector. Circular 08/387, point 144, reiterates that article 41, paragraph (4), 2nd indent, of the law of 5 April 1993 on the financial sector, authorises this type of exchange of information between internal control bodies of the group to which the financial sector professional established in Luxembourg belongs.

Furthermore, disclosure of information in the framework of a suspicious transaction report is also possible between certain professionals who are subject to equivalent obligations as regards combating money laundering and terrorist financing and carry on their professional activities

Newsletter

within the same legal entity or in a “network” which corresponds to a larger structure to the which the person belongs and which shares common ownership, management or compliance control.

Finally, certain professionals falling within the same professional category and subject to equivalent obligations as regards professional secrecy, protection of personal data and combating money laundering and terrorist financing, may exchange information relative to a suspicious transaction report concerning the same customer and the same transaction, but solely for the purpose of preventing money laundering and terrorist financing.

In conclusion, the redundancy of controls carried out by each professional to combat effectively money laundering and terrorist financing is limited by articles 3-3 and 5, paragraph (5) of the Law insofar as these texts allow professionals to rely on information previously collected from a customer by another professional. Moreover, in order to avoid material performance of their customer due diligence obligations, professionals may choose to delegate this duty to a third party pursuant to article 3-3, paragraph (5). It is important however to specify that ultimate responsibility for performance of these obligations lies with the professional who uses the services of a third party. Exchanges of information between professionals therefore allow for greater flexibility in the performance of their obligations as regards combating money laundering and terrorist financing.

Emilie Hugue
Deputy Manager
The ICE Breakers SA

Interview

Interview with Mr Cyril Pierre-Beausse, Attorney-at-Law, Counsel at Allen & Overy Luxembourg (President of FedISA Luxembourg) and Mr Jean Brisbois, Senior Manager at Alter Domus (Chair of the Scientific Committee of FedISA Luxembourg)

Electronic Archiving

1 – Gentlemen, what is FedISA Luxembourg and what are its objectives?

FedISA (Federation of ILM “Information Lifecycle Management”, Storage and Archiving) began as a French association. It was set up 10 years ago and operates in the form of a network of local associations grouped together within FedISA International. At the current time, France, Belgium, Luxembourg, Canada and Monaco are already part of the network. Germany, Ireland, Morocco and Tunisia have expressed an interest in joining.

Although France was behind the development of FedISA and initially led the way in legislation on electronic archiving, other countries have rapidly caught up with it. In this regard, the dynamism of Luxembourg is particularly noteworthy. Moreover, FedISA International which will oversee the various national chapters of FedISA will eventually be based in Luxembourg.

FedISA Luxembourg is not a club of technology providers or archiving services. At least half of its members are users. These are particularly present in the decision-making bodies of FedISA. The scientific committee (chaired by Jean Brisbois), which takes decisions on the association’s events and working groups, is therefore composed only of users and researchers.

The objective of FedISA is to federate and inform the electronic archiving community, to deliver content to it on new technologies, new processes and new regulations, while promoting exchanges of experiences between members. Committees and working groups meet regularly to discuss a given theme and deliver value-added documents for members (examples of subjects discussed in committee: electric vaults, dematerialisation and international probative value).

We also regularly organise events in cooperation with major players (banks, etc.), in all cases in the interests of our members and not for commercial purposes.

Newsletter

2 – Why has electronic archiving become increasingly important in everyday work? What are its pros and cons?

Development of electronic archiving has been driven mainly by storage cost savings and reducing the risk of lost information. In addition, electronic archiving makes it easier to find information, which considerably boosts the efficiency of work processes.

While there are many advantages there are nevertheless some obstacles and drawbacks. Given the role of technology, experience acquired in this area is relatively recent (electronic archiving technology has existed for only a few years, compared with 2000 years for the use of paper). In addition, because of rapid technological development, some technologies quickly become obsolete.

It must be borne in mind that for 25 years it has been possible for companies in Luxembourg to digitize their archives and they are no longer under any obligation to keep paper files (except for an original of their accounts –article 16 of the Commercial Code).

However, the law of 1986 is difficult to apply since its implementing conditions are not easy to satisfy. According to article 1334 of the Civil Code, a scanned document will only be considered a true copy provided that it complies with a Grand-Ducal regulation dating from 1986 and largely obsolete, in particular as regards the keeping of archives and storage formats. This regulation, and indeed the legislation as a whole, needs to be brought up to date. Moreover, that is the aim of a government bill first tabled several years ago, but still being prepared. Nevertheless, it would appear that the text is about to be finalised and that the bill and accreditation specifications for service providers will be published shortly.

3—What impact will this bill have on electronic archiving?

According to the bill, archiving may be outsourced to a third party or a PSDC (provider of dematerialisation and/or archiving services) approved by the State. As soon as a company outsources its archiving to a PSDC (or becomes a PSDC itself), its archives shall be presumed to be true copies of the originals and must therefore be accepted by courts in Luxembourg in the event of a dispute.

This bill is therefore very ambitious. There is no Community precedent and Luxembourg wants to play a pioneering role. This means being inventive. Some financial players in Luxembourg are understandably impatient for the bill to be adopted, but it is important to be patient because the stakes are high and there is no room for error.

In France, for example, a law exists which provides for electronic archiving, but the courts retain the ultimate power to decide whether or not to accept a scanned document as proof. This type of provision does not create confidence and that is exactly what the Luxembourg bill wants to avoid.

The objective of the bill is to make Luxembourg a leader in this area.

4- How does electronic archiving benefit Compliance Officers?

The first thing to note is the respect of workflows. Electronic archiving or the implementation of electronic document management solutions makes it possible to model workflows and thus “standardise” different actions by avoiding any risk of deviance.

Next, electronic documents obviously have many advantages over paper from the point of view of long-term storage.

Newsletter

The ideal solution for Compliance Officers would be to ensure that the processing of archives is delegated to an accredited PSDC or, if the company wants to digitize its archives itself, to become a PSDC. If that is not the case, the risk will persist that the courts will not accept scanned documents and will request the original, which will encourage companies to retain paper documents.

To conclude

FedISA, from the point of view of its objectives and the way in which it operates, has many points in common with ALCO and is open to collaborating with ALCO in the interests of our respective members, in particular by participating in a working group or a joint event on a theme or practical case study relating to the compliance aspects of electronic archiving.

Thank you Mr Pierre-Beausse and Mr Brisbois for your time.

Marie-Hélène Claude
Senior Compliance Officer at Alter Domus Sàrl
Member of the Board of Directors of ALCO and Treasurer of ALCO

New model letter for the distribution of Funds

“Dear Members,

Please find below a new model “anti-money laundering” letter of comfort drawn up by ALCO’s WG 35 in collaboration with the ABBL.

This type of document is often issued by natural persons or legal entities subject to obligations in the area of prevention of money laundering and terrorist financing to national counterparties but above all to foreign counterparties that require certain assurances in the context of banking or financial transactions.

It replaces the previous model which, although widely used, contained certain aspects which needed to be updated and enhanced.

The objective was to draw up a document that could be made available to all interested parties in order to explain the measures implemented for the application of current AML/CTF regulations.

To that end, the work was carried out with the intention of respecting the provisions contained in various reference texts such as:

- the Wolfsberg Group’s questionnaire;*
- the European directives and the FATF’s recommendation;*
- the anti-money laundering regulation in force in Luxembourg.*

This document will be available in the “members” environments of the websites of both associations.

*We trust that you will find it useful.
WG35.”*

Dear Sirs,

Luxembourg is one of the charter members of the Financial Action Task Force on Money Laundering (FATF) and, as a member of the European Union, is subject to EU regulations concerning anti money laundering and the prevention of terrorism financing (“AML/CTF”). Therefore, our country has established laws and regulations designated to combat Money Laundering and Financing of Terrorism in line with FATF standards and controls.

We hereby confirm that our credit / financial institution (the “entity”), established in Luxembourg, submitted to the rules on the prevention and the fight against money laundering and terrorism financing, is supervised by the Commission de Surveillance du Secteur Financier (the “CSSF” or the “Regulator”). As evidence for our licence as a regulated entity, please refer to the CSSF website: www.cssf.lu.

Newsletter

Our entity strictly complies with the laws and regulations on the prevention of money laundering and terrorism financing, as well as with the Circulars and Regulations issued by the CSSF on that subject.

AUDIT AND MANAGEMENT VALIDATION

As imposed by the Regulator, our entity has implemented a compliance function, responsible for the elaboration of an AML/CTF programme. This programme –validated by Senior Management – and its implementation are checked by the external auditor on a regular basis and results are reported to the Regulator.

In addition, our procedures and practices are audited by an independent internal audit function or an independent third party. In compliance with such rules, our entity has elaborated, and continuously adapts and improves, its respective procedures and policies.

PROCEDURES

The AML/CTF procedures and policies, including duties as regards Customer Due Diligence obligations, Suspicious Transaction Reporting as well as transaction monitoring processes, have been approved by the Senior Management of the entity.

CUSTOMER DUE DILIGENCE

As such, Customer Due Diligence rules are applied. More specifically, each client of our entity has to be identified before entering into a business relationship -including beneficial owners where applicable- and documentary evidence of their identity is held. We are also legally bound to keep all the documents related to the client's files and transactions for at least five years after the end of the business relationship.

Knowledge of the customer is based not only on the formal identification of that client but also on its risk profile. According to the risk-based approach principle, our entity understands the client risk profile through a monitoring programme with regards to its transactions and activities, and based on documentation collection and risk assessment.

SPECIFIC ENHANCED DUE DILIGENCE

High risk clients and Politically exposed persons. Business relationships with high risk clients and politically exposed persons (as well as their family and close associates) if any are covered by our policies consistent with legal requirements and industry best practices.

Shell banks. We comply with rules on correspondent banking activities. Our entity has also a policy prohibiting accounts/relationships with “shell banks” (i.e. a foreign bank without any physical presence in any country and that is unaffiliated with a regulated financial group).

COOPERATION WITH AUTHORITIES AND SUSPICIOUS TRANSACTION REPORT

Our procedures and practices also aim at preventing, detecting and reporting suspected money laundering or terrorism financing activities to the competent Financial Intelligence Unit (FIU).

In the context of preventing the financing of terrorism and complying with embargoes and restrictive measures, we use lists issued by international bodies, supervisory and judiciary authorities. Therefore, we ensure that clients' files and transactions are checked regularly.

Newsletter

In accordance with applicable laws and regulations, including privacy and data protection laws, our entity fully co-operates with governmental and law enforcement authorities. We are strictly complying with any information request from those authorities to which client information and documentation may be made available upon request.

BRANCHES AND SUBSIDIARIES

As required by applicable laws and regulations, our AML/CTF procedures and practices apply to our branches and subsidiaries.

AML/CTF TRAINING

We provide appropriate training on the prevention measures to our employees on a regular basis.

This only reflects current legal obligations incumbent to the entity that reserves the right to adapt its procedures at all times with the legal or regulatory framework and professional guidelines.

Yours sincerely,

XXXXXXXXXXXX

Roundtable Summaries

Custodian Bank Controls

Session of 6 May 2012

INTRODUCTION

This 2nd 2012 roundtable was attended by 13 ALCO members and coordinated by **Sabine Sauder-Vetter**, Group Internal Audit Manager KBL epb and **Sylvain Aubry**, Compliance Officer of Crédit Suisse. All the participants were interested in the role of Compliance Officers in **Custodian Bank Controls**.

This issue which remains a grey area for many Compliance Officers has become very topical following the subprime crisis and in the aftermath of the bankruptcy of Lehman Brothers and the Madoff and Luxalpha scandals.

On the basis of the answers received to the questionnaire, Sylvain Aubry had prepared a PowerPoint¹ presentation which we used as the framework for our discussions.

The roundtable attracted the interest not only of banks, but also of lawyers from asset management companies and other fund service providers.

The presentation highlighted the difficulties inherent in this issue, since a multitude of parties may be involved between the end clients that entrust their financial assets and the ultimate custodian of the underlying financial instruments.

Finally, the roundtable confirmed that the organisation of the custody business line varies considerably from one bank to another and from one group to another. Some are in the position of a subsidiary, while others have to rely solely on themselves to ensure the quality of their network of sub-custodians. Some participants represented MANCOs or funds, while others represented custodians or sub-custodians.

I. Regulatory framework

The law of 17 December 2012 on UCI (the UCI Law)² requires that the assets of all Luxembourg registered UCI (irrespective of their status or legal form) must be entrusted to a custodian bank. The law on the financial sector³ refers to the tasks of *safekeeping* and *administration*, including *custody* and related services.

¹ Available on request; some elements are included in the annex

² **Art. 17.** (1) The assets of a mutual fund must be entrusted to a custodian for safekeeping. (2) The custodian must either have its registered office in Luxembourg, or be established in Luxembourg if its registered office is in another Member States. (3) The custodian must be a credit institution within the meaning of the Law of 5 April 1993 on the financial sector, as amended. (4) The custodian's liability shall not be affected by the fact that it has entrusted to a third party all or some of the assets in its safekeeping.

³ Law of 5 April 1993, amended by that of 13 July 2007 **Article 26 Professional custodians of securities or other financial instruments.** (1) Professional custodians of securities or other financial instruments are professionals who engage in the receipt

Chapter E of Circular IML 91/75 (as amended by Circular 05/177) clarifies the obligations and responsibilities of custodian banks:

- They have a **safekeeping** duty.
- They have above all a general mission which consists in **supervising** the assets deposited with them, which implies that the custodian must have knowledge at any time of *how* the assets of the UCI have been invested and *where* and *how these assets are available*, even when most of the assets are not kept by the custodian itself, but are kept with “correspondents”. The custodian must organise its relations with its correspondents so as to ensure that it is immediately informed of any operation executed by them as part of the day-to-day administration of the assets deposited with them. The text also refers to more specific monitoring duties. In some countries, there is apparently an obligation of results, although the situation is not totally clear. The roundtable’s discussions focused on the general supervisory mission.

The regulatory framework is therefore very general which complicates the role of control bodies. To learn the precise obligations of custodian banks we will have to wait for the implementing measures of the AIFM Directive which the European Commission will adopt in principle in the 2nd half of 2012.

The participants

As noted above, a wide range of structures are concerned: UCITS, SIF, SICAR and other FCP and ‘SICAV’⁴. Accordingly, the participants also represented a wide cross-section of stakeholders: custodians and sub-custodians, promoters, management companies (MANCOs, Portfolio Managers) and investment advisors, transfer agents/registrars, administrators and prime brokers all have their share of responsibilities. Who controls whom? The bank to which the client, the UCI, entrusts its assets must control the way in which its sub-custodians deal with the assets. We note, however, that a certain number of sub-custodians are imposed, that is of course the case of transfer agents, but also of certain other counterparties, such as prime brokers. It is therefore in the bank’s interest not only to select carefully its sub-custodians but also to put in place a monitoring system. Upstream, the UCI or external asset manager or client will control their bank (custodian).

Acceptance of (sub-) custodian mandates

In the answers received, some participants allude to an acceptance committee in charge of account opening, while others refer to a committee with specific responsibility for the process of accepting sub-custodian mandates. In the first case, the risks involved concern AML⁵ and reputation issues, while in the second case concerns will focus more on solvency, communication, professionalism, safekeeping of assets and more operational issues.

Answers to the questionnaire seem to indicate that not only sub-custodians, but also distributors, as well as directors of management of UCI are not sufficiently analysed during the acceptance process.

into custody of securities or other financial instruments exclusively from financial sector professionals and who are entrusted with the safekeeping and administration thereof and with the task of facilitating their circulation. [...]

⁴ Undertakings for Collective Investment in Transferable Securities, Specialised Investment Funds, Venture Capital Investment Companies Mutual Funds, Open-Ended Mutual Funds.

⁵ Anti-Money Laundering

Monitoring relations: monitoring transactions and due diligence

Once a mandate has been awarded and the relationship established, the custodian will monitor how the sub-custodian performs its safekeeping, supervisory tasks and administrative tasks and, more generally, will ensure that all relevant data are kept up-to-date as part of its due diligence process. Centralised monitoring of operational aspects is very important. For example, regular use and updating of questionnaires⁶ can provide a significant amount of key information. It is also noteworthy that often pre-completed due diligence questionnaires may be transmitted to custodian banks by sub-custodians themselves. Depending on the reputation/prestige of these sub-custodians, banks may “waive” their own questionnaires. The work carried out to “challenge” the quality of the information provided in this context varies from one participant to another. Information included in the answers to questionnaires may then be cross-tabulated with information obtained from operating departments in regular contact with the sub-custodians or - more periodically - during video conferences or local visits which, according to the professionals present are becoming increasingly frequent. The formulas will depend on the quality of the relationship, as well as the level of risk (country, solvency, reputation, etc.). The types of controls often differ according to whether or not the sub-custodian belongs to the bank’s network. A promoter may in certain cases request that a specific sub-custodian should be used for certain types of securities. This calls for reinforced vigilance. It must be remembered, however, that the law does not distinguish between intra-group and other types of due diligence.

It is advisable to put in place controls to monitor market abuse (note: this is also money laundering and that is why I have deleted the introduction), segregation of assets, the quality of information provided to investors, solvency (credit/bankruptcy risk), anti-fraud and other measures, compliance with applicable laws and regulations, the BCP⁷, profiles of Board members, reputation risk, etc. Close collaboration with risk management is desirable. Given that this issue covers a wide range of areas, it is advisable to consult all other departments concerned so as to be able to draw up a single questionnaire and thereby avoid a situation where each department sends its own questions at different times. Unfortunately, the risk criteria may vary significantly from one area to another. A custodian may be classified as “low risk” as regards AML but “high risk” as regards BCP.

Some banks have a **procedure which requires questionnaires to be sent on a regular basis** to sub-custodians, whose answers are then analysed, or use other recurring controls. Others work **in an informal way** and ensure that there are frequent exchanges of information between the various teams involved, in order to obtain a precise idea of the quality of the services provided.

Cash flow monitoring is often used as part of the process for monitoring potentially “abnormal” transactions from an AML point of view. Is this really relevant for UCITS? Probably for the purpose of ensuring compliance with embargos and to avoid transfers in favour of or from blacklisted parties. Otherwise, the AML filters should be parameterized differently than for customary banking transactions.

It would seem that in many cases controls not related to AML are not yet extensively formalized. More formalisation is desirable and will sooner or later become indispensable. An external auditor confirmed that, at this stage, formalisation should be seen as a ‘best practice’ which undeniably facilitates the Compliance Officer’s work.

Delegation & SLA

⁶ These questionnaires may vary significantly as regards the details of the questions asked; some are limited to around a hundred short questions, while others are more than a hundred pages long and require numerous supporting documents. The frequency with which they are sent out also varies, from between 1 to 3 years, according to our survey.

⁷ Business Continuity Plan

Newsletter

The controls do not necessarily have to be carried out by Compliance Officers themselves. However, Compliance Officers must be in a position at all times to satisfy themselves that the necessary checks have been properly carried out. The survey shows that at least half of the participants use one form or another of delegation.

It is therefore possible to **delegate** this task. The details and formal nature of this delegation may vary. However, if the task is delegated to another legal entity, it is desirable to sign a **Service Level Agreement (SLA)** listing the tasks to be carried out and specifying how they are to be accomplished.

It seems that all **Due Diligence** tasks are frequently entrusted to a specialised team within the group (“network management”), often at parent company level. This team may therefore be based, for example, in Luxembourg, Paris, London or Frankfurt, etc. The basic information used for the due diligence will often be provided by way of a detailed questionnaire that each sub-custodian is required to complete/provide as the case may be.

Some require a copy of **external auditors’ reports**. It is to be noted however that auditors are not always willing to accept that reports produced as part of a specific audit engagement be used in another context. Moreover, business line specialists are often more competent than an external auditor to check the quality of specific tasks carried out (e.g. NAV calculated in accordance with European regulations).

The Compliance Officer may, via a SLA or in an informal way, request regular reports on each sub-custodian, or even a copy of all the due diligence reports on each of them.

Sensitive points

The main concerns of the participants do not involve UCITS, since these are already highly regulated. Some participants referred to the difficulties that they have in mastering various more specific risk categories. How can they obtain the necessary AML assurances when the beneficial owners of certain SIF are natural persons, residing in exotic countries?

How can they supervise market abuse risks or asset valuation risks of private equity funds?

How can fraud and corruption risks be limited in the case of forestry activities or funds speculating on the value of agricultural land, etc?

Funds of funds can, by their nature, be complex, even opaque. Their investment policy may appear vague, even unspecified, and they may fall within the jurisdiction of off-shore centres, where there is little regulation or supervision, etc.

The complexity of certain master-feeder⁸ type structures with custodians located in a wide range of often exotic countries can cause problems.

In all these situations, it is invaluable for a Compliance Officer to be able to count on a detailed SLA.

In all cases it is important to understand the *raison d’être* and role of each of the parties involved in the structure, since the custodian must be capable of demonstrating that it understands the asset holding chain, by comparing for example the organisational structure of the fund and/or its instruments of incorporation. This organisational structure must be regularly updated to integrate any changes following acquisitions/sales, etc.

Conclusion

⁸ A so-called *feeder* UCITS is an undertaking whose assets are fully invested at all times in units or shares of a single so-called *master* UCITS and in an ancillary way in cash.

Newsletter

This roundtable highlighted, once again, the variety of challenges which Compliance Officers face on a daily basis.

Would the Bernard Madoff fraud have been possible if all the controls that now exist had been put in place at the end of the 1990s?

We must learn from past experiences to avoid stumbling over the same obstacles. But it is not enough “to chase Madoff”. Merely putting in place safeguards based on past events is not enough. It is also and above all important to be forward-looking to avoid the next scandal, the next fraud, the next bankruptcy which will in all likelihood be different in nature from earlier ones.

It is not enough to rely on collecting certificates and other documents, without carrying out a carefully-thought out, thorough analysis.

It is in the interests of the financial centre of Luxembourg, as well all financial sector professionals who operate there, to have a reputation for closely controlling custodian banks. It is likely that the perpetrators of the next scandal will choose to operate in places where their bad practices are the least likely to be detected. The custody business is very important for Luxembourg. Anything which might damage its reputation in this area would be detrimental.

We wish to extend our warmest thanks to Sabine Sauder-Vetter for having contributed her expertise and to Sylvain Aubry for his welcome initiative and excellent preparation of this roundtable.

For WG34 “ALCO Roundtables”

Charles van Doorslaer

Enclosed: Summary of the main answers to the questionnaire (Sylvain Aubry)

DELEGATION OF CONTROLS

Have you organized any kind of delegation of these controls?

● Yes ● No



Some examples of delegated controls:

- Sub Custodian due-diligence
- Network Management
- Due diligence on emerging markets

ACCEPTANCE COMMITTEE

Do you have an acceptance committee devoted to control-risk reviews?

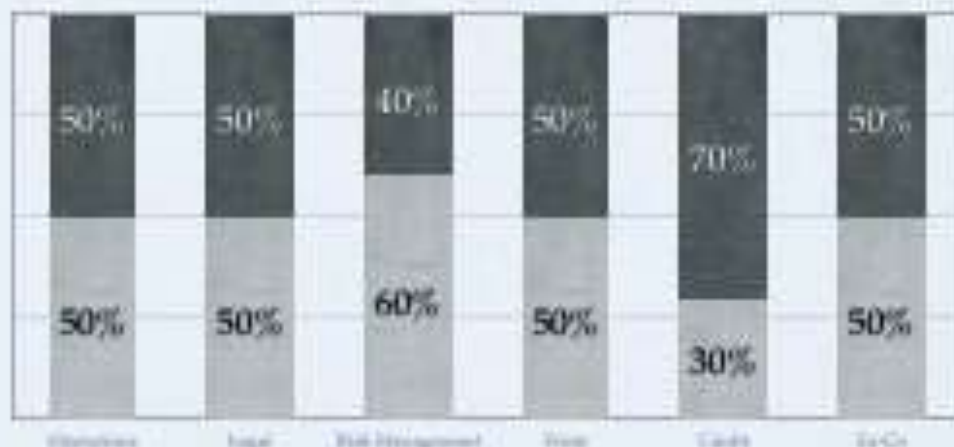


Is controlling a permanent member of this entity?



● Yes
● No

Other Departments Participating



● Yes
● No

KYC Monitoring

Are you bound to a revision process



● No
● Yes

Do you have a Risk Based Approach



Frequency of the review



● Yearly
● Every 2 years
● Every 3 years

Review depends on the risk category of the client

Follow Up - KYC Monitoring



Compliance within Cross-border business perspectives

Session of 19 June 2012

INTRODUCTION

What's the role of the compliance officer in the challenge to respect, not only the Luxembourg & EU rules, but also the rules of any country in which your company extends **it's** business activities?

A recent speech of Mr. Jean Guill⁹, general manager of the CSSF has stressed the importance of giving ourselves the means of penetrating new markets, turning our back to outdated off-shore business models.

Increasing our cross-border activities within EU and outside EU, without breaching any foreign rules is indeed a difficult and expensive undertaking.

The subject attracted participants mainly from banks and asset management companies. 30 ALCO members have shown interest, 20 have sent back the questionnaire and 17 attended the meeting. Many thanks to all of them for their active participation.

We wish to thank, in particular, Mr Stanislas Chambourdon, Partner at KPMG. He is member of the KPMG private banking team who has drafted country manuals for cross-border business. In this context KPMG has collaborated with ABBL for making the promotion of the country manuals. His presentation and his answers and comments to our various questions and remarks were highly appreciated.

THE COMPLIANCE OFFICER'S ROLE

Mr. Stanislas Chambourdon opened the discussion by providing an explanation on how and where cross-border issues have been in the spotlights first. FINMA in Switzerland asked banks to set up a cross-border framework. Certain Luxembourg subsidiaries of Swiss banking groups consequently appear to already have implemented cross-border policies.

But all Luxembourg banks should in fact adopt such a policy. However, it was clear from the questionnaires returned, that not all banks have it in place yet. One of the reasons might be that cross-border issues and risks are not sufficiently known by the Luxembourg financial institutions market.

What does "crossing a border" really mean?

Our attention was drawn on the fact that the definition of cross border services from the General agreement on trade in Services (GATS) is to be seen as very broad: Every act that has direct implications in another jurisdiction than the one where it was initiated. Clients as well as services can cross borders, for example, by selling products abroad or to residents of other countries. Employees can cross borders by travelling, by phone, by e-mail, by fax, by advertisement. Cross-border business can also be performed indirectly, through a representative or a branch, by a client introducer or any kind of financial intermediary. Cross-border can be active (when the bank initiates the relationship) or passive (when the client takes the initiative).

Some of the risks identified are:

⁹ At the annual meeting of the ABBL, 24 April 2012

Newsletter

- ⇒ Regulatory risks
- ⇒ Breaching tax and/or criminal law
- ⇒ Breaching Anti-Money Laundering regulation
- ⇒ Breaching business law, social law, labour law...

A few examples:

- ⇒ Granting a loan to a Belgian client might in some cases mean that you need to respect Belgian consumer protection laws & regulations and therefore further legal analysis should be performed.
- ⇒ Giving advice to French clients in the Paris office of a French financial institution, may re-qualify not only the commercial transaction itself as being a French transaction but also the status of the person giving the advice into a 'local service representative'.
- ⇒ The use of mobile phones might be, in some case sensitive as well. Some companies limit the use of mobile phones within some countries to a certain number of days per year (i.e. maximum 30 days in the UK).
- ⇒ The use of marketing material, of introducers, of insurance brokers might prove to be difficult exercises.

In some cases financial institutions under investigation might have tried to argue that they have not acted against the regulations (but only within a loophole). Authorities could easily reply that there are no loopholes in the regulations, only a wrong interpretation of them. Meanwhile reputation might have been hampered and time consuming problems shown up.

Compliance Officers are expected to contribute to drafting of a cross-border policy. They also can be expected to provide advice on how the business strategy of their institution should take into account the cross-border policy and the compliance situation within targeted countries.

They can be active by developing expertise in house (some information is freely available on the internet or through contacts with specialists from parent companies). But a number of banks prefer to save time by subscribing (through the ABBL or directly via KPMG) to country manuals on cross-border issues prepared by KPMG¹⁰.

A risk based approach (countries involved, types of customer approached, types of products offered) might be proposed to the management. From a compliance perspective, reputation should remain in the line of sight.

Compliance Officers need to:

- ⇒ monitor (ensure appropriate documentation is handed over to clients, log visits & trips abroad¹¹, etc.);
- ⇒ draft internal guidelines (ensure principles and organisational measures are in place);
- ⇒ organise or provide training (test the client relationship managers on their cross-border knowledge);

We went through the results of the questionnaire that was provided to the ALCO members. The presentation of Mr. Sylvain Aubry was focused on 4 main points:

- ⇒ Decision process: Surprisingly the board seems not to be involved systematically on cross-border topics.
- ⇒ How people perceive the cross-border risks: Front office and even senior management seem clearly to be insufficiently aware of the risks.

¹⁰ At the time of the meeting, already 28 ABBL members had access thereto. KPMG is currently working on extending them to insurance related aspects. The subscription fee is designed to be decreasing with an increasing number of participants.

¹¹ Some institutions have developed a data basis in which all travels are recorded. Keeping such a table up to date seems to be a requirement from the FINMA (Swiss authority).

Newsletter

- ⇒ Conduct of Business/Cross-border policy/Implementation of rules/training should be improved.
- ⇒ Controls seem not yet sufficient: cross-border compliance controls are often not included in the compliance monitoring programme. Feedback of Client Relationship Managers seems often not to be entered in the CRM tool and can consequently not be monitored adequately by certain Compliance Officers.

CONCLUSION

Cross border risk awareness need to be supported by a clear and permanent ‘tone from the top’. The Board and the senior management should be involved in all aspects of cross border business set up.

We are at the dawn of a climate change in Luxembourg banking. Although banking secrecy will most likely survive for quite some time in Luxembourg, doubtful origin of wealth cannot be **hidden** behind professional secrecy considerations. Sustainable perspectives are to be found in the adoption of a clear tax transparent strategy. This will probably imply more work to do and fewer clients to serve.

Improve the awareness of all financial sector professionals to cross border risks is a heavy task. It implies not only to make available the necessary trainings, policies and documentation but also to include additional controls in the Compliance Monitoring Programme.

For WG34¹²

¹² Sylvain Aubry (moderator), Renata Hoes and Charles van Doorslaer (redactors of the summary)

Questions from members

QUESTION

Fund Investment restrictions

Risk diversification requirements for SIFs:

The CSSF circular 07/309 provides clarification on the investment restrictions that SIFs must be adhered to in order to comply with the principle of risk-spreading.

Nevertheless, these risk diversification requirements do not apply to the following investments:

- . “securities issued or guaranteed by OECD Member States or supranational organisations”
- . “target UCIs that are subject to risk-spreading requirements at least comparable to those applicable to SIFs.”

“Similarly, the CSSF considers that the concept of risk-spreading can be interpreted in a flexible way.”

Does the CSSF consider that, under the SIF law, the above-mentioned investments are not subject to any risk diversification requirement?

If so, does the CSSF consider that the principle of risk-spreading is complied with where a SIF portfolio only consists of securities of the exact same type which are issued by a single issuer and are not subject to any risk diversification requirement?

ANSWER

Please find hereafter our current view regarding the two questions raised regarding the risk diversification limits as defined in the CSSF circular 07/309.

1). Does the CSSF consider that, under the SIF law, the following investments are not subject to any risk diversification requirement?

- . “securities issued or guaranteed by OECD Member States or supranational organizations”
- . “target UCIs that are subject to risk-spreading requirements at least comparable to those applicable to SIFs.”

A. Securities issued or guaranteed by an OECD member state or a supranational organization: Securities meeting one of those criteria's are not subject to any risk diversification requirements as per CSSF circular 07/309.

It is our **understanding, that** a SIF could invest up to 100% of its net assets in a single security issued or guaranteed by an OECD member state or a supranational organization, under the condition that such an investment is in line with the investment policy as defined in the prospectus of the fund.

B. Target UCI's that are subject to risk spreading requirements at least comparable to those applicable to SIF's:

Newsletter

As per our understanding, the regulator considers it as acceptable a SIF having a portfolio composed of only one target UCI under the condition that the risk-spreading principle is ensured at the underlying level of the target fund.

2). Does the CSSF considers that the principle of risk spreading is complied with where a SIF portfolio only consists of securities of the exact same type which are issued by a single issuer and are not subject to any risk diversification requirement?

A portfolio composed of securities of the same type issued by the same issuer is not meeting the risk diversification criteria's of the CSSF circular 07/309. (except for securities meeting the two above-mentioned conditions)

However securities issued by the same issuer but not of the same nature should not be aggregated for the 30% risk diversification limit. A SIF could invest up to 30% in bonds and up to 30% in shares all issued by the same issuer.

In a nutshell, it is recommended that practical implementation of the diversification rules for a SIF are pre-cleared by the fund's external auditors in case of any doubt.

Disclaimer

It should be noted that the information obtained in answers provided by the GT 33 is of general nature and is not necessarily comprehensive. Besides, any answer released by the GT 33 should not be interpreted as providing legal advice or legal opinion whatever its nature. ALCO accepts no responsibility for any loss or damage, whether direct or indirect that you may suffer as a result of your use of or reliance on any information contained in answers from the GT 33 or accessed via the ALCO website.

Avertissement

Les informations fournies dans le cadre des réponses du GT 33 ne sont pas nécessairement exhaustives. Par ailleurs, une réponse formulée par le GT 33 ne saurait en aucun cas constituer un avis, une consultation ou une opinion juridique de quelque nature qu'il soit. L'ALCO décline dès lors toute responsabilité en cas de pertes ou de dommages directs ou indirects subis par les utilisateurs des informations contenues dans les réponses données par le GT 33 ou accessibles sur le site internet de l'ALCO ainsi que pour toute action ou omission fondée sur ces informations.

*** Could I ask you what is your opinion of the professional secrecy level for the non-life insurance sector (international health insurance) in Luxembourg? Could you please give us your thoughts about confidentiality versus data protection? Is it the same as for bank secrecy/medical secrecy?**

The regulations for this sector are article 111-1 \ "Loi modifié du 6 Décembre 1991 sur le secteur des assurances\"

In reference to the Law of December 06th 1991 in the insurances sector and especially to the Article 111 as mentioned in your question, there are the following items to underline:

The article 111-1 cites all the concerned professionals by the obligation of the professional secrecy and the dispositions which are ensuing from this obligation:

“Directors, members of the management and supervisory bodies, executives and other employees of insurance undertakings and their agents, as well as insurance brokers, insurance sub-brokers and other employees of insurance brokers, shall be obliged to maintain secrecy regarding any confidential information entrusted to them in connection with their professional activities”.

We have to know that the non-life insurances are composed of goods and liability as well as those linked to disease and physical accidents. To the extension, can be added the activities linked to the financial protection (security, loans coverage, unemployment guarantee, ..), to the juridical area (Defense-Recourse, juridical protection...) as well as assistance services;

Article 111-2 specifies that these dispositions shall apply to:

- “insurance undertakings approved or authorised in the Grand Duchy of Luxembourg for transactions governed by point II of the annex;
- “pension funds under the prudential supervision of the Commissariat aux assurances;
- “persons approved to manage pension funds under the prudential supervision of the Commissariat aux assurances;
- “insurance brokers approved or authorised in the Grand Duchy of Luxembourg for transactions governed by point II of the annex”
(law of 17 July 2008)
- “insurance intermediaries approved or authorised to conduct their business in Luxembourg when they deal with life insurance and other investment-related services.”
(law of 27 October 2010)
- “insurance and reinsurance undertakings and insurance intermediaries approved or authorised in the Grand Duchy of Luxembourg when they conduct credit and caution activities.”

The last point of this Article, related to credit or caution activities, is also related to non-life insurances. These insurances are then also under the obligation of professional secrecy in the context of mentioned activities above.

Newsletter

The Law specifies that penal consequences in case of violation of this obligation are detailed in the Article 458 of the Penal Code as well as for the banking sector.

The scenarios where the professional secrecy is not applicable are detailed in the Article 111-1, point 2 to 6.

It is important to note that the Article 111-1 point 6 specifies that the obligation to professional secrecy is not compulsory anymore for any kind of insurance (life or non-life), if the insurance provides information in the context of services contract with one of PSF listed in the articles 29-1, 29-2, 29-3 and 29-4 of the law of April 05th 1993 related to the financial sector.

It is also good to note the Article 111-3 which concerns professional obligations as defined by the law of November 12th 2011 related to the anti-money laundering and terrorist financing. The obligations of cooperation with authorities in case of suspicion are an exception to the obligation of professional secrecy.

Disclaimer

It should be noted that the information obtained in answers provided by the GT 33 is of general nature and is not necessarily comprehensive. Besides, any answer released by the GT 33 should not be interpreted as providing legal advice or legal opinion whatever its nature. ALCO accepts no responsibility for any loss or damage, whether direct or indirect that you may suffer as a result of your use of or reliance on any information contained in answers from the GT 33 or accessed via the ALCO website.

Avertissement

Les informations fournies dans le cadre des réponses du GT 33 ne sont pas nécessairement exhaustives. Par ailleurs, une réponse formulée par le GT 33 ne saurait en aucun cas constituer un avis, une consultation ou une opinion juridique de quelque nature qu'il soit. L'ALCO décline dès lors toute responsabilité en cas de pertes ou de dommages directs ou indirects subis par les utilisateurs des informations contenues dans les réponses données par le GT 33 ou accessibles sur le site internet de l'ALCO ainsi que pour toute action ou omission fondée sur ces informations.

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

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

Groupe de travail 20

Funds practices and recommendations AML

Responsable Guillaume BEGUE
Téléphone +352 26 96 22 31
guillaume.begue@bnpparibas.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 30

Domiciliation de société

Coordinateur Sophie RASE
Téléphone +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

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

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

Working group 20

Funds practices and recommendations AML

Owner Guillaume BEGUE
Phone +352 26 96 22 31
guillaume.begue@bnpparibas.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 30

Domiciliary agent

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

Groupe de travail 33

Réponses aux questions des membres

Coordinateur Christophe BECUE
Téléphone +352 48-48-80-80
cbecue@efa.lu

Groupe de travail 34

Tables rondes

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

Groupe de travail 35

Doctrine

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

Groupe de travail 38

Assurance

Coordinateur Rob SONNENSCHNEIN
Téléphone +352 319 911 313
rob.sonnenschein@luxglobal.lu

Groupe de travail 39

Problématique de l'outsourcing

Coordinateur David RENAUD
Téléphone +352 26 05 21 81
david.renaud@rbcdexia-is.net

Groupe de travail 40

Responsabilité du CO dans les sociétés de gestion

Coordinateur Bernard PONS
Téléphone +352 26 39 86 54
bpons@purecapital.eu

Groupe de travail 41

Gouvernance

Coordinateur Jean Noël Lequeue
Téléphone +352 26 63 86 27
jean-noel.lequeue@icesa.lu

Working group 33

Answers to questions of members

Coordinator Christophe BECUE
Phone +352 48-48-80-80
cbecue@efa.lu

Working group 34

Round tables

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

Working group 35

Doctrine

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

Working group 38

Insurance

Coordinator Rob SONNENSCHNEIN
Phone +352 319 911 313
rob.sonnenschein@luxglobal.lu

Working group 39

Outsourcing's issues

Coordinator David RENAUD
Phone +352 26 05 21 81
david.renaud@rbcdexia-is.net

Working group 40

CO responsibilities for a Man Co

Coordinator Bernard PONS
Phone +352 26 39 86 54
bpons@purecapital.eu

Working group 35

Governance

Coordinator Jean Noël Lequeue
Phone +352 26 63 86 27
jean-noel.lequeue@icesa.lu

MEMBRES ET VIE ASSOCIATIVE

MEMBERS AND ASSOCIATION ACTIVITIES

Nombre de membres (au 30/06/2012):

Banques	242
Fonds	139
Fonds / Banques	22
Assurances	53
Consultants / Réviseurs	50
Admin. et domiciliation de sociétés	21
Avocats	12
PSF	49
Gestion de fortune	31
Autres	22
Effectif total:	641

Membres effectifs	507
Membres d'honneur	134
Membres de courtoisie	10

Effectif total: 641

Réunions et activités:

Mensuellement	Réunions du conseil d'administration
1 / 2 x par an	Réunions plénières
2 / 3 x par an	Rencontres informelles autour d'un thème

Number of members (as per 30/06/2012):

Banking sector	242
Funds sector	139
Funds / Banking sector	22
Insurance sector	53
Consultants / Auditors	50
Admin. and company domiciliation	21
Law firms	12
SFP	49
Asset management	31
Other	22
Total number:	641

Active members	507
Honorary members	134
Courtesy members	10

Total number: 641

Meetings and activities:

Monthly	Board meetings
1 / 2 x per year	Plenary assemblies
2 / 3 x per year	Informal meetings on a subject

– **Board of Directors:**

Jean-Noël LEQUEUE	President
Claudine FRUTSAERT	Vice-President, insurance section
Patrick WATELET	Vice-President, fund section
Vincent SALZINGER	Vice-President, bank section
Marie-Hélène CLAUDE	Treasurer
Guillaume BEGUE	Director
Patrick CHILLET	Director
Rolland DILLIEN	Director
Olivier GILSON	Director
SUNDHEVY GOÏOT	Director
Thierry GROSJEAN	Director
Rob SONNENSCHNEIN	Director
Emmanuelle HENNIAUX	Adviser
Bernard PONS	Adviser
Patrick SCHOTT	Adviser
David RENAUD	Adviser
Tim WINFIELD	Adviser

– **ALCO Secretariat:**

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

– **Bulletin Secretariat:**

Emilie Schmitt
secretariat@alco.lu

VISIT OUR WEBSITE: www.alco.lu
