Focus
January 2009

The risk of money laundering:
Prevention, challenges, outlook
Introduction 4

The pressure of dirty money at a national and international level 5

- What is money laundering? 5
- Types of money laundering 5
- How can we combat money laundering? 7
- Cooperation of international police departments 7
- Working with the private sector 8
- The pressure of dirty money: why companies need to be vigilant 8
- The objective of a criminal who approaches a bank or an insurance company 8
- What are the risks involved for the company? 8

Anti-money laundering procedures and their objectives 9

- Risk mapping 10
- Risks linked to the product 10
- Risks inherent in client relationships 10
- Risks inherent in distribution networks 11
- Professional recommendations serve stringent requirements 12
- Assessment and adoption of internal procedures 12

Reporting a suspicion 13

- Financial Intelligence Units: at the centre of the States’ anti-money laundering procedures 13
- Reporting a suspicion to a Financial Intelligence Unit 15

Reinsurance and the prevention of money laundering 18

- Situation of reinsurance with regard to anti-money laundering conformity rules 18
- Vigilance rules adapted to risk 18
- Knowledge of the client 18
- Knowledge of facultatives 19
- Checking the flow of funds 19

Conclusion 20

- Appendix 1: Risk assessment table 21
- Appendix 2: Main points of the anti-money laundering procedure recommended by the FATF to financial operators including insurers 23
The laundering of dirty money plays a key role in a large proportion of criminal activity which, according to international experts, generates around 1,500 billion dollars per year. To introduce these funds in the legal economy, the holders must provide them with an appearance of legitimacy, subjecting the dirty money to a whole series of transformations, with varying degrees of complexity, most often using mechanisms and techniques to facilitate the conclusion of the transactions, the circulation of clean money and the smooth running of the economy.

Funds which have thus been laundered, apart from supporting and further increasing organised crime, threaten the international financial system and, on an institutional level, promote the development of corruption and risk to threaten the very foundations of the rule of law.

Added to this threat generated by cross-border crime, is that of the financing of international terrorism, since the attacks of 11 September 2001. On the recommendation of the FATF, the international community as well as many States have combined these two phenomena in the same fight. This double threat has therefore led the national and international authorities to increasingly put pressure on financial establishments.

Indeed, since the FATF was created by the G7 in 1989, the complex and evolving regulations have demonstrated the desire of the States to reinforce and refine the partnership between the financial intelligence units, which aim to gather and react to reported suspicions, and those parties subject to the rules of vigilance.

For their part, professional organisations have drawn up recommendations that link all of their members.

The third European directive adopted on 26 October 2005 after the Madrid attacks in March 2004, is innovative on two points:

• the extension of the preventative facility,
• a graduated approach depending on the money laundering risk involved.

It will oblige insurers to adapt their procedures by determining the exposure level of their products to the risk of money laundering and by defining profiles of clients at risk. This directive will increase the professionalization of anti-money laundering officers within insurance companies.

With a network of offices, subsidiaries and branches throughout the world, SCOR Global Life, one of the top 5 Life reinsurers worldwide, has a strong local presence that makes it particularly sensitive to the problems of money laundering. In light of this, we organised a conference in Paris in January 2008 designed to present the latest developments in money laundering and to promote reflection on the technical side of organising financial vigilance under the new regulations. We have drawn from the presentations and discussions that took place during this event in January for the last part of this document, which deals with the problems specific to reinsurance in the face of money laundering.

We would like to thank all of the speakers at this conference:

• Béatrice Créancier, from the TRACFIN investigation department,
• Christophe Perez-Baquey, Division Commissioner, Head of the Central Office for the Suppression of Serious Financial Crime (Office Central pour la Répression de la Grande Délinquance Financière - ORCGDF),
• Jérôme Robin, Chief Customs Inspector, former anti-money laundering project manager with the supervisory authority for insurance companies and mutual insurance companies (Autorité de Contrôle des Assurances et Mutuelles).

We would also like to thank all our clients who attended this conference/debate and contributed to the proceedings with a large number of questions.

(1) The Financial Action Task Force is an inter-governmental body whose purpose is the development of national and international policies to combat money laundering. Its Secretariat is housed at the OECD headquarters in Paris.

(2) The number of people and organizations obliged to follow rules of vigilance is constantly increasing: financial professions (banks, insurance companies, investment houses etc.), legal professions (notaries, bailiffs etc.), gambling establishments, certain service providers (real estate agents, dealers of precious stones, antiques etc.).
What is money laundering?

The reasoning behind the fight against money laundering consists of reducing the incitement to commit this kind of crime by suppressing the profits it generates. Such an objective presupposes in the first instance that money laundering is defined as a criminal offence, i.e. that in as many countries as possible it is the object of a similar legal definition, in order to facilitate cross-border suppression of the phenomenon.

Based on the conventions of the United Nations (Vienna convention of 20 December 1988) and the Council of Europe (held in Strasbourg on 8 November 1990), the FATF has significantly helped to expand the definition of money laundering offences. According to the Taskforce’s experts, the process involved may include:

- “the transformation or transfer of goods in the knowledge that such goods have resulted from criminal activity, with a view to concealing or disguising their illicit origins or in order to help anyone implicated in committing these criminal acts by shielding them from the legal consequences involved;
- receiving such goods or concealing their true origins, location or sale in the knowledge that they are the result of criminal activity;
- the acquisition, harbouring or use of goods by someone who knows that they are the result of criminal activity.”

The gradual definition by many States of money laundering as a crime, plus the fact that they have incorporated this definition into their internal legislations, in accordance with FATF recommendations, constitutes a major legal step forward in terms of eliminating the phenomenon. Now not only the profits generated by the drugs trade are targeted, but also the profits resulting from a number of different crimes: the illegal sale of arms, terrorism, smuggling, scams, corruption, computer fraud, procurement, fraudulent use of corporate property, etc.

In the strict sense of the law, money laundering implies a combination of offences based on an underlying crime such as the trading of stolen vehicles, for example. It is up to the courts to connect the double proof consisting of the link between the two crimes and the guilty knowledge of the money launderer.

Nevertheless, the regular improvement of anti-money laundering tools over the past twenty years has led money launderers to devise new techniques. It is therefore important to draw up a list of these techniques in order to help bankers and insurers to detect suspicious operations.

No country has been spared by this phenomenon. France, like other European countries where monitoring facilities have been implemented, remains a hub for criminal funds. Take for example business linked to the Russian oligarchs who have invested in magnificent properties on the Côte d’Azur. The money came from the misappropriation of public funds and tax evasion during the incredible creation of wealth that followed the liberalisation of the Russian economy.

Money laundering crimes whose products are exported abroad are also perpetrated in France. Money is laundered from drug trafficking by individuals or family networks, producing an annual turnover of around €600,000. The laundered money is used to acquire goods, often real estate, in the home countries of the criminals involved.

Types of money laundering

Money laundering is a shifting reality that constantly adapts itself to its circumstances. Very often, the police only detect new laundering schemes when they have already been used by criminals. Leaving to one side the instant or deferred consumption of dirty money that does not figure in the laundering process, these schemes can be divided into three categories:

► From the simple to the complex

Take the example of drug trafficking, which rests on a family-style organisational structure and invests its income in real estate and commercial goods through non-trading real estate companies, which provide the possibility to acquire and manage the real estate.

The police is initially alerted to the phenomenon when small businesses spring up in urban areas where there is no particular reason for them. Initially the trend was to open high-end sports accessory shops in disadvantaged areas; these were followed by “telephone centres” and finally by kebab style restaurants, set up of course using dirty money. The latter present the added advantage of being able to recycle business; their turnover may be high and it is difficult for the authorities to monitor the clientele.
In one instance the police even found a link between a restaurant of this sort and the financing of terrorism – customers were able to leave donations in a trunk in the restaurant and the money collected was then given to an association, which transferred it to a suspect wanted under an international arrest warrant for involvement in a terrorist attack.

There are also more complicated schemes that use dummy corporations and holding companies etc. An example of this is timeshare scams. In one case, French and Spanish victims bought non-existent apartments on a timeshare basis. The income from the scam was very high and was invested in a château in Normandy, after having passed through dummy accounts all around the world. An ordinary accidental fire meant that funds were transferred to finance repairs. These transfers caught the attention of the police, who launched an inquiry. Their investigations revealed that the château was used to launder the proceeds of criminal scams. The owner, a British man, was going to sell the château for 10 million Francs, having bought it in the 1990s for 2 million Francs. The capital gain would have been spectacular if the operation had succeeded.

➡️ From amateurs to professionals

The Normandy château scheme clearly required more than just money laundering skills and must have had professional assistance. Two lawyers were investigated, having constructed the entire legal structure for money laundering purposes. It should be emphasised that the recycling of funds of dubious origin is increasingly dealt with by professional money launderers who rent out their services to criminal organisations anxious to clean dirty money quickly.

The cases dealt with by the law have also put bankers into question. One inquiry revealed that certain French banks accepted cash deposits in metal pails. The money was then transferred abroad. The banks had even held anti-money laundering training sessions, which were proven ineffective due to human weakness.

The police also deal with insurance professionals. An inquiry was recently conducted following the murder of a broker in Africa who was working for a French insurance company. The inquiry revealed that he had made dubious investments for his one and only client, an African man well known to the local police.

Since banks have installed detection tools, part of the money laundering process has tended to proceed through parallel routes. Thus the money is entrusted to third parties who deposit it and give it back to the criminal on request. In the interim, it can be used to make high interest loans. Casinos are a favourite target for these criminal organisations because casino banks can use funds as they wish.

Alongside these professional outfits there are genuine amateurs. For example the proceeds of trafficking are placed in the criminal’s bank account, who then takes out an insurance policy. The inquiry is simple and the various elements involved are easy to trace.

➡️ International or local

Schemes may be international, using dummy corporations, or they may be restricted to a local level, mainly in the case of drug traffickers.

All money laundering operations rest on contradictory objectives:
- speed of execution, since criminals need their funds immediately,
- complexity of the operation in order to cover their tracks and prevent being traced,
- need for constant security for the people and entities involved in the laundering process.
These objectives give rise to elaborate schemes that appear to respect the law. For example, the creation of dummy corporations, conducting real business but used as a facade to mix commercial proceeds with dirty money; bogus companies (known as ghost companies in FATF terminology) with no actual business activities and whose sole objective is to provide the appearance of respectability and ensure anonymity. These companies are generally spread across several continents and are often located in regulatory havens.

Fraudulent use of documentary credit technology, for example, implies the mobilisation of several commercial companies to ship fictional merchandise, under the control of criminal organisations. This internationalisation of the money laundering process of course makes it very difficult to trace funds.

The trafficking of narcotics from Afghanistan provides a perfect illustration of an underground economy working on a worldwide scale: 6,000 tonnes of opium harvested every year facilitates the production of 1,200 tonnes of heroin, with a market value of US$ 195 billion. The distribution of the product and the laundering of this colossal sum imply a veritable and perfectly structured criminal engineering network, with global ramifications. The network uses the most diverse techniques possible: dummy corporations, electronic transfers, life insurance investments, fake bills, stock market investments, foreign currency transactions, and so on.

However, money laundering can also take place on a local level. Thus funds collected in cash by a trafficker from his numerous dealers will not be placed in a single bank account so as not to arouse suspicion; instead they will be spread across a number of accounts opened with several different banks under different names. These funds may then be invested in several different life insurance companies. There is no international network involved in this essentially local scheme, which was uncovered by police several years ago.

How can we combat money laundering?

The mobilisation of the international community and the implementation of legal means to combat money laundering go hand in hand with the reinforcement of the investigatory powers of the police, the improved coordination of legal services and the cooperation of financial institutions.

Cooperation of international police departments

The International Criminal Police Organisation (ICPO-INTERPOL), which has police representatives in 187 countries, is one of the largest international organisations in the world, after the United Nations. It is the global mainstay of police information exchange. Each member country maintains a National Central Bureau (NCB) which acts as a contact point between INTERPOL’s General Secretariat, based in Lyons, and all of the NCBs in other member states. The organization has made money laundering one of its priorities. It has recently developed the Millennium project which consists of an information-sharing system and a pooled database of over 125,000 known criminals. Alongside managing this operational file, INTERPOL updates all the qualitative data relating to the development of major international trafficking and, at the request of the legal authorities, issues international arrest warrants.

Created more recently, EUROPOL is a European law enforcement organization which represents the law enforcement authorities of the European Union Member States. Its mandate has been extended to cover money laundering. Its mission is to facilitate operations for combating crime within the EU by providing its expertise and technical support for police investigations carried out by the Member States and organizes the exchange of information between liaison officers seconded by the Member States to its head office in The Hague. There is close cooperation between INTERPOL and EUROPOL; however, it is worth clarifying that the latter is not the European sub-division of INTERPOL.

Many countries have a department specializing in financial crime and in particular money laundering. These departments generally aim to coordinate suppression on a national level, to analyse the information from local departments and to inform the government and the international organizations about the development of the situation.
Working with the private sector

Since the end of the 1980s, most States with money laundering legislation have instituted a system that obliges financial organisations to report to the authorities any transaction that may be concealing money laundering activity.

The fight against money laundering can therefore be described as the ringing of a line of successive alarm bells. The first is set off by the suspicious transaction report. The alarm is communicated to the Financial Intelligence Unit (FIU), which in turns rings a bell to warn the public prosecutor and then the specialised police department involved. If one of the bells fails, the job is not done. Relations with the private sector are therefore based on partnership.

They may also be based on implied involvement in a case. During investigations into criminal organisations the police conduct searches. If these searches reveal documents confirming the existence of an insurance policy, the insurer will be questioned in order to obtain more information on the investments made by the criminals and the conditions under which the contracts were concluded.

The system of partnership with the private sector has developed in a similar fashion in all those countries that have integrated FATF standards into their legislation. There are now around 106 Financial Intelligence Units around the world. They are in charge of collecting information regarding suspicious transactions.

The pressure of dirty money: why companies need to be vigilant

The objective of a criminal who approaches a bank or an insurance company

The criminal's objective is to invest his money, to make it clean and to be certain of recovering it. In the 1980s, Columbian drug traffickers had accumulated considerable quantities of dollars that remained idle. Money laundering was the only way to use these funds, by creating companies, opening bank accounts and buying real estate and insurance products.

The criminal's priority is to find a point of entry, and he is prepared to do anything to achieve this, including trickery, corruption, blackmail and threats. The challenge for finance professionals is to detect this kind of activity.

The authorities do not demand the impossible of finance professionals, what they need to do is identify anything out of the ordinary. Typically this involves a totally unknown, dream client who suddenly appears bearing considerable amounts of money.

For certain bank branches in France, for example, it is turnover that is at stake. In one instance, pressure from management to increase business was so great that a branch manager, seeking easy solutions for growth, ended up agreeing to deal with a Columbian drug trafficker who was recycling money from the trafficking of cocaine.

What are the risks involved for the company?

There are two kinds of risk involved: criminal and reputational. A criminal or police matter has the same effect as a rumour. We live in an information society. The reputational risk is very real and any failing immediately becomes common knowledge. Once the media machine has started moving, it ceases to be controllable. The company’s image plays a major role in its results. How can a financial operator maintain a decent image when it is likely to be implicated in a money laundering case? By proving he has made the necessary efforts towards detection. The police and the courts know how to distinguish an error made in good faith from a dishonest one.

On a penalty level, the professional who takes part in a money laundering operation by turning a blind eye to it risks indictment as the result of a chain of lapses: openness to organised crime, non-detection of a suspicious client, weakness when faced with a dream client who will bring a “plus” to the company's business, but who, if detected, risks a maximum penalty.

The pressure of dirty money is therefore very strong on all those who allow criminals to enter into the legal financial system. These criminals are very inventive and today's schemes are constantly changing; the mission of finance professionals is tricky but above all centres on common sense and reactivity. The authorities are not asking for the detection of money laundering or terrorist financing networks, which would be difficult to achieve, but simply that professionals notice anything out of the ordinary and set off a chain of reactions beginning with the reporting of any suspicions to the Financial Intelligence Unit.
Anti-money laundering procedures and their objectives

The International Association of Insurance Supervisors, which groups the representatives of the supervisory authorities of around 160 countries, has developed the core principles, based on the recommendations of the FATF, for developing the internal procedures of insurance companies. The supervisory authorities have become increasingly involved in ensuring the profession’s compliance with these procedures. This can be explained by the fact that this sector implemented its internal procedures later than in the banking sector.

In France, following the indictment of leaders of French financial institutions and the events of 11 September 2001, the French insurance supervisory authority ACAM, developed a series of specific actions for combating money laundering in the insurance sector. A report based on the examination of the procedures of a sample of life insurance and capitalisation companies revealed a number of breaches in their anti-money laundering systems, particularly compared to the banking sector. Since then, things have improved. Money laundering is now seen as an integral rather than isolated risk.

In the UK, the Financial Services Authority (FSA) has defined strict rules for financial institutions to encourage them to cooperate with the authorities.

In several countries of Latin America, the supervisory authorities required the insurance companies to implement anti-money laundering procedures before a set date, beyond which they could be penalised for non-cooperation.

Like the supervisory authorities of several States, the FSA has a duty to inform the law and the police when it detects irregularities in a financial establishment during an inspection.

“The FSA is working closely with the Police and other law enforcement agencies to fight money laundering. In this case (acting to stop the activities of an insurance broker suspected to have laundered £8 million) we have joined forces with the Police Service. All financial firms must play their part and follow the FSA’s rules on identifying, reporting and preventing money laundering. Where we identify shortcomings we will not hesitate to take appropriate action.”

Carol Sergeant, Managing Director at the FSA.

The aim of internal anti-money laundering procedures is to reduce exposure to the risk of money laundering. The creation and application of such procedures constitute added pressure. However, these procedures ensure the security of the company’s business activities, protect its image and that of its employees, and preserve its financial assets.

The sums managed by insurance companies are considerable: 75% of premiums earned are for life insurance, with the remainder scattered between P&C and the other branches. So life insurance is considered, by the majority of experts, to be the most vulnerable sector in terms of money laundering. P&C insurance is not safe from all risk, but it has proved to be less attractive to criminals. Life insurance is therefore the predominant sector involved in money laundering, nevertheless it does not have a monopoly on risk.


(5) ACAM: Autorité de Contrôle des Assurances et des Mutuelles (Supervisory Authority for Insurance Companies and Mutual Insurance Companies) – France (www.acam-france.fr)
Risk mapping

Anti-money laundering procedures depend on the capacity of a company to map its risks. There are three types of risk involved:

1. risk linked to the product itself,
2. risk inherent in client relationships,
3. risk linked to distribution networks.

These may be incorporated and represented in a risk assessment table. Their assessment therefore constitutes the framework of the anti-money laundering procedures, the objective of these being to anticipate this risk.

As insurers correctly repeat, along with bankers, they are not the police. Money laundering procedures represent obligations of due care for them. These professionals are obliged to implement certain facilities, but they have no obligation to produce results.

The procedures are based on regulatory obligations originating from the law, which itself is inspired by the FATF's recommendations. The existence of a procedure is evidence of the Anglo-Saxon influence, and combines notions of anti-money laundering procedures, internal monitoring and auditing.

The international FATF standards, contained within the framework of 40 recommendations drawn up in 1990 and updated notably in 2003 in a new version which integrates anti-terrorist financing, cover all the obligations of the financial sector.

The 15th recommendation obliges financial organisations to “perfect anti-money laundering and terrorist financing programmes”. Such programmes should include:

- policies, procedures and internal monitoring, including facilities to monitor compliance and appropriate procedures during the hiring of employees, in order to ensure that this is conducted according to demanding criteria,
- a continuing employee education programme,
- an internal monitoring facility to check the efficiency of the system.

Risks linked to the product

These risks relate to the vulnerability of the insurance contract to money laundering risks, for example relating to the nature and duration of the services offered, the possibility of repurchase, advance payments or cancellation, ease of capitalisation or adjustment in terms of cover. Anti-money laundering procedures should accurately reflect the characteristic differences between products and establish the measures necessary to best define the scope of the risks involved.

Risks inherent in client relationships

These risks relate to customer due diligence – “Know Your Customer” (KYC). This idea initially came from the banking sector, having been originally defined by the Basel Committee.

It has now been taken up by financial organisations, be they banks, investment or insurance companies.

When a financial operator is faced with an atypical risk or transaction, it must be able to react using a detailed study of the client’s profile. Based on this assessment, it should be able to understand all of the client’s transactions and report any suspicions as necessary.

(6) Cf. example of risk assessment table in appendix.

(7) The Basel Committee or “Basel Committee on Banking Supervision” is an institution created in 1974 by the central bank governors of the “Group of Ten” (G10) nations within the Bank of International Settlements in Basel. The committee meets 4 times per year and is currently composed of central bank and supervisory authority representatives from the following 13 countries: Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Spain, Sweden, Switzerland, the United Kingdom and the United States.

The missions of the Basel Committee are as follows:
+ to reinforce the security and reliability of the financial system,
+ to establish minimum prudential auditing standards,
+ to broadcast and promote the best banking and monitoring practices,
+ to promote international cooperation in terms of prudential standards.

Finally, the Committee serves as an informal forum for the exchange of information regarding developments in regulations and monitoring practices on a national level, as well as current events in the financial field.
The first component of the “Know Your Customer” principle relates to the client’s professional environment. An individual with few resources or a socio-professional profile that is unsuited to a large underwriting contract would be an initial warning factor. During an inspection which gave rise to disciplinary sanctions, it appeared that an insurance company was recording very large cash deposits in a very short space of time, by individuals in their early twenties with no known resources living in inner city areas. Knowledge of these clients could have prevented the company from accepting these underwriting contracts.

This issue of knowing the client is not unequivocal. Insurers develop in a competitive environment. Requesting a certain amount of information from a client regarding himself, his assets and even his tax situation, is likely to deter the client, but also his broker. A dichotomy is emerging between fully comprehensible competitive requirements and the requirements of the public authorities. This is undoubtedly one of the major difficulties involved: finding a proper balance between detailed and exhaustive knowledge of the client, commercial requirements and the respect of regulatory obligations.

Risk may also be geographical or geopolitical. It may relate to corporations, notably for certain legal structures that may be more exposed than other organisations.

### Risks inherent in distribution networks

A network of employees enables good risk management, since the people who make up the network apply the procedures prescribed by the company. The same is true of a network of agents. Conversely, relations with a network of brokers should be approached differently, based firstly on the principle that insurers and brokers are subject to the same duty of vigilance and to identical obligations of declaration, and secondly on the interpretation of the courts and the supervisory authorities with regard to their respective responsibilities.

The French insurance supervisory authority, along with the Banking Commission, consider brokers to be individually, publicly, disciplinarily and even criminally liable with regard to money laundering. The insurance company and the broker are two distinct legal parties, each with their own responsibilities. The jurisprudence of the courts has adopted an identical position: responsibility is not shared, which means that any failing on the part of the broker could impact the insurer. Brokers and insurers share a contractual relationship. In view of this, the supervisory authority wanted brokers to be subject to anti-money laundering procedures similar to those imposed on insurers, which is moreover in line with the law.

Beyond this, should insurers supervise brokers? The supervisory authority would tend to say yes, however without the prior consent of the two parties involved this seems difficult on both a practical and legal level.

In practice and in order to avoid any administrative and/or legal issues, it is highly advisable for brokers and insurers to work together transparently and to secure their commercial relationships through agreements, as they are encouraged to do by professional organisations. Under the terms of such agreements they will then commit to respecting anti-money laundering regulations.

These different risk criteria may be transposed into anti-money laundering procedures through a risk assessment table. This is in line with a very strong obligation of vigilance as well as a prevention policy from the insurance company or its broker. This duty of vigilance, which is restrictive and formalistic but essential, is based on complex legal texts that nevertheless allow financial operators a large degree of freedom in terms of organising their anti-money laundering facilities.
Professional recommendations serve stringent requirements

This freedom of organisation is an important prerogative. The supervisory authority transposed the discretion granted to insurers into the recommendations they published in 2005. In doing so, they established, for certain obligations, a level of requirement stretching beyond what is prescribed by the law. Nevertheless, each player is free with regard to the organisational structure it implements in order to meet such requirements. These recommendations notably underline the following points:

• drawing up and adopting written rules and procedures relating to contract marketing and client follow up;
• publishing these rules and procedures in paper format, if possible accompanied by an online version;
• computerised analysis of operations in order to better detect suspicious transactions and conduct regular reporting. Computer analysis should facilitate the monitoring of payments and reimbursements by amount, date, origin, destination and sums accumulated for any one client;
• establishing client ID files that include information on the knowledge of co-contractors;
• so-called atypical transactions or transactions involving large sums of money: the supervisory authority recommends heightened vigilance with regard to the following points: logistics of the transaction, the identity of the co-contractors (and a good knowledge of the latter), the origin and destination of the funds involved, the gathering of information on the financial establishments from which the funds came and to which they are going, and methods of payment used (bank cheques, transfers etc.).

Assessment and adoption of internal procedures

Procedures should be audited, assessed and corrected.

An internal anti-money laundering procedure is not a dormant document, but an operational, non-static support, which must permanently evolve and which takes account of new contracts, new partners and new regulatory obligations.

In summary, it is not a dormant document, but an active process that will evolve in tune with the company, its products and its structure.

First of all, in France, the supervisory authority, in the same way as the banking commission and the financial markets authority, assesses the procedures’ level of conformity with the regulations in force.

Have the procedures included all of the legal obligations imposed on the financial establishment – identity checks, knowledge of the client, position of anti-money laundering manager, relevance and quality of the suspicions reported, etc.?

Once the convergence between the procedures and the legal terms and conditions has been examined, the supervisory authority assesses the operational application of the internal procedures based on a sample selection of files.

For example, the authority does its best to assess the role, position and influence of the anti-money laundering officers, along with the way in which ID checks are conducted and the client profile is drawn up. The way in which the company applies the principle of determining the origin of funds is subject to in-depth checks.

The identification of the origin of funds is a very sensitive element of the relationship between the client and the insurer - when an investment advisor proposes a solution of several million euros to a very demanding client, anxious for discretion, the company may enter into a risk zone because the information necessary will be harder to obtain than for clients with a standard profile. This is the reality of the anti-money laundering field. The disciplinary sanctions imposed by the insurance supervisory authority but also by the banking commission, have to a large extent been related to the failure to determine the origin of funds by the insurance company or banking institution.

Supervision also extends to analysis of the product distribution network and to the impact of this network on the anti-money laundering facilities in place. The analysis of the network enables us to identify risk zones in which the company is situated according to whether it works with employees, brokers or banking partners.

The supervisory authority produces a report similar to that of an audit or inspection. We should point out here that the public authorities do not have a monopoly over this kind of supervision; the inspection, internal audit and risk management departments of companies also conduct regular audits on the application of their internal procedures.
Reporting a suspicion constitutes the concretisation of the partnership process between certain professionals and the authorities responsible for the fight against money laundering. The principle of reporting a suspicion, as recommended by the FATF, rests on the idea that the fight against this phenomenon will only be fully productive if the bodies leading the fight have access to certain financial information and transactions. Consequently, States must solicit the cooperation of certain financial players in the surveillance of criminal operations and transactions.

The receiving and use of reported suspicions is the responsibility of a Financial Intelligence Unit, a specialised department whose powers are fixed by the law of each country. Once we have presented the FIUs, we will deal with the notion of suspicion and the conditions under which a suspicion should be reported, along with the relevance criteria that such a report should observe in order to be useable.

Financial Intelligence Units: at the centre of the States’ anti-money laundering procedures

It may appear surprising that the 40 recommendations of the FATF in 1990 do not explicitly mention the FIUs; they simply recommend that suspicious transactions are reported to the “competent authorities” (without defining who these are) and specifies some of the tasks of the aforementioned authorities: receiving suspicious transaction reports, instructions to financial institutions, database management, international exchange, etc. Nevertheless several countries created the first FIUs at this time.

It was not until 2003 that the FATF, in its revised version of the 40 recommendations, mentioned for the first time the term FIU as the recipient of reported suspicions. The organisation was thus clearly inviting the States to create a specialised department at the centre of the national procedure for combating money laundering.

The Egmont Group gives us a definition of the FIU:

“A central, national agency responsible for receiving (and as permitted, requesting), analysing and disseminating to the competent authorities, disclosures of financial information:

1. concerning suspected proceeds of crime and potential financing of terrorism,
or
2. required by national legislation or regulation,
in order to combat money laundering and terrorism financing.”

In 1995, a group of FIUs meeting at the Egmont-Arenberg Palace in Brussels decided, in view of the benefits inherent in the development of a FIU network, to establish an informal group for the stimulation of international cooperation. Now known as the Egmont Group, these FIUs meet regularly to find ways to cooperate, especially with regard to information exchange, training, and the sharing of expertise.

The number of FIUs has been constantly increasing. Numbering around 40 at the beginning of the 1990s there are currently 106 such units and their means are constantly being strengthened. Thus, the workforce of TRACFIN, the French unit, has increased from 50 in 2005 to 70 today. In view of the development of methods used by money launderers and the increase in reports of suspicious activity, the technical resources provided to the FIUs, particularly in terms of database processing, are a lot more efficient.

This development demonstrates the political will of the States to step up their efforts with a view to combating money laundering and the financing of terrorism.
Although the FIUs follow the same objectives, they differ in certain respects in terms of their methods of creation and functioning. This is due to the specific characteristics of each State, its legal and administrative system, the type of financial crime, the budget allocated to each unit etc. There are thus 3 main categories of FIU:

**the administrative model**
This model is not under the control of the law enforcement or judicial authorities. It is generally placed under the supervision of a Ministry of Finance or the Central Bank. Its activity depends on the flow of intelligence that it receives and which it cannot take up itself. It acts as a “buffer” between the professionals subject to reporting obligations and the law enforcement authorities. The reporting institutions generally prefer to entrust their suspicions to this kind of FIU: indeed the dissemination of information to a law enforcement department may give the feeling that it is an accusation rather than a suspicion.

The administrative model, which is adopted by the majority of countries, has the advantage of taking away from the police departments the burden of selecting between the suspicion reports, in terms of those which can be used and those filed without consequences. The following countries have opted for the administrative-type FIU: Andorra, Australia, Belgium, Bulgaria, Canada, Colombia, France, Malta, Poland, Russia, Spain, Ukraine, USA, Venezuela.

**the law enforcement model**
The authorities use this model as it is a means of establishing a body without having to create a new entity, and the intelligence transmitted can be used quickly thanks to the investigative capacities and the databases of the police networks. Nevertheless, the reporting institutions may be reluctant to disclose information to law enforcement departments on transactions that are no more than suspicions. Examples of law enforcement FIUs include Austria, Germany, Hungary, Sweden, UK.

**the judicial model**
This type of FIU is generally established within the judicial branch of the country and often under the prosecutor’s jurisdiction. When suspicions are reported, the judiciary’s powers are immediately brought into play: seizing funds, conducting searches, interrogations. However, the reporting professionals may feel the same reserve as with the law enforcement departments when disclosing information with this type of unit. Examples of this model include Cyprus and Luxembourg.

Each FIU aims to carry out international activities through the institutional links existing with the FATF, the Egmont Group and foreign FIUs. TRACFIN, the French FIU, therefore has the authority to continue in France investigations begun by its foreign counterparts on their territory. Conversely, a money laundering case beginning in France, but with implications in the UK and Italy, could be updated thanks to TRACFIN’s cooperation with its two counterparts in these countries: “l’Ufficio Italiano dei Cambi/Servizio Antiriciclaggio” and the “National Criminal Intelligence Service/Financial Intelligence Division”.

---

### Basic FIU Concept

1. Reports and additional information upon request transmitted to FIU and Statement of Disclosure transmitted to Financial Institution.
2. FIU receives additional information from Law enforcement.
3. FIU receives information requests from Prosecutorial Authorities. After analysis disclosures are transmitted to Prosecutorial Authorities.
4. Possible exchange with foreign counterpart FIU.

*Source: Egmont Group.*

---
Reporting a suspicion to a Financial Intelligence Unit

Reporting a suspicion is an original obligation which differs from other legal obligations such as the obligation to notify the relevant authorities about a crime or an offence, for which it is possible to prevent or limit the effects, or the obligation to denounce the offender in the case of child abuse.

These denunciations are easy to formulate because they relate to crimes and offences which have already been committed, they are therefore easy to identify, whereas the suspicion is, by nature, subjective.

Some professionals subject to this system of reporting wrongly believed that the law required investigations similar to those carried out by the police, despite the fact that they do not have the same resources. This is precisely what concerned the professionals. Worried about the subjective notion of suspicion, they feared that the law was providing them with an obligation that is difficult to fulfil. In actual fact, the banker or insurer merely makes a simple report of suspicion, based on information in his possession, whereas the police have to establish the reality of a crime, taking into account the constituent elements.

British author Alastair N. Brown says the term “suspicion” includes the idea of “imagining something without evidence or on slender evidence”. He considers that, in the context of the obligation to report, “The term suspicion designates a state of mind in which we consider that there is a real possibility that the person is a criminal”\(^{(10)}\). To this definition may be added the IMF’s study on this subject, “The suspicion is the conclusion that a reporting institution comes to after having taken into account all the relevant factors”\(^{(11)}\).

The suspicion is formed from a combination of warning indicators set out in an internal procedure for insurance companies. Detecting a suspicious transaction (on which the report of suspicious activity is made) is only possible if the financial operator has sufficient knowledge of his client and the nature of the transaction being made, and if he is aware of the problem of money laundering. After analyzing the transaction, he must assess whether it appears to conceal suspicious activities.

Reports of suspicious activity made by professionals to the FIUs which are members of the Egmont Group have almost doubled over the last eight years. The distortions that exist between the figures can be explained by the obligation made by certain legislations to report not only suspicious transactions, but all cash transactions exceeding a certain threshold, as well as cross-border cash movements. This is an automatic reporting system, which is interesting for collecting information on the flow of cash\(^{(11)}\). In 2007, Belgium recorded 12,820 reports, Canada recorded over 17 million (of which 39,000 reports of suspicious activity), Chile recorded 3,778 (of which 419 reports of suspicious activity), Colombia recorded 8,390, Spain recorded 748,275 reports of cash movements and 2,783 reports of suspicious activity, the USA reported nearly 20 million including around 1 million reports of suspicious activity, France recorded 12,481 reports of suspicious activity, the UK recorded 220,484 and Singapore 7,621.

This financial vigilance requires the involvement of the company’s staff, who must be trained and regularly made aware, and is based on an internal procedure, the key points of which are indicated by national legislations, inspired by the FATF recommendations.

The Financial Intelligence Units expect reports of suspicious activity from financial operators to be clearly defined; unfortunately this is not always the case. All too often, the document involved is unusable because the description of the suspicion is vague or even non-existent. The law requires that financial operators disclose anything they find suspicious in a transaction, or in other words, those elements in a client profile, product or transaction that appear unclear or likely to be linked to a money laundering operation.

At the present time this covers drug trafficking, organised crime, corruption, financial fraud against the interests of the European Community and the financing of terrorism. What factors could arouse the suspicion that a transaction is linked to criminal activity?

---


\(^{(11)}\) Financial Intelligence Units: An Overview. International Monetary Fund.

\(^{(12)}\) In the USA, the financial institutions must report all cash transactions exceeding $ 10 000. Australia, Canada, Chile and Spain have implemented similar measures.
The following three case studies may be helpful in understanding the concept of suspicion:

- a life insurance contract for an elderly person who has been known to the company for a long time and with regard to whom there has never been anything suspicious. This person’s account suddenly shows several payments and withdrawals for very significant sums. The insurer notices that a close relative is behind this movement of funds. The absence of any financial justification and the fact that these transactions do not fit the client’s profile warrant a report of suspicion;

- in a second case where intersecting flows of capital appear between several companies in France and abroad, funds are moved into the accounts of two minors, then to the life insurance contract taken out by their father. The large amounts involved and the anomaly in the fact that a father’s insurance contract is being fed by the children’s accounts, justify a report of suspicion by the establishment;

- an individual with a badly-defined profession takes out a life insurance contract for €500,000. He makes an initial payment with several cheques from bank accounts in his name. Then, on several occasions, the premiums are paid by cheques or transfers from third parties. The insurance company, whose attention has been drawn by this abnormal method of payment, asks his client for explanations. As the explanations were not convincing, the insurance company makes a report of suspicious activity. The inquiry shows that the client was in fact a drug trafficker who, in order not to attract the attention of his bankers, split the dirty money received from selling drugs between various accounts in his name or in the names of third parties.

The analysis of some FIUs shows that money laundering from certain financial or economic crimes is difficult to demonstrate. Thus, the laundering of funds originating from the misuse of corporate assets or from transactions concealed behind a life insurance contract is a relatively common phenomenon and is, paradoxically, more difficult to detect than more episodic cases that rely on complex arrangements, where payments are made from exotic tax havens. In the latter case, there is actually a whole series of warning indicators involved, which is not always true of the first scenario.

Financial operators are not asked to investigate their clients, but to isolate any elements within the transaction itself that could justify suspicion. The right questions should therefore be asked before a suspicion is reported.

These questions must be asked at the right moment; all too often insurance professionals start wondering about a transaction once the funds have been paid out rather than at the underwriting stage. Take the example of a client who buys back his entire contract six years after taking it out. Although he has a modest professional and family background, he is able to produce significant funds without raising the slightest suspicion. It may not be entirely redundant to wonder about this six years down the line, but such doubts come too late as the statute of limitations may be invoked.

After two years of investigations, the customs and immigrations offices of the USA, the customs office on the Isle of Man and the Columbian security departments revealed a laundering process concerning 80 million dollars. Columbian drug traffickers had invested dirty money with insurance companies based mainly in the USA and on the Isle of Man, via brokers. The premiums were paid by electronic transfers and cheques from third parties from different countries. The contracts were then subject to early withdrawals or cancellations, leading to payments from the insurers to the traffickers’ accounts.

In this case there were many warning indicators: underwriting in the countries in which the underwriters were not resident, payments made by third parties, early repurchase, etc.

**Capstone Operation – Oct. 2000 to Dec. 2002**

- 250 insurance policies written for US$ 80 M
- Columbian drug traffickers
- Premiums paid from abroad
- Brokers
- Insurance companies
  - USA
  - Isle of Man
  - Other countries
- Repeated early withdrawals
- Beneficiaries CARTELS
We should always remember the purpose of a report of suspicion. There is no point in reporting something as suspicious simply as a protective measure. Certain insurance companies make large numbers of suspicion reports, however these are practically empty and unusable. The analysis should relate to elements contained in the file, bearing in mind that these elements do not always justify a report of suspicion. The semi-systematic reporting of suspicions should be avoided. This is not always easy for insurers dealing with intermediaries, notably brokers, who constitute a screen between the company and the client. Things are different in the banking sector, where professionals may have direct knowledge of their clients.

It should be noted that the bancassurance sector has developed significantly. A banking group’s insurance entity may thus benefit from the banking sector’s good knowledge of its client. An atypical transaction cannot be analysed without taking into account the nature and economic environment of the client.

Many financial operators frequently complain about the fact that it is not possible to access police files when analysing certain cases. Such access is, of course, impossible in France, as in other countries, for reasons linked to data protection and the confidential nature of legal inquiries.

The third European directive which was supposed to be implemented by 15 December 2007 has been delayed in several countries. Finally, this text will not be transposed in all member states until the first half of 2009. Some States, like France, took advantage of this transposition to re-examine their anti-money laundering regulations and make them clearer. It is likely, therefore, that this new text will provide a real increase in the number of reports of suspicious activity due to the expansion of the scope of obligations of vigilance and the reporting of serious offences. That is, according to the directive, “all offences punishable by a penalty involving deprivation of liberty of at least one year”. This clearly covers hundreds of crimes and offences. The text marks a real turning point in the fight against organised crime. The obligations that it prescribes, based on the FATF’s recommendations, should be implemented by the countries of the Organisation for Economic Co-operation and Development (OECD) in the medium term.

Indicators of suspicious activity (non-exhaustive list)\(^{13}\):

- ✔ a potential client wishes to take out a contract far away from his zone of residence, even though he could find the same product at home,
- ✔ client contact made by an agent/intermediary in a country with no or insufficient anti-money laundering legislation, or where organised crime and corruption are widespread,
- ✔ the client is asked to provide additional information or is late in providing the information required to complete checks,
- ✔ unusual advance payment of insurance premiums,
- ✔ client accepts highly unfavourable conditions that do not correspond to his health or age,
- ✔ collateral payment emanating from abroad,
- ✔ single premium or first premium payment made from a bank located abroad,
- ✔ the premium amount does not correspond to the client’s apparent situation,
- ✔ the client requests a product with no financial justification and is reluctant to explain the reasons for his choice,
- ✔ transaction involving an unidentified third party,
- ✔ whilst the contract is in force, the beneficiary is replaced by a person with no connection to the underwriter,
- ✔ an abnormally high payment is made on a file where the underwriter is used to paying out small sums on a regular basis,
- ✔ the client tries to use a third party cheque at the time of underwriting,
- ✔ the client seems more concerned by his right to cancel the policy quickly than by the profitability of his investment,
- ✔ the client wishes to make a very large payment by electronic transfer or in a foreign currency,
- ✔ the client makes a large payment at the time of underwriting and, shortly thereafter, cancels the contract and asks that the reimbursement be made to a third party.

---

\(^{13}\) Source: International Association of Insurance Supervisors, Guidance paper on anti-money laundering and combating the financing of terrorism – 2004.
We may wonder if there is actually any risk of exposure to money laundering for the reinsurer, since everything is working together to keep it away from suspicious transactions: is it not protected early on in the process by the vigilance of the insurer and even that of the banker?

Due to the considerable volume of capital looking for ways to be recycled and the ingenuity of criminals, this risk must nonetheless be taken into account. The 2004/2005 FATF report on the vulnerability of the insurance sector underlines the fact that reinsurance is not immune from dirty money.

The “Guidance paper on anti-money laundering and combating the financing of terrorism” published by the International Association of Insurance Supervisors (IAIS) in 2004 makes a number of recommendations to reinsurers.

Situation of reinsurance with regard to anti-money laundering conformity rules

Unlike insurers who are subject to a relatively uniform regulatory process – implementation of a procedure, appointment of an anti-money laundering officer, training of personnel – the reinsurance regime appears to differ widely in terms of financial vigilance obligations. In some countries reinsurers are subject to the same obligations as insurers (Colombia, Australia, Morocco), whilst in others they are ignored by local legislation (Germany, Spain, Switzerland). In France, reinsurers must report to the Public Prosecutor any “operations of which they are aware involving sums of money they know to emanate from organised criminal activity”. The lack of standardisation in reinsurance regulations may be due to the lack of legal connections between insured and reinsurers, because the latter is actually insuring the insurers’ assets and is therefore not in a position to know all the details of what was originally underwritten.

Nonetheless, whatever the legal situation may be (i.e. detailed laws or legal vacuum), the legal authorities would have good reason to investigate a suspicious transaction with an insurance company, regardless of whether or not the reinsurer is aware of the fraudulent nature of the transaction. The reinsurer could be held liable on the basis of complicity.

Vigilance rules adapted to risk

The vigilance of a reinsurer may only be defined and exercised in relation to the information that its business allows it to know, which excludes all the contracts underwritten in its cedants’ portfolios that it does not see individually. On the other hand the reinsurer should know its client, i.e. the insurer, and the facultative business that the latter may propose. The reinsurer also has visibility regarding the financial exchanges made with its cedant.

Knowledge of the client

The “know your customer” principle may be transposed to reinsurance. Before embarking on a business relationship with a cedant, the reinsurer must not only verify the cedant’s commercial reputation and financial strength, but must also be aware of its governing bodies and gather, if necessary, information on its controlling entities and, of course, ensure that it has obtained the approval of the supervisory authorities. The reinsurer should also assess whether the cedant has properly implemented the legal vigilance obligations insofar as the cedant is located in a country where FATF standards have been transposed into the internal legislation. This recommendation is clearly stated by the above-mentioned IAIS. The level of vigilance will be higher with regard to companies located in countries lacking in supervision.
The FATF mentions the existence of purely fictitious insurance companies, constituted for money-laundering purposes. For its part, INTERPOL reports the case of a criminal group taking control of an insurance company. This same group goes on to acquire a maritime company with a fleet flying flags of convenience. The ships, acquired with dirty money, are assessed by the insurance company and significantly overvalued. These ships unfortunately sink on the other side of the world and the ship owner, who can prove that he paid his insurance premiums, is reimbursed14.

The author of the above-mentioned report does not specify whether the insurance company was covered by a reinsurance treaty. If this were the case, the reinsurer would certainly have been incriminated as the co-perpetrator of a serious money laundering offence. This case involves P&C insurance, but similar scenarios may be created in life insurance.

Knowledge of facultatives

The reinsurer can and should inspect the facultative contracts proposed by cedants. The underwriting file should enable the reinsurer to grasp the legitimate objective, financial justification and details of the matter if it is a complex transaction. If the underwritten contract is in any way abnormal, the reinsurer should exchange information with the insurer, who may then sue the client in order to remove any ambiguity.

Sometimes the information provided by cedants does not allow the reinsurer to form an opinion, due to the imprecise identity of the client, vague business activity, unclearly documented revenue and a complex financial structure. If the file continues to produce obscure or doubtful elements, the reinsurer will decide, along with its cedant, how to proceed with the contract request and will assess whether or not to make a suspicious transaction report, in accordance with local legislation.

Checking the flow of funds

As a general rule, the flow of incoming and outgoing payments between the reinsurer and its clients should correspond to perfectly identifiable commercial transactions and should be duly validated in accordance with the company’s internal procedures. Certain movements of funds may actually contain clues indicating an abnormal transaction, such as for example a payment over and above the premium amount due, followed by a request that the overpayment be reimbursed. Alternative Risk Transfer also provides opportunities for creating money laundering schemes. However, the risks attached to financial transactions will be reduced all the more if the reinsurer has applied the principles of vigilance (which enable him to know his client well) at the very beginning of the business relationship.
Money laundering has many faces. It may cross borders through highly elaborate schemes, or it may be more rudimentary and restricted to a smaller area. Whatever the case may be, the objective is to develop and maintain criminal activity that can sap companies and inflict considerable damage on their image. The problems encountered by the international community and national authorities in tackling money laundering have led them to solicit the cooperation of private partners. The system depends on the cooperation of financial operators and other concerned professionals. These entities should tailor their organisational structure accordingly and mobilise their human resources departments.

In order to protect itself from money laundering and take an active role in the fight against this scourge, SCOR Global Life has internal procedures tailored to its reinsurance activities and raises the awareness of its employees through dedicated training courses. The company intends to protect itself, but above all it wishes to provide assistance to its clients in this field, through the following:

- staff training,
- advice on the creation and implementation of anti-money laundering procedures,
- advice on underwriting,
- involvement in claims monitoring.

One of the main roles of a reinsurer is to keep its clients informed of major developments in terms of risk selection. This obligation should extend to the new risk constituted by money laundering.

For more detailed information or for assistance with regard to the implementation of your internal anti-money laundering procedures, please do not hesitate to get in touch with your usual SCOR Global Life contact.
### RISK ASSESSMENT TABLE

<table>
<thead>
<tr>
<th>N°</th>
<th>Risk indicator</th>
<th>Risk assessment (1 to 4)</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>1. EXPOSURE TO PRODUCT RISK</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td><strong>Investment growth bonds</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>Bearer bonds</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>Anonymous investment growth bonds</td>
<td>3.5</td>
<td></td>
</tr>
<tr>
<td>1.2</td>
<td><strong>Pure protection products</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2</td>
<td>Temporary insurance</td>
<td>0.5</td>
<td></td>
</tr>
<tr>
<td>1.2</td>
<td>Whole life insurance</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1.2</td>
<td>Deferred capital whole life insurance</td>
<td>0.5</td>
<td></td>
</tr>
<tr>
<td>1.3</td>
<td><strong>Life insurance</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.3</td>
<td>Insurance such as unit-linked savings</td>
<td>3.5</td>
<td></td>
</tr>
<tr>
<td>1.3</td>
<td>Insurance such as euro savings</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>1.3</td>
<td>Insurance with deferred capital</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>1.4</td>
<td><strong>Retirement insurance</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.4</td>
<td>Life annuity</td>
<td>1.5</td>
<td></td>
</tr>
<tr>
<td>1.4</td>
<td>Collective individual retirement savings schemes(*)</td>
<td>0.5</td>
<td></td>
</tr>
<tr>
<td>1.5</td>
<td><strong>Geographical risk</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.5</td>
<td>Extended blacklist</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>1.5</td>
<td>Off-shore centres</td>
<td>3.5</td>
<td></td>
</tr>
<tr>
<td>1.5</td>
<td>Countries with exposure to organised crime</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>1.5</td>
<td>Highly-corrupt countries (TI's top 20)</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>1.5</td>
<td>Sensitive regions</td>
<td>3.5</td>
<td></td>
</tr>
<tr>
<td>1.5</td>
<td>Other FATF-regulated countries (such as EU)</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td><strong>2. EXPOSURE RISKS INHERENT IN CLIENT RELATIONSHIPS</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td><strong>The client's professional environment</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td>Hierarchical position: weight 1, 2 or 4 (employee, manager, director)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td>Liquidity risk</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td>Regulated liquidity risk</td>
<td>3.5</td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td>Investment consulting</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td>Sectors sensitive to corruption</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>2.2</td>
<td><strong>Corporations</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2</td>
<td>Dummy corporations</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>2.2</td>
<td>Limited liability company under sole ownership/non-trading real estate company/ economic interest group</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>2.2</td>
<td>Clients who are likely to be mistreated</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

(*) Without repurchase clause, non-transferable, and without using as guarantee.
### 3. RISKS LINKED TO DISTRIBUTION NETWORKS

#### 3.1. Employee network

<table>
<thead>
<tr>
<th>Risk</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insurance company in difficulty</td>
<td>2.5</td>
</tr>
<tr>
<td>High-risk location</td>
<td>2.5</td>
</tr>
<tr>
<td>No culture of values: ethics/integrity</td>
<td>2</td>
</tr>
<tr>
<td>High turnover amongst business development staff</td>
<td>2</td>
</tr>
<tr>
<td>High turnover of managers and directors</td>
<td>3.5</td>
</tr>
<tr>
<td>Recent takeover/merger</td>
<td>3</td>
</tr>
<tr>
<td>Different subsidiary/market segment</td>
<td>2.5</td>
</tr>
<tr>
<td>No synergies/sharing between services</td>
<td>3</td>
</tr>
<tr>
<td>Client portfolio linked to one business developer</td>
<td>3</td>
</tr>
<tr>
<td>Abnormal increase in business developer's client portfolio</td>
<td>3.5</td>
</tr>
<tr>
<td>Production linked to one administrator</td>
<td>2.5</td>
</tr>
<tr>
<td>Absence of an integrated IT system</td>
<td>2.5</td>
</tr>
<tr>
<td>Absence of one training session per year</td>
<td>3.5</td>
</tr>
</tbody>
</table>

#### 3.2. Agent network

<table>
<thead>
<tr>
<th>Risk</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Absence of supervision of agent's contracts (once a year)</td>
<td>3</td>
</tr>
<tr>
<td>Contracts with similar addresses to those of the agency</td>
<td>3</td>
</tr>
<tr>
<td>Production abnormally high per client</td>
<td>2.5</td>
</tr>
<tr>
<td>High-risk location</td>
<td>3</td>
</tr>
<tr>
<td>Staff = one agent</td>
<td>2.5</td>
</tr>
<tr>
<td>Client portfolio linked to one business developer</td>
<td>3</td>
</tr>
<tr>
<td>Seniority of agent under 5 years</td>
<td>2.5</td>
</tr>
<tr>
<td>Less than one visit per year for awareness</td>
<td>4</td>
</tr>
<tr>
<td>More than 3 partners</td>
<td>1.5</td>
</tr>
</tbody>
</table>

#### 3.3. Broker network

<table>
<thead>
<tr>
<th>Risk</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small structures (staff less than 5 people)</td>
<td>2</td>
</tr>
<tr>
<td>High-risk location</td>
<td>3.5</td>
</tr>
<tr>
<td>High contributions per business developer per year</td>
<td>4</td>
</tr>
<tr>
<td>Client portfolio linked to one business developer</td>
<td>3.5</td>
</tr>
<tr>
<td>More than 3 partners</td>
<td>2</td>
</tr>
<tr>
<td>Number of contacts with business inspector less than 5/year</td>
<td>2.5</td>
</tr>
<tr>
<td>Less than one visit per year for awareness</td>
<td>4</td>
</tr>
<tr>
<td>Production abnormally high per client and per office</td>
<td>3</td>
</tr>
<tr>
<td>Contracts with similar addresses to those of the agency</td>
<td>3</td>
</tr>
</tbody>
</table>

### TOTAL SCORE

Main points of the anti-money laundering procedure recommended by the FATF to financial operators including insurers

Implementing an in-house procedure
This must reflect the strategy for preventing money laundering and the financing of terrorism implemented by the company with relation to:
- risk linked to the product;
- risk inherent in client relationships;
- risk linked to distribution networks.

The procedure must be operational in nature and should simply describe the actions and reactions to be implemented depending on the information found in the underwriting file. Its purpose is to make use of the different combinations of warning indicators in order to come to a conclusion (geographical criteria, sum of money and economic purpose of transaction, currencies used, etc.).

This procedure shall prescribe the following:
- identification of the client or beneficiary (corporation or natural person) and a good knowledge of them;
- documented analysis of complex, abnormal or atypical transactions;
- conservation of all transactions underwritten for a period prescribed by the law (5 or 10 years);
- management of reports of suspicious activity.

The procedure must specify under which conditions the report of suspicious activity has been established: methods used to circulate information, authorized persons who finally decide what action should be taken regarding the risk underwritten, as well as grounds to make a report of suspicious activity, name of the person in charge of anti-money laundering who completes the report of suspicious activity and contacts the financial intelligence unit.

Appointing a person in charge of anti-money laundering
The person's position in the company's organisation can vary: anti-fraud department, audit department or legal departments. He should be:
- trained so that he is recognised as competent by the sales teams;
- informed about the development of money laundering problems, as well as changes taking place in legislation;
- integrated into the company's information system so that he is able to make a decision about suspicious items of business.

Training personnel
Analysing risks underwritten and detecting suspicious items of business cannot be solely carried out by the person in charge of anti-money laundering. This work requires the participation and involvement of all departments. It is therefore important that all staff who take part in risk analysis receive basic training in the problem of money laundering.

Checking the application of prescribed measures
This measure has been provided for by the FATF recommendation no. 19. It should be implemented as follows:
- an annual report by the person in charge of anti-money laundering,
- periodical audits,
- updating of procedures to make sure they are actually effective.

Countries signing the FATF recommendations undertook to integrate four main principles in their national legislation
- Financial operators act as crucial players in the State-controlled system preventing money-laundering
- Financial operators are released from banking secrecy
- Co-operation of financial operators implies that they know their clients well and the nature of their transactions
- They are under obligation to notify the relevant State-controlled financial entities of any suspicious transactions. This is a confidential statement, and no legal action can be taken against the author of such a statement
The risk of money laundering: Prevention, challenges, outlook