Association Luxembourgeoise des Compliance Officers

# LE BULLETIN 31

## Parole aux membres

PARTIE 2

# SOMMAIRE





31 LE BULLETIN
LE MAGAZINE DE L'ALCO

ALCO Association Luxembourgeoise des Compliance Officers

**Rédacteurs en chef :** Karine Vilret et Thierry Grosjean
**Contributeurs :** Stéphane Badey, Florence Barrière, Elisa Da Silva, Ross Main, Bob Moris, Eric Sohn, Filip Verbeke, Matthias Verbeke
**Conception & coordination :** 360Crossmedia
studio@360Crossmedia.com - 35 68 77
**Directeur artistique :** Franck Widling
**Photo couverture :** © DR
**Tirage :** 500 copies

# EDITORIAL

## CHERS MEMBRES DE L'ALCO, CHERS AMIS LECTEURS,

© DR

À la lumière d'une situation internationale qui n'a jamais semblé aussi incertaine depuis plusieurs dizaines d'années avec pèle mêle la montée des populismes, l'inflation des actes de terrorisme, le Brexit, la nouvelle administration américaine, l'influence géopolitique croissante de la Russie, le ralentissement de la croissance économique des principaux pays en voie de développement, quel pourrait être le rôle de l'Union Européenne ?

Celle-ci saura-t-elle se mouvoir en un refuge idéal pour la société civile en général ? Saura-t-elle particulièrement être ce garant en matière de transparence financière pour tous les investisseurs grâce notamment à une législation en matière de lutte AML/FT qui est l'une des plus strictes au monde ? Une législation encore renforcée par la transposition de la 4e Directive et la mise en œuvre du « Tax Crime » comme infraction primaire. Saura-t-elle in fine devenir cet eldorado pour les investisseurs du monde entier qui souhaitent bénéficier d'un cadre fiscal et juridique transparent dans un marché sain, débarrassé des affres des LuxLeaks et autres Panama Papers ?

Toute la question est de savoir si nos hommes politiques européens souhaiteront emprunter cette voie et en faire une juste promotion afin que les investisseurs étrangers ne nous considèrent pas à tort comme un marché imperméable du fait d'un déferlement législatif et règlementaire parfois mal maîtrisé et sans nul doute mal expliqué.

Au final, ce début d'année pose beaucoup plus de questions qu'il n'apporte de réponses et ce n'est pas les spécialistes de tout bord qui le démentiront. Mais c'est le plus souvent dans l'incertitude, dans les difficultés que naissent les plus belles idées, les projets les plus innovants à la base d'une nouvelle croissance économique que chaque citoyen européen attend.

Excellente lecture à toutes et à tous,

**Thierry Grosjean**
*Président ALCO*





## DEAR ALCO MEMBERS, DEAR READER FRIENDS,

In the light of an international situation which for several decades now has never seemed so uncertain, with the rise of populisms, the inflation in terrorist attacks, the Brexit, the new American administration, the growing geopolitical influence of Russia, the economic slowdown hitting the main developing countries, what might the role of the European Union be?

Will it be able to transform into an ideal refuge for the civil society as a whole? Will it in particular be that guarantor in the area of financial transparency for all investors thanks to the strictest legislation in matters of AML/FT fight in the world? Legislation that is yet strengthened by the transposition of the 4th Directive and the implementation of the « Tax Crime» as a primary infraction. Will it in fine know how to become that Eldorado for investors throughout the world who wish to benefit from a transparent tax and legal framework in a healthy market freed from the throes of the LuxLeaks and other Panama Papers?

The true question is to know whether our European politicians will want to take that course and justly promote it so that foreign investors do not wrongly consider us as a watertight market resulting from a legal and regulatory tidal wave, oftentimes poorly mastered and without any doubt inadequately explained.

In the end, this beginning year poses more questions than it answers, and specialists of every kind would be hard put to deny it. But it is more often in the uncertainty and when facing difficulties that are born the best ideas, the more innovating projects at the heart of the new economic growth that every European citizen hopes for.

Excellent reading to all.

**Thierry Grosjean**
*Chairman, ALCO*

© DR

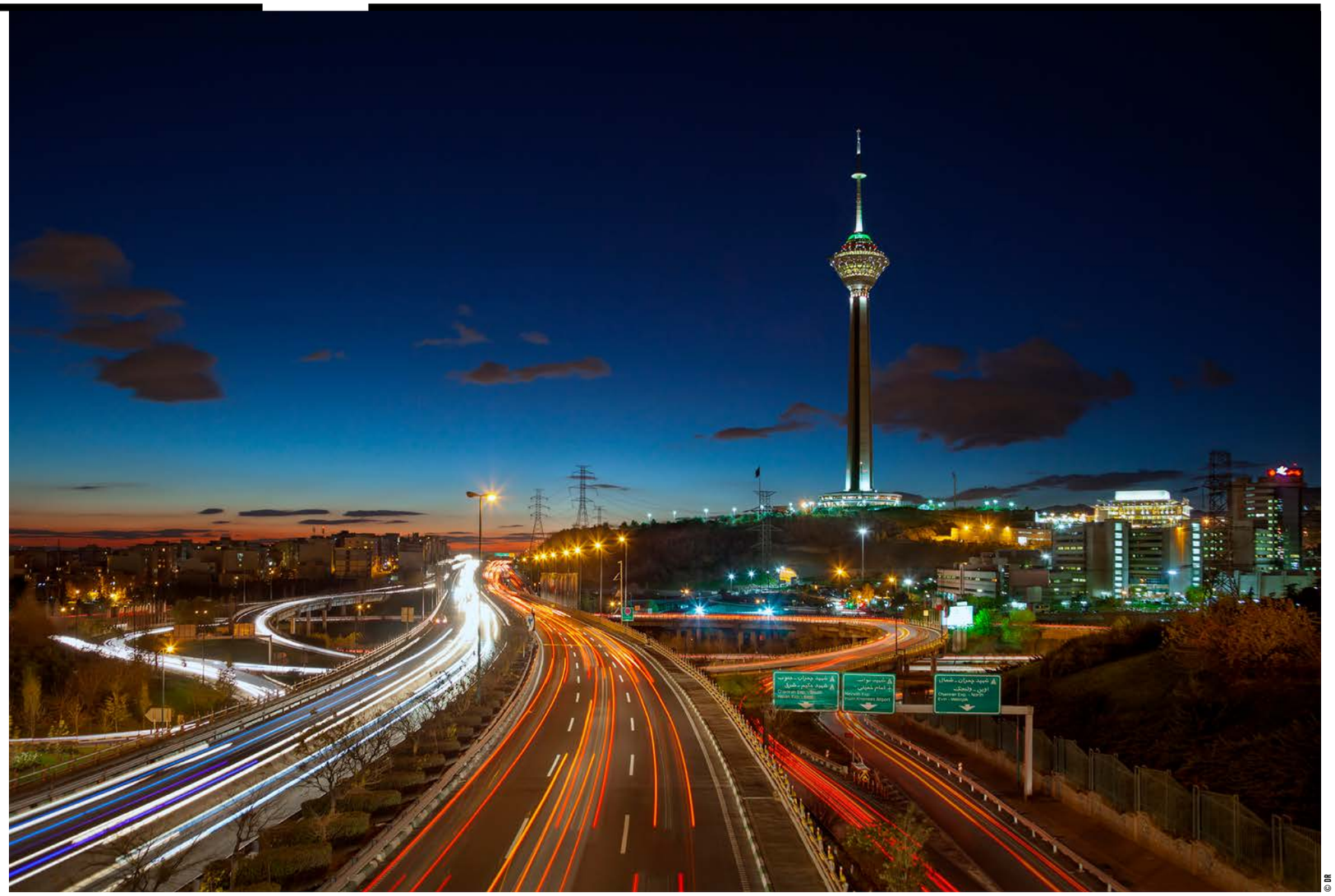
# IRAN, CASSE-TÊTE DES BANQUES EUROPÉENNES


© DR

BOB MORIS

L'essentiel des sanctions contre la République islamique d'Iran (l'Iran) a été levé par la communauté internationale depuis la mise en œuvre de l'« Accord de Vienne », qui est entré en application le 16 janvier 2016. Cette date est appelée, en anglais, l'Implementation Day par l'accord.
Le régime juridique, en droit international public, de l'« Accord de Vienne » revêt la forme d'une résolution prise par le Conseil de sécurité de l'Organisation des Nations-Unies : il s'agit

>>>


© DR

## IRAN, A PUZZLE FACING EUROPEAN BANKS

The international community lifted most of the sanctions against the Islamic Republic of Iran (Iran) following signature of the "Vienna Agreement", which was implemented on 16 January 2016. That date is called Implementation Day in the agreement.
In public international law, the legal framework for the "Vienna Agreement" takes the form of a resolution adopted by the United Nations Security Council. The resolution in question is 2231(2015).
The European Union's sanctions, most of which were put in place from 2010 onwards, were lifted by a European Council decision of 18 October 2015.
Under US federal law, sanctions were lifted, on Implementation Day, by means of Waivers and by making the appropriate changes to the law.
So we can only really speak of sanctions against Iran being lifted from Implementation Day.

### EUROPEAN UNION SANCTIONS

Since Implementation Day, European Union law allows European persons and entities to access the Iranian banking and financial sectors, without being affected by sanctions.
It is, however, important to note that this absence of sanctions, brought about by the "Vienna Agreement", applies only if the Iranian banking or financial entity is not expressly subject to the freezing of assets and is not included on the list of persons that are still subject to sanctions[1].
Therefore, in order to avoid any compliance risk, it is necessary to check in advance that the Iranian counterparty is not subject to individual sanctions, the lists of which can be consulted[2].
The Iranian banks currently named as being subject to sanctions include Ansar Bank, Bank Saderat Iran, Mehr Bank and Bank Saderat plc.
Since 16 January 2016, Iranian banks disconnected from the SWIFT system since sanctions were put in place, can reconnect to the SWIFT system and send SWIFT messages, provided they are not subject to individual sanctions.
The major issue of the sanctions imposed on the Central Bank of Iran (Bank-e-Markazieh Iran) placed a block on the Iranian banking system.
Upon implementation of the "Vienna Agreement", the European Union lifted all previous sanctions against the Central Bank of Iran.
The general prohibition on transfers of funds from and to Iranian banking institutions (which are not currently named as being subject to sanctions) is now governed by European law. Since 16 January 2016, European law allows funds to be transferred to and from Iran.
Moreover, it is no longer necessary to apply for authorisation or to notify the national authorities for this type of transfer of funds.
Finally, it should be noted that since Implementation Day, European law allows EU banking and financial institutions to establish branches, subsidiaries and representative offices in Iran.

### US SANCTIONS

The "Vienna Agreement" also applies between the United States of America (United States) and Iran. Here too, it was implemented on 16 January

>>>

>>>

de la résolution 2231(2015).
Quant à l'Union européenne, elle a supprimé ses sanctions, imposées principalement depuis 2010, par une décision du Conseil européen du 18 octobre 2015.
En droit fédéral américain, la levée de sanctions, le jour de l'Implementation Day, a eu lieu par des Waivers et par les modifications juridiques adéquates en ce sens.
Par conséquent, l'on ne peut véritablement parler de la levée des sanctions contre l'Iran qu'à partir de l'Implementation Day.

## SANCTIONS DE L'UNION EUROPÉENNE

A compter de l'Implementation Day, le droit européen permet aux personnes et entités européennes d'accéder aux secteurs bancaire et financier iraniens, sans qu'elles ne soient inquiétées de sanctions.
Toutefois, il est important de relever que cette absence de sanctions, mise en place par l'« Accord de Vienne », n'est pas valable pour autant que l'entité bancaire ou financière iranienne ne fasse pas expressément l'objet de gel de ses avoirs ou ne soit incluse sur la liste des personnes toujours sous sanctions[1].
Il convient donc, afin d'éviter tout risque lié à la conformité, de vérifier au préalable que la contrepartie iranienne ne soit pas visée par des sanctions individuelles, dont les listes sont accessibles[2].
A noter que les banques iraniennes actuellement nommément sous sanction sont notamment : Ansar Bank, Bank Saderat Iran, Mehr Bank et Bank Saderat plc.
S'agissant maintenant des banques iraniennes déconnectées du système SWIFT depuis la mise en place des sanctions, elles ont le droit, depuis le 16 janvier 2016, à condition de ne pas être nommément sanctionnées, de se reconnecter au système SWIFT et ainsi de transmettre par ce biais des messages SWIFT.
La question majeure des sanctions prises contre la Banque centrale iranienne (Central Bank of Iran ou Bank-e-Markazieh Iran) a bloqué le système bancaire iranien.
L'Union européenne a supprimé toutes les sanction antérieures à son encontre à partir de la mise en application de l'« Accord de Vienne ».
Quant à l'interdiction généralisée de transférer des fonds de et vers les institutions bancaires iraniennes (qui ne sont pas nommément actuellement sous sanction), elle est désormais réglée par le droit européen. Depuis le 16 janvier 2016, le droit européen permet de transférer des fonds vers et depuis l'Iran.
Il faut ajouter qu'il n'est plus nécessaire de déposer une demande d'autorisation ou de notifier les autorités nationales pour ce type de transfert de fonds.
Enfin, notons ici qu'à partir de l'Implementation Day, le droit européen permet aux institutions bancaires et financières de l'Union d'établir, en Iran, des succursales, filiales et des bureaux de représentation.

## SANCTIONS AMÉRICAINES

L'« Accord de Vienne » s'applique également entre les Etats-Unis d'Amérique (Etats-Unis) et l'Iran. Son entrée en application commence également le 16 janvier 2016.
D'emblée, il convient de relever la définition donnée par le droit fédéral américain à un terme en particulier, qui est redondant, celui de non-U.S. Persons.
Ce terme désigne généralement toute personne, physique ou morale, à l'exclusion des citoyens des Etats-Unis, des résidents permanents de ce même pays, de toute entité établie par les lois des Etats-Unis ou par les lois d'une entité géographique des Etats-Unis (y compris les succursales et filiales (« Branches ») étrangères établies aux Etats-Unis ou toute personne se trouvant aux Etats-Unis. Il s'agit donc d'un terme qui a une définition large, pour y inclure un grand nombre d'acteurs.
Il faut noter qu'une entité qui est contrôlée par ou est la propriété d'une U.S. Person, et qui est établie hors des Etats-Unis, est autorisée à participer à des transactions ou activités prévues par l'« Accord de Vienne » uniquement dans les limites autorisées par l' OFAC (Office of Foreign Assets Control), l'OFAC étant l'autorité fédérale en charge de l'application des sanctions américaines.
Les sanctions américaines contre l'Iran sont de deux sortes : les Primary U.S. Sanctions et les Secondary U.S. Sanctions.
Les premières (Primary U.S. Sanctions) sont des sanctions imposées par les Etats-Unis, invariables même après l'« Accord de Vienne ». Elles visent concrètement l'interdiction pour toute U.S. Person, y compris les sociétés commerciales américaines, de s'engager dans des transactions ou relations avec l'Iran ou son gouvernement.
De plus, les avoirs du gouvernement iranien et ses propriétés aux Etats-Unis continuent d'être bloqués, en vertu de l'Executive Order

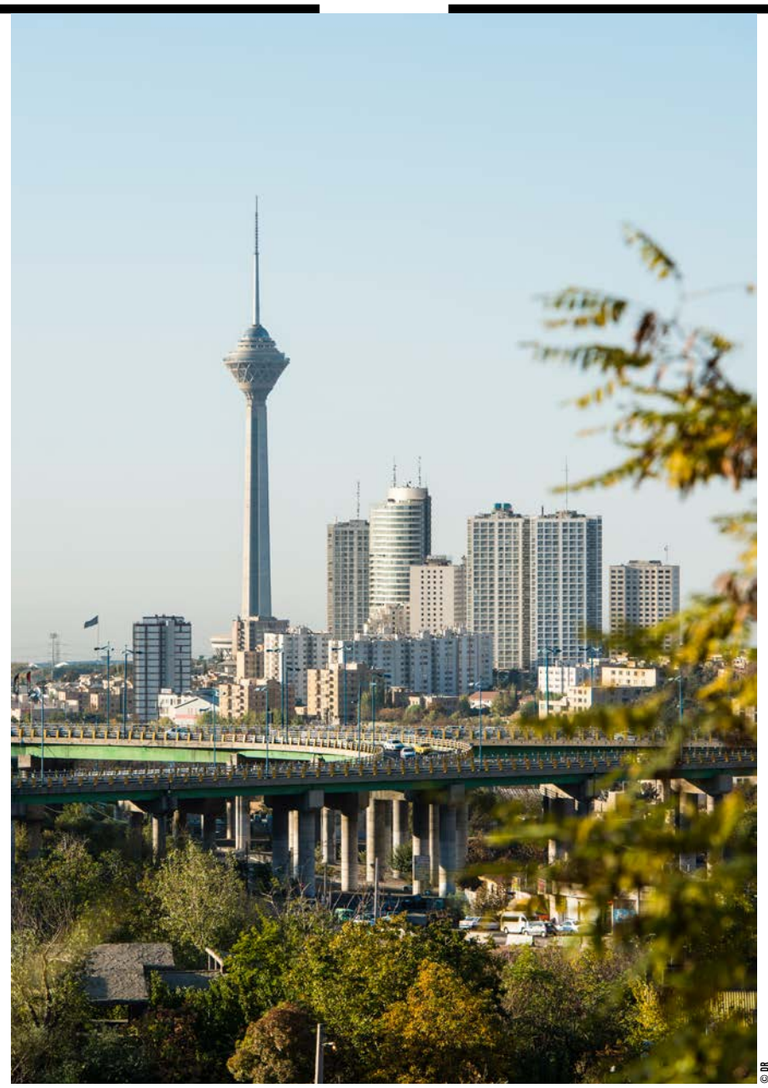
>>>

>>> 2016.
It is important first to note the definition that US federal law gives to one term in particular: "non-US Persons". This term generally designates any natural or legal person other than citizens of the United States, permanent residents of the United States, any entity established under the laws of the United States or the laws of a geographical entity of the United States (including foreign branches and subsidiaries) established in the United States or any person in the United States. This term therefore has a broad definition, covering a large number of actors.
It must be noted that an entity controlled or owned by a U.S. Person and established outside the United States is authorised to participate in transactions or activities provided for by the "Vienna Agreement" only subject to the limits put in place by OFAC (Office of Foreign Assets Control), which is the federal authority in charge of applying US sanctions.
US sanctions against Iran are of two types: Primary US Sanctions and Secondary US Sanctions.
Primary US Sanctions are sanctions imposed by the United States and remain unchanged even after the "Vienna Agreement". They concern, in concrete terms, the prohibition on any US Person, including US commercial companies, engaging in transactions or relationships with Iran or its government.
In addition, the Iranian government's assets and properties in the United States continue to be frozen, by virtue of Executive Order 13599 in particular. Any exemption from this general prohibition must have prior authorisation from OFAC.
Moreover, even non-US Persons are prohibited from knowingly seeking to evade the remaining US sanctions against Iran.
Secondary US Sanctions apply to non-US Persons, i.e. any person who is not a US Person under federal law. These Secondary US Sanctions continue to apply even after 16 January 2016, but only as regards "significant" transactions with:
- Iranian nationals appearing on OFAC's "Specially Designated Nationals and Blocked Persons List" ("SDN List");
- the Islamic Revolutionary Guard Corps and its designated agents or affiliates;
- any other person appearing on the SDN List because of their involvement in the proliferation of Iran's nuclear weapons or weapons of mass destruction, etc.
While it is true that the United States has lifted its sanctions against Iran for non-US Persons, it must be borne in mind that the US administration stipulates that this only applies if the transactions and relationships between Iran and such non-US Persons remain "outside the US financial system". This therefore means nothing can pass through the US banking and financial system, on pain of prosecution by the United States.
Furthermore, even after the date of implementation of the "Vienna Agreement", the United States requires that foreign (non-US) financial institutions ensure that they do not carry out transactions in US Dollars if Iran is involved in those

>>>

>>>

13599 notamment. Toute dérogation à cette interdiction générale devra être préalablement autorisée par l'OFAC.
Par ailleurs, même les non-U.S. Persons se voient une interdiction de s'engager, en connaissance de cause, à contourner les sanctions américaines restantes contre l'Iran.
Quant aux secondes (Secondary U.S. Sanctions), elles s'appliquent aux non-U.S. Persons, c'est-à-dire toute personne qui n'est pas, aux termes du droit fédéral, une U.S. Person.
Ces Secondary U.S. Sanctions s'appliquent même après le 16 janvier 2016, mais seulement en ce qui concerne les transactions dites « significatives » avec :
- les personnes de nationalité iranienne qui figurent sur la liste de l'OFAC dite « Specially Designated Nationals and Blocked Persons » ou « SDN List » ;
- les Gardiens de la Révolution islamique (Islamic Revolutionary Guard Corps) et leurs agents désignés ou leurs affiliés ;
- et toute autre personne figurant sur la « SDN List » en raison de leur participation à la prolifération d'armes nucléaires de l'Iran ou d'armes de destruction massive, etc.
S'il est vrai que les Etats-Unis ont levé leurs sanctions contre l'Iran pour les non-U.S. Persons, il ne faut cependant pas perdre de vue que l'administration américaine précise que ceci n'est valable que pour autant que les transactions et relations entre l'Iran et ces non-U.S. Persons demeurent hors du « système financier américain ». Ceci exclut donc tout transit par le système financier et bancaire américain, sous peine de poursuites par les Etats-Unis.



© DR

Par ailleurs, les Etats-Unis, même après la date de mise en œuvre de l'« Accord de Vienne », exigent que les institutions financières étrangères (non-américaines) s'assurent de ne pas mener de transactions en US Dollars lorsque l'Iran est impliqué dans celles-ci.
Car les U.S. Persons ne sont toujours pas autorisées à exporter des biens, des services ou des technologies, que ce soit directement ou indirectement, vers l'Iran (y compris des services de nature financière, sauf lorsqu'une autorisation a été délivrée en vertu de la législation fédérale américaine).
Il est important de noter également que les Etats-Unis interdisent toujours aux U.S. Persons de s'impliquer dans des transactions avec l'Iran, et ce même lorsque la devise utilisée n'est pas la devise américaine.
Heureusement, depuis le 16 janvier 2016, les Etats-Unis ne sanctionnent plus les non-U.S. Persons qui fournissent le gouvernement iranien en billlets de banque en devise américaine. Cependant, ceci doit rester hors du système financier américain.
En outre, la réglementation fédérale américaine requiert des institutions financières américaines de mettre en place, afin de pouvoir réduire le risque de s'exposer à des sanctions, des procédures, des note internes, ceci dans le but d'appliquer la conformité en adéquation avec le risque.
La bonne nouvelle, annoncée par les Etats-Unis, est qu'ils ne sanctionneront pas les institutions financières étrangères (non-américaines) qui effectueront des ou faciliteront les transactions concernant des activités qui faisaient l'objet de sanctions

>>>

>>> transactions.
Because U.S. Persons are still not authorised to export goods, services or technologies, either directly or indirectly, to Iran (including services of a financial nature), unless a permit has been issued by the US competent authority (OFAC).
It is also important to note that the United States still prohibits US Persons from being involved in transactions with Iran, even in a currency other than the US Dollar.
Fortunately, since 16 January 2016, the United States no longer applies sanctions to non-US Persons that provide the Iranian government with US Dollar bank notes, although this must remain outside the US financial system.
In addition, US federal regulations require US financial institutions to put procedures and internal guidelines in place in order to reduce the risk of exposing themselves to sanctions, with the aim of ensuring their compliance is in line with the level of risk.
The good news, announced by the United States, is that they will not sanction foreign (non-US) financial institutions that carry out or facilitate transactions involving activities that were subject to sanctions before implementation of the "Vienna Agreement".
So what about a situation in which a foreign (non-US) financial institution carries out transactions with an Iranian financial institution which itself has a relationship with an Iranian person or entity on the SDN List?
In these circumstances, the United States will not apply sanctions to the foreign financial institution in question, provided that it does not carry out or facilitate, and more generally is not involved in, banking relationships or transactions involving Iranian persons or entities on the SDN List.
The final situation considered in this article is where a financial institution, which is not a US or Iranian financial institution but has directors or senior executives who are US Persons (for example, its chief executive officer, chief financial officer, chief operating officer or chief compliance officer), carries out transactions with an Iranian person or entity that is not on the SDN List.
A European financial institution will not necessarily be exposed to US sanctions in the case of transactions with Iranian entities or persons simply because it has US Persons on its management bodies (provided, of course, that the Iranian persons or entities are not on the SDN List).
However, in this situation the US Persons on the management bodies must exercise a systematic right of withdrawal in the event of transactions or services with an Iranian entity or person and that right must be provided for by the procedures of the European financial institution or bank.
In conclusion, European banks and financial institutions must exercise enhanced due diligence in view of potential exposure to US sanctions, although that in itself should not dissuade them from working with Iran.
In short, following implementation of the "Vienna Agreement", European banks are better protected against

>>>

>>>
avant l'entrée en application de l'« Accord de Vienne ».
Alors, qu'en est-il du cas de figure où une institution financière étrangère (non-américaine) mène des transactions avec une institution financière iranienne qui, elle, a une relation avec une personne ou entité iranienne figurant sur la SDN List ?
Dans ce cas, les Etats-Unis ne sanctionneront pas l'institution financière étrangère en question, dans la mesure où celle-ci ne mènera, ni facilitera, et plus généralement ne sera pas impliquée dans des transactions ou relations bancaires impliquant des personnes ou entités iraniennes figurant sur la SDN List.
La dernière hypothèse traitée dans cet article est celle où une institution financière, qui n'est ni américaine, ni iranienne, mais dont certains de ses dirigeants sont des U.S. Persons (par exemple des membres de son conseil d'administration, directeurs, Chief Executive Officer, Chief Financial Officer, Chief Operating Officer ou Chief Compliance Officer), mène des transactions avec une personne ou entité iranienne qui ne figure pas sur la SDN List.
La seule présence de U.S. Persons dans les instances de direction d'une institution financière ou bancaire européenne, par exemple, n'exposera pas nécessairement celle-ci à des sanctions américaines en cas de transactions avec des entités ou personnes iraniennes (ne figurant évidemment pas sur la SDN List).
Néanmoins, il est demandé, dans ce cas de figure, que les U.S. Persons, dans les instances dirigeantes de notre hypothèse, fassent usage d'un droit de retrait systématique, qui devrait être prévu par les procédures de l'institution financière ou bancaire européenne, en cas de transactions ou services avec une entité ou personne iranienne.
En conclusion, les banques et institutions financières européennes doivent exercer une vigilance accrue en ce qui concerne l'exposition à d'éventuelles sanctions américaines, mais qui, en soi, ne devrait pas les dissuader de travailler avec l'Iran.
En somme, les banques européennes, après la mise en œuvre de l'« Accord de Vienne », sont mieux protégées contre des sanctions américaines, mais elles doivent faire preuve de diligence et de vigilance en ce faisant.
Il convient d'ailleurs de souligner l'implication du gouvernement luxembourgeois dans les relations avec l'Iran depuis la mise en œuvre de l'« Accord de Vienne », notamment par la venue d'une délégation officielle iranienne, accompagnée de chefs d'entreprises iraniens, mais également et surtout le voyage de la délégation luxembourgeoise, conduite par le vice-premier ministre Etienne Schneider, accompagné d'entreprises luxembourgeoises, y compris des institutions financières de la place.
Ceci démontre donc un changement certain de ton et dans les mentalités des deux côtés.

## LE GAFI[3] & LA CSSF[4]

Toute banque luxembourgeoise, en menant des transactions avec l'Iran, comme tout autre Etat non-membre du GAFI, devrait également prendre en considération, ainsi que le requiert la Commission de surveillance du Secteur financier (CSSF), une vigiliance accrue quant au risque lié au « pays ».
Jusqu'à récemment, le GAFI considérait l'Iran comme l'un des deux seuls Etats au monde ayant des défaillances stratégiques substantielles en matière de lutte contre le blanchiment et le financement du terrorisme (l'autre étant la Corée du Nord).
Toutefois, le GAFI a retiré l'Iran de cette catégorie et l'a désormais qualifié d'Etat dont le régime de lutte contre le blanchiment et le financement du terrorisme requiert l'application de mesures de vigilance renforcées proportionnelles aux risques.
Aussi, la CSSF a relaté ce changement dans sa circulaire du 4 juillet 2016, adressée aux entités qu'elle a la charge de surveiller.
En conclusion, nombre d'opportunités attendent les banques luxembourgeoises en Iran. Il est par conséquent impératif pour celles-ci, si elles envisagent des relations d'affaires avec l'Iran, de respecter les termes de l'« Accord de Vienne », en ce y compris la réglementation américaine des sanctions, surtout si elles ont une activité ou présence aux Etats-Unis.

**Maître Bob MORIS**
Senior Lawyer, et ancien Chief Compliance Offcer

1. En effet, même après l'entrée en application de l' « Accord de Vienne », le 16 janvier 2016, certaines personnes ou entités iraniennes restent sous sanctions. Celles-ci sont nommément inscrites sur une liste officielle.
2. Voir par exemple la liste des noms http://www.tresor.economie.gouv.fr/11448_liste-unique-de-gels
3. GAFI :Groupe d'Action Financière)
4. CSSF: Commission de surveillance du Secteur financier, Luxembourg

>>> US sanctions, but must exercise diligence and be extra vigilant, as US administration sanctions.
The Luxembourg government's involvement in relations with Iran since the implementation of the "Vienna Agreement" must also be highlighted, including the visit of an official Iranian delegation, accompanied by Iranian business leaders, and in particular the visit to Iran of the Luxembourg delegation, led by the deputy prime minister Etienne Schneider, accompanied by Luxembourg businesses, including Luxembourg financial institutions.
This shows a definite change in tone and in mind-sets on both sides.

## FATF[3] & THE CSSF[4]

Any Luxembourg bank that carries out transactions with Iran, as with any other state that is not a member of the FATF, should also take into account the need for enhanced due diligence with regard to "country" risk, as required by the Commission de surveillance du Secteur financier (CSSF).
Until recently, the FATF considered Iran to be one of only two states in the world with substantial strategic deficiencies in the area of anti-money laundering and financing of terrorism (the other being North Korea).
However, the FATF has removed Iran from this category and now classifies it as a state whose anti-money laundering and financing of terrorism regime requires enhanced due diligence to be applied in proportion to the risks.
The CSSF communicated this change in its circular of 4 July 2016, sent to the entities it supervises.
In conclusion, Iran holds many opportunities for Luxembourg banks. So it is essential that, if they are considering business relationships with Iran, they comply with the terms of the "Vienna Agreement", including US sanctions regulations, especially if they operate or have premises in the United States.

## NEW TRUMP SANCTIONS

Since this article was drafted, a real change in the US administration (the Trump administration) has begun.
The Trump administration has announced sanctions on companies and individuals suspected of involvement in Iran's missile program and its support for foreign armed groups, warning there will be more pressure on Tehran to come.
A senior administration official described the measures as "initial steps" while a broader review of Iran policy was under way.
As a result, Compliance risk is very high when it comes to be working with Iran at this time for European banks.
However, the Vienna Agreement cannot be revoked unilaterally by the new US administration, due to its multilateral aspect.

**Maître Bob MORIS**
Senior Lawyer, and former Chief Compliance Officer

1. In fact, even following the entry into force of the "Vienna Agreement" on 16 January 2016, some Iranian persons or entities remain subject to sanctions. They are named on an official list.
2. See, for example, the list of names: http://www.tresor.economie.gouv.fr/11448_liste-unique-de-gels
3. FATF: Financial Action Task Force
4. CSSF: Commission de surveillance du Secteur financier, the Luxembourg financial sector supervisory authority

# PLACE AUX RISQUES

© DR

L'acceptation du Plan d'action global commun (JCPOA) a suscité beaucoup d'enthousiasme car il allait permettre de profiter des nouvelles opportunités commerciales offertes par l'Iran. En effet, selon le dernier classement établi par la Banque mondiale, l'Iran est non seulement la deuxième plus grande économie du Moyen-Orient (bien qu'elle représente moins des deux tiers de l'économie saoudienne), mais elle est aussi la 26e économie mondiale. Devenue un marché cible, les années d'isolement international font également de cette nation un vivier d'opportunités, avec peu de concurrents établis à déloger sur place.

Cette liberté de conclure des marchés pourrait-elle se payer au prix fort dans le cadre des futures actions coercitives de l'OFAC ? Bien que l'encre de l'accord ait séché depuis longtemps, les entreprises font preuve de prudence, craignant les amendes gigantesques infligées par les régulateurs américains il n'y a pas si longtemps encore.

Un article paru le 31 août dans le Wall Street Journal est révélateur de cette situation. Malgré une grande agitation dans le monde des affaires allemand, avec notamment des délégations commerciales qui se sont rendues en Iran avant même le Jour de mise en œuvre (soit le 16 janvier 2016, date à laquelle le JCPOA est entré en vigueur) et des annonces de grands projets industriels en Iran faites par de grands groupes tels que Siemens, les exportations vers l'Iran n'ont progressé que de 15% au cours des six premiers mois de l'année 2016. Gregor Wolf, directeur de la Fédération allemande du commerce de gros, du commerce extérieur et des services, a imputé cette

>>>

ERIC SOHN

## LET DANGEROUS TIMES ROLL

When the Joint Comprehensive Plan of Action (JCPOA) was agreed to, there was great excitement about taking advantage of the business opportunities available in Iran. After all, according to the latest World Bank listings, not only is Iran the second largest economy in the Middle East (despite being less than two-thirds the size of Saudi Arabia's economy), it is also the world's 26th largest. The years of international isolation also makes the nation, as a target market, a very attractive "greenfield opportunity," with few entrenched incumbents to dislodge.

Could that freedom to close deals have a stiff price in future OFAC enforcement actions? The ink on the agreement has long since dried, yet companies are proceeding cautiously, afraid of the outsized fines doled out in the not-so-distant past by US regulators.

An August 31st article in the Wall Street Journal is illustrative. Despite great hoopla in the German business community, including business delegations traveling to Iran even before the Implementation Day (January 16, 2016, when the JCPOA went into effect) and announcements by the likes of Siemens of large industrial projects in Iran, exports to Iran only climbed 15% in the first six months of 2016. Gregor Wolf, a director at the Federation of German Wholesale Foreign Trade and Services, laid the blame for local reticence to pursue Iranian business on firms' fear of U.S. sanctions enforcement. On the other hand, a contemporaneous article notes Michael Tockuss, head of the German-Iranian Chamber of Commerce, as saying that bank's reluctance to finance larger deals was receding, albeit slowly.

As one might expect, Iranian officials are also not happy with the pace of change. Another recent article quotes multiple government sources, including Iran's supreme leader, of accusing the US of intimidating firms into not reestablishing business ties, for fear of running afoul of US regulations and enforcement.

There is one noticeable exception, however, to the current state of affairs. According to an August 10th article on rt.com, Iranian petroleum exports have returned to pre-sanctions levels. That jump, from 1 to 2.5 million barrels daily, represents a 150% increase in a little over 6 months. Perhaps, as the restrictions on Iranian energy products was the most notable and one of the last major restrictions on trade with Iran to be imposed, it should not be surprising to see it bounce back first.

So, will European firms find ways to do business with Iran without running afoul of US sanctions, which have largely not been removed? To start to answer this

>>>

© BR

>>>
réticence locale à développer des activités en Iran au fait que les entreprises redoutent l'application des sanctions américaines. Par contre, un article contemporain indique que selon Michael Tockuss, responsable de la Chambre de commerce germano-iranienne, la réticence des banques à financer des transactions plus importantes s'estompait, quoique lentement.

Comme on pourrait s'y attendre, les responsables iraniens ne sont pas non plus satisfaits de la lenteur des changements. Un autre article récent cite plusieurs sources gouvernementales, dont le chef suprême iranien, accusant les États-Unis d'intimider les entreprises pour qu'elles ne rétablissent pas leurs relations commerciales avec l'Iran, ces entreprises craignant ainsi de se mettre en infraction avec la réglementation américaine et son application.

Cependant, il existe une exception notable à l'état actuel des choses. Selon un article paru sur rt.com le 10 août, les exportations iraniennes de pétrole sont revenues aux niveaux antérieurs aux sanctions. Ce bond de 1 à 2,5 millions de barils par jour représente une augmentation de 150% sur un peu plus de 6 mois. Dans la mesure où les restrictions sur les produits énergétiques iraniens étaient les plus notoires et comptaient parmi les dernières restrictions majeures imposées sur le commerce avec l'Iran, peut-être ne devrait-il pas être surprenant de voir ce secteur rebondir en premier.

Alors, les entreprises européennes trouveront-elles un moyen de faire des affaires avec l'Iran sans se heurter aux sanctions américaines qui, pour la plupart, n'ont pas été levées ? Pour commencer à répondre à cette question, un examen de l'histoire récente des sanctions de l'UE et des mesures d'application connexes de l'OFAC pourrait s'avérer instructif.

Pour le dire simplement, l'Union européenne ne possède pas une tradition aussi longue que celle des États-Unis en matière de sanctions internationales. Cette méconnaissance, ajoutée à une appréciation erronée de la valeur que les clients effectuant des transactions internationales attachent aux paiements libellés en dollars américains, a contribué à générer un environnement, dans le monde des services financiers, qui a entraîné un très grand nombre de sanctions au cours de ces dernières années. Alors que le programme européen de sanctions contre l'Iran date de 2010, avant 2012 celles-ci se limitaient au gel des avoirs de quelques individus et organisations spécifiques ainsi qu'à des embargos commerciaux limités. Ce n'est que depuis la décision 2012/35/PESC du Conseil que les importations de pétrole, de produits pétroliers et de produits pétrochimiques iraniens, qui constituent le principal moteur de l'économie iranienne, ont été interdites. Un peu plus tard cette année-là, la décision 2012/635/PESC du Conseil a interdit tout soutien aux échanges commerciaux avec l'Iran. A aucun moment le commerce et les services financiers n'ont été aussi limités que lorsqu'ils l'ont été par les États-Unis. De ce point de vue, les sanctions imposées par l'OFAC à l'Iran ont été perçues comme une ingérence dans l'environnement commercial et industriel de l'Europe.

Les attitudes bien documentées vis-à-vis des sanctions américaines que l'on trouve dans les documents américains d'exécution fédérale et étatique constituent peut-être les meilleurs indicateurs des comportements qui seront adoptés à l'avenir.

>>>

>>> question, perhaps an examination of recent EU sanctions history and related OFAC enforcement would be instructive.

Simply put, European Union's does not have the same long-lived history of compressive sanctions on any country as the United States This unfamiliarity, coupled with an under-appreciation of the value that clients conducting international trade plane on payments denominated in the US dollar, contributed to the environment within the financial services community that resulted in the slew of outsized enforcement actions over the last few years. While the EU's Iranian sanctions program dates to 2010, prior to 2012, these were limited to asset freezes for specific individuals and organizations, and limited trade embargoes. It wasn't until Council Decision 2012/35/CFSP that imports of Iranian oil, petroleum products and petrochemical products, which are the primary driver of the Iranian economy, were prohibited. Later that year, Council Decision 2012/635/CFSP prohibited support for trade with Iran. At no time was trade or financial services ever restricted to the extent that it was by the US. To that extent, OFAC's sanctions on Iran were seen as outside interference with Europe's trade and business environment.

Perhaps the best indicators of future behavior are the well-documented attitudes toward US sanctions present in US federal and state enforcement documents.

Probably the most notable (and the most well-publicized) example of European animus is the Standard Chartered Bank's (SCB) Group Director's response to concerns about US sanctions. An officer from SCB's New York branch quoted him as saying "You <expletive deleted> Americans. Who are you to tell us, the rest of the world, that we're not going to deal with Iranians."

Similarly, an executive at BNP Paribas (BNPP) was reported to have asked, in response to sanctions concerns about their dealings with Sudan" whether or not "Switzerland declared an embargo on Sudan."

This attitude, while it may reflect some provincialism by those being quoted, is more clearly a reflection of the large volume of business being discussed. For example, SCB believed that providing US dollar payments for CBI/Markazi, an OFAC sanctioned bank, for the receipts from oil sales made by the National Iranian Oil Company (NIOC), "could lead to increased business activity with [other Iranian] banks." In fact, when Lloyds TSB London withdrew from Iranian business due to its concern about reputational risk, SCB pursued the newly-available business opportunities. Additionally,

>>>
L'exemple le plus remarquable (et le plus médiatisé) de l'animosité européenne à cet égard est sans doute la réponse du directeur de la Standard Chartered Bank (SCB) aux préoccupations concernant les sanctions américaines. Un dirigeant de la succursale new-yorkaise de SCB l'a cité en ces termes : « C* (juron effacé) d'Américains. Qui êtes-vous pour nous dire, à nous le reste du monde, que nous n'allons pas traiter avec les Iraniens. »

De même, un dirigeant de BNP Paribas (BNPP) aurait demandé, en réponse aux craintes de sanctions concernant leurs relations avec le Soudan « si oui ou non la Suisse avait décrété un embargo contre le Soudan.

Cette attitude, bien qu'elle puisse refléter un certain provincialisme de la part des personnes citées, reflète plus certainement l'important volume d'affaires concerné. Par exemple, la SCB croyait que le fait de fournir des paiements en dollars américains à CBI/Markazi, une banque sanctionnée par l'OFAC, pour les recettes provenant des ventes de pétrole réalisées par la National Iranian Oil Company (NIOC), « pourrait conduire à une activité commerciale accrue avec [d'autres banques iraniennes] ».
En fait, lorsque Lloyds TSB London s'est retirée des affaires iraniennes en raison de ses craintes en termes de risques pour sa réputation, la SCB a exploité les nouvelles opportunités d'affaires qui se sont alors présentées. En outre, un mémorandum de décembre 2005 rédigé par le PDG émirati de la SCB et son responsable groupe pour la conformité et le risque réglementaire observait que la stratégie à court et moyen terme de la SCB était de « développer le commerce de gros en élargissant notre portefeuille à partir des relations existantes avec des institutions financières et des entreprises iraniennes et en nouant de nouvelles relations avec des entreprises iraniennes et des [intermédiaires] dans les activités pétrolières et gazières ». Il serait sans doute plus pertinent de dire que les activités de virements frauduleux (« wire stripping ») de la SCB étaient justifiées afin d'éviter des retards en raison d'articles immobilisés pour examen par l'OFAC à New York, ce qui aurait constitué une pierre d'achoppement pour les efforts déployés par la SCB en matière de développement de ses activités iraniennes.

Dans le cas de la BNPP, le détail des documents d'exécution de la loi fait apparaître qu'en dépit du fait que l'entreprise savait qu'elle enfreignait la loi américaine, elle a maintenu des relations d'affaires avec des entités visées par les sanctions contre le Soudan parce que « BNPP Genève ne voulait pas compromettre ses relations de longue date avec des clients soudanais ». Un email résumant une réunion tenue en 2006 et lors de laquelle l'entreprise acceptait de poursuivre ces opérations, relève que « les enjeux commerciaux sont importants », tandis qu'un mémo rédigé un peu plus tard cette année-là précise que BNPP « maintient des relations commerciales avec les banques [satellites] qui offrent un potentiel commercial important ».

Dans le cas du Crédit Agricole, le règlement de l'OFAC observe, à propos des activités soudanaises du Crédit Lyonnais (qui l'a précédé) que la « liquidité considérable de nos livres (une moyenne de 10 à 15 millions CHF) offre une couverture considérable pour les engagements ainsi que pour les paiements commerciaux. Le [produit bancaire net] prévu pour 2004 est de 4 à 500.000,00 CHF avec [la banque soudanaise] ».

Enfin, lorsque le département Conformité de HSBC Group a ordonné à HSBC Europe de cesser ses virements frauduleux, HSBC Europe a fait appel de cette décision en invoquant les « opportunités d'affaires significatives » qu'offraient les parties sanctionnées ; le Responsable de la Conformité a alors autorisé la poursuite de ces pratiques en Europe et au Moyen-Orient pendant un certain nombre d'années.

Ainsi, la recherche de débouchés commerciaux a conduit plusieurs banques européennes à adopter des pratiques visant à tromper les entreprises de services financiers américaines parce que leurs clients sanctionnés voulaient des paiements en dollars américains et parce que l'UE n'avait pas imposé de sanctions aussi strictes que celles imposées par les États-Unis. Il n'en demeure pas moins une question cruciale : maintenant que l'écart entre les sanctions européennes et américaines s'élargit de nouveau, les entreprises européennes tenteront-elles à nouveau de trouver des moyens de se soustraire à l'OFAC sans contourner les marchés américains et la compensation en dollars américains ? Compte tenu de la frustration publique suscitée par la lenteur du rétablissement des relations commerciales quelques mois seulement après le Jour de mise en œuvre, peut-être devrions-nous nous attendre à lire des récits de subterfuge et d'occultation d'ici cinq à dix ans.

>>> a December 2005 memorandum written by SCB's UAE CEO and their Group Head of Compliance and Regulatory Risk noted SCB's short to medium term strategy was to "grow the wholesale business by growing our wallet share from existing relationships with Financial Institutions and Iranian companies and establishing new relationships with Iranian companies and [intermediaries] in oil and gas related businesses." Perhaps more to the point, SCB's wire stripping activities were justified in order to prevent delays by items stopping for OFAC review in New York which would be a "deal-breaker" for SCB's Iranian business development efforts.

In BNPP's case, enforcement details note that, despite the firm being aware that they were breaking US law, they continued business relationships with Sudanese sanctions targets because "BNPP Geneva did not want to risk its longstanding relationships with Sudanese clients." An email summarizing a 2006 meeting in which the firm agreed to continue these transactions noted that "the commercial stakes are significant," while a memo written later that year noted that BNPP "maintain commercial relations with these [satellite] banks which offer significant commercial potential."
In Credit Agricole's case, the OFAC settlement notes about the Credit Lyonnaise (a predecessor institution) Sudanese business that the "considerable liquidity in our books (an average of 10 to 15 million CHF) provides considerable coverage for the commitments as well as for the commercial payments. The anticipated [net banking income] for 2004 is CHF 4 to 500,000.00 with [the Sudanese bank]."
Lastly, when HSBC Group Compliance ordered HSBC Europe to stop wire stripping, when HSBC Europe appealed due to the "significant business opportunities" available with the sanctioned parties, the Head of Compliance allowed the practice to continue, both in Europe and the Middle East for a number of years.
So, the pursuit of business led multiple European banks to adopt practices aimed at deceiving US financial services firms because their sanctioned clients wanted payment in US dollars, and because the EU had not imposed sanctions as strict as those levied the US. That leaves a burning question: now that the gap between EU and US sanctions widens again, will European firms again try to find ways to evade OFAC without bypassing US markets and US dollar clearing? Given the public chafing at the slow pace of the re-establishment of business ties mere months after Implementation Day, perhaps we should not be surprised to read tales of subterfuge and obfuscation five to ten years hence.

# LE PLAN DE CONTRÔLE COMPLIANCE « UN CHANTIER À CHOIX MULTIPLES »

STÉPHANE BADEY

Le métier de responsable de la conformité (ci-après, le « Compliance Officer ») est un métier formidable. Quel que soit le secteur d'activité, il est au croisement du droit et de l'opérationnel. Etre Compliance Officer requiert une curiosité des développements réglementaires mais également du fonctionnement de la société pour laquelle il va agir. La nécessité de cette double compétence se retrouve à tous les instants : que ce soit dans la mise en œuvre des politiques résultants de la réglementation applicable, lesquelles devront nécessairement être adaptées à l'environnement de la société pour faire sens ou dans celle des contrôles, étape nécessaire pour s'assurer du bon respect des politiques et procédures qui auront été préalablement approuvées et mises en œuvre par les équipes opérationnelles, le Compliance Officer ne chôme pas.

Pour rappel, dans le secteur financier, « la mise en place d'une fonction Compliance a pour but d'organiser, de coordonner et de structurer les contrôles en matière de Compliance déjà effectués en vertu d'autres réglementations, mais qui sont, à l'heure actuelle, souvent répartis sur différents niveaux de l'organisation ».

L'exercice n'est pourtant pas si simple, sauf à le rendre

>>>

## COMPLIANCE CONTROL PLAN "A MULTIPLE-CHOICE CHALLENGE"

The role of the compliance officer is a formidable one. Whatever the sector of activity, this role lies at the intersection of the law and a company's operations. A compliance officer must be interested both in regulatory developments and in how the company in which he or she will act operates. These dual areas of competence are needed at all times: the compliance officer always has work to do, whether in the implementation of the policies resulting from the regulations applicable to the company, which, to be meaningful, must have been adapted to the company's environment, or in the implementation of controls, which is a necessary step in ensuring compliance with the policies that have been approved and implemented by the operational teams.

As a reminder, in the financial sector "the role of the compliance function is to organise, coordinate and provide a structure for the compliance controls that have already been introduced under other regulations but which are, currently, often spread over several levels of the organisation.»

Nevertheless, how the compliance function works in practice is not as simple as this might suggest, except if it is over-simplified. The scope of the control plan and the nature and form of the controls depend directly on the way in which the compliance function is organised and how the compliance officer approaches his or her role.

**THERE IS NO STRICT DEFINITION OF THE SCOPE OF ACTION OF THE COMPLIANCE FUNCTION**

The establishment of a control plan requires a precise definition of the compliance officer's scope of action. The reality is, however, often more complex than the regulations suggest. In this article we will consider only the financial sector in which two circulars (12/552 and 04/155) define the compliance function. The purpose of the Compliance Function is to protect the establishment from any harm that could result from non-compliance with the regulations in force [...]

In this context "Regulations in force" must be understood to mean all the rules to which the establishment is subject in the exercise of its activities in the different markets [...].

Circular 04/155 also stipulates that "internal codes of conduct or ethics and the codes of professional associations and financial markets (stock markets or other regulated markets) must also be taken into account, particularly for the purposes of risk assessment."

Circular 12/552 also helpfully states that "the areas that fall directly within the scope of the compliance function are typically anti-money laundering and counter financing of terrorism, prevention of market abuse, personal account dealing, the integrity of financial instruments markets,

>>>


© BR

>>>

simpliste. Le champ d'intervention du plan de contrôle, la nature et la forme des contrôles dépendent directement de la façon dont la fonction compliance est organisée et dont le Compliance Officer envisage sa fonction.

## IL N'Y A PAS DE DÉFINITION STRICTE DU CHAMP D'INTERVENTION DE LA FONCTION COMPLIANCE

La réalisation d'un plan de contrôle suppose une définition précise du périmètre d'intervention du Compliance Officer.
Or, la réalité est souvent plus complexe que ce que les textes réglementaires peuvent laisser paraître. Considérons seulement le secteur financier où deux circulaires (12/552 et 04/155) définissent la fonction compliance. La fonction Compliance a pour objet de protéger l'établissement de tout préjudice qui pourrait résulter du non-respect des normes en vigueur [..].

Par « normes en vigueur », il faut entendre dans ce contexte toutes les règles auxquelles l'établissement est soumis dans l'exercice de ses activités dans les différents marchés [..].

La circulaire 04/155 stipule également que « les codes de conduite ou de déontologie internes ainsi que les codes d'associations professionnelles et de marchés financiers (bourses ou autres marchés réglementés) sont à considérer également, notamment pour l'évaluation du risque ».

La Circulaire 12/552 précise aussi utilement que « Les domaines qui relèvent directement de la fonction compliance sont typiquement la lutte contre le blanchiment et le financement du terrorisme, la prévention en matière d'abus de marché et de transactions personnelles, l'intégrité des marchés d'instruments financiers, la protection des intérêts des clients et des investisseurs, la protection des données et le respect du secret professionnel, la prévention et la gestion des conflits d'intérêts, la prévention de l'utilisation du secteur financier par des tiers pour contourner leurs obligations réglementaires et la gestion du risque de conformité lié aux activités transfrontalières ».
Enfin, les circulaires laissent la liberté à l'établissement de décider si, compte tenu des particularités des activités exercées, sa fonction Compliance couvre le contrôle du respect des règles n'ayant pas directement trait aux activités bancaires et financières à proprement parler, telles que les règles relevant du droit de travail, du droit social, du droit des sociétés ou du droit de l'environnement.

## QUI DIT FONCTION À GÉOMÉTRIE VARIABLE DIT PLAN DE CONTRÔLE À GÉOMÉTRIE VARIABLE

En pratique, dans le monde financier, la lutte contre le blanchiment d'argent est systématiquement du ressort de la compliance, alors que par exemple le respect de la réglementation en matière de capitaux propres est souvent laissé à des équipes aux compétences plus financières, relevant du contrôle interne. Cette répartition des sujets réglementaires entre les diverses fonctions de contrôles n'est pas critiquable en tant que telle, d'autant que ceci est même

>>>

>>> protection of client and investor interests, data protection and compliance with professional secrecy, prevention and management of conflicts of interest, prevention of use of the financial sector by third parties to avoid their regulatory obligations, and management of the compliance risk associated with cross-border activities".

Finally, the circulars leave it up to the establishment to decide whether, in view of the specific features of the activities it carries on, the compliance function is responsible for monitoring compliance with rules that are not directly related to banking and financial activities in the strict sense, such as rules under employment law, social security law, company law or environmental law.

**DIFFERENT TYPES OF CONTROL FUNCTION MEAN DIFFERENT TYPES OF CONTROL PLAN**

In practice, in the financial world, anti-money laundering systematically falls under the responsibility of the compliance function, while compliance with regulations concerning capital adequacy, for example, is often the responsibility of teams more concerned with financial matters falling under internal control. There is nothing wrong with this distribution of regulatory matters across the different control functions, particularly as it is envisaged by the regulations.

Moreover, since in practice some areas that give rise to compliance risk can also be the concern of other functions, such as the risk control function, the finance function or the legal function, it is acceptable for areas other than those listed above not to be directly covered by the compliance function in order to avoid duplication of compliance controls. It is understood that in this case the compliance risk must be covered by the other internal control functions under a compliance policy that clearly defines the duties and responsibilities of the various functions involved, with segregation of tasks being respected. In such a case, the chief compliance officer's role is to coordinate, centralise and verify that the other areas that are not included directly within his or her scope of action are properly covered[1].

Finally, it is very clear that the growing complexity of regulations requires expertise that is sometimes difficult to combine within a single team. The regulations themselves create specific control functions for matters that, according to the regulations, are the direct responsibility of the compliance function (e.g. data protection officer)[2].

Quite clearly, not all regulated entities enjoy the luxury of having dedicated teams for each area of compliance (the organisation of a bank's compliance function will be very different from the compliance function of a management company or a small investment firm).

>>>
envisagé par la réglementation.

En outre, dans la mesure où dans la pratique certains domaines donnant lieu à des risques de compliance peuvent aussi relever d'autres fonctions telles que la fonction de contrôle des risques, la fonction finance ou la fonction juridique, et dans un souci d'éviter une duplication des contrôles de compliance, il est admissible que les domaines autres que ceux énumérés ci-dessus ne soient pas directement couverts par la fonction compliance. Il est entendu que dans ce cas, le risque de compliance est alors à couvrir par les autres fonctions de contrôle interne suivant une politique de compliance définissant clairement les attributions et les responsabilités des différents intervenants en la matière et moyennant le respect de la ségrégation des tâches. Dans ce cas, le « Chief Compliance Officer » assume un rôle de coordination, de centralisation et de vérification que les autres domaines ne relevant pas directement de son champ d'intervention soient bien couverts[1].

Il est bien clair enfin que la complexité croissante de la réglementation demande une expertise qu'il est parfois difficile de réunir au sein d'une seule équipe. La réglementation même créé des fonctions de contrôles spécifiques sur des sujets qui relèvent selon la règlementation directement de la fonction compliance (e.g. le Data Protection Officer)[2].

Bien évidemment, toutes les entités réglementées n'ont pas le luxe d'avoir des équipes dédiées par sujet (l'organisation de la fonction compliance au sein d'une banque aura peu de similitude avec la fonction compliance d'une société de gestion ou d'une petite entreprise d'investissement).

Même à considérer les thèmes qui relèvent uniquement de la fonction compliance, le programme de contrôle peut se trouver bien chargé. Il existe aujourd'hui des solutions sur le marché pour assister les Compliance Officers dans cette tâche. La réglementation permet aussi au Compliance Officer d'utiliser les travaux faits par d'autres équipes. A tire d'exemple, les 2 Circulaires précédemment citées prévoient que « pour les contrôles en matière de risque de compliance ainsi que pour la vérification des procédures et des instructions, les dispositions de la présente circulaire n'empêchent pas que la fonction compliance prenne en compte les travaux de l'audit interne ».

S'il est indiscutable que la fonction compliance peut donc utiliser des relais au sein de l'organisation, il semble aussi indiscutable que l'exécution des contrôles par un autre département ne dispense pas la fonction compliance de la responsabilité quant à la conformité de la société. En d'autres termes, la fonction compliance est comme un délégant qui pourrait s'exonérer de l'exécution du contrôle (elle est faite par son délégataire) mais reste responsable pour sa bonne exécution (et donc la mise en conformité). Pour rappel, la fonction compliance centralise toutes les informations sur les problèmes de compliance (entre autres les infractions aux normes, le non-respect de procédures ou encore les conflits d'intérêts) détectés dans l'établissement.

Pour autant qu'elle ne tire pas ces informations de sa propre implication, elle procède à un examen des documents pertinents, qu'ils soient internes (par exemple rapports de contrôle et d'audit interne, rapports ou comptes rendus de la direction autorisée ou, le cas échéant, du conseil d'administration) ou externes (par exemple rapports du réviseur externe, correspondance de la part de l'autorité de contrôle).

## CONCLUSION

En prenant en considération l'exigence que la fonction compliance doive agir comme un agent centralisateur et toujours avec l'objectif de définir un plan de contrôle cohérent, le premier travail consistera à délimiter le champ d'intervention de la fonction compliance. Si on s'en tient aux thèmes classiques de la réglementation financière tels que cités par les circulaires, la tâche peut très facilement s'avérer dantesque pour une seule personne.

A l'inverse, au vu des textes précédemment cités, on peut légitiment s'interroger sur la pertinence d'une fonction compliance qui ne serait concernée que par le blanchiment d'argent ou par un nombre très limités de sujets en deçà des prescriptions réglementaires.

Pour ceux qui en douteraient encore, quelle que soit la taille de la société, Compliance Officer est une fonction bien remplie.

1. Circulaire CSSF 12/552 (telle que modifiée par les circulaires CSSF 13/563, 14/597 et 16/642 – point 135
2. Règlement du Parlement Européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel à la libre circulation de ces données.

>>> Even if we consider only those areas that fall directly within the scope of the compliance function, the control regime can be onerous. Today there are solutions on the market to assist compliance officers with this task. The regulations also allow the compliance officer to use work carried out by other teams. For example, the two circulars mentioned above provide that "for controls relating to compliance risk and for the verification of procedures and instructions, the provisions of this circular do not prevent the compliance function taking account of the work of the internal audit function".

While there is therefore no doubt that the compliance function can piggyback on the work of other areas of the organisation, there also seems to be no doubt that the performance of controls by other departments does not exempt the compliance function from responsibility for the company's compliance. In other words, the compliance function is like a delegator that can exempt itself from performing a control (which is done by its delegatee) but remains responsible for the proper performance of that control (and therefore for compliance). It should be borne in mind that the compliance function pools all the information on the compliance issues (including regulatory breaches, non-compliance with procedures and conflicts of interest) detected in the establishment.

Where it does not obtain this information by carrying out the controls itself, it examines the relevant documents, whether internal (for example internal audit and control reports, reports by the authorised management or, where appropriate, the board of directors) or external (for example reports by the external auditor, correspondence from the supervisory authority).

**CONCLUSION**

Given that the compliance function is required to act as a central focal point and always with the objective of establishing a coherent control plan, the first task will be to define the compliance function's scope of action. Even in terms of the traditional aspects of financial regulation mentioned in the circulars, the task can very easily prove complex and overwhelming for one person.
Conversely, in the light of the texts mentioned above, it is legitimate to question the relevance of a compliance function that deals solely with money laundering or a very limited number of subjects that fall short of the regulatory requirements.
For those who might still be in doubt, the role of the compliance officer is a very full and busy one, whatever the size of the company.

1. (Financial Services Supervisory Authority) Circular 12/552 (as amended by CSSF circulars 13/563, 14/597 and 16/642) – point 135
2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

# ANALYSE DES RISQUES DE LA DISTRIBUTION DES FONDS D'INVESTISSEMENT





**ELISA DA SILVA**

Elisa Da Silva est à la tête de DS Compliance
Elisa Da Silva is the Managing Director of DS Compliance

Le Luxembourg est le leader mondial en matière de distribution transfrontalière de fonds d'investissement. La distribution est un élément important de la commercialisation d'un fonds ou encore appelée marketing, qui est faite sur la base d'une stratégie commerciale décidée par le Conseil d'administration du fonds. La stratégie commerciale définit aussi bien les pays de distribution que le type de distribution, les techniques de commercialisation ainsi que la typologie d'investisseurs et les canaux de distribution par pays.
La mise en place de canaux de distribution est essentielle pour l'accroissement des actifs du fonds et l'identification des risques encourus apparaît comme un préalable.

## 1. LES ACTEURS INTERVENANT DANS LA DISTRIBUTION D'UN FONDS :

**• Pour les fonds de type OPCVM :**
Le Conseil d'administration du fonds décide des lignes directrices de la stratégie commerciale et nomme un distributeur global pour son exécution. Souvent, il s'agit de la société de gestion qui va jouer ce rôle mais ce n'est pas toujours le cas.
Une sélection va ensuite être faite parmi des intermédiaires financiers, ou encore appelés, distributeurs qui semblent les plus adéquats pour la mise en œuvre de cette stratégie.
La nomination d'agents de placement est également possible dans le but du placement du fonds dans les pays où il n'est pas enregistré.

**• Pour les fonds de type alternatif :**
Les organes de décision du fonds peuvent faire leur marketing à condition qu'ils aient les ressources nécessaires en interne. L'autre possibilité est que le fonds délègue son marketing au gestionnaire, communément appelé l'AIFM. Par ailleurs, dans la phase de lancement ou d'accroissement du fonds, des agents de placement peuvent être nommés.

## 2. L'OBLIGATION DE VIGILANCE OU DE « DUE DILIGENCE » DES DISTRIBUTEURS :

Les distributeurs font l'objet d'une due diligence par la société de gestion. Cette obligation aussi appelé « Know Your Distributor », signifie deux choses.

**1.** La vigilance initiale exercée sur le distributeur, préalablement à la signature du contrat de distribution, permet d'évaluer les risques auxquels s'expose le fonds. Et de plus, le distributeur est présenté en interne à un Comité d'acceptation.

**2.** La vigilance continue permet d'identifier les risques qui peuvent surgir, dans la distribution du fonds, au cours de la relation contractuelle.
Ce n'est pas l'objet de la présente analyse et nous vous renvoyons à cet égard aux questionnaires de « due diligence » développés en la matière par l'ALCO et d'autres associations au niveau national et européen.

>>>

## RISK ANALYSIS OF INVESTMENT FUND DISTRIBUTION

Luxembourg is the world leader in the cross-border distribution of investment funds. Distribution is a key element of the marketing of a fund, which is carried out based on a marketing strategy adopted by the Board of the Fund.
The marketing strategy defines both the country of distribution and the type of distribution, the marketing techniques as well as the type of investors and the distribution channels for each country.

The establishment of distribution channels is essential for the growth of the fund's assets, and the identification of the risks incurred appears to be a prerequisite.

### 1. THE STAKEHOLDERS INVOLVED IN THE DISTRIBUTION OF A FUND:

**• For UCITS funds:**
The Board of Directors of a fund draws ups the marketing strategy guidelines and appoints a global distributor to implement the strategy.
Often, the management company plays this role, but this is not always the case.
The most suitable financial intermediaries or distributors to implement this strategy will then be selected.
Investment agents can also be appointed with the aim of investing the fund in countries where it is not registered.

**• For alternative funds:**
The decision-making bodies of the fund may handle their marketing provided they have the necessary internal resources.
The other possibility is that the fund delegates its marketing to the manager, commonly referred to as the AIFM.
In addition, during the launch or growth phase of the fund, investment agents can be appointed.

### 2. DUE DILIGENCE OF THE DISTRIBUTORS:

The distributors are subject to due diligence by the management company.
This duty, also referred to as «Know Your Distributor», means two things.
**1.** The initial vigilance exercised on the distributor, prior to signing the distribution contract, enables assessment of the risks to which the funds are exposed. The distributor is also introduced internally to an acceptance committee.
**2.** Continued vigilance allows any risks that may arise, in the distribution of the fund, to be identified over the course of the contractual relationship.
This is not the subject of this analysis; please consult the due diligence questionnaires developed by ALCO and other national and European associations.

### 3. RISK IDENTIFICATION:

It should be pointed out that the distribution of the fund is often associated with the risk of money laundering or terrorist financing and rightly so, since the consequences can be particularly damaging for the fund's reputation. This issue has, moreover, been subject to a joint study by associations such as ABBL, ALCO, ALFI, and ALRIM.
In this respect, numerous key stakeholders of the financial centre consider themselves to be only partially affected by the issue of money laundering/terrorist financing, as they distribute their funds mainly in the European Union and/or in countries that pose a low risk in terms of money laundering.
However, countering money laundering represents only one aspect of fund distribution.
It is not possible to comprehensively list all risks, and each stakeholder performs its own analysis and identifies the risks posed when marketing the fund, which covers both investors and distributors.
As regards the risks associated with the marketing of the fund, there are four types of risk: the country risk (i.e. money laundering, political, economic, legal and market risks associated with the country where the

>>>

>>>

**3. IDENTIFICATION DES RISQUES :**

Il convient de préciser que la distribution de fonds est souvent associée au risque de blanchiment et de financement du terrorisme et à juste titre, puisque les conséquences peuvent être particulièrement dommageables en termes de réputation pour le fonds.
D'ailleurs, ce sujet a fait l'objet d'une étude conjointe de la part d'associations telles que l'ABBL, l'ALCO, l'ALFI, et l'ALRIM[1].
A cet égard, de nombreux acteurs de la place considèrent qu'ils ne sont que partiellement concernés par la question de la LBC/FT, car ils distribuent leurs fonds essentiellement dans l'Union européenne et/ou dans des pays considérés à faible risque en termes de blanchiment. Cependant, la lutte contre blanchiment n'est qu'un des aspects de la distribution des fonds.
Il n'existe pas de liste exhaustive de risques et chaque acteur fait sa propre analyse et identifie les risques posés lors de la commercialisation du fonds, par ses investisseurs ainsi que ses distributeurs. Concernant les risques liés à la commercialisation du fonds, il en existe quatre types : le risque-pays (c'est-à-dire, les risques de blanchiment, politique, économique, juridique, de marché liés aux pays où est distribué le fonds) ; le risque lié aux canaux de distribution ; le risque concernant le type de commercialisation et le risque marketing, c'est-à-dire de non-conformité avec les règles locales. En ce qui concerne les risques liés à l'investisseur, on compte le risque concernant le type d'investisseur et les services d'investissement proposés ; le risque de plainte de l'investisseur. Enfin, le dernier risque à prendre en compte est celui du défaut d'information de l'investisseur. Il convient de garder à l'esprit les nouvelles exigences introduites par MIFID 2[2] et PRIIPS[3] qui seront applicables à compter de janvier 2018.
Ensuite, les risques posés par les distributeurs sont : le risque lié à leur gouvernance interne ; le risque opérationnel & IT ; le risque de blanchiment ; le risque de sous-distribution et le risque posé par les rétrocessions versées à ces distributeurs. Enfin, les deux derniers risques à considérer sont le risque réglementaire et de réputation.

**4. MESURES DE MITIGATION DES RISQUES :**

Les mesures sont données à titre indicatif et chaque acteur est à même de prévoir celles qui lui semblent les plus adéquates pour ses risques.
Le suivi réglementaire semble une des mesures de mitigation envisageable que ce soit la règlementation du pays de commercialisation du fonds (en particulier sur les règles marketing locales) que la réglementation applicable aux investisseurs et aux distributeurs. Un changement réglementaire peut avoir un impact certain sur le réseau de distribution.
Par ailleurs, il convient de mettre en place des contrôles internes au sein des acteurs ayant la responsabilité de la distribution comme des listes de pays de distribution et une analyse de ces pays ; des listes détaillées de distributeurs et de sous-distributeurs, incluant, entre autres, les rétrocessions versées. Les contrôles possibles sont également le suivi des investisseurs et de leurs plaintes ainsi que le suivi des distributeurs qui peut aller jusqu'à mandater un audit de ce distributeur ou bien faire une visite sur place, pour obtenir le confort nécessaire.
Enfin, l'autre mesure de mitigation peut être l'envoi, par le distributeur à la société de gestion et/ou au fonds, de rapports (à une fréquence à déterminer) contenant des informations en matière de lutte contre le blanchiment et d'identification des investisseurs ; sur les plaintes reçus d'investisseurs et sur les incidents intervenus dans la distribution.

**CONCLUSION :**

Chaque stratégie commerciale étant spécifique, suppose que les acteurs du marché fassent leur propre analyse de risques et la documentent, la finalité étant d'être en mesure de démontrer que l'on a une connaissance suffisante de son réseau de distribution.
De nombreux moyens sont bons pour atteindre cette finalité, l'important étant d'avoir identifié et mitigé les risques posés par son réseau, ceci n'étant pas, à mon avis, une option mais une obligation eu égard aux nouvelles exigences posées par MIFID 2.

**Elisa Da Silva**
Gérante de la société
DS Compliance

1. Practices and recommendations aimed at reducing the risk of money laundering and terrorist financing in the Luxembourg Fund industry, July 2013.
2. Directive 2014/65/UE
3. Règlement UE n° 1286/2014 du 26 novembre 2014 en matière de « PRIIPS » qui concerne les documents d'informations clés relatifs aux produits d'investissement packagés de détail et fondés sur l'assurance destinés aux investisseurs de détail.

>>> fund is distributed); the risk associated with the distribution channel; the risk associated with the type of marketing, and the marketing risk, i.e. non-compliance with the local rules.
The risks associated with the investor include the risk concerning the type of investor and the investment services offered, as well as the risk of complaints from investors. Finally, the last risk to be taken into account is that of the risk of failing to properly inform the investor. It is important to bear in mind the new requirements introduced by MIFID 2 and PRIIPS which will be applicable as of January 2018.
The risks posed by distributors include: the risk associated with their internal governance; the operational and IT risk; the risk of money laundering; the risk of under-distribution and the risk posed by the commissions transferred to these distributors.
Finally, the last two risks to be taken into account are the regulatory risk and the reputational risk.

**4. RISK MITIGATION MEASURES:**

The measures are given as an example only, and each stakeholder should be in a position to include measures that it considers adequate for the particular risks involved.

Regulatory monitoring appears to be one of the conceivable mitigation measures, whether this relates to regulations in the country in which the fund is marketed (in particular on the local marketing rules) or the regulations applicable to investors and distributors.
A regulatory change may impact on the distribution network.

Moreover, internal controls should be introduced among stakeholders who are responsible for distributing a particular fund, such as lists of the distribution countries and an analysis of these countries; detailed lists of the distributors and sub-distributors, including, among others, the commissions transferred. Other possible controls include the monitoring of investors and their complaints as well as the monitoring of distributors, which may include commissioning an audit of this distributor or making a site visit to obtain the required reassurance.

Lastly, another mitigation measure could be the transmission, by the distributor to the management company and/or to the fund, of reports (at an interval to be determined) containing information on countering money laundering and identifying investors; on the complaints received from investors and on incidents that have occurred in the distribution of the fund.

**CONCLUSION:**

As each marketing strategy is specific, assuming that the market players carry out their own risk analysis and document it, the goal is to be in a position to demonstrate sufficient knowledge of their distribution network.

There are a number of ways to attain this goal, with emphasis placed on identifying and mitigating the risks posed by its network, as this is not, in my opinion, an option but an obligation, given the new requirements introduced by MIFID 2.

**Elisa Da Silva**
Managing Director of DS Compliance

1. Practices and recommendations aimed at reducing the risk of money laundering and terrorist financing in the Luxembourg Fund industry, July 2013.
2. Directive 2014/65/EC
3. EU Regulation n° 1286/2014 of 26 November 2014 on "PRIIPS" relating to key information documents for packaged retail and insurance-based investment products intended for retail investors.

# LA FINTECH ET LA SÉCURITÉ DES DONNÉES

© DR

**ROSS MAIN**

Pour les prestataires de services financiers, la FinTech (technologie financière) fait partie des domaines qui connaissent la plus forte croissance. Son aptitude à révolutionner n'importe quelle institution financière et à changer la donne pour tout le secteur financier a conduit de nombreux acteurs à constater et suivre ses différents développements. Toutefois, pour de nombreuses start up de FinTech, la réalité se traduit couramment par une incapacité à connaître un succès sur le long terme, des failles de sécurité inattendues et une incapacité à évoluer plus rapidement que la concurrence intense.
La rapidité du changement provient de petites start up de FinTech qui s'appuient sur une approche mondiale. La dernière solution miracle de FinTech aurait pu être conçue à Londres, sa partie logicielle développée en Inde, son assemblage effectué en Chine et les serveurs hébergés dans un silo à missiles abandonné du désert du Nevada.
La variété infinie des produits FinTech et la chute de leur prix a conduit de nombreux acteurs à réévaluer leurs plans stratégiques informatiques avec la possibilité de concrétiser des objectifs stratégiques plus tôt que prévu. Pourquoi miser sur le développement d'une solution interne lorsque les produits FinTech sont proposés à un niveau de coût inférieur à la moyenne mensuelle des salaires pour un département informatique, et plus encore, lorsque les institutions financières ont la possibilité d'investir dans des startups FinTech et de développer conjointement la technologie ?
Un certain nombre de startups FinTech ont orienté leurs initiatives de commercialisation vers les compliance officers qui font l'objet de démarchage téléphonique de la part des sociétés de FinTech souhaitant faire la démonstration de leur produit au « compliance officer ». Il s'agit d'une stratégie de développement intéressante et astucieuse. Cette stratégie visant à se tourner directement vers les compliance officers et leurs appréciations sensées des menaces potentielles et de l'impact sur l'institution liés à l'introduction d'une nouvelle solution FinTech, permet d'identifier l'obstacle de référence que doivent surmonter les FinTech.
Une des menaces réside dans le fait que l'introduction d'une solution FinTech au sein d'un département a des incidences négatives sur les flux de travail des autres départements, car elle entraîne des interventions manuelles excessives. Le fait d'apporter une révolution à des processus d'un département peut compromettre les processus d'autres départements, y compris en ce qui concerne les questions d'interdépendance, de contrôle et de sécurité entre les départements. Il est également possible de négliger le fait qu'une solution de FinTech récemment mise en œuvre et jouant seulement un rôle mineur dans les processus de l'institution est

>>>

## FINTECH AND DATA SECURITY

Fintech is one of the fastest growing areas for financial service providers. Its potential to revolutionise any financial institution and create a game changer for the entire financial industry has made many to take notice and track developments. However it is a common reality that many Fintech start-ups don't achieve sustainable success, have unforeseen security flaws or are structurally unable to evolve faster than the intensity of competition.
The speed of change is being driven by small Fintech start-ups utilising a global approach. The latest Fintech wonder could have been designed in London, the software developed in India, the assembly undertaken in China and the servers located in an abandoned missile silo in the Nevada desert.
The endless variety of Fintech products and the fall in their price has many re-assessing their strategic IT plans with the potential of realising strategic goals earlier than anticipated.
Why gamble on developing an in-house solution when Fintech products are being offered at less than the average monthly payroll for an IT department? And more so when financial institutions have the opportunity to invest into Fintech start-ups and jointly develop the technology.
A number of Fintech start-ups have targeted their marketing towards Compliance Officers who receive cold calls from Fintech companies wanting to demonstrate their product to "the Compliance Officer". This is an interesting and clever development. Going straight to the Compliance Officer with their sobering appraisal on the potential threats and impact to the institution by the introduction of a new Fintech solution, provides the benchmark hurdle which Fintechs need to satisfy.
One threat is that the introduction of a Fintech solution in one department negatively impacts the workflows of other departments creating excessive manual intervention. Revolutionising one department's processes may undermine the processes of other departments, including the issue of inter-departmental interdependence, control and security. It can be also overlooked that a newly implemented Fintech solution which plays only a minor role in the institution's processes could breach their entire IT infrastructure.
The variety of Fintech opportunities that can potentially revolutionise workflows makes it difficult to make an in-depth assessment more than the traditional methodology of due diligence interviews and checklist questionnaires.
Such methods may have a limited impact in controlling anxieties towards the threat of being hacked through the implementation of a flawed technology.
And when a new Fintech solution is structured as an interface between the institution and the consumer through the internet, data protection and security issues take on more complex dimensions. Internet security measures associated with data collection, transfer, processing and storage are rapidly evolving, requiring robust and layered protections which need continuous monitoring and dynamic remodeling.
Having been fully compliant with regulatory assessments does not guarantee security, nor guarantees that the new technology is going to revolutionise the

>>>

>>>
capable de violer toute l'infrastructure informatique.
La variété des opportunités FinTech susceptibles de révolutionner les flux de travail rend plus difficile la conduite d'une évaluation en profondeur par rapport à la méthodologie traditionnelle des entretiens et des questionnaires avec liste de vérification des diligences nécessaires. De telles méthodes peuvent avoir un impact limité pour la maîtrise des angoisses devant la menace pirate se profilant à travers la mise en œuvre d'une technologie défectueuse.
Et lorsqu'une nouvelle solution est structurée comme une interface entre l'institution et le client via Internet, la protection et la sécurité des données prennent des dimensions plus complexes. Les mesures de sécurité Internet associées au recueil, au transfert, au traitement et au stockage des données ont évolué rapidement, nécessitant de sérieuses protections réparties par couche qui requièrent une surveillance permanente et un remodelage dynamique.
Une conformité parfaite aux évaluations réglementaires ne garantit pas la sécurité et n'assure pas non plus que la nouvelle technologie révolutionnera l'institution.
Alors qu'elle est loin de garantir un certain niveau de contrôle, l'introduction d'une nouvelle solution FinTech peut être à l'origine de risques inattendus pour la sécurité des données.
Des enseignements peuvent être tirés des défaillances et failles de sécurité de données que les États-Unis ont rencontrées sur des données médicales pour lesquelles on pouvait s'attendre à ce que les normes de sécurité de données soient plus élevées que celles des institutions financières ; et ces enseignements peuvent être mis en pratique.
Les praticiens aux États-Unis qui travaillent avec des PHI (informations protégées sur la santé) doivent se conformer à la loi HIPAA (loi sur la portabilité de l'assurance maladie et la responsabilité). La conformité à la loi HIPAA constitue la norme pour la protection des PHI, y compris en matière de stockage de données médicales dans des installations de cloud dans le désert du Nevada par exemple.
Toutefois, des problèmes de sécurité pour les PHI ont été observés avec l'introduction par le Gouvernement fédéral des États-Unis du site Web ObamaCare (healthcare.gov).
Le site Web fonctionne, entre autres, comme un marché centralisé pour l'assurance maladie aux États-Unis. Les experts en cybersécurité ont découvert de profondes failles de sécurité susceptibles d'exposer des PHI et des données précises d'identification des personnes, y compris leur numéro de sécurité sociale et leurs antécédents médicaux.
De plus, le site Web avait la capacité de détourner l'ordinateur de l'utilisateur, y compris sa caméra, son microphone et ses disques durs.
Cela illustre l'importance de procéder à des tests de manière indépendante pour tous les nouveaux produits FinTech avant de les mettre en service. Faire appel à une société de cybersécurité à la fois indépendante de l'institution et de la solution FinTech dans le but de tester complètement la technologie depuis l'extérieur peut considérablement renforcer la confiance et améliorer les évaluations sur l'adéquation des contrôles exercés sur les infrastructures informatiques.
À l'inverse, les tests indépendants peuvent mettre à jour des failles de la technologie et des faiblesses structurelles. La découverte de failles technologiques ne doit pas être perçue de manière négative. La découverte de l'inconnu avant que la technologie ne soit mise en œuvre est salutaire et renforce la compréhension par l'institution des limitations de l'informatique.
En outre, au moment de l'évaluation de l'intégration d'une nouvelle FinTech au sein de l'infrastructure informatique d'une institution, l'emploi de diagrammes cartographiant l'infrastructure informatique de l'institution, y compris ses composants externalisés, constitue un outil utile qui renforce davantage la confiance et se montre gratifiant en termes de compréhension. Les cartographies qui détaillent l'endroit où est intégrée la nouvelle FinTech et fait ressortir son interaction avec les autres technologies peuvent illustrer les emplacements où devraient se concentrer les mesures d'évaluation indépendantes.
Ces évaluations sont fondamentales pour la bonne compréhension de la façon dont une brèche de sécurité pourrait interagir à travers l'infrastructure informatique de l'institution.
L'essor actuel que connaissent les progrès technologiques offre un très grand nombre de possibilités. Les institutions financières qui tirent parti des développements de FinTech tout en maintenant un équilibre avec le besoin lié à la protection des données sensibles et critiques réalisent qu'il n'existe pas de réponse unique pour maintenir la sécurité de l'infrastructure informatique de l'institution.
La sécurité des données nécessite de multiples approches qui doivent être réévaluées et modifiées au fil des progrès technologiques.

**Ross Main**
Compliance Officer
BAUM Management S.à r.l.

>>> institution. Far from guaranteeing a level of control, the introduction of a new Fintech solution may create unforeseen data security risks.
Lessons can be learnt and applied from the data security failures and flaws experienced in the USA involving medical data which one would expect to have a higher data security standard than financial institutions.
Medical practitioners in the USA processing PHI (protected health information) need to comply with HIPAA compliance (Health Insurance Portability and Accountability Act). HIPAA compliance is the standard for protecting PHI, including the storage of medical data in cloud facilities in, for example the Nevada desert.
However, PHI security problems were observed with the introduction by the US federal government of the ObamaCare website (healthcare.gov). The website acts, inter alia, as a centralised market for health insurance in the USA.
Cyber-security experts discovered gaping security flaws which could expose PHI and the identification details of individuals, including their social security numbers and medical history. Furthermore, the website had the potential to hijack the user's computer, including the computer's camera, microphone and hard-drives.
This illustrates the importance of independently testing all new Fintech products before going live. Employing a cyber-security firm independent from both the institution and the Fintech to fully test the technology from the outside can greatly enhance confidence and assess the adequacy of controls over the IT infrastructure.
Conversely, independent testing can discover technology flaws and structural weaknesses. The discovery of technology flaws shouldn't be seen as negative. Knowing the unknown before the technology is implemented is beneficial and improves the institution's understanding of IT limitation.
Furthermore, when assessing the integration of a new Fintech into the institution's IT infrastructure, the use of diagrams mapping the institution's IT infrastructure including the outsourced components is a helpful tool which further builds confidence and compliments understanding. Maps detailing where the new Fintech fits into the IT infrastructure and highlighting its interplay with other technologies can illustrate where independent assessment measures should be concentrated. These assessments are the foundation of understanding how a security breach could interplay across the institution's IT infrastructure.
The current up-swing in technological progress is presenting a wealth of opportunities. Financial institutions taking advantage of Fintech developments while balancing the need to protect sensitive and mission-critical data, realise that there is no single answer in keeping the institution's IT infrastructure secure. Data security requires multiple approaches which need to be re-assessed and modified with technology's progression.

**Ross Main**
Compliance Officer
BAUM Management S.à r.l.

# ÉVALUATION

## DE L'ÉTAT DE PRÉPARATION À L'APPLICATION DE LA QUATRIÈME DIRECTIVE EUROPÉENNE SUR LA LUTTE CONTRE LE BLANCHIMENT DE CAPITAUX (LAB)

FILIP VERBEKE

MATTHIAS VERBEKE

**L'adoption de la quatrième directive anti-blanchiment de l'Union européenne (4AMLD) modifie le paysage réglementaire européen, et la préparation à la conformité est essentielle afin d'éviter des amendes réglementaires ou des atteintes à la réputation dans les années à venir. Comment les entreprises de services financiers peuvent-elles faire face aux nouveaux obstacles présentés par la directive ? Les programmes de conformité à la LAB axés sur les risques, spécialement adaptés à votre profil de risque, forment la réponse à cette question.**

>>>

© DR

## EUROPEAN UNION FOURTH ANTI-MONEY LAUNDERING DIRECTIVE READINESS ASSESSMENT: SOME

**The introduction of the European Union Fourth Anti-Money Laundering Directive (4AMLD) is changing the European regulatory landscape, and preparation for compliance is essential to avoid regulatory fines or reputational damage in the coming years. How can financial services organisations face the new hurdles presented by the directive? Risk-based AML compliance programs tailored to your risk profile are the answer.**

The recently proposed amendment have moved up the date of compliance to Jan. 1, 2017, and among other provisions calls out specific measures to combat terrorist financing. All point towards a common thread: mapping the specific risk, assess the coverage, monitor the risk on an ongoing basis. This requires a fundamental change, away from a static, tick the box approach, to a dynamic and pro-active continuous management of the ever evolving and changing risk.
It also requires a shift in attitude towards AML compliance: management must accept that rather than a hindrance, AML prevention reduces the general risk of the institution.
In this regard it is quite interesting to note that the Dutch regulator, De Nederlandse Bank, in its Guidance document on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act[1], labels money laundering an integrity risk: "Preventing the misuse of the financial system for money laundering and terrorist financing purposes and controlling integrity risks". Hereby a statement from the DNB:
"A good integrity risk analysis is essential for being able to comply with the requirements for corporate integrity and the regulations set forth in the Financial Supervision Act (Wft), the Act on the Prevention of Money Laundering and Financing of Terrorism (Wwft), and the 1977 Sanctions Act (SW)."
"In practice, institutions often seem to implement the regulations with a process based and fragmented approach. As a result, the available capacity is not used effectively and efficiently."[2]
Let us have a look now at a number of areas we think are the most impacted by the 4th EU Directive.

**CUSTOMER DUE DILIGENCE**

The requirement to identify all beneficial owners of businesses and trusts and the removal of automatic entitlements to apply simplified CDD represents a dramatic shift from the status quo.
When crafting a program to comply with the commission's new standards on CDD, consider these questions:

- Do we have procedures to identify beneficial ownership of our business and trust clients? This poses the question whether self-declaration policies should be reviewed; will these be sufficient for instance for customers coming from high risk countries, or whose occupancy is deemed high risk?
- How should we leverage the proposed

>>>

>>>
La modification récemment proposée a reporté la date de conformité au 1er janvier 2017 et requiert, entre autres dispositions, des mesures spécifiques de lutte contre le financement du terrorisme.

Ces mesures convergent toutes vers la nécessité commune de cartographier le risque spécifique, d'évaluer la couverture, et de surveiller le risque sans interruption. Cela nécessite un changement fondamental impliquant l'abandon d'une approche statique et passive au profit d'une gestion continue, dynamique et proactive du risque en constante évolution.

Cela exige également un changement d'attitude envers la conformité en matière de LAB : la direction doit accepter le fait que la prévention dans le domaine de la LAB ne constitue pas une entrave mais réduit le risque général de l'institution.

À cet égard, il est assez intéressant de noter que l'organisme de réglementation néerlandais, De Nederlandse Bank (DNB), dans son document d'orientation sur la loi relative à la lutte contre le blanchiment de capitaux et contre le terrorisme et sur la loi relative aux sanctions[1], qualifie le blanchiment d'argent de risque lié à l'intégrité : « Prévenir l'utilisation abusive du système financier à des fins de blanchiment de capitaux et de financement du terrorisme et maîtriser les risques liés à l'intégrité ».

Ainsi, selon DNB :
« Une bonne analyse des risques liés à l'intégrité est essentielle afin de pouvoir satisfaire aux exigences en matière d'intégrité de l'entreprise ainsi qu'aux règlements énoncés dans la loi sur la surveillance financière (Wft), la loi sur la prévention du blanchiment des capitaux et du financement du terrorisme (Wwft), et la loi de 1977 sur les sanctions (SW). »
« Dans la pratique, les institutions semblent souvent appliquer les règlements avec une approche fragmentée et basée sur des processus. En conséquence, la capacité disponible n'est pas utilisée de manière efficace et efficiente. »[2]
Examinons à présent un certain nombre de domaines qui, selon nous, sont les plus affectés par la quatrième directive européenne.

## OBLIGATION DE DILIGENCE À L'ÉGARD DES CLIENTS (CDD)

L'obligation d'identifier tous les propriétaires effectifs d'entreprises et de fiducies et la suppression des droits automatiques d'application de l'obligation simplifiée de diligence à l'égard des clients constituent un changement radical par rapport au statu quo.

Lors de l'élaboration d'un programme visant à vous conformer aux nouvelles normes de la Commission en matière d'obligation de diligence à l'égard des clients, posez-vous les questions suivantes :
• Disposons-nous de procédures d'identification de la propriété effective des clients de nos entreprises et fiducies ? Cela pose la question de savoir si les politiques d'auto-déclaration doivent être contrôlées ou non ; seront-elles suffisantes, par exemple, pour les clients issus de pays à haut risque, ou dont l'établissement est considéré comme étant à haut risque ?
• Comment devons-nous tirer parti du registre de propriété effective proposé qu'exige l'unité de renseignement financier de chaque nation ? Très peu de pays ont d'ores et déjà mis en place ces registres. Sommes-nous exemptés de tout contrôle de diligence raisonnable tant que ces registres ne sont pas disponibles ? Le fait de se fier à des données fournies par des tiers est-il suffisant pour ne pas avoir à procéder à un contrôle de diligence raisonnable renforcé en interne ? Et quelle fiabilité accorder aux informations reçues de la part des « services publics » ? En l'absence d'indications précises, nous recommandons d'opter pour l'interprétation la plus stricte.
• Comment allons-nous réévaluer, documenter et signaler nos relations avec des clients issus de pays figurant sur la liste noire désormais révoquée ?
• Comment devons-nous tenir compte de ces nouvelles informations dans l'évaluation des risques de notre institution ? Et de quelle manière notre modèle de risque reflète-t-il le risque réel ? Le calibrage de ce modèle ne s'applique pas uniquement à la surveillance des transactions ; l'évaluation du risque lié au client est un modèle qui est censé être géré et adapté à intervalles réguliers. Les techniques analytiques sont préférables aux modèles de risque à dire d'expert et apportent l'avantage supplémentaire d'une évaluation du risque plus précise, et donc d'une meilleure détection du risque de blanchiment de capitaux.
• Quelles procédures guideront la définition et le filtrage des personnes nouvellement désignées comme étant politiquement exposées (PPE) au niveau national ? Cet aspect est tout à fait sous-estimé, l'impact du dépistage des PPE au niveau national sur les systèmes de contrôle des clients est considérable : la probabilité de trouver des PPE au niveau national ayant des noms similaires à des clients existants est beaucoup plus
>>>

>>> beneficial ownership repository required by each nation's financial intelligence unit? Very few countries have yet put in place such repositories. Are we absolved from doing due diligences as long as these are not available? Is relying on 3d party data sufficient to not conduct an enhanced due diligence in-house? And how reliable is information deemed when received from "utilities"?
In the absence of specific guidance, we would recommend opting for the strictest interpretation.
• How will we re-evaluate, document, and report our relationships with clients drawn from nations on the now-revoked white list?
• How should we reflect this new information in our institution's risk assessment? And how does our risk model reflect the actual risk? Model tuning does not only apply to transaction monitoring, customer risk rating is a model, which is supposed to be managed and tuned on a regular basis. Analytical techniques prime expert-based risk models, and bring the added benefit op more accurate risk rating, and hence better detection of Money Laundering risk.
• What procedures will guide the definition and reconciliation of newly designated domestic politically exposed persons? This aspect is quite underrated, the impact of screening domestic PEP's on customer screening systems is massive: the likelihood of finding domestic PEP's with names similar to existing customers is much higher than with foreign PEP's, this having a massive impact on the number of alerts generated, and false positives. Admittedly, this issue is of lesser importance in many Luxemburgish operations, as most do not engage in domestic retail banking.
• Are our systems capable of collecting and maintaining additional CDD information? Additional data sources are available, in structured format (mainly through third party data providers) and unstructured format (search engines, social media, press…); is your institution ready to absorb these, how organised is the approach? Are you using text mining techniques which automate the approach and facilitate the gathering of relevant and meaningful information? How open are your existing systems to ingest this information?
A key question will be how to deal with due diligences for corporates, in order to perform KYB (Know Your Business partner). There seems to be a strong tendency towards stricter interpretation of "best efforts". In particular, the need to look for accurate and timely information on corporates, seems to become a requirement from a growing number of regulators; this would entail checking information on corporates directly into the registries from the country where the corporate is located, and providing a time stamp to ascertain the information was retrieved at the moment of the onboarding, or at the moment new elements occur in the status of the corporate.

A further question will pertain to identifying not only customers, but


© DR

>>>
élevée qu'avec des PPE étrangers, ceci ayant un impact considérable sur le nombre d'alertes générées et sur le nombre de faux positifs. Certes, cette question est de moindre importance dans de nombreuses opérations luxembourgeoises dans la mesure où la plupart ne sont pas concernées par l'activité nationale de banque de détail.
• Nos systèmes sont-ils capables de collecter et de gérer des informations supplémentaires en matière d'obligation de diligence à l'égard des clients ? Des sources de données supplémentaires sont disponibles, dans un format structuré (principalement par le biais de tiers fournisseurs de données) et non structuré (moteurs de recherche, réseaux sociaux, presse...) ; votre institution est-elle prête à les absorber, quelle est l'organisation de cette approche ? Utilisez-vous des techniques analytiques d'exploration de texte qui permettent d'automatiser l'approche et de faciliter la collecte d'informations pertinentes et significatives ? Dans quelle mesure vos systèmes actuels sont-ils capables d'intégrer ces informations ?

Une question clé sera de savoir comment gérer les contrôles de diligence raisonnable pour les entreprises afin d'effectuer des contrôles de vérification de l'identité des partenaires commerciaux (KYB). Il semble y avoir une forte tendance à l'interprétation plus stricte des « meilleurs efforts ». En particulier, la nécessité de rechercher des informations précises et actualisées sur les entreprises semble devenir une exigence chez un nombre croissant de régulateurs ; cela impliquerait de vérifier les informations sur les entreprises directement dans les registres du pays où chaque entreprise se trouve et de fournir un horodatage permettant de s'assurer que les informations ont été obtenues au moment de l'intégration des nouveaux clients ou au moment où de nouveaux éléments interviennent dans la situation de l'entreprise.

Une autre question portera sur l'identification non seulement des clients, mais aussi des contreparties, en vue de déterminer vers ou depuis quelles zones à haut risque (géographiquement, mais également en termes de type d'activités) vos clients envoient ou reçoivent des fonds. Ces informations nécessitent de disposer de la capacité de cartographier les flux entrants et sortants. Ce sont notamment les transferts internationaux effectués par le biais de correspondants bancaires et les opérations de financement des opérations commerciales qui seront soumis à cet examen. Tous les formats MT, MX et SEPA feront l'objet d'un examen particulier par les organismes de réglementation.

## MONITORING DES TRANSACTIONS

La directive et ses modifications ultérieures stipulent également que les institutions doivent mettre en œuvre des pratiques plus solides en matière de gestion des risques liés aux modèles et en matière de validation des modèles afin de confirmer que la conception du modèle de surveillance des transactions est appropriée au profil de risque de l'entreprise. Bien que la validation et l'optimisation des modèles puissent contribuer à garantir la conformité, la confirmation de seuils de surveillance des transactions documentées peut également améliorer l'efficacité opérationnelle en renforçant l'efficacité du système de monitoring des transactions.

Lors de l'évaluation de votre programme de transactions liées aux nouvelles exigences, posez-vous les questions suivantes afin de vous aider à évaluer votre état de préparation :
• Nos scénarios de

>>>

>>> also counterparties, to determine to which or from which high risk areas (geography, but also business type) your customers send or receive funds to and from. Such information requires the ability to map flows "from and to". In particular international transfers via correspondent banking, and trade finance operations will be the subject of such scrutiny.

All MT-, MX and SEPA formats will be the subject of particular scrutiny from regulators.

## TRANSACTION MONITORING

The directive and subsequent amendments also stipulate that institutions implement stronger model risk management and model validation practices to confirm transaction monitoring model design is appropriate to the risk profile of the organisation. Whilst model validation and optimisation will assist in maintaining compliance, the confirmation of documented transaction monitoring thresholds can also improve operational efficiencies by increasing the effectiveness of the transaction monitoring system.
When assessing your transaction program related to the new mandates, consider these questions to help determine your readiness:
• Do our automated monitoring scenarios and manual processes appropriately leverage beneficial ownership information? This poses the question of entity resolution and link analysis: if beneficial owners have been identified, how are these linked to other accounts, other account holders, and other entities? Can your monitoring systems create new entities which need to be investigated as a whole?
• Do we understand the operational impacts of these monitoring changes? For instance, how will threshold setting impact your organisations: above the line analytics are meant to reduce false positives, but below the line analytics could seriously impact the number of alerts generated, and hence the number of investigators required to monitor these.
• Is our transaction monitoring model appropriately documented and validated? Documenting and time-stamping tuning exercises will become an area of scrutiny of regulators. And how do you validate the tuning? On what dataset? A sub-set of all transactions; but on what basis has the sampling been organised to ensure consistency with the general customer population?
• Are our thresholds set appropriately, considering the risks presented to the institution? How many smurfers, flying below the radar, can you detect? What is the risk appetite: do you want to ensure 98% or 95% detection ratios?
• How do we document our rationale for adjustments to system settings and parameters? Ideally such exercises are conducted using data exploration and analytical tools; most of these tools have an audit trail, but bear in mind they must record more than the outcome; we recommend documenting the underlying hypothesis, the data used for the parameter setting,

>>>
surveillance automatisés et nos processus manuels permettent-ils de tirer le meilleur parti des informations relatives aux bénéficiaires effectifs ? Cela pose la question de la résolution des entités et de l'analyse des liens : si les bénéficiaires effectifs ont été identifiés, de quelle manière sont-ils liés à d'autres comptes, à d'autres titulaires de compte ainsi qu'à d'autres entités ? Vos systèmes de surveillance peuvent-ils créer de nouvelles entités qui doivent être examinées dans leur ensemble ?
• Comprenons-nous les impacts opérationnels de ces changements de surveillance ? Par exemple, comment la fixation de seuils impactera-t-elle vos entreprises : l'analyse au-delà des seuils vise à réduire les faux positifs, mais l'analyse en-deçà des seuils pourrait sérieusement affecter le nombre d'alertes générées et donc le nombre d'enquêteurs nécessaires à leur surveillance.
• Notre modèle de monitoring des transactions est-il documenté et validé de manière appropriée ? Les exercices de paramétrage de la documentation et de l'horodatage deviendront un domaine de contrôle des régulateurs. Et comment validez-vous ce paramétrage ? Sur quel ensemble de données ? Un sous-ensemble de toutes les transactions ? Mais sur quelle base l'échantillonnage a-t-il été organisé afin de garantir la cohérence avec la population générale des clients ?
• Nos seuils sont-ils établis de façon appropriée, compte tenu des risques présentés à l'institution ? Combien de fraudeurs bancaires, évoluant en dessous des seuils, pouvez-vous détecter ? Quel est le niveau de risque garanti : voulez-vous assurer un taux de détection de 98% ou de 95% ?
• Comment documentons-nous notre justification des ajustements apportés aux réglages et aux paramètres du système ? Idéalement, ces exercices sont effectués à l'aide d'outils d'exploration et d'analyse des données ; la plupart de ces outils ont un journal d'audit, mais gardez à l'esprit qu'ils doivent enregistrer plus que le résultat ; nous recommandons par conséquent de documenter l'hypothèse sous-jacente et les données utilisées pour le réglage des paramètres, ainsi que l'enregistrement des résultats des différentes itérations.
Un examen particulier est prévu pour la couverture. Dans quelle mesure votre système de surveillance des transactions couvre-t-il tous les risques identifiés dans votre évaluation des risques ? Suivant l'exemple des régulateurs américains, les régulateurs européens souhaiteront une évaluation formelle de la couverture et l'on prévoit que des vérifications seront effectuées en conséquence par des auditeurs externes et internes. Les zones à risque élevé qui ne sont pas prises en compte dans votre monitoring des transactions, et les activités de moindre envergure ou accessoires qui ne sont pas considérées comme suffisamment importantes pour être soumises à un monitoring dans les mises en œuvre antérieures de la surveillance des transactions, seront particulièrement ciblées.

## GOUVERNANCE INTERNE

Presque chaque niveau d'une entreprise sera confronté à la nécessité de procéder à des ajustements basés sur les nouvelles exigences. Une communication interne, une documentation et une formation appropriées sont nécessaires afin d'assurer la conformité à l'échelle de l'entreprise. Tout manquement à une mise en œuvre systématique des changements peut entraîner des problèmes sur le plan réglementaire.

Dans le cadre de la conformité aux exigences de gouvernance interne, les entreprises doivent prendre en compte les questions suivantes :
• Nos normes, politiques et procédures mettent-elles l'accent sur une approche axée sur le risque et intègrent-elles correctement les exigences de la quatrième directive européenne ? Une validation externe est recommandée ; elle constitue un élément clé des évaluations de préparation que prévoient les organismes de réglementation mais elle est généralement très sous-estimée. Cela pose également la question de la gestion du changement en général ; la quatrième directive européenne n'apporte pas seulement un nombre supplémentaire d'exigences plus strictes, elle nécessite aussi un changement de mentalité et une prise de conscience dont l'impact sur l'entreprise ne doit pas être sous-estimé.
• Disposons-nous d'un processus documenté de contrôle des changements ? Ce processus est-il automatisé ? Nous sommes d'avis que, dans de nombreux cas, l'utilisation d'un système EGRC sera obligatoire afin de satisfaire à ces exigences.
• Notre documentation permet-elle facilement à un tiers d'examiner et de comprendre notre programme ? Les régulateurs, mais aussi les auditeurs externes et les
>>>

>>> the results of various iterations should be recorded.
Particular scrutiny is expected to coverage. In how far is your transaction monitoring system covering all the risks identified in your risk Assessment. Following the example of the US regulators, European regulators will expect a formal coverage Assessment, and it is expected checks will be performed accordingly by external and internal auditors. High risk areas which are not reflected in your transaction monitoring detection, and smaller or ancillary activities not deemed large enough to undergo monitoring in previous implementations of transaction monitoring, will be particularly targeted.

## INTERNAL GOVERNANCE

Nearly every level of an organisation will encounter the need for adjustments based on the new mandates. Proper communication, documentation, and training are required to confirm enterprise-wide compliance. Any failure to consistently implement changes can lead to regulatory concerns.
As a component of compliance with internal governance requirements, organisations should consider the following questions:
• Do our standards, policies, and procedures emphasise a risk-based approach and appropriately incorporate the requirements of the 4AMLD? External validation is recommended; this is a key element in the readiness assessments regulators are expecting, and is usually much underrated. Tis also poses the question on change management in general; the 4th EU directive is not just an additional number of stricter requirements, it requires change of mindset and awareness, the impact of which on the organisation is not to be underestimated.
• Do we have a documented change control process? Is this process automated? We are of the opinion that in many cases, using a EGRC system will be mandatory in order to comply with these requirements
• Does our documentation easily allow a third party to review and understand our program? Can regulators, but also external auditors and internal controllers easily gain access to these data? And what about Correspondent Banking due diligences your institution might be undergoing? Are you in a position to swiftly produce the required information?
• Is our training continuously updated to align with new regulations and internal policies? This is an often overlooked but essential part of a 4th EU Directive readiness assessment. The changes brought about by the new requirements are a shift change, impacting the whole organisation. Awareness training, regulatory updates, training in analytical and data exploration techniques and clear communication on operational changes and internal guidance will greatly assist in reducing the impact on the organisation and alleviating operational risk.
Systems keeping track and monitoring the above mentioned adjustments should be able to provide auditable evidence

>>>
contrôleurs internes, peuvent-ils facilement accéder à ces données ? Et qu'en est-il des contrôles de diligence raisonnable des activités de correspondant bancaire que votre institution pourrait subir ? Êtes-vous en mesure de produire rapidement les informations requises ?
• Notre formation est-elle continuellement actualisée afin d'être conforme aux nouveaux règlements et procédures internes ? Il s'agit là d'une partie souvent négligée mais essentielle de toute évaluation de l'état de préparation à l'application de la quatrième directive européenne. Les changements générés par les nouvelles exigences constituent un changement de régime qui impacte l'ensemble de l'entreprise. Les sensibilisations, mises à jour réglementaires, formations aux techniques d'analyse et d'exploration des données, accompagnées d'une communication claire sur les changements opérationnels et de conseils en interne, contribueront grandement à réduire l'impact sur l'entreprise et à atténuer les risques opérationnels.
Des systèmes permettant de suivre et de surveiller les ajustements mentionnés ci-dessus devraient pouvoir fournir des preuves vérifiables des changements effectués et des améliorations obtenues.

## AMÉLIORATION DE L'ACCÈS AUX INFORMATIONS RELATIVES À LA PROPRIÉTÉ EFFECTIVE

La quatrième directive européenne prévoit un registre centralisé des bénéficiaires effectifs (BE). Compte tenu du nouveau délai imposé aux gouvernements pour mettre en œuvre la quatrième directive européenne, rares sont ceux qui ont été en mesure de fournir cette infrastructure à temps.

Cela présente un risque, car certains pourraient espérer repousser le suivi des BE jusqu'à ce que ces registres soient opérationnels. Mais la directive est claire : la vérification des BE doit être effectuée. Nous recommandons par conséquent qu'elle soit effectuée indépendamment de la disponibilité des registres.
Actuellement, une vague considérable d'améliorations du programme KYC/CDD est en cours au sein de l'industrie européenne des services financiers. L'externalisation des processus opérationnels se fait à grande échelle en vue de garantir qu'une vérification détaillée puisse être effectuée et que des économies d'échelle puissent être réalisées afin d'éviter de mobiliser des ressources excessives. Les enquêtes sur les BE, pour les cas complexes, en sont un parfait exemple. Différentes formes de « services mutualisés » sont envisagées.

## OBLIGATIONS EN MATIÈRE DE GESTION DES RISQUES LIÉS AUX MODÈLES

Un aspect moins connu de la quatrième directive européenne concerne l'obligation en matière de gestion des risques liés aux modèles. Elle découle des Recommandations prudentielles sur la gestion des risques liés aux modèles (OCC 2011-12) du Bureau américain du Contrôleur de la Monnaie, qui ont eu de profondes répercussions sur les institutions financières américaines au cours de ces 5 dernières années.
Selon des analystes de l'industrie tels que le groupe Aite[3], la gestion des risques liés aux modèles constitue un point de focalisation croissant pour les régulateurs de la LAB car ils veulent s'assurer que les institutions financières comprennent bien comment fonctionnent leurs analyses dans le cadre de la LAB et que toute adaptation ne fait pas obstacle aux efforts de détection. Ils veulent s'assurer que les systèmes fonctionnent par le biais de la démonstration, de l'explication et de la documentation. Il est essentiel que les solutions offrent une flexibilité permettant de modifier rapidement les scénarios et qu'elles puissent montrer visuellement comment et pourquoi des changements ont été apportés.
La note d'orientation de l'organisme de réglementation néerlandais De Nederlandse Bank, mentionnée plus haut dans le présent article, met spécifiquement l'accent sur la gestion des risques liés aux modèles et sur les exigences en matière de documentation. Les régulateurs néerlandais ont déjà intensifié leurs efforts sur leurs institutions financières en vue de se conformer à cette note.
D'autres régulateurs en Europe ont aussi récemment commencé à prendre des mesures.
Comme indiqué précédemment, cet aspect lié à la documentation exigera dans de nombreux cas que les institutions financières utilisent des systèmes GRC afin de se conformer aux nouvelles obligations.

**Filip et Matthias Verbeke**

1. www.toezicht.dnb.nl/en/binaries/51-212353.pdf
2. Source : Thema's DNB toezicht 2015 (thèmes de supervision de DNB pour 2015)
3. AITE - Evaluation globale des prestataires en matière de LAB : gestion des risques à évolution rapide, juin 2015

>>> of changes and improvements.
**IMPROVED ACCESS TO BENEFICIAL OWNERSHIP INFORMATION**
The 4th EU Directive calls for a centralised registry of Ultimate Beneficial Owners. Given the new deadline for governments to implement the 4th EU Directive, few have been able to provide this infrastructure in time. This poses a risk, as some might hope to push out the tracking of UBO's until these registries will be operational. The directive is clear: UBO checking needs to happen, we recommend it should be done regardless of the readiness of the registries.
There is currently a massive wave of KYC/CDD program improvements under way in the European financial services industry. Business Process Outsourcing is happening at a large scale, in order to ensure detailed checking can be performed, and economies of scale can be achieved to avoid mobilizing excessive amounts of resources. UBO investigations for complex cases are a prime case in point. Various forms of "utilities" are being considered.

**MODEL RISK MANAGEMENT OBLIGATIONS**
A lesser known aspect of the 4th EU Directive concerns the Model risk Management obligation. It stems from the Supervisory Guidance on Model Risk Management (OCC 2011-12) from the US Office of the Comptroller of the Currency, which has had a profound effect on US financial institutions over the last 5 years.
According to industry analysts such as the Aite Group[3], Model risk management is an increasing point of focus for AML regulators – they want to know that financial institutions understand how their AML analytics work, and that any tuning is not hampering detection efforts. They want to see evidence that systems work via demonstration, explanation and documentation. It's critical that solutions provide the flexibility to quickly modify scenarios and can visually show how and why changes were made.
The guidance note from the Dutch regulator, De Nederlandse Bank, mentioned earlier in the article, is putting specific emphasis on model risk management, and on documentation requirements. Dutch regulators have already stepped up efforts on their financial institutions to comply with this guidance. Other regulators in Europe have recently also started to undertake action.
As indicated before, the documentation aspect of this will in many cases require financial institutions to use GRC systems to align with the new obligations.

**Filip and Matthias Verbeke**

1. www.toezicht.dnb.nl/en/binaries/51-212353.pdf
2. Source: Thema's DNB toezicht 2015 (themes DNB supervision 2015)
3. AITE Global AML Vendor Evaluation: Managing Rapidly Escalating Risk, June 2015

JEAN-NOËL LEQUEUE (JNL)

# LES COMPLIANCE OFFICERS EN 2017

**QUELLE EST VOTRE ANALYSE DU MARCHÉ DE LA COMPLIANCE EN 2017 ?**
Notre marché fonctionne selon les règles traditionnelles de l'offre et de la demande : la réglementation correspond à la demande et elle ne fait qu'augmenter ! Je constate trois évolutions principales :

**1.** Les réglementation européennes émanant de la commission et du parlement sont à l'origine des nouvelles obligations locales de deux types : les directives d'une part, que les Etats doivent transposer et les règlements d'autre part, qui s'appliquent d'office et qui impliquent parfois de modifier la loi d'un pays. Ces règlements sont utilisés de plus en plus souvent afin d'harmoniser les règles en Europe, mais ils réduisent l'autonomie nationale.
**2.** Les autorités nationales cèdent une partie de leur autorité à l'EBA et à l'ESMA qui émettent des obligations supplémentaires et participent aux contrôles. Les établissements systémiques par exemple, sont contrôlés directement par les autorités européennes, or ces dernières ne connaissant pas bien le terrain local, elles formulent des demandes exhaustives et lourdes.
**3.** Le Luxembourg veut être perçu parmi les «premiers de la classe», tant au niveau de la vitesse de transposition qu'au niveau de la précision réglementaire. Cela rompt avec le passé et il n'est pas rare que le Grand-Duché aille au-delà des demandes !
Ces trois points reflètent la pression réglementaire très forte qui pèse aujourd'hui sur les compliance officers dans tous les domaines.
La quantité et la diversité des réglementations nécessitent soit une quasi-omniscience, soit la mise en place d'équipes spécialisées. Parallèlement, le nombre de membres de ALCO croît avec aujourd'hui plus de 800 membres.

**QUELLES OPPORTUNITÉS ET MENACES SE PRÉSENTENT POUR LE LUXEMBOURG ?**
Le Brexit semble représenter une opportunité car le Luxembourg sert souvent de point d'entrée dans l'Union Européenne pour des groupes financiers internationaux. L'attractivité historique de Londres a longtemps été supérieure, mais si le Luxembourg parvient à élargir ses compétences, il pourra bénéficier de cette évolution. Il n'est pas rare de voir un fonds basé au Luxembourg avec un promoteur en France et un manager à Londres ! Même en Asie, la marque « Luxembourg UCITS » bénéficie d'une renommée importante.
Ceci implique un besoin de compétence très large pour le compliance officer, tant au niveau des langues que de la compétence spécifique de chaque marché. Je pense qu'un gros besoin de formation existe ici, notamment pour les jeunes experts qui sont devenus compliance officers ou qui ont rejoint récemment la CSSF. À part cela, le projet de réduction de l'opposabilité du secret bancaire risque d'avoir un fort impact sur notre profession, et au niveau des nouvelles technologies, j'observe une grande effervescence, mais pour l'instant, peu d'innovations arrivent à maturité.

**Jean-Noël Lequeue**
PDG de jnl




© 360 CROSSMEDIA

***«L'outsourcing de la fonction compliance permet de fournir une forme d'omniscience, très vite et à un coût raisonnable.»***

*"Outsourcing the compliance function makes it possible to provide a kind of omniscience, very quickly and at a reasonable cost."*

**Jean-Noël Lequeue**

## COMPLIANCE OFFICERS IN 2017

**HOW WOULD YOU ANALYSE THE COMPLIANCE MARKET IN 2017?**
Our market operates according to the traditional rules of supply and demand: regulation corresponds with demand and it's definitely increasing! There are three main developments:
**1.** European regulations from the Commission and the Parliament are behind two types of domestic obligations: directives, which States must transpose, and regulations, which apply automatically and sometimes involve changing a country's laws. These regulations are increasingly being used to standardise European law, but they reduce national sovereignty.
**2.** National authorities give up part of their authority to the EBA and the ESMA, which issue additional obligations and play a role in carrying out checks and inspections. For example, systemic institutions are inspected directly by the European authorities. However, since the latter are not familiar with the local situation, they make exhaustive and onerous requests.
**3.** Luxembourg wants to be seen among the "top of the class", both in terms of the speed of transposition and the level of regulatory precision. This breaks with the past and it's not uncommon for the Grand Duchy to go above and beyond such demands! These three points reflect the very intense regulatory pressure which compliance officers face today on all fronts. The quantity and diversity of regulations require either a quasi-omniscience or the setting up of specialist teams. At the same time, the number of members of ALCO is growing: it currently has more than 800 members.

**WHAT OPPORTUNITIES AND THREATS ARE THERE FOR LUXEMBOURG?**
Brexit seems to be an opportunity because Luxembourg is often used as a point of entry into the European Union for international financial groups. The historic attractiveness of London has long been superior, but if Luxembourg is able to expand its skills, it will benefit from this development. It's not unusual to see a fund based in Luxembourg with a developer in France and a manager in London! Even in Asia, the «Luxembourg UCITS» brand has a considerable reputation. This requires a compliance officer to have a very wide range of skills, both in terms of languages and the specific skills for each market. I think that there's a real need for training here, especially for young experts who have become compliance officers or who have recently joined the CSSF. Apart from that, the proposed reduction in the enforceability of banking secrecy risks having a strong impact on our profession. While new technologies are an exciting subject, for the moment, very little innovation is actually being implemented.

**Jean-Noël Lequeue**
CEO of jnl

# NEWS PAR FLORENCE BARRIÈRE

## À JOUR AU 17 FÉVRIER 2017

## ACTUALITÉS INTERNATIONALES

**GAFI**

- 28 Oct 2016 Terrorist Financing in West and Central Africa
- 21 Oct 2016 Guidance Correspondent Banking Services
- 21 Oct 2016 Guidance on Criminalising Terrorist Financing

## ACTUALITÉS EUROPÉENNES

- COM (2016) 450 : Proposition de DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme et la directive 2009/101/CE

## ACTUALITÉS LUXEMBOURGEOISES

- Loi du 23 décembre 2016 portant mise en oeuvre de la réforme fiscale 2017 et portant modification (…) du Code pénal (…)
- Loi du 23 décembre 2016 portant transposition de la directive 2014/17/UE du Parlement européen et du Conseil du 4 février 2014 sur les contrats de crédit aux consommateurs relatifs aux biens immobiliers à usage résidentiel et modifiant les directives 2008/48/CE et 2013/36/UE et le règlement (UE) n° 1093/2010 ; et
- Loi du 23 décembre 2016 relative aux abus de marché

**CSSF**

**Règlements CSSF**

- Règlement CSSF N° 16-15 sur la fixation du taux de coussin contracyclique pour le premier trimestre 2017
- Règlement CSSF N° 16-08 concernant les établissements d'importance systémique agréés au Luxembourg
- Règlement CSSF N° 16-07 relatif à la résolution extrajudicaire des réclamations

**Circulaires CSSF**

- Circulaire CSSF 17/650 du 17.02.2017 : Application de la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme (ci-après « Loi LBC/FT ») et du règlement grand-ducal du 1er février 2010 portant précision de certaines dispositions de la loi LBC/FT (ci-après « RGD LBC/FT ») aux infractions primaires fiscales
- Circulaire CSSF 17/649 du 09.02.2017 : Adoption des orientations émises par l'Autorité bancaire européenne (ABE/EBA) sur les modalités de fourniture d'informations sous une forme résumée ou agrégée aux fins de l'application de l'article 84, paragraphe 3, de la directive 2014/59/UE (« Banking Recovery and Resolution Directive », en abrégé « BRRD »), (EBA/GL/2016/03)
- Circulaire CSSF-CODERES 17/03 du 09.02.2017 : Adoption des orientations émises par l'Autorité bancaire européenne (ABE/EBA) sur les modalités de fourniture d'informations sous une forme résumée ou agrégée aux fins de l'application de l'article 84, paragraphe 3, de la directive 2014/59/UE (« Banking Recovery and Resolution Directive », en abrégé « BRRD »), (EBA/GL/2016/03)
- Circulaire CSSF 17/648 du 11.01.2017 : Orientations de l'Autorité Européenne des Marchés Financiers (AEMF-ESMA) relatives aux facteurs, mesures et enregistrements que les personnes visées par les sondages de marché doivent prendre en compte et mettre en œuvre conformément à l'article 11, paragraphe 11, du règlement n° 596/2014 sur les abus de marché (« MAR »)
- Circulaire CSSF 16/647 du 22.12.2016 : Mise à jour de la circulaire CSSF 12/552 relative à l'administration centrale, gouvernance interne et gestion des risques suite à l'adoption des orientations de l'Autorité bancaire européenne (ABE/EBA) en matière de limites pour les expositions sur des entités du système bancaire parallèle qui exercent des activités bancaires en dehors d'un cadre réglementé au titre de l'article 395, paragraphe 2, du règlement (UE) n° 575/2013 (EBA/GL/2015/20)
- Circulaire CSSF 16/646 du 20.12.2016 : Orientations de l'Autorité Européenne des Marchés Financiers (AEMF-ESMA) concernant le retard de la publication d'informations privilégiées conformément à l'article 17, paragraphe 4 du règlement (UE) n° 596/2014 sur les abus de marché (« MAR »)

**CAA**

**Circulaires CAA**

- Lettre circulaire 17/1 du Commissariat aux assurances portant modification à la lettre circulaire 16/5 du Commissariat aux assurances précisant les conditions d'exemption pour la remise d'informations sur les notations externes dans les états détaillés des placements et des dérivés
- Lettre circulaire 16/12 relative aux taux d'intérêt techniques maxima applicables aux nouveaux contrats d'assurance vie
- Lettre circulaire 16/10 du Commissariat aux Assurances portant modification de la lettre circulaire 15/12 relative aux taux d'intérêt techniques applicables aux entreprises de réassurance

## NEWS UP-TO-DATE AS OF 17 FEBRUARY 2017

**INTERNATIONAL NEWS**

**FATF**

- 28 Oct 2016 Terrorist Financing in West and Central Africa
- 21 Oct 2016 Guidance Correspondent Banking Services
- 21 Oct 2016 Guidance on Criminalising Terrorist Financing

**EUROPEAN NEWS**

- COM (2016) 450: Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC

**LUXEMBOURGISH NEWS**

- Loi du 23 décembre 2016 portant mise en oeuvre de la réforme fiscale 2017 et portant modification (…) du Code pénal (…)
- Law of 23 December 2016 (only in French) transposing Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010; and
- Law of 23 December 2016 (only in French) on market abuse

**CSSF**

**CSSF Regulations**

- CSSF Regulation N° 16-15 (only in French) on the setting of the countercyclical buffer rate for the first quarter of 2017
- CSSF Regulation N° 16-08 (only in French) concerning systemically important institutions authorised in Luxembourg
- CSSF Regulation N° 16-07 relating to out-of-court complaint resolution

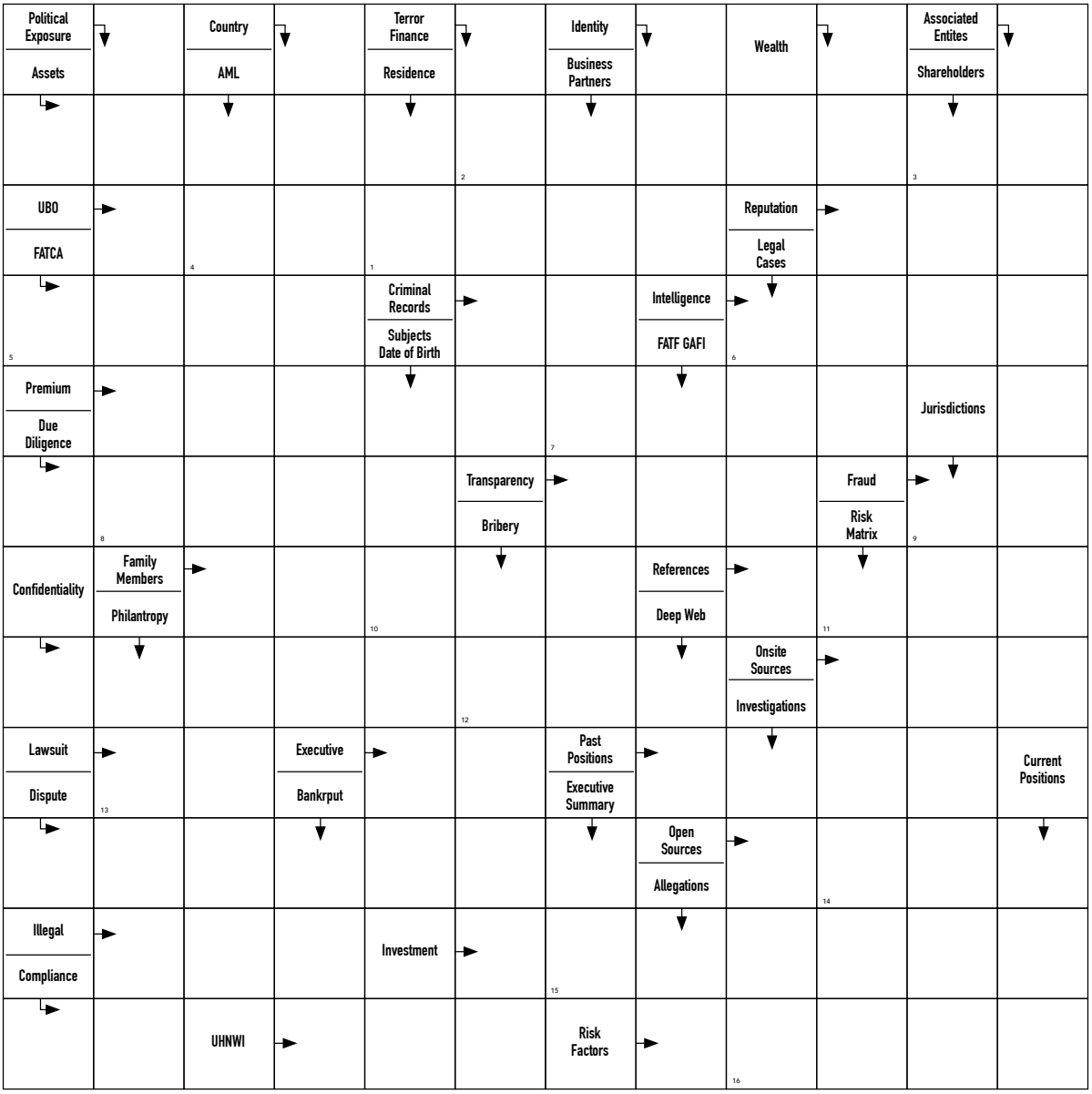
**CSSF Circulars**

- Circular CSSF 17/650 (only in French) 17.02.2017: Application of the Law of 12 November 2004 on the fight against money laundering and terrorist financing, as amended (hereinafter the "AML/CFT Law"), and of the Grand-ducal Regulation of 1 February 2010 providing details on certain provisions of the AML/CFT Law (hereinafter the "AML/CFT GDR") to primary tax offences
- Circular CSSF 17/649 (only in French) 09.02.2017: Adoption of the guidelines issued by the European Banking Authority (EBA) on the provision of information in summary or collective form for the purposes of Article 84(3) of Directive 2014/59/EU («Banking Recovery and Resolution Directive», in abbreviated form «BRRD») (EBA/GL/2016/03)
- Circular CSSF-CODERES 17/03 (only in French) 09.02.2017: Adoption of the guidelines issued by the European Banking Authority (EBA) on the provision of information in summary or collective form for the purposes of Article 84(3) of Directive 2014/59/EU («Banking Recovery and Resolution Directive», in abbreviated form «BRRD») (EBA/GL/2016/03)
- Circular CSSF 17/648 (only in French) 11.01.2017: Guidelines of the European Securities and Markets Authority (ESMA) in relation to the factors, the steps and the records that the persons receiving the market soundings shall consider and implement according to Article 11(11) of Regulation (EU) No 596/2014 on market abuse («MAR»)
- Circular CSSF 16/647 (only in French) 22.12.2016: Update of Circular CSSF 12/552 on the central administration, internal governance and risk management following the adoption of the EBA Guidelines on the limits on exposures to shadow banking entities which carry out banking activities outside a regulated framework under Article 395(2) of Regulation No 575/2013 (EBA/GL/2015/20)
- Circular CSSF 16/646 (only in French) 20.12.2016: ESMA Guidelines on the delay in the disclosure of inside information under Article 17(4) of Regulation (EU) No 596/2014 on market abuse («MAR»)

**CAA**

**CAA Circulars**

- Lettre circulaire 17/1 du Commissariat aux assurances portant modification à la lettre circulaire 16/5 du Commissariat aux assurances précisant les conditions d'exemption pour la remise d'informations sur les notations externes dans les états détaillés des placements et des dérivés
- Lettre circulaire 16/12 relative aux taux d'intérêt techniques maxima applicables aux nouveaux contrats d'assurance vie
- Lettre circulaire 16/10 du Commissariat aux Assurances portant modification de la lettre circulaire 15/12 relative aux taux d'intérêt techniques applicables aux entreprises de réassurance




YOUR ADVANTAGE :

| K | N | O | W | I | N | G | | I | N | | A | D | V | A | N | C | E |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | | 8 | 9 | | 10 | 11 | 12 | 13 | 14 | 15 | 16 |

**Sqope is a leading provider of advanced Due Diligence Reports** that empower financial executives to evaluate risk and make decisions. Our clients benefit from Premium Intelligence, based on transparent sources. We deliver results quickly and ensure full confidentiality of our clients' identity and sensitive information.

www.sqope.lu

SQOPE

INTELLIGENCE
FOR DECISION MAKERS