



Association Luxembourgeoise
des Compliance Officers
du Secteur Financier

Newsletter

N°21

January 2011

Editorial



Dear ALCO member, dear reader,

I would like to begin by extending to you, on behalf of the Board of Directors, our very best wishes for 2011. We hope that all your expectations will be satisfied in 2011 and that the year will bring you both professional and personal fulfilment. 2011 is also, as you are aware, the year in which we celebrate our association's 10th anniversary. We look forward to welcoming all of you on 20 January at the Conservatoire de Musique in Luxembourg City for a fitting celebration.

The 21st ALCO newsletter starts the New Year with an interview with Gérard Lommel, Head of the CNPD, in which he explains the main tasks of the independent administrative authority with responsibility for the protection of personal data. In an open discussion, he deals with the key issues and in particular the Compliance Officer's role in this area, which varies from one institution and FSP to another.

In another article, where she again does not mince her words, Catherine Bourin, the ABBL representative to ALCO, takes a realistic look at the new anti-money laundering system put in place in Luxembourg following the severe FATF evaluation. The law of 27 October 2010 and the other legal provisions in this area suffer from this unequivocal objective but appear inevitable. We are now awaiting the CSSF regulation to complete the system.

The following article, dealing with money laundering risks in electronic commerce, illustrates new money laundering methods which largely escape the checks of Compliance Officers or banks and other financial institutions.

Two roundtables, organised successively in English and French, focused on a risk-based approach to accepting and monitoring clients. Although all the institutions concerned have now adopted a risk-based approach, its implementation and form logically vary according to the specific risks of each financial sector professional.

Happy reading,

Jean Noël Lequeue
President of ALCO

Interview

Meeting with Mr Gérard LOMMEL, President of the CNPD

Question 1: the CNPD's resources

Gérard Lommel: (with a broad smile) – informed us that there is a consensus among the members of the Article 29 working group (see “below on this subject”, question 6) not to make any declarations to the effect that the resources available are sufficient; more seriously, he then discussed the Commission's remit and provided us with details of its powers and resources;

The National Data Protection Committee (National Commission) is an independent administrative authority set up by the law of 2 August 2002, which entered into force on 01.12.2002, on the protection of persons with regard to the processing of personal data. The National Commission's remit is essentially to control and check the legality of personal data processing and to ensure that the fundamental rights and freedoms of natural persons as regards the processing of personal data are respected.

Its main responsibilities include in particular:

- checking the legality of the collection and use of data subject to processing, in particular through a system of prior authorisations and à posteriori controls;
- providing guidance and information to data processing controllers about their obligations;
- raising awareness about respect for the fundamental rights and freedoms of natural persons, particularly their private lives, and informing the public of the rights of the persons concerned;
- examining complaints and requests for checks on the legality of processing;
- advising the government on this subject.

The National Commission also has responsibility for ensuring the application of the provisions of the amended law of 30 May 2005 on the protection of personal data in the electronic communications sector and its implementing regulations.

Among its prerogatives, it has investigative powers which give it a right of direct access to premises other than residential premises where data is processed as well as to the data processed and to carry out the necessary checks.

It also has the possibility (used only on a few occasions so far) to impose various disciplinary sanctions subject to a right of appeal.

After a difficult start because of its limited resources, especially given the large number of cases it had to handle, the Commission is now fully operational – it currently has 10 staff (including the College), including 6 lawyers and an IT engineer.

Le Bulletin

Question 2: the role played Compliance Officer within financial institutions:

- a. Data processing?
- b. Data protection?

Article 4 of the amended law of 2 August 2002 sets out the accountability procedures resulting from directive 95/46/CE and stipulates “The controller will ensure that he processes the data in a fair and lawful manner.” Whereas the data controller is, pursuant to article 2, letter **n** of the law of 02 August 2002, amended as a “natural or legal person, public authority, agency or any other body which solely or jointly with others determines the purposes and methods of processing personal data”, article 40 of the same law provides the possibility for any controller to appoint a data protection official, whose identity is to be communicated to the National Commission. The role of these data protection officials is to advise (being familiar with internal processes or a close external consultant) the company that has commissioned them to fulfil its data protection obligations and to ensure compliance with the law. They liaise directly with the CNPD to agree on the interpretation of legal texts and are, as it were, “in-house” correspondents that act as a mediator in dealing with complaints and handling the initial examination of complaints and first-line legality checks for the CNPD.

Mr Lommel was forthright in saying that he was disappointed by the lack of enthusiasm of banks regarding the possibility of appointing their “Compliance Officer” as their data protection official. To date only around twenty banks have used this possibility, which is disappointing, especially as it is a natural role for a “Compliance Officer”. He added that the ABBL had been approached to promote this idea. German banks seem to be the most positive about the idea of appointing their “Compliance Officer” as a data protection official (the latter must have a certain independence and be a high ranking official within the bank). Moreover their role must not be seen as that of a “police officer” or a “spy” within the organisation. For the President of the CNPD, they are a special contact person who speaks the same language as the CNPD which also shows a certain restraint when such a data protection official is appointed. In principle, no on the spot controls for institutions with a data protection official.

Question 3: In general, are you satisfied with the attitude of the entities under your supervision as regards the CNPD’s directives?

As regards the banking sector in particular, the cooperation of banks can be described as very good. The President of the CNPD attempts to maintain a commercial attitude at this level and spreads the good word whenever the opportunity arises – for example he recently participated in a meeting of a working group of German banks and intends, in the future, to further develop this awareness-raising role at all levels. In this regard, he sees R. Diligent, the President of the CNIL (French counterpart), as a good example to follow – he describes him as an “expert in communication” who has significantly reinforced the CNIL’s visibility in France.

In Luxembourg, it is not the banking sector which causes concern, but it is always tricky to give concrete examples of problems other than those which have already received considerable media coverage, such as the video-surveillance of the Aldringen centre, the Domaine Thermal de Mondorf, Auchan, Google, etc.

Basically, the CNPD’s short history can be summarised in three phases:

- initially, during the first phase, it focused on publicising the law,
- the second phase consisted of putting in place complaint handling procedures,
- today, the CNPD is in a transitional stage, moving towards phase three which will involve increasing and improving “guidance”.

Le Bulletin

Question 4: Some entities consider that the restrictions imposed by the CNPD on recording telephone conversations undermine their security.

Gérard Lommel: It is true that the provisions and procedures of the Luxembourg law are more elaborate than those of most other Member States as regards employee protection. Moreover, article 11 of the law has been integrated into the Labour Code and the point of view of the trade unions has been widely taken into account. The cases when files may be opened are set out in an exhaustive list and implement, albeit in a somewhat rigid way, the principles of need, loyalty and proportionality provided for in the directive in order to achieve a balance between the interests of the respective parties.

Although some observers consider that the law is too strict, it has nevertheless allowed us to authorise the recording of e-mails and telephone conversations (provided that this is justified by the need to obtain proof).

As regards video-surveillance, employee workstations cannot be subject to such surveillance on a permanent basis, but it is nevertheless authorised in entrances, exits and other high-risk areas, etc.

Question 5: Coordination of the CNPD and the CSSF.

Gérard Lommel: The CNPD has always tried to foster such coordination but it is clear that the perspectives of the two bodies are sometimes different, given that they are governed by specific laws. Both watchdogs may have their own point of view. The CSSF has recently shown itself to be more open to the idea of data storage in third countries.

Question 6: the CNPD's position as regards its counterparts in other European countries (CNIL).

Gérard Lommel: Article 29 of the European Directive no. 95/46 of 24 October 1995 specifies: "A Working Party on the Protection of Individuals with regard to the Processing of Personal Data, hereinafter referred to as 'the Working Party', is hereby set up". This group consists of a representative of the authority designated by each Member State, as well representatives of Community institutions and bodies.

This group meets regularly and the various national authorities exchange their experiences and develop joint positions favouring the homogeneous application of the directive throughout the EU. However, some of the authorities – such as the CNIL – have succeeded in establishing a visibility which strengthens their influence.

The importance of the cooperation between the data protection authorities of the various Member States has increased spectacularly in recent years following globalisation and technological advances. Difficulties in determining the applicable law have increased in line with the difficulties in determining where data is actually processed. In practice, it is very difficult in an IT network to determine the "place" where data is processed (take the example of "cloud computing" or simply that of multi-outsourcing. This problem is even more crucial given that third countries may be involved.

Finally, in general, the positions of the various data protection commissions of the Member States are very close. There are however some significant differences between some Northern European countries, the United Kingdom and practices in some domains in comparison with the rest of the European Union.

There are some differences even as regards the concept of personal data: the Anglo-Saxon concept is limited in a far more restrictive way to that of nominative data, whereas we take into account all

Le Bulletin

information that may relate to an identifiable person. However, we believe that we are capable of being just as pragmatic and of adopting a business-friendly attitude, whenever there is a real determination to find a balanced solution which takes account of legitimate expectations concerning respect for individual privacy rights.

Interview conducted by Jean-Marie Legendre and Patrick Schott

Articles

The new “post-FATF evaluation” anti-money laundering system or “Might is Right”¹

In May 2009, a FATF delegation visited Luxembourg to evaluate its anti-money laundering system and to assess its compliance with the recommendations issued by this intergovernmental body. The resultant report, published in February 2010, was fairly mediocre, with poor compliance ratings: 9 “non-compliant” and 30 “partially compliant” versus only 9 “largely compliant” and 1 “compliant” ratings.

Given the threat hanging over Luxembourg of a “grey list” classification and the extremely harmful consequences of such a classification for Luxembourg’s position as a financial centre, the Luxembourg government issued a government bill in August 2010 which was adopted on 13 October 2010 by the Chamber of Deputies. Thus, the (sole) objective of the law of 27 October 2010, reinforcing the legal framework for combating money laundering and terrorist financing, is to respond to the FATF’s criticism. The aim of this new law is to integrate a series of amendments into the system in force in Luxembourg affecting no less than 21 different laws as diverse as the law of 7 March 1980 on the organisation of the judicial system, the amended law of 31 January 1948 on the regulation of air navigation and the amended law of 20 April 1977 on gaming and betting on sports events.

1. A patchwork text for cosmetic purposes

The feeling among many people that legal language is obscure will be reinforced by the text of the law of 27 October 2010. It seems to be a model of “legalese”, containing an incredible number of cross-references and formulas which non-lawyers will find puzzling. By way of example, article 5 of this law stipulates: *In article 8-1, point 3 of the aforementioned law of 19 February 1973, the reference to “article 8, points (a) and (b)” is replaced by a reference to “article 8, paragraph 1, points (a) and (b)”*. The text is a patchwork of sporadic amendments and as a result is practically illegible and incomprehensible for novices.

This curious legislative technique is, in reality, the consequence of the avowed objective of this law, which is intended solely to adapt the legislative framework in force in Luxembourg relating to combating money laundering and terrorist financing to the requirements of the FATF. This is obvious in the comments on articles in the government bill from the number of references to the aim of: *“...responding to the criticism resulting from paragraphs [x,y,z] of the mutual evaluation report”*.

Solely motivated by this concern, this law contributes nothing to Luxembourg law, in particular when it limits itself to giving a legal character to certain well-established case-law positions. Thus, pursuant to the new article 506-8 of the Criminal Code, *“the offences defined in article 506-1 are punishable irrespective of any proceedings or convictions delivered for any of the predicate offences listed in article 506-1”*. It has however always been clear, according to the authorities and case law in Luxembourg, that proof of a predicate offence does not depend on a prior conviction and that the offence of money laundering is indeed an autonomous offence².

To quote another example, article 506-1 (2) of the Criminal Code is supplemented by a reference to “disguise”, so that the offence of money laundering is also that by which a person knowingly

¹ The opinions expressed in this article are solely those of the author.

² A ruling of the Court of Appeal of 3 June 2009 specifies: *‘...there is however no need for the perpetrator of the predicate offence to have been the subject of prior proceedings or a conviction identifying the crime or offence with the help of which the material benefits were obtained’*.

provides assistance to the “*investment, concealment, disguise, transfer or conversion*” of property, even though the notion of “*concealment*” logically covers that of “*disguise*”.

Moreover, as regards identification of the beneficial owner, the law requires professionals to take “*reasonable*” measures instead of “*risk-based and adequate measures*” (article 4, point 8, of the law of 27 October 2010). Another example is the fact that suspicious transactions must now be reported “*without delay*” instead of “*promptly*” (article 4 point 20). In practice, these purely cosmetic amendments will have only a limited impact on the practices of professionals.

2. Confusion and inconsistencies

At a time of regulatory simplification, there is a risk that the law of 27 October 2010 may make our law more confused and inconsistent. The following are examples of this.

First, the aim of satisfying the FATF leads to some duplication between various laws. For example, it is specified that professional secrecy obligations no longer apply to the Financial Intelligence Unit (FIU) (new article 5-4 of the amended law of 12 November 2004). The aim of this provision is to emphasise that there are no legal obstacles preventing professionals from reporting suspicious transactions to the FIU. However, as regards cooperation with the authorities, professional secrecy obligations do not apply pursuant to article 41(2) of the law of 5 April 1993 on the financial sector. This same precision is again specified in article 39 of the same law in order to specify that the rules of professional secrecy do not apply when the information requested by the authorities concerns “*information accompanying transfers of funds and corresponding recorded information*”. Thus, we find the rule whereby professionals cannot refuse to disclose information to the authorities on the grounds of professional secrecy in three different places (including two in the same law). While this situation should not be clear to the FATF, it was already obvious to professionals in Luxembourg.

Secondly, a curious legislative technique has led to the same law being amended by two different texts. Article 10 of the law of 27 October 2010 is intended to amend article 3 of the law of 8 August 2000 concerning mutual legal assistance so that this provision concerns exclusively fiscal related matters. At the same time, on the same day, the law of 27 October 2010 on international legal assistance in criminal matters reforms certain provisions of the law of 8 August 2000, and in particular the same article 3, without however including the word “*exclusively*” in the text. This therefore creates a problem of conflict of law, with two laws on the same date changing the content of the same law.

Furthermore, the legislative technique used by the law of 27 October 2010 is fairly surprising and creates a new type of law: the “Russian Doll” law, since articles 24 and 25 of this law introduces ... two new laws, on the one hand, that of 27 October 2010 on the organisation of measures to monitor the physical transportation of cash entering, transiting via or leaving the Grand Duchy of Luxembourg, and, on the other hand, that relating to the implementation of United Nations Security Council resolutions as well as acts adopted by the European Union concerning prohibitions and restrictive measures in financial matters with regard to certain persons, entities and groups in the context of combating terrorist financing. Rather than enacting several separate, autonomous laws, we now have two legal texts interlinked in a third text, the anti-money laundering law. However, these texts are stand alone texts and could have been adopted separately.

The aim of the law of 27 October 2010, established by the aforementioned article 24, is to introduce controls at Luxembourg’s borders on cash movements. However, Regulation (EC) no. 1889/2005, considering Europe to be a single territory, had established these controls at the European Union’s borders. The law of 27 October 2010 is thus a negation of not only the idea of the common European space, but also the Schengen process and the principle of the free movement of capital enshrined in the founding treaties. The FATF is forcing European States to backtrack on the process initiated many years ago with a view to creating the single market. In this regard, the FATF bases its actions on the poor results of controls on traffic from third party States: “*Between July 2008 and May 2009, only 12 declarations were recorded whereas more than 1800 flights from countries outside the European Union arrive every year in Luxembourg. No cases of failure to declare or false declarations were detected and no assets were seized. The particularly low number of declarations leads the evaluation team to question the quality of the implementation of the system and the controls carried out in order to ensure compliance with the declaration obligation*”.

3. Would we dare to be “politically incorrect”?

From a strictly legal point of view, the standards laid down by the FATF are not compulsory as such and have no direct effect. They have no place in the hierarchy of standards. They are recommendations addressed to governments. These recommendations are not addressed to professionals, who are not bound by them. They have no legal status other than that which States choose to give to them, that is to say whether or not to transpose them into national law. However, because of the possible penalties if the FATF rules are not taken into consideration, it is in the interests of States to integrate the FATF rules into their national legal system. It is important to specify that the fight against money laundering and terrorist financing as such are not called into question here, as professionals have long since introduced the means of preventing these scourges into their internal procedures.

The economic consequences of not complying with the conclusions of the report adopted in February 2010 by the FATF on Luxembourg could be dramatic for the financial centre. However, Luxembourg's legislative system was fully in compliance with the third European Directive on combating money laundering and terrorist financing (Directive 2005/60/EC). In reality, the Community texts seem to be out of synch with the FATF standards. By way of example, the third directive allows simplified due diligence measures to be applied in certain special cases. Thus, credit institutions and financial institutions located in the European Union or the European Economic Area qualify for simplified due diligence measures. The FATF, taking the view that this is purely and simply a total exemption from the due diligence obligations, considers that these rules do not comply with those of the FATF. The evaluation report notes that *“all these provisions are based on equivalent obligations regarding combating money laundering and terrorist financing to those of Luxembourg issued by the Community Directive. They do not relate to the FATF recommendations which constitute a higher standard”*.

It is also important to emphasise that the FATF evaluation concerns not only the legal texts but also the effectiveness of the system put in place. This is assessed on the basis of one major criterion: the importance of Luxembourg as a financial centre in relation to the statistics which were submitted to it by the authorities. The report notes that *“in the light of the importance of the financial centre, the low number of significant convictions in Luxembourg for money laundering matters is not dissuasive for criminals”*. Similarly, as regards combating terrorist financing, the report notes that *“the effectiveness of the system cannot be tested in the absence of the prosecution of terrorist financing”*. The FATF does not seem to be convinced by the argument that as Luxembourg is an international financial centre, that it does not have purely domestic cases, only cases inevitably linked to other States. It also seems to disregard the argument that it is thanks to effective mutual legal assistance and cooperation between the authorities of various States that it has been possible to judge some cases ... but in a State other than Luxembourg.

In conclusion, the law of 27 October 2010 has not revolutionised Luxembourg's anti-money laundering system. In reality, the FATF has essentially criticised the lack of proof of the effectiveness of anti-money laundering mechanisms in Luxembourg. To do this, it has based its findings on the low number of declarations of suspicious transactions in comparison with the number of financial institutions established in Luxembourg.

It is important to be aware that, at the time of the next evaluation of Luxembourg as part of the 4th round of mutual evaluations, due to start in 2012, the FATF will primarily endeavour to verify changes in relation to its observations. Therefore, first and foremost, Luxembourg will have to demonstrate the effectiveness of its system, if indeed there is an evaluation... it must be borne in mind in this regard that the FATF is an intergovernmental body, created by an economic declaration of the G7 and not by an international convention that is binding on the signatory States. Its existence is based on a temporary 8 year mandate which is due to expire in 2012. As Jean-Jacques Rousseau³ wrote: *“The strongest is never strong enough to always be the master, unless he transforms strength into right, and obedience into duty”*.

Catherine BOURIN
Doctor of Law

³ “The Social Contract”.

Money laundering risks in electronic commerce: some new money laundering techniques

Nowadays, the risks of money laundering have shifted to new areas, even if the highest risk sectors are still car dealers, the recreational and marine sector, real estate, lotteries and games of chance, horse racing and casinos. Nevertheless, alongside these so-called “traditional” sectors, there are also numerous cases of money laundering on the Internet. In its 2007 annual report, Luxembourg’s Financial Intelligence Unit mentioned among others the case of a local bank specialised in electronic payments: *“Over the last six months of 2007, one bank submitted some 112 declarations to the FIU. This figure can be explained by the specific activities of the bank in question which mainly executes financial transactions in connection with electronic commerce between private persons, which enables this professional organisation to have direct access to information concerning the operation behind the financial transaction. This advantage is, however, mitigated by the difficulties which exist regarding the identification (even simplified) of the parties beyond the link that can be established between a party and the bank card used for the transaction”*.

Over and above online banking and electronic purse systems, it is clear that the development of telephone banking and Internet-based casinos could facilitate money laundering transactions. The intensive use of 24/7 telephone banking services represents a significant obstacle to investigations regarding money laundering and terrorist financing. In Asia, it is now possible to use a mobile phone to make payment, either via an optical reader or by sending an SMS. This payment and therefore financial transaction possibility can be easily exploited by criminal networks wanting to launder money, since most mobile phones can be topped-up by buying telephone cards which are readily available almost everywhere, in supermarkets, petrol stations, bookshops, etc. The transaction is routed via the telephone operator’s network, but the card itself can be paid for in cash in a store without any prior identification requirements for this type of telephone. Anyone can buy a mobile phone in a supermarket and obtain a rechargeable smart card in the same supermarket without having to provide any ID.

Remote banking implies a distance relationship between the bank and its customer, thereby reducing or even eliminating the banker-customer physical contact on which the traditional concept of identification and customer knowledge was based. Although these services obviously have practical advantages for customers in terms of flexibility, they make it more difficult to detect money laundering activities in the absence of traditional control methods. On the basis of the information available on the Internet, casinos in several countries offer complete anonymity to potential players, who use their credit card to bet. The money laundering risk is even more obvious if the casinos in question also manage the accounts of their customers who have played over the Internet.

The casinos and gaming sector in general is a potential cause of concern for the authorities, because it is an expanding sector which is at the heart of the development of the tourist industry in many countries. However, the consequences of multiplying non-casino gambling and in particular its development on the Internet (such as “Bingonet”) should be analysed in far greater detail since most physical casinos are highly regulated⁴. The same applies to commercial transactions on the Internet.

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

Le Bulletin

The Internet can facilitate the anonymity of its users, since in certain cases all they have to do in order to register is provide an electronic address, which does not at all guarantee the user's identity. Consequently, every transaction made using this address will be completely anonymous.

The highest risk electronic transactions are those which are directly executed between users, in particular when the seller and buyer operate on an e-commerce site where there is no internal control system to prevent the risk of money laundering or terrorist financing⁵.

The highest risk payment methods which are currently used are prepaid debit cards issued by leading card issuers or gift cheques or cards since these methods provide users with total anonymity, as they can be obtained almost anywhere and paid for in cash. It is important to note that the companies which offer electronic payment services sometimes find it difficult to distinguish between a bank debit card and a prepaid card since the companies which issue debit cards often use the same card numbers⁶.

Commercial websites as well electronic means of payment can be used not only to sell or buy illegal products, such as drugs or counterfeit articles, but also to avoid paying taxes (VAT or income tax). They can also make it easier to split money collected illegally, thereby facilitating the transfer of funds to another account or another country or quite simply by making other online purchases.

Criminals can also open their own commercial website in order to sell illegal products via the site and use an electronic payment service provider to execute their transactions. Another possibility involves executing fictitious commercial transactions between two commercial websites, bearing in mind that it is not compulsory to use an electronic payment services provider for this purpose, since all the seller needs to do is link a bank account to the site or obtain payment by postal transfer to receive payment for fictitious articles or products which will never be delivered to the buyer. The buyer will not complain since there is collusion between the two parties. The beneficiary will not have any problems explaining the source of the funds received, since they come from a sale and the buyer can justify the expenditure with a purchase. Commercial websites authorise large-value transactions which enable criminals to launder large sums of money rapidly. The same criminals are sometimes even willing to accept a small loss for money laundering purposes, in particular by sending emissaries to buy luxury products, paid for in cash, which will then be sold on an Internet site at a very attractive price to facilitate the disposal of the goods.

The above examples demonstrate that it is possible to disguise the criminal origin of the laundered assets without necessarily having to involve a credit institution or a financial sector professional. Fast-moving technological advances increase the money laundering possibilities for criminal networks which often join forces with a wide-range of specialists with substantial financial resources in order to achieve their aims.

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

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

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

Round Tables

NEW PRODUCTS: Approval Process

Present: 14 ALCO members

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

For WG 34:

- Jean-Michel Righi, Société Générale, moderator
- Charles van Doorslaer, KBL European Private Bankers, secretary

Introduction

For this 3rd thematic roundtable of 2010, 21 members expressed an interest and 14 of them participated in the roundtable devoted to questions concerning new product approval processes. The panel was made up of bankers, asset managers, as well as fund and insurance specialists. The main exchanges are set out in the below summary.

Answers to the questionnaire

A questionnaire was sent to all ALCO members. You will find below a summary of the answers to the 11 questionnaires which were returned duly completed. The main lessons that can be drawn from them are included in the minutes. Some aspects, such as examples of definitions of the “new product/service” concept, are annexed to this document.

Why a New Products/Services Approval Committee (NPC)?

The NPC is seen as a fundamental **risk management tool**. It can be linked to the ICAAP⁷ process as a whole, but it is also, and above all, an **awareness-raising and decision-making tool**, a forum which enables participants with different competences to express their views and understand the approaches and constraints of each of the services or departments concerned. The involvement of participants in this type of committee also facilitates the gradual development of a spirit of close cooperation and trust between the various services and departments concerned by new products/services.

An NPC process is often put in place as a result of a parent company initiative, as part of a group policy.

Several participants confirmed that the existence of this type of committee in their company is a recent phenomenon (less than 2 years). In many cases, the decision to set up an NPC or reactivate a committee or process that had become a pure formality (or in some cases had unfortunately even been ignored) was triggered by the financial crisis, or even by a specific incident.

In many cases, the NPC, composed of business line experts, is set up by the Executive Committee which then delegates to it the power to decide whether or not to approve new products and services. If there is a disagreement within the NPC, the decision may be “escalated” to the Executive Committee.

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

Is the committee's existence formalised within the company? Is there a specific procedure governing the way it works? Timing? Risks?

The answer is clearly “yes” for the vast majority of participants. However, some participants had decided to take part in the roundtable precisely because they were considering putting in place or formalising such a committee.

Generally, the new product/service initiator takes the initiative of presenting it to the NPC. The product/service should be presented to the NPC as early as possible in the process, so that the product and/or the way in which it is described can be improved, thanks to the input and questions of other departments. Some project initiators may hesitate about submitting their project at an early stage to the committee for its opinion for fear that this might increase criticism and slow down the process. When a product is presented to the committee at a very advanced stage, this can help to obtain a decision more rapidly and even force the hand of the committee (“you can take it or leave it”, “this project is the fruit of many hours of work, so... don’t put a spanner in the works by “nit-picking”!).

It is necessary therefore to strike a delicate balance between the presentation of a project which is sufficiently advanced so as not to invite criticism and that of a product, not yet finalised, so that suggestions for improving it can still be taken on board.

When, in some cases, the approval process is completed whereas the product marketing process has already been launched, the presentation of the product to the NPC is above all intended to reach agreement on a final document, including not only a detailed product description and commercial documents, but also the various risk analyses.

What is the purpose of the NPC? How should the “new product/service” concept be regarded?

Definitions and approaches inevitably vary from one company to another. The answers can in fact vary considerably according to the company’s activity or culture. For examples of **definitions** of the concept, readers should consult the annex. Among the proposals, a very broad definition is likely to satisfy most people: “Any product or service for which a risk analysis has not yet been carried out or validated”.

The objective for **bankers and fund managers** is to anticipate clearly all the risks which the new products or services which they have developed or selected might entail.

Insurers also (and above all) want to understand clearly and categorise existing products, developed by their banking counterparts and others. It would seem that the **UCI** sector is the most experienced, even the best organised as regards approval processes. As for **private clients**, designers and distributors of new products and services seem less inclined to submit their new ideas to colleagues of other entities for approval.

It is also interesting to note that, irrespective of the business line, the **approach** may be “marketing” focused or, conversely, “operationally” focused. Some institutions feel that priority should be given to ensuring that a product and its marketing are not likely to be criticised, or even result in complaints being made to the authorities or a court ruling against the institution. Others are above all concerned about the operational risks: are their systems, processing chains, the infrastructure and know-how capable of handling the follow-up to these new products/services? In some cases, the risk does not stem from the product itself, but concerns more the organisation’s

organisational capacity to handle the products. Nevertheless, in both cases, the aim seems to be to adopt a “**global**” approach rather than merely carrying out a ‘**technical**’ analysis.

The parties involved

In principle the business line concerned is responsible for **submitting a project** to the NPC. In some cases, a designated department is responsible for the process, for example the Marketing, Compliance or Risk Management Departments, or even a dedicated department.

The **composition of the NPC membership** may be variable, depending on which projects are on the agenda for approval. The survey clearly shows that the core permanent members tend to come from the Risk Management, Legal and Compliance Departments. They are then joined, in the vast majority of cases, by representatives of the Management, “Operations” (BO and MO) and IT Departments.

The non-involvement of Compliance Officers is, for most of the institutions an error from the past which needed to be corrected. It now seems to be accepted that Compliance Officers must be involved on a permanent basis in the process.

Who acts as secretariat? Approaches also vary on this subject: a permanent dedicated NPC secretariat in one case, a rotating secretariat among participants in another case, and various designated departments (such as the Compliance, Risk Management and Marketing Departments) for the rest of the participants.

One of the challenges is the speed of the approval process

The creation of **2 different procedures** is conceivable: a **plenary** validation (the procedure can take time) or a **rapid** validation procedure, by means of a circular approval.

The latter solution makes it possible for several new products to be approved every day, thanks to the use of e-mail which facilitates communication between all the NPC members. It is above all used in cases where the new product/service is similar to a product which has already been approved, or is part of an existing range of products already reviewed by the NPC. In such cases the main risk stems from a change to an element which might initially appear insignificant, but which could nevertheless be grounds for rejecting the new product.

By way of example, take the case of a change of issuer for an unchanged underlying instrument. If the rating and reputation of the new issuer are good, the product will be approved without difficulty. On the other hand, if it transpires that the new issuer of the structured product is also, for example, the issuer of the underlying instrument, a conflict of interest may be raised as reason for refusing the change.

In order to facilitate rapid and efficient decision-making, **guidelines** may be drawn up in order to make it easier to detect borderline cases for which a prior consultation of NPC members is indispensable. Some basic rules can be established, such as for example the principle that the issuer of the underlying product cannot be the same as the issuer of the product itself, or a rule that products whose “term sheets” are difficult to understand for professionals cannot be marketed to private clients, or a rule that “lottery” type products are not approved.

Some participants also raised the possibility of a very formal NPC approach, with the committee meeting only once a quarter. To satisfy the need for rapidity and efficiency, other approaches and meetings used for partial approvals would then need to be organised in between formal meetings. In this case the quarterly meeting would mainly be used to formalise the process as a whole and ratify the (partial) decisions thereby formalising them as a commitment of the Executive Committee.

As a result of the crisis some NPCs have been given the task of **reviewing all existing products** (that is to say those still present in client portfolios) in order to re-examine their risk in the light of the events and problems highlighted by the crisis.

Decision-making and formalisation process

In general, decisions are adopted on a unanimous basis. All the participants must sign to indicate agreement. In some cases, the approval may be subject to specific conditions. In the absence of unanimous agreement, the file has to be escalated, either to the managers of the participants who have been unable to reach an agreement or to the upper management or to the parent company's NPC.

The decision-making of the NPC can be formalised in different ways and organised by procedures varying in complexity. Often the signature of all participants or of all the NPC members must be appended to the descriptive documents. The decision is then circulated by e-mail to the NPC members and the people concerned (e.g. the Executive Committee). These addressees can then, in turn, convey the decisions to the interested parties. As regards the formalism of the document recording the decision, each bank seems to have its own practices as regards the structure, form and content of this document.

What is the Compliance Officer's role in the decision-making process?

In some NPCs, all participants are called upon to analyse and comment on the new product, while limiting their comments strictly to their area of competence. In others, on the contrary, all participants can express themselves freely on all aspects and risks.

It seems accepted that the **Compliance Officer's main role** is to analyse the investor protection risks (suitability, best execution, conflicts of interest, etc.), to check whether the documentation intended for clients is understandable and transparent and complies with all the presentation rules (depending on the institution, this role may be shared with the Legal Department). The Compliance Officer is also required to check that the product name and its description are not misleading for clients and do not create any confusion. The Compliance Officer also has to check whether, from an ethical point of view, any complaints could be detrimental to the institution's reputation. Both the regulatory aspect and the reputation risk are therefore among the points on which the Compliance Officer's opinion is sought.

Are Compliance Officers also involved when the institution is acting on its own behalf? This is far less frequent. However, they could certainly contribute added value, especially in the case of conflicts of interest, or where ethical issues or a reputation risk is involved. Some major financial institutions caught up in the turbulence of the crisis probably now regret not having involved their Compliance Officer.

Risk indicators and classification of risks related to new products

For lack of a single European classification, the products are classified according to the geographical regions where they are distributed or according to the classification used by the parent company. The following aspects were raised:

- The most frequently used risk indicators are the level of capital protection, the complexity of the product and the internal risk level.
- "Should the NPC limit itself to a purely technical approach to the product/service, or should it adopt a global approach?"

From an efficiency point of view, the approach should be global, but very often the approach is centralised and then "adapted to the local source". This can lead to the emergence of new risk elements not identified upstream.

- Is the reputation risk also analysed by the NPC?

This reputation risk is particularly difficult to ascertain and measure.

Le Bulletin

One of the participants mentioned a scoring system which apparently can be used to assess the risk on the basis of answers to 6 or 7 objective questions (size of the issue, type of underlying instrument, issuer, area where the product is to be marketed, etc.).

Others mentioned a more subjective approach, which could however also produce an elimination criterion.

“Group” perspective

In some groups, the NPC is also tasked with coordinating, and even managing approvals of new products and services of subsidiaries/branches. The Chief Investment Officers of the group’s various entities are then called upon to participate in the NPC and in any event receive the agendas and minutes of meetings in order to be kept informed of the discussions and positions adopted by the group. The difficulties related to local constraints and particularities remain the main challenge to be met.

Conclusion

Despite the limited number of regulatory provisions in this area, most of the participants confirmed that their institution has a duly formalised NPC. However, some of them were still planning to set up or formalise such a committee. For them, the roundtable was an opportunity to glean ideas and benefit from the experiences of the institutions which have already put in place a formal NPC process.

For a large number of institutions, the non-involvement of Compliance Officers in the approval process is an error from the past which has already been corrected. It now seems to be a given that the Compliance Officer, as well as Risk Management and Legal Departments have become key actors in this process.

Compliance Officers (as well as the Legal Department) which were in the past sometimes regarded as "deal killers", no longer have this image. A satisfactory *modus operandi* has gradually developed between commercial departments and support services. Indeed, over time, it has become clear that the questions raised by Compliance Officers, as well as the requirements for a more detailed and more transparent description of new products, do not make it more difficult to market the products and that, on the contrary, since this situation is to the client’s advantage... it also benefits sales teams.

The roundtable participants welcomed the opportunity to share their questions, experiences and ideas with their peers. We wish to thank them for the open discussion and their active participation. We also wish to thank in particular Mr Tim Geyens who, as technical facilitator for our discussions, used all his expertise to raise the debate and enhanced it with numerous examples.

For the WG 34 Roundtables, Charles van Doorslaer

Summary of answers received

ANSWERS TO THE QUESTIONNAIRE				
BANKS	ASSET MANAGERS	FUND ADMINISTRATION	INSURANCE	OTHERS
31.82%	27.27%	22.73%	9.09%	9.09%

EXISTENCE OF THE NPC	Yes
Is there a structured approach to the concept of new products/services in your institution?	90.9%
Are new products/services subject to a clearly established, formalised validation process before they are marketed?	90.9%
Has a “new products/services” committee (NPC) been set up for validation purposes?	81.8%
Does your Management support the analysis and principle of NPCs?	63.6%

Working of the NPC	Yes
If an NPC is put in place, who are its permanent members?	
Markets expert	22.2%
Private banking sales	22.2%
Asset management	44.4%
Marketing	22.2%
Legal	100%
Risks	88.9%
Compliance	100%
Tax	33.3%
Middle/back office – operations	66.7%
IT	77.8%
Management	66.7%
What are the products/services which require NPC approval?	
All products	55.6%
Only those of a new type	44.4%
What is the Compliance Officer’s role in the NPC?	
Gives his/her opinion	77.8%
Has a right of veto	22.2%
Can trigger an escalation procedure	66.7%
Does the NPC limit itself to a technical approach to the product/service, or does it have a more global approach to:	
Cross-border marketing? Specific risks?	66.7%
Conflicts of interest, trailer fees, inducements?	77.8%
Public offerings vs. private offerings?	44.4%
Publication of Term Sheets on the Internet, freely available in branches?	33.3%
Analysis of the secondary market, redemption options?	33.3%
Monitoring products during their life?	66.7%
Is there a risk indicator / ranking of the product?	66.7%
Compatibility with the other strategies developed by the bank (discretionary management, consultancy)?	33.3%
Ethics?	44.4%
Analysis of issuers and counterparties?	66.7%
Product name, quality and transparency of client information?	88.9%
Which risk indicators do you use?	
Capital protection level	55.6%
Internal risk indicator	55.6%
Volatility	44.4%
Liquidity	55.6%
Complex or non-complex classification	55.6%
Maturity	25.0%

Who is responsible for preparing a project to be submitted to the NPC?	
Business line concerned	62.5%
Marketing	12.5%
Compliance	12.5%
Who is responsible for the NPC secretariat?	
Compliance	25.0%
Legal	12.5%
Risks	12.5%
Others (business line concerned, Research and Development, Marketing, etc.)	25.0%
Are the NPC's decisions readily available to all departments/services?	
Yes	44.4%
No	33.3%
On request	22.2%

Scope of a New Products Committee – definition of the “new product/service” concept **Examples of definitions taken from the questionnaires, illustrating the variety of approaches:**

1. For bankers and asset managers:

- very wide-ranging concept, including all new instruments (derivatives, UCOI and others), investment strategy or any significant operational change affecting existing products, etc.;
- all products or services which enlarge the existing range or which will result in marketing operations, new contracts, new billing;
- any product or service whose introduction results in a substantial change in a chain;
- any new product/service which does not fall within the scope of customary activities;
- any product or service whose introduction results in a substantial change in a processing chain (BO, IT, risk) or in the product risk profile (complexity, financial risk, etc.);
- any financial instrument which cannot be considered as “simple”, that is to say derivatives and/or structured products (via UCI or other structures).

2. For insurers:

- any new products and services in the area of management audits, localisation, technologies, risks, etc.;
- new life insurance structures and products: how to classify them in relation to the CAA rules and avoid differences of interpretations between banks and insurers. For example, ETF and ETC (Exchange Traded Funds and Certificates respectively). In the event of a difference of opinion between banks and insurers, how can the two points of view be reconciled in the framework of controls to be put in place for compliance with investment restrictions?

Examples of names of bodies which approve new products and services:

- New Business Committee
- Comité de Construction de Produits et Services
- Comité pour l'Autorisation et la Supervision des Instruments Financiers
- New Product Approval Committee
- Comité nouveaux Produits (possibly in conjunction with a more formal “products” committee which meets less frequently)

Examples of questions asked concerning new products and services

- Can we provide some selected clients with access to the work of the Group Financial Research Department?
- Can we agree to market structured products to private clients on an OTC⁸ basis? Can ISDA contracts apply to our private clients?

⁸ Over-The-Counter, that is to say traded on a bilateral basis with professional counterparties, as opposed to standardised, exchange-traded transactions.

Implementation of a risk-based approach to accepting and monitoring clients

Present: 30 members of ALCO, representing banks, insurance companies and asset management companies, spread over two sessions.

Facilitator of the 2 sessions: Patrick Schott, to whom we extend our special thanks.

For WG 34:

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

It is to be noted that this summary of the discussions is intended not to reflect points of view but only the content of the discussions of Compliance Officers representing different professions in the financial sector.

Legislative changes in Luxembourg

From the first law on money laundering enacted in Luxembourg in 1989 to the law of 27 October 2010, and including the law of 12 November 2004⁹, legislation on this subject has evolved constantly. In particular, circular IML 89/57 represented a mini revolution in the financial sector in Luxembourg, in that it required financial institutions in particular to identify their clients. Since then, after the creation of the FATF in Paris in 1989 at the initiative of the G8, the financial sector has continuously been required to improve its regulatory arsenal for combating money laundering. The last stage was the 3rd European Union Directive n° 2005-60 transposed into the laws of Luxembourg by the law of 17 July 2008 and by circular CSSF 08/387. The 3rd Directive makes it compulsory to use risk criteria as the basis of any KYC and KYT¹⁰ approach and deals specifically with Politically Exposed Persons and Beneficial Owners.

In its spring 2010 report on Luxembourg, the FATF declared that Luxembourg was non-compliant as regards the implementation of its 40 recommendations, since only one recommendation had been fully implemented. Moreover, it noted that Luxembourg was partially compliant with 30 other recommendations and not at all compliant with 9 others. In order to avoid measures or sanctions being imposed against it, Luxembourg has therefore adapted its legislation rapidly throughout 2010.

The Grand-Duchy regulation of 1st February 2010 is intended to reinforce and clarify certain existing measures regarding the **obligations of professionals**, in particular as regards transaction surveillance and measures of due diligence to be respected.

The Law of 3 March 2010 established the **criminal liability of legal entities** and provides for penalties to be imposed in particular on companies in the case of infringements.

The Law of 27 October 2010 (and its implementing regulation) reasserts the obligation to comply with United Nations and European Union provisions on restrictive measures adopted in the framework of the **fight against terrorist financing** (freezing funds, prohibition or restriction of financial services, etc.).

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

¹⁰ Know your customer & Know Your Transaction

Le Bulletin

The Law of 27 October 2010 reinforcing the fight against money laundering amended 21 legal texts. It is based mainly on penal and judicial provisions (mutual assistance, methods of investigation, etc.).

The new law also provides for the reinforcement and clarification of the competences of professional bodies, as self-regulatory organisations (Chamber of Notaries, Bar Council, Institute of Chartered Accountants, Institute of Corporate Auditors, etc.). Other rules concern the creation of an obligation to report cash entering, passing through or leaving Luxembourg from €10,000.

The new article 506-8 of the Criminal Code enshrines the principle, already established in case-law, that a sentence for money laundering does not require a sentence or prior proceedings to have been instituted for the predicate offence from which the funds laundered are derived.

The new law introduces not only an obligation to institute proceedings but also a new concept, namely a “mini” preliminary investigation that is swifter than the traditionally slow procedure, based on investigating the case for both the prosecution and the defence.

The CSSF can now impose administrative fines of up to €250,000 in addition to any criminal penalties. The Customs and Excise have responsibility for controlling high-value goods. The Financial Intelligence Unit (FIU) remains under the authority of the State Prosecutor’s Department but with enhanced human resources and greater operational independence.

As regards the risk-based approach, the latest law has not made any significant changes. PEP are more closely defined, in particular as regards family ties to be taken into consideration. The law specifies that there is no risk-based approach as regards reporting suspicious transactions. Financial sector professionals are required to report any suspicions they may have to the FIU.

On the other hand, the new law requires risks to be determined according to the professional’s business model by fixing quantitative geographical criteria for PEP and for correspondent banks (it is to be noted that this is a completely theoretical notion since no Luxembourg bank works with “shell banks”).

Roundtable and discussions

A roundtable was organised on the basis of a series of fifteen questions circulated to participants before the roundtable (see annex). It is to be noted that the rate of return was particularly high. We wish to thank all those who contributed to the exercise.

The AML obligations of professionals are obligations of means. This means that professionals must provide proof that they have done everything necessary for the performance of their obligations, while it is for the regulator to ensure that the necessary means exist to check that professionals have put in place an appropriate organisation enabling them to fulfil all their obligations (for example as regards training and awareness-raising, controls, procedures, IT systems, etc.).

As regards AML, insurance companies are in the same situation as banks. They are guided by the CAA circulars whose wording is similar to that of the CSSF circulars.

UCI have a specific problem when dealing with nominees and in particular with nominees in “exotic” countries.

The FATF has reiterated that it is not in favour of a list of countries applying equivalent AML rules as such a list could create a presumption of “good standing”. Consequently, the Grand-Duchy regulation on equivalent supervision has been repealed and circular CSSF 10/476 has abolished automatic equivalence. European Economic Area countries are still considered as countries with equivalent laws. For other countries, it is therefore necessary for professionals to carry out a risk assessment and be able to demonstrate, in this area also, that they have fulfilled their obligation of means. As for Circular CSSF 10/469, it lists countries which have not satisfied their money-laundering obligations, including Greece alongside Angola, among others.

Le Bulletin

Putting in place a risk-based approach

All the professionals present at the RT have put in place a risk-based approach for their new clients. This general approach is however very diversified in practice:

- for some professionals, certain categories of clients are automatically excluded according to the professional's lines of business;
- for others, the client profile attributed at the start of the client relationship is reviewed in the light of the initial transactions carried out with the professional;
- for others, the principle of equal treatment is applied and the same approval procedure is followed for all prospects before a client relationship is established;
- there are also some compromises between group requirements and local requirements, with for example the notion of "country" risk determined and managed at the level of the parent company, while the "activity" risk is managed at the level of subsidiaries;
- some professionals have to deal with the requirements of their parent company and must negotiate to implement local criteria which may be required depending on the various lines of business of the Luxembourg-based subsidiary.

Exclusion – Refusal of new clients

The question is to ascertain on what basis new clients should be rejected in an increasingly difficult context. Either professionals limit themselves to traditional markets or they become more outward-looking and develop into new emerging markets, such as Asia, Russia, etc.

Consequently, the development of new markets raises various questions:

- how to manage the risks inherent in the language (when the documents received are in a language not known to the professional), the activity (is it possible to check the activity given the distance involved?) and local practices?
- how to manage resources: who collects the information? This is a structural problem. The front office wants to sell, driving the middle offices/back offices to support them in this role while requiring them to become increasingly involved in the due diligence process;
- how can professionals avoid being over-reliant on "profiling" which facilitates the analysis of potential clients but does not provide for a specific analysis?
- can the Compliance Officer assume the obligation of means of the middle office/back office?
- who is responsible for following up controls in order to prepare for CSSF inspections?

The use of a check-list as a basis for making decisions regarding the acceptance of new clients was discussed. The risk of this type of list occurs when its use becomes too automatic, too routine. In such cases, there could be a danger of seeing only what is on the list. This type of review is different from a risk assessment which is intended to be more of an "attitude" to be adopted in a given case. The danger of using tools that have not been updated was also raised, as they can be misleading. It is important to determine the potential client's activity in order to be able to monitor more closely transactions on the account with the professional so as to comply with the relevant legislation.

The lack of objectivity was also underscored and therefore the lack of historical points of reference vis-à-vis emerging countries and so-called "exotic" countries. It was noted that no exclusion list exists for these jurisdictions. The risk-based approach must therefore be a case-by-case approach, in line with the professional's policy.

Le Bulletin

Acceptance Committee

The concept of an acceptance committee (AC) seems to be a given for almost all the professionals, involving, for the vast majority, physical meetings. Only complete files seem to be submitted to the committee for an acceptance decision.

Small structures, mainly FSP, recognise that an AC often tends to make its decisions using the “circular” procedure. The separation of tasks, as required by the regulator, is not always easy to respect within small authorised structures.

The discussions also dealt with the question of whether or not Compliance Officers should participate in AC meetings and the nature of their voting rights. Should Compliance Officers have a right of veto within the AC? Different schools of thought were represented around the table:

- Compliance Officers having a right of veto; in some cases the Compliance Officer’s right of veto has evolved naturally, based on the professional’s past experiences;
- Compliance Officers not having a right of veto but for whom the AC’s voting procedure, requiring unanimous acceptance, gives the Compliance Officer a de facto right of veto, except when he is absent and not represented; often if a unanimous decision cannot be reached, the decision is “escalated” to the management;
- Compliance Officers having the right to abstain, noted in the minutes of the AC meeting;
- Compliance Officers having the right to issue a “qualified opinion” having an informative value for the other AC members;

The investment funds industry has to deal with the problem of the succession of intermediaries or change of intermediaries. In addition, local national criteria which may be different from criteria in Luxembourg make the client acceptance process more complicated. In some countries, for example, the definitions of the words “business introducers” and “intermediaries” are sometimes not compatible with local definitions. For professionals this raises the question of the limits of identification delegation. The participants recognised the need for them to have a contract with third-party business introducers covering AML issues, including risk analysis.

The notion of the existence of suspense accounts

This notion seems to be disappearing. Most professionals completely prohibit their use for private clients. The use of these accounts must be fully documented with a complete due diligence and risk analysis file and must be considered as exceptional.

Analysis of dormant accounts

This analysis is difficult because of the lack of a definition of what constitutes a “dormant account”. Professionals choose the duration that they consider appropriate for their definition of a “dormant” account, often between 6 and 24 months, depending on the composition of the portfolio or the client’s activity. Some professionals require their front office to have a minimum direct contact with clients during the year. Others require clients to certify balances on an annual basis.

An analysis of dormant accounts goes hand-in-hand with an analysis of accounts opened and closed during the year or within 12 months after their opening.

Periodic reviews of client files

This review usually involves an examination of not only the documentation but also transactions. This must be a fairly in-depth examination, in accordance with the risk analysis carried out at the beginning of the client relationship. An analysis of the answers to the questionnaire shows considerable differences in the frequency with which client account reviews are conducted. It all seems to depend on the nature of the professional’s business activity (insurance, bank, FSP, asset management company, etc.) and the risk generated by the client. The review is based on:

- the documentation provided by the client/asset manager at the time the relationship is established;
- whether the client's activity over a given period of time complies with the activity specified, described when the account was opened.

Some professionals represented at the roundtable have already, because of the urgency or scope of the task, chosen to outsource the review work.

Some professionals have software that generates reminders, which may or may not block the account, flagging up review dates or documents that need to be updated.

FSP may have some difficulties in monitoring client transactions because they do not have the same resources as banks. FPS sometimes feel as though they are there to provide documentation to banks and their Compliance Officers are faced with the challenge of an ever-increasing workload.

The review of client files naturally leads to the question of whether the client relationship should be maintained, in particular in the event of a sudden change of activity or profile, where the new activity or profile no longer corresponds to the initial activity or profile, or in the case of an activity featuring on the professional's list of exclusions, etc. The professionals recognised that such a decision is the responsibility of the acceptance committee which must then decide whether or not the business relationship should be continued.

Conclusion

This roundtable highlighted that the notion of risk is a notion that is perfectly integrated into our profession. There is no standard response to the problems raised at this roundtable, since the notion of risk is defined by the different professionals in Luxembourg according to their line of business, their culture and their acceptance of risk. Compliance Officers recognise their role in the implementation of this approach in order to satisfy, to their best of their ability, the obligation of means imposed on professionals.

The participants expressed their satisfaction with the meeting as an opportunity to compare points of view and exchange views on interpretations and ideas for solutions. Moreover, this type of exercise enables participants to benchmark themselves against business practices in Luxembourg.

© Working Group 34 "Roundtables"¹¹

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

Le Bulletin

Type d'institution :

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

Risk based approach : How is it implemented ?

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

Yes 28 No 0

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

Yes 16 No 12

Do you have to implement "group" critererias?:

Yes 16 No 12

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

Yes 10 No 18

Is your risk based approach process

Static (independent criteria):

Yes 16 No 12

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

Yes 14 No 14

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

Yes 23 No 5

If yes, on which basis :

Geographical

Yes 20 No 8

Business/ occupation

Yes 11 No 17

Predicted activities with the institution

Yes 15 No 13

Origin of funds

Yes 20 No 8

Legal structure of the owner of the account

Yes 10 No 18

Other

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

Yes 25 No 3

Has a new client acceptance committee been implemented within your

Yes 20 No 15

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

Veto

Yes 10 No 18

Requirement of the unanimity of the committee members

Yes 7 No 21

Circular resolution

Yes 4 No 24

Resolution in formal meetings

Yes 15 No 13

Other

Yes 2 No 26

Are the following business lines part of the acceptance process?

Front

Yes 15 No 13

Executive Committee

Yes 24 No 4

Compliance

Yes 25 No 3

Other

Yes 7 No 21

In which way?

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

Dormant accounts

Yes 16 No 12

Hold mail accounts

Yes 5 No 23

Pseudonyms' / numbered accounts

Yes 7 No 21

Transitory account (internal & external)

Yes 8 No 20

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

Yes 16 No 12

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

Is the review of the client files based on:

Geographical

Yes 18 No 10

Type of Business of the Ultimate Beneficila Owner / Client

Yes 18 No 10

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

Yes 19 No 9

Type of transactions

Yes 14 No 14

Threshold of transactions

Yes 13 No 15

Mix of above

Yes 14 No 14

Vie associative

VIE ASSOCIATIVE

GROUPES DE TRAVAIL ACTUELS

Groupe de travail 11

Site Internet

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

Groupe de travail 16

Commission permanente juridique et relations publiques

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

Jean-Marie

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

Groupe de travail 20

Funds practices and recommendations AML

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

Groupe de travail 21

Interprétation pratique des restrictions d'investissements de fonds

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

Groupe de travail 27

Formations IFBL

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

Groupe de travail 29

Abus de marché

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

Groupe de travail 30

Domiciliation de société

ASSOCIATION ACTIVITIES

CURRENT WORKING GROUPS

Working group 11

Website

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

Working group 16

Legal and public relations

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

Jean-Marie

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

Working group 20

Funds practices and recommendations AML

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

Working group 21

Practical interpretation of fund investment restrictions

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

Working group 27

Training IFBL

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

Working group 29

Market abuse

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

Working group 30

Domiciliary agent

Le Bulletin

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

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

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

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

Groupe de travail 33

Working group 33

Réponses aux questions des membres

Answers to questions of members

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

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

Groupe de travail 34

Tables rondes

Working group 34

Round tables

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

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

Groupe de travail 35

Doctrine

Working group 35

Doctrine

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

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

MEMBRES ET VIE ASSOCIATIVE

MEMBERS AND ASSOCIATION ACTIVITIES

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

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

Effectif total: 545

Membres effectifs 440

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

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

Total number: 545

Active members 440

Le Bulletin

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

– **Conseil d'administration:**

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

– **Secrétariat de l'ALCO:**

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

– **Secrétariat du Bulletin:**

Emilie Schmitt
secretariat@alco.lu

– **Comité de rédaction:**

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

Le Bulletin

VISITEZ NOTRE SITE WEB : www.alco.lu