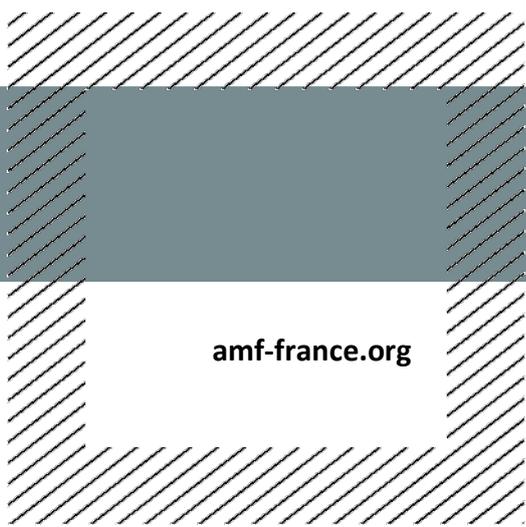


DECEMBER 2019  
**SECTOR RISK ASSESSMENT ON  
MONEY LAUNDERING AND  
TERRORIST FINANCING**



[amf-france.org](http://amf-france.org)

## Table of Contents

1.	Sector risk ASSESSMENT objectives and methodology .....	3
1.1.	The demand for a better understanding of money laundering and terrorist financing risks .....	3
1.2.	Sources used .....	3
1.3.	Methodology .....	4
2.	Regulatory and institutional framework of the financial services sector.....	5
2.1.	Regulatory framework: the European directives.....	5
2.2.	Institutional framework: AMF and ACPR shared supervision.....	6
3.	Main threats weighing on the financial services sector .....	7
3.1.	Threats identified on the national level.....	7
3.2.	Threats identified on the European level.....	8
4.	The asset management sector.....	10
4.1.	Overview .....	10
4.2.	Collective management of financial instruments (listed equities, listed bonds and money market instruments) .....	11
4.3.	Private equity .....	13
4.4.	Real estate investment.....	15
4.5.	Discretionary management.....	17
5.	Financial Investment Advisors (FIA):.....	19
6.	CROWDFUNDING INVESTMENT ADVISORS (CIAs).....	22
7.	The Central Securities Depository and securities settlement system manager: Euroclear	24
8.	Crypto-assets or "digital assets" .....	27
8.1.	DASPs.....	27
8.2.	Token issuers (ICOs) .....	30
9.	Recap of the ratings .....	33

## 1. SECTOR RISK ASSESSMENT OBJECTIVES AND METHODOLOGY

### 1.1. THE DEMAND FOR A BETTER UNDERSTANDING OF MONEY LAUNDERING AND TERRORIST FINANCING RISKS

The first FATF<sup>1</sup> recommendation requires that states identify, assess and understand the money laundering and terrorist financing risks to which they are exposed. This recommendation was replicated at the European level by the fourth anti-money laundering directive<sup>2</sup> and the task was entrusted to the Steering Committee on the Fight against Money Laundering and Terrorist Financing ("**COLB**").<sup>3</sup>

The COLB published its National Risk Assessment (hereinafter "**NRA**") on 21 September 2019.

In its capacity as competent national authority for the supervision of part of the financial sector, the AMF is also required to contribute to this objective of a better understanding of the money laundering and terrorist financing risks to which the entities under its supervision are exposed.

The present sector risk assessment ("**SRA**") contributes to this, by sharing with the financial sector an overview of the conditions of materialisation of these various risks, their level, and the objectives to be pursued in each sector and sub-sector.

The purpose of this sector risk assessment is therefore:

- Upstream, to define and enrich for the future the deliberations conducted on the national level, in the COLB;
- Downstream, to assist the entities under AMF supervision which may assimilate it in order to better deploy it, in light of their field of activity and their business model, in their procedures and internal documents.

Finally, this SRA should also serve as a tool for the AMF to enable it to implement the risk-based approach on which its monitoring and inspection activities are based, in accordance with the requirements stipulated by the fourth directive<sup>4</sup> and the guidelines regarding risk-based supervision<sup>5</sup> with which the AMF complies.

This document constitutes a guide, but does not replace the more detailed assessments conducted by the AML/CFT obliged entities. The general assessments concerning a sub-sector do not prevent distinguishing between different risk levels when the assessments are conducted on a more detailed level (e.g., at the level of an operator or a product). This document endeavours to include the factors to be considered for this purpose.

The entities under supervision may usefully refer to the NRA, but also to the sector risk assessment by the ACPR.<sup>6</sup>

### 1.2. SOURCES USED

To carry out this risk assessment, the AMF based its work on:

- The data collected in August 2019 in reply to the questionnaire on anti-money laundering and combating the financing of terrorism sent to portfolio asset management companies;
- The annual AML/CFT internal control reports of portfolio asset management companies as at 31 October 2019;

<sup>1</sup> International standards on anti-money laundering and combating the financing of terrorism and proliferation, available on the [FATF website](#).

<sup>2</sup> Article 7 of Directive (EU) 2015/849 of 20 May 2015.

<sup>3</sup> Articles D. 561-51 et seq. of the Monetary and Financial Code.

<sup>4</sup> Article 48 of Directive (EU) 2015/849 of 20 May 2015.

<sup>5</sup> Joint Guidelines on the characteristics of a risk-based approach to anti-money laundering and terrorist financing supervision, and the steps to be taken when conducting supervision on a risk-sensitive basis. ESAs 2016 72 [here](#).

<sup>6</sup> Sector risk assessment on money laundering and terrorist financing in France, published by the ACPR on 18 December 2019, [here](#)

- The data contained in the Annual Fact Sheets sent to the AMF by portfolio asset management companies in May 2019;
- Data from the Annual Fact Sheets of FIAs;
- Data from the Annual Fact Sheets of CIAs;
- The results of inspections on documents and on-site.

The AMF also took into account the reports published by TRACFIN, and in particular the report on Money laundering and terrorist financing risk trends and assessment, 2017-2018, and the 2018 annual report.

This SRA of course takes into account the supranational risk assessment produced by the European Commission<sup>7</sup> and the opinion of the joint committee of the European Supervisory Authorities on risks affecting the European Union's financial sector.<sup>8</sup>

### 1.3. METHODOLOGY

The threats and vulnerabilities were objectively established by means of criteria in accordance with the FATF methodology which consists in combining both threats and vulnerabilities.

- The money laundering and terrorist financing threats are activities which could result in money laundering or terrorist financing offences, whether on the national level or cross-border;
- The vulnerabilities make it possible to identify the areas, systems, factors and specific features of each sector or product which could result in misappropriations for purposes of money laundering or terrorist financing.

The **assessment of threats** was produced based on the quantitative data available (size of the sector, number of reports) and a qualitative analysis of the ML/TF scenarios identified by the AMF or by TRACFIN. Based on this analysis, **the exposure of each product or sector to the threat** was assigned a **score on one of three levels** (low, moderate or high exposure).

**Vulnerabilities** were also evaluated by a quantitative and qualitative assessment designed to assess, for each product, service or transaction, how its intrinsic characteristics could make it vulnerable to the ML or TF threat. Examples of factors of vulnerability are:

- Potential for anonymity offered by the product or sector;
- Potential for opacification of the transaction;
- The cross-border aspect;
- Speed or complexity of the product; and
- Sensitivity to documentary fraud.

Where applicable, measures taken to attenuate these "gross" vulnerabilities lead to selection of the residual vulnerability level represented by each product, service or transaction. The AML/CFT regulations, other relevant regulations, the action of the regulator and marketplace good practice rules are all measures liable to attenuate the identified vulnerabilities.

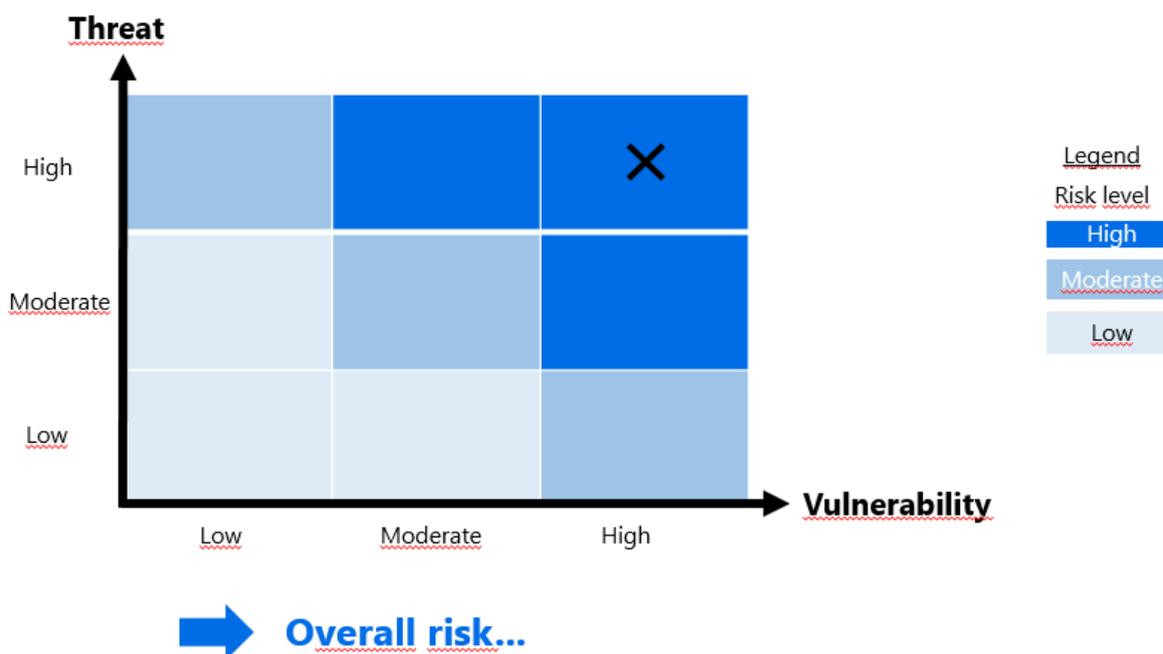
The combination of these threats and vulnerabilities made it possible to identify the risk level associated with each sector or product, in the form of a coloured matrix:

---

<sup>7</sup> Report of the Commission to the European Parliament and the Council on the assessment of money laundering and terrorist financing risks weighing on the internal market and related to cross-border operations, 24 July 2019, COM(2019) 370

<sup>8</sup> Joint opinion of the European Supervisory Authorities on money laundering and terrorist financing risks affecting the European financial sector, 4 October 2019, JC2019 59, available [here](#).

## XY Product Sector



The identification of a risk level for the identified sectors or products does not mean that all the professionals involved are liable to commit money laundering or terrorist financing offences. Quite the contrary, they are the first to work to ensure that their industry is most exemplary and most immune to such offences. The present assessment will enhance knowledge of the risks so that risk vigilance may be performed as effectively as possible.

## 2. REGULATORY AND INSTITUTIONAL FRAMEWORK OF THE FINANCIAL SERVICES SECTOR

### 2.1. REGULATORY FRAMEWORK: THE EUROPEAN DIRECTIVES

France has taken part actively in establishing European AML/CFT legislation. The fourth directive was transposed into French national law by Order No. 2016-1635 of 1 December 2016,<sup>9</sup> by Decree No. 2017-1094 of 12 June 2017,<sup>10</sup> and by Decree No. 2018-284 of 18 April 2018.<sup>11</sup>

The fifth directive (2018),<sup>12</sup> revising the fourth directive, is likewise the result of an initiative promoted by France, in order to reinforce the effectiveness of European measures for combating money laundering and terrorist financing in the wake of the 2015 terrorist attacks. During the negotiations, France supported **more stringent obligations of transparency relating to the register of ultimate beneficial owners** and the creation in all the Member States of a **file of bank accounts** making it possible to identify their owners, trustees and ultimate beneficial owners. Moreover, the fifth directive **includes the sector of digital assets in the scope of AML/CFT obliged entities** and reinforces **the additional vigilance measures taken by the obliged entities with regard to high-risk third countries**.

<sup>9</sup> Order No. 2016-1635 of 1 December 2016 reinforcing the French measures for combating money laundering and terrorist financing.

<sup>10</sup> Decree No. 2017-1094 of 12 June 2017 relating to the register of ultimate beneficial owners of corporate bodies and legal structures.

<sup>11</sup> Decree No. 2018-284 of 18 April 2018 reinforcing the French measures for combating money laundering and terrorist financing.

<sup>12</sup> Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 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 Directives 2009/138/EC and 2013/36/EU.

It came into force on 10 July 2018 and stipulates a period of eighteen months for transposition, i.e. up to 10 January 2020.

The process of transposition of the fifth directive is accordingly undergoing finalisation in France, and several of these measures enacted on the European level are already in force in France. The "**PACTE**"<sup>13</sup> Act No. 2019-486 of 22 May 2019 has already transposed its provisions relating to digital assets and authorised the government to adopt an order transposing the remainder of its provisions into national law.

Under these provisions, substantial precise obligations, described in detail in Chapters I and II of Title VI of the Monetary and Financial Code, are imposed on AML/CFT obliged entities, to be able to prevent ML/TF risks. The main such obligations concern, in particular:

- Vigilance with respect to clients, whose identity must be collected and verified, and with respect to the ultimate beneficial owner;
- The application of more stringent additional vigilance measures to the client and beneficial owner in the case of heightened risk factors (high-risk countries, establishment of a relationship at a distance, Politically Exposed Persons, etc.);
- The obligation to transmit suspicion reports to TRACFIN, in order to report any suspicious transaction, failing which their liability may be involved;
- The obligation of implementing and complying with UN, European and national asset freezes;
- Document retention;
- The establishment of a robust internal control organisation and procedures capable of combating money laundering and terrorist financing.

The AML/CFT obligations are adjusted according to the transaction risk. More stringent vigilance obligations must therefore be applied when the risk is considered high by either the legislator or the obliged entity following its risk assessment. Conversely, simplified vigilance measures are permitted when the risk is considered low by either the obliged entity itself or the legislator.

The AMF has replicated the relevant provisions in its General Regulation in order to clarify for asset management companies,<sup>14</sup> the central depository,<sup>15</sup> financial investment advisors,<sup>16</sup> and crowdfunding investment advisors<sup>17</sup> the obligations incumbent on them.

The AMF and ACPR supervise the effective compliance, by the obliged professionals, with all the obligations to which they are subjected, and contribute jointly, through their expertise, to reducing these risks.

## 2.2. INSTITUTIONAL FRAMEWORK: AMF AND ACPR SHARED SUPERVISION

Entities belonging to the financial sector are subject to the control and power of sanction of the Autorité de Contrôle Prudentiel et de Résolution (ACPR) and the Autorité des Marchés Financiers (AMF). The following come under the AML/CFT supervision of the AMF:

- The 633 asset management companies;
- The 5152 financial investment advisors;
- The 51 crowdfunding investment advisors;
- The Euroclear Central Depository.

The following also come under the AML/CFT supervision of the AMF:

- Digital service providers having applied for an optional authorisation for services of exchange of digital assets for other digital assets (broking), operation of a digital-asset trading platform (stock

<sup>13</sup> French Act No. 2019-486 of 22 May 2019 on business growth and transformation.

<sup>14</sup> Articles 320-14 et seq., and 321-141 et seq.

<sup>15</sup> Article 560-9 et seq.

<sup>16</sup> Article 321-143 to 321-148 and 321-150 in accordance with Article 325-22.

<sup>17</sup> Article 321-143 to 321-148 and 321-150 in accordance with Article 325-62.

exchange) and other digital-asset services, inspired by the investment services regulated by the European Union's Markets in Financial Instruments Directive ("MiFID"), such as the receipt and transmission of third-party orders, third-party portfolio management, advice to investors in digital assets, underwriting, guaranteed placement and non-guaranteed placement (these services are not highly developed as yet);

- Digital token issuers if the issue has received the AMF's approval.

The AMF checks the effectiveness of implementation of the AML/CFT preventive rules by the professionals under its supervision through constant supervision, ahead of the launch of their business (authorisation procedure, integrity check on the managers and shareholders) and throughout their business operations (follow-up). Its supervision activity follows the risk-based approach in accordance with the Joint Guidelines of the European Supervisory Authorities published in 2017.<sup>18</sup>

The other professionals in the financial sector (credit institutions, investment firms, market undertakings, intermediaries in banking transactions and payment services, crowdfunding intermediaries and service providers for the third-party custody of digital assets and buying and selling of digital assets against legal tender, subject to mandatory registration) come under AML/CFT supervision by the ACPR.

### 3. MAIN THREATS WEIGHING ON THE FINANCIAL SERVICES SECTOR

#### 3.1. THREATS IDENTIFIED ON THE NATIONAL LEVEL

As indicated by the COLB in the National Risk Assessment, tax evasion and scams are among the main threats to which France is exposed.

The AMF plays its role in combating these threats via (i) surveillance of marketing practices for so-called atypical products when they are carried out by financial investment advisors under its supervision, and (ii) initiatives to alert or warn against identified sites or persons via its website.

##### Marketing of atypical products by Financial Investment Advisors

The inspections carried out on FIAs revealed scams concerning the following atypical products: hotel products, forests,<sup>19</sup> and even balsamic vinegar.

Through collaboration with Banque de France, the AMF has established an increasingly precise map of atypical products in France, characterised by:

- promises of high returns often combined with guarantee mechanisms or liquidity promises which are inconsistent with the nature of the investment vehicle (e.g. unlisted equities or partnership shares);
- atypical underlying assets in the case of mass-marketed products (see below: teak forests, hotels);
- atypical structures (e.g. investments in equity securities issued by organisations of a different nationality from that of the underlyings);
- final destination of the funds not easily identifiable, or even impenetrable;
- financial arrangements promising tax breaks.<sup>20</sup>

Through its activity of supervision of FIAs, the AMF contributes to the combat against scams and frauds that are threats identified on the national level.

<sup>18</sup> Joint Guidelines on the characteristics of a risk-based approach to anti-money laundering and terrorist financing supervision, and the steps to be taken when conducting supervision on a risk-sensitive basis. ESAs 2016 72 [here](#).

<sup>19</sup> At the end of 2016, the AMF inspected and fined an FIA for failure to fulfil its professional obligations in marketing shares of a Panamanian company: 27 of the FIA's clients invested a total amount of €1,047,735 by subscribing to an offer on the basis of misleading information.

<sup>20</sup> Marketing of products similar to so-called "Girardin" or "TEPA" or "Dutreuil" products but which do not fulfil the relevant legal conditions

#### Case "A"

In 2015, an FIA collected €24.3m worth of products promoted by Group A, which generated €2.4m in commissions for it for financial years 2012-2013 to 2014-2015, of which €5.2m was collected via loan agreements that the FIA had its clients sign for the benefit of Group A entities. As a reminder, these investments, marketed within the framework of offers on varying conditions, involved taking stakes in hotel operating companies. The FIA was fined by the AMF for failure to comply with rules of good conduct concerning marketing, and the case was reported to the ACPR and the Public Prosecutor's Office of Marseille with regard to the behaviour of the FIA and Group A. At the end of 2017, the Marseille Commercial Court imposed a court-ordered receivership procedure on all the companies of Group A (more than 200 companies).

Other FIAs were inspected for having marketed these products.

In a letter sent to the FIA's professional associations, and reproduced extensively, the AMF reminded FIAs of their professional obligations when they make investment recommendations to their clients.

#### [Watch on fraudulent advertising and marketing practices<sup>21</sup>](#)

Throughout 2018, the AMF and ACPR continued their activity of monitoring market participants which are not authorised to market their products or services in France, in order to alert the public to detected fraudulent or suspicious behaviour.

For this purpose, the AMF and ACPR regularly publish blacklists of the websites or entities not authorised to propose their offers to the public, notably on the ABEIS website. In particular, around 150 extra names were added to the four lists already fed with data by the authorities devoted to **miscellaneous assets (diamonds, wine, balsamic vinegar, etc.), binary options, and Forex and credit/passbook savings account/payment offers.**

Moreover, faced with the growing number of sites proposing **investments in crypto-assets**, a fifth list, identifying sites proposing crypto-asset derivatives without complying with the regulations in force, was established in July 2018. The creation of this list is based on the AMF's assessment that platforms proposing crypto-asset derivatives settled in cash must comply with the regulations applicable to financial instruments. This implies, in particular, that platforms providing crypto-asset CFDs, for example, be authorised as investment service providers. 77 websites were registered on this list for 2018.

Fraudulent **credit** offers, which prompt private individuals to pay a sum of money to be able to obtain a consumer loan, continue to thrive on the web. Passbook savings account scams are also increasing.

The AMF and ACPR note, moreover, that many platforms and websites fraudulently use the name or contact details of regularly authorised or registered financial market participants, deliberately creating a confusion that is harmful to savers.

In all, more than 750 names of fraudulent or suspect websites or market participants are identified on these lists.

Professionals are obliged to step up their vigilance regarding these risks of identity theft on the internet. The public is also invited to show the utmost vigilance regarding offers presented as risk-free, and especially those offering returns far greater than those customarily offered by the market.<sup>22</sup>

### 3.2. THREATS IDENTIFIED ON THE EUROPEAN LEVEL

<sup>21</sup> Excerpts from the 2018 annual report of the Assurance Banque Epargne unit (AMF-ACPR)

<sup>22</sup> Latest press release published on 27 November 2019.

At the end of their joint opinion,<sup>23</sup> the European Supervisory Authorities identified the following cross-sector risks:

- Brexit;
- New technologies, "Fintech" and "Regtech";
- Virtual currencies;
- Legislative divergences between Member States;
- Divergences in supervision practices;
- Weaknesses of the internal control systems of obliged entities;
- Terrorist financing;
- "De-risking": a practice by which obliged entities out of precaution exclude risky clients, encouraging them to turn to unregulated financing circuits.

**The special Brexit context** was indeed a feature of the year: many of the initial applications for authorisation were due to the partial or complete relocation to France of the UK operations of investment management companies. The whole asset management spectrum is concerned: from the entrepreneurial company specialised in unlisted or real estate assets, to the large pan-European market participant which decided to make Paris its European hub. Insofar as these were AML/CFT obliged entities, under the supervision of the competent UK authority, the examination of the quality of their AML/CFT system revealed no major difficulty.

**Fintech and Regtech** are enjoying significant growth in France. Regarding AML/CFT, most of the Paris marketplace clearly uses **external technological solutions and other databases**, mainly for "filtering" their clients. A few names of service providers and/or solutions recur repeatedly. This potential data market concentration raises questions regarding:

- The quality of the data thus used by a majority;
- The lack of personalised intellectual analysis;
- The exacerbation of de-risking.

The risk related to Fintech and Regtech is therefore clearly identified in the French financial sector, although without being considered significant.

According to data collected from asset management companies, the practice of "**de-risking**" mentioned by the European Supervisory Authorities is an established fact in France. AMCs prefer not to enter into a relationship with clients or not to invest in assets which represent a risk considered excessive. As a result, most of them declare their business as being, on the whole, exposed to a low ML/TF risk.

---

<sup>23</sup> Joint opinion of the European Supervisory Authorities on money laundering and terrorist financing risks affecting the European financial sector, 4 October 2019, JC2019 59, available [here](#).

## 4. THE ASSET MANAGEMENT SECTOR

### 4.1. OVERVIEW

With around €3,674bn in assets under management at the end of 2018 (of which €1,573bn in personal asset management), the asset management sector occupies an important position in the French economy and its financing. Highly integrated into global and European financial systems, the personal and collective French asset management industry ranks as the leader in continental Europe, accounting for one-quarter of this market.

Under the supervision of the AMF, **the asset management sector comprises 633 portfolio asset management companies**, all authorised for the collective investment management business (UCITS and/or AIFs). Many of them also have an authorisation enabling them to provide investment services governed by MiFID:

- For example, over half of them (363) are authorised to provide discretionary personal investment management services;
- 10% are accredited for Receipt and Transmission of Orders; and
- Nearly all of them (over 95%) are accredited for investment advisory services (chiefly related to the marketing of managed funds).

The asset management sector in France is characterised by **high concentration** (60% of assets under management are managed by the leading 10 management companies), together with **great heterogeneity of the market participants' profiles**:

- Entrepreneurial companies represent more than two-thirds of asset management companies in France, and this proportion of entrepreneurial organisations is constantly increasing;
- One-third of asset management companies are subsidiaries of regulated banking, insurance or financial groups: they manage 91% of total assets under management.

**The asset management sector is also a highly regulated sector, and portfolio asset management companies are subject to one or other of the AIFM and UCITS sector directives, or even both**, while complying with the rules of MiFID whenever they provide investment services such as discretionary management or investment advisory services.

It is prohibited for asset management companies to receive deposits of funds or securities from their clients.<sup>24</sup>

Apart from portfolio asset management companies, asset management requires the assistance of a number of professionals, and in particular:

- The depository: which keeps the securities and cash accounts of the funds' assets and verifies the lawfulness and correct execution of the AMC's decisions; its control is a rampart against the risk of fraud or abuse that could be committed by the fund manager;
- The registrar which keeps the register of the fund's units on behalf of the AMC;
  - o either the units are kept as "registered units", and investors are registered there by name;
  - o or the units are "bearer units", and the register does not contain the investors' names but those of the custody account keepers;
- The custody account keepers which hold the units of collective investment products on behalf of their clients, and which appear on the register of funds whose units are issued as "bearer units".

These professionals are **credit institutions or investment firms**, authorised, AML/CFT obliged entities under the supervision of the ACPR.

Subject to the rules on anti-money laundering and combating the financing of terrorism, under AMF supervision, for all their activities, the asset management companies are themselves exposed to AML/CFT risks liable to vary depending on the products or services offered, the distribution channels used, client characteristics, and the country of origin or destination of the funds.

---

<sup>24</sup> Article L. 533-21 of the Monetary and Financial Code.

The risk assessment was carried out making a distinction between the main families of businesses, strategies or assets.

#### 4.2. COLLECTIVE MANAGEMENT OF FINANCIAL INSTRUMENTS (LISTED EQUITIES, LISTED BONDS AND MONEY MARKET INSTRUMENTS)

##### Description of the sector

The "conventional" asset management of financial instruments is performed by portfolio asset management companies authorised for the management of funds investing in transferable securities traded on financial markets, and UCITS in particular. Under the terms of European regulations, listed equities, listed bonds and money market instruments constitute the priority investment universe of UCITS and, by extension, 'FIVG' general investment funds.<sup>25</sup> This investment management can also be performed indirectly, by subscribing to investment funds (CIUs) themselves investing in these conventional financial instruments.

This covers a majority of portfolio asset management companies. 78% of them are authorised to select such instruments in their investment funds (UCITS or AIFs) or discretionary management portfolios.

With €1,064bn<sup>26</sup> in assets under management, conventional asset management represents 70% of the collective investment management sector in France.

##### Threats and main scenarios of use for purposes of money laundering and/or terrorist financing

While the investment in units of collective investment products is, in theory, a way of reintroducing criminal funds into the financial sphere, the AMF has no information making it possible to prove and measure this threat.

The collective management of financial instruments is not exposed to the risk of terrorist financing, either.

The threat level is **LOW**.

##### Vulnerabilities

###### Intrinsic vulnerabilities

Regarding the assets of conventional asset management funds, the investment universe is, as mentioned above, constrained by strict eligibility rules: this universe consists of assets representing a low risk of money laundering (transferable securities listed on a regulated market, money market instruments).

Conventional asset management in France is characterised by a high level of intermediation. AMCs managing funds for which the units are distributed via the Central Securities Depository (Euroclear) are not able to know, in real time, the end investors in the managed funds, nor their identity or the source of the funds invested. In this sense, this intermediation constitutes a vulnerability.

Because of this intermediation, but given the low risk to the assets, the intrinsic vulnerabilities of conventional asset management are of a **MODERATE** level.

###### Mitigation measures and residual vulnerabilities

In addition to regulatory factors relating to the authorisation and supervision of AMCs, allowance should be made for mitigation measures related to the quality of the professionals operating in the asset management ecosystem.

---

<sup>25</sup> 'FIVG' general investment funds subjected, by French regulations, to the same constraints as UCITS.

<sup>26</sup> AUM of UCITS managed by French AMCs estimated at €1,110 billion at the end of 2018, including €757 billion worth of French UCITS. AUM of French 'FIVG' general investment funds managed by French AMCs estimated at €306 billion.

As mentioned, the fund's assets are kept by a depository which checks both the lawfulness of the fund manager's decisions and instructions and the cash flows. This is a credit institution or investment firm, subject to AML/CFT rules, and is a rampart against the risk of fraud.

The identified vulnerability which is due to the fact that the AMC does not know its end investors when its units or shares are distributed on Euroclear is considerably attenuated, precisely by the intermediation of Euroclear (see Chapter 7) and also by the assurance that the unit subscription circuit includes only AML/CFT obliged entities:

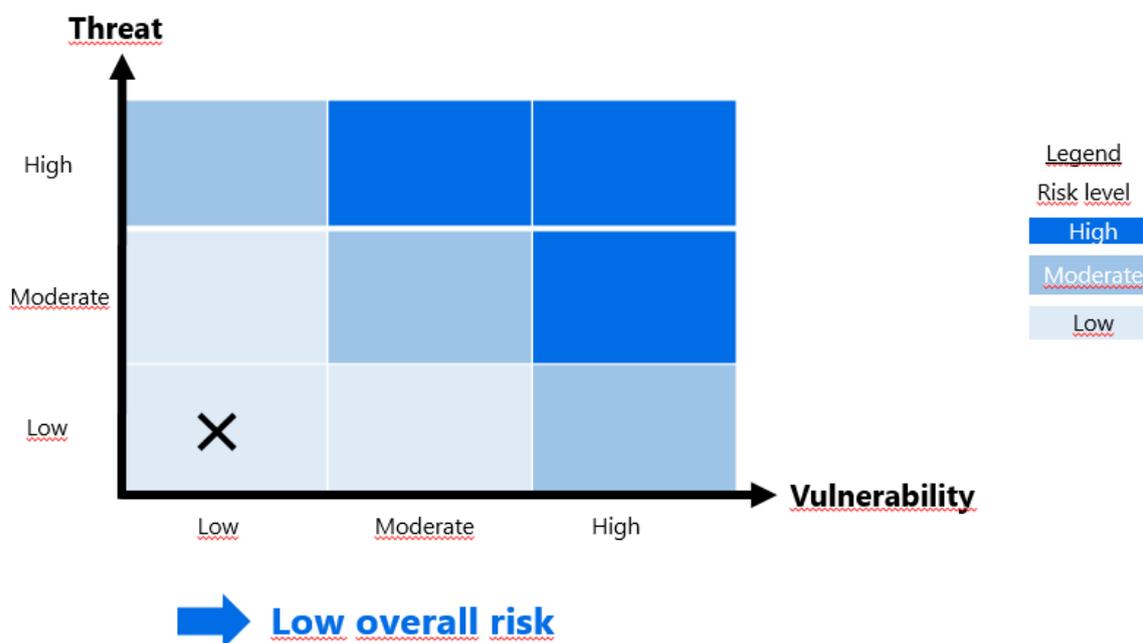
- Insurance companies proposing investments in units of account;
- Credit institutions or investment firms providing advisory or discretionary management services to their own clients;
- Custody account-keepers, also credit institutions or investment firms which receive funds from clients that they know, directly or indirectly.

These factors justify selecting a **LOW** residual vulnerability level.

### ML/TF risk rating

The combination of the threat and vulnerability levels leads to the selection of a **LOW** risk level.

## Management of financial instruments



### 4.3. PRIVATE EQUITY

#### Description of the sector

One out of five AMCs has made this type of investment management its specialty. It is a growth sector (€36bn raised in 2018 for equity and debt financing of companies and infrastructure),<sup>27</sup> on which the new market participants are becoming positioned.

These AMCs manage AIFs exclusively:

- Either in the form of funds with conditions of access limited to professional or quasi-professional investors (professional private equity funds, specialised professional funds): the AUM of these funds stand at €60.2 billion;
- Or in the form of AIFs open to subscription by the general public, which are usually eligible for a tax benefit. These funds may in this case take the form of venture capital funds (FCPRs), local investment funds (FIPs) or innovation venture capital funds (FCPIs); the AUM of these funds stand at €10.9 billion.

Private equity in France is mostly intended for institutional investors, which either invest in this on their own account or intermediate the investments of retail investors. This intermediation takes several forms: discretionary management, or unit-linked life insurance, within which an insurer (institutional client) may lodge professional private equity investment funds.

Of the €18.7bn in capital raised in 2018, 85% came from institutional investors: funds of funds (of which half were of foreign origin), insurance companies, mutual insurance companies, retirement funds and pension funds. The proportion of funds invested by individuals (including family offices) is approximately 15% (of which 73% French capital).

#### Threats and main scenarios of use for purposes of money laundering and/or terrorist financing

By nature, private equity funds are not very attractive for criminals, due to the lock-in period frequently involved in each investment, which may be up to 10 years for funds invested in by retail investors.<sup>28</sup> This lock-in is often a condition for granting a tax benefit, which obliges the client to provide justification of their income tax liability.

In this case, the risk of money laundering and terrorist financing applies generally to the assets of funds:

- investing in companies established in high-risk countries;
- investing in high-risk industrial sectors.

However, according to the data collected, private equity asset management companies invest exclusively in French companies, or companies established in the EEA.

That said, it appears that French private equity investments are attracting an increasing amount of foreign capital, which requires greater due diligence by fund managers with regard to knowledge of the customer and the source of funds.

Therefore, although the available data in terms of identified volumes and cases make it possible to relativise the threat related to the funds' assets, the sector's exposure to foreign capital nevertheless obliges us to select a **MODERATE** threat level with regard to money laundering and terrorist financing.

---

<sup>27</sup> Source: France Invest Annual Report

<sup>28</sup> Professional investors, for their part, can have access to investment funds that have longer lock-in periods.

## Vulnerabilities

### Intrinsic vulnerabilities

The vulnerabilities are mostly related to the nature of the assets, more risky than those for conventional fund management.

Also unlike conventional fund management, private equity AMCs are in direct relation with their investors insofar as the units of private equity funds are often held as registered units. Accordingly, the obligations regarding knowledge of the customer are incumbent mainly on them, without them being able to rely on other professionals in the financial sector. Depending on investors' profile, whether they are institutional or retail investors, whether they are established in France or outside France, this due diligence is more or less complex to implement.

Private equity therefore represents a **HIGH** level of vulnerability with regard to money laundering and terrorist financing.

### Mitigation measures and residual vulnerabilities

Private equity is highly regulated: all funds for the "general public" (FCPRs, FCPIs and FIPs) are subject to the prior authorisation of the AMF and to strict rules in terms of investment ratios. The other funds, reserved for institutional investors (or retail clients investing at least €100,000), are declared to the AMF. All have a statutory auditor who audits the fund's accounts, and of course a depository who provides asset custody but also checks the lawfulness of management decisions and cash flows.

Another measure to attenuate asset risk is the regulatory requirement provided for in Articles 320-22 and 321-149 of the AMF General Regulation according to which: *"when it implements its investment policy, the asset management company shall assess the risk of money laundering and terrorist financing and establish procedures to oversee the investment selections made by its employees"*.

In general, it is clear from discussions with the private equity AMCs that extensive due diligence is performed on the assets, both for ML/TF risk and for credit risk and reputational risk.

As a consequence of these requirements, French AMCs choose to invest mostly in France or in EU countries rather than in third countries or high-risk countries.

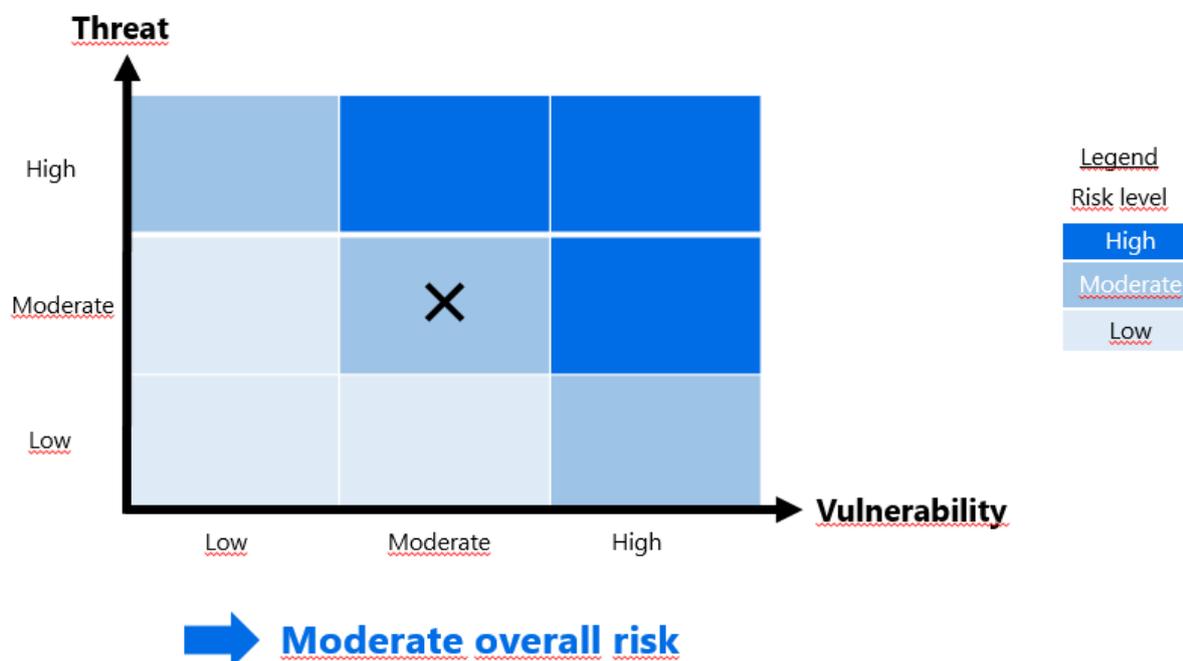
As regards the risk related to the funds' investors, as mentioned above, it depends in particular on their nationality or domiciliation. In the European Union, the regulations in favour of fiscal transparency contribute to a better knowledge of the customer.

For these reasons, the residual vulnerabilities represented by private equity are of a **MODERATE** level.

### Risk rating

The combination of the threat and residual vulnerability levels leads to the selection of a **MODERATE** risk for the private equity sector.

## Private equity



#### 4.4. REAL ESTATE INVESTMENT

##### Description of the sector

Like private equity (see above), real estate is the most dynamic sector in which new AMCs are becoming positioned in France (63% of new AMCs are specialised in either real estate or private equity). At the end of 2018, 18% of French AMCs were authorised to select real estate assets.

At the end of 2018, the net asset value of real estate funds stood at **€109bn**<sup>29</sup> (data taken from AIFM reports). 53% of these funds are held by institutional investors, notably via professional real estate collective investment undertakings (OPPCIs). Funds intended for retail investors manage assets worth **€51.8bn** concentrated in OPCIs (**€15.1bn**) and SCPIs (**€36.7bn**).

##### Threats and main scenarios of use for purposes of money laundering and/or terrorist financing

As mentioned in the NRA, real estate buying and selling businesses are exposed to a high level of threat regarding money laundering, due to the amounts involved, which are large, and the relative security offered by this type of investment. The luxury real estate sector, especially in Paris and the French overseas territories, is, again according to the NRA, more exposed than others to threats related to tax evasion, scams and drug trafficking.

Distinctly, the real estate investment sector is, for its part, focused more on real estate assets that could generate regular rents which are distributed to investors over a fairly long period (at least five years for SCPIs). Luxury residential real estate is not the preferred investment target of real estate funds.

<sup>29</sup> Data coming from AIFM reports

Due to these differences with the real estate sector in general, the real estate investment sector's exposure to the threat of money laundering is lower, and of a **MODERATE** level.

It is not particularly exposed to the terrorist financing threat.

## Vulnerabilities

### Intrinsic vulnerabilities

The real estate sector's vulnerabilities are mainly related to the nature of the assets: prestige real estate is more vulnerable to money laundering threats, due to the volatility of selling prices, the absence of a reference system making it possible to verify price consistency, and the often highly confidential nature of these transactions. In the real estate investment sub-sector, the vulnerabilities are related more to the financial arrangements, the structures owning these assets which correspond to specific tax-related needs.

The profile of the investor-client is also a risk factor: depending on whether they work in a sector characterised by large cash flows, depending on their PEP status (risk of corruption), and depending on their tax residence.

The intrinsic vulnerabilities of the real estate investment sector are potentially **HIGH**.

### Mitigation measures and residual vulnerabilities

Due to these vulnerabilities, the sector is heavily regulated. All real estate professionals are AML/CFT obliged entities. Asset management companies operating in this sector are subject to regulation on two levels:

- **Under the supervision of the AMF**, in their capacity as a portfolio asset management company managing real estate AIFs, referred to in 6°); and
- **Under the supervision of the French fraud prevention authority (DGCCRF)**, where applicable, in their capacity as real estate professionals referred to in 8°): carrying out the activities mentioned in 1°, 2°, 4°, 5°, 8° and 9° of Article 1 of Act No. 70-9 of 2 January 1970 regulating the conditions of exercise of activities relating to certain transactions involving buildings and intangible business assets ("Hoguet Law").

Real estate assets undergo a valuation performed by one (or several) independent appraisers mandated by the asset management company.

Like for private equity, real estate fund managers comply with the requirement of ML/TF due diligence on the assets, as summarised in Articles 320-22 and 321-149 of the AMF General Regulation according to which: *"when it implements its investment policy, the asset management company shall assess the risk of money laundering and terrorist financing and establish procedures to oversee the investment selections made by its employees"*. Investment decisions are taken collectively, in a committee.

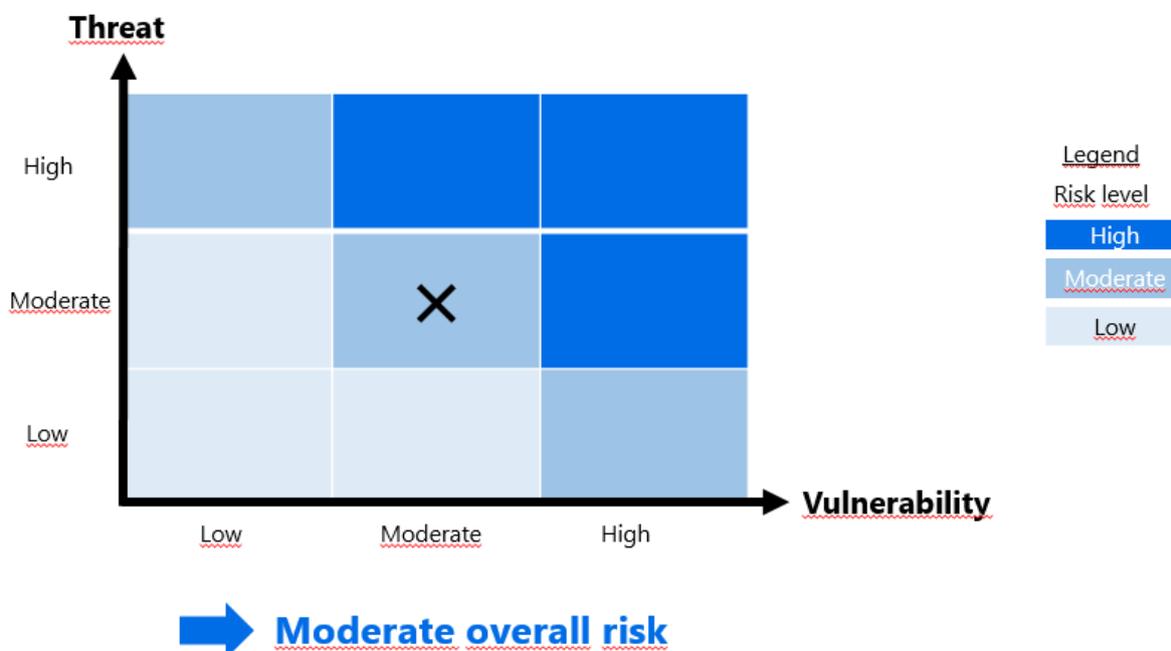
Cash transactions are prohibited. They are long to conclude, and alongside the company involve numerous professionals (lawyers, notaries), which are themselves AML/CFT obliged entities.

This significant regulatory oversight of the sector and the efforts made by all the professionals in the sector lead us to select a **MODERATE** residual vulnerability.

## Risk rating

The risk level of the real estate sector is **MODERATE**.

## Real estate management



### 4.5. DISCRETIONARY MANAGEMENT

#### Description of the sector

"Personalised discretionary management", or more simply "discretionary management", is a customised service of management of a portfolio of financial instruments provided for clients by investment service providers, including AMCs. This service is always personalised, because it is adapted to an investor's situation and objectives and is concluded following a Know Your Customer (KYC) process. For these reasons, moreover, it is often reserved for investors having a certain level of resources.

As mentioned earlier, assets under discretionary management amounted to €1,573 billion at the end of 2018.

While over half of French AMCs (361 out of 652) are authorised to offer discretionary management services (one out of two asset management companies offers this service to its clients), the sector is highly concentrated: the 20 leading actors together account for 91.9% market share<sup>30</sup> (around €1,487 billion in assets under management). Also, the shareholder profile is different from that in collective investment management. Of these 20 leading actors, 50% are subsidiaries of insurance companies and mutual insurance companies and 45% are subsidiaries of credit institutions.

Moreover, this activity frequently extends to a more general service offering related to the overall management of financial and/or real estate assets, commonly grouped together under the term "*private banking*".

<sup>30</sup> The five leading actors manage 69% of assets under discretionary management.

## Threats and main scenarios of use for purposes of money laundering and/or terrorist financing

The discretionary management activity which involves investing, on the client's account, in financial instruments in order to obtain the best return from them may allow unlawful revenues to be reintroduced into the legal economy.

Designed for an affluent clientele with substantial wealth or high incomes, potentially non-residents coming from high-risk countries, "Politically Exposed Persons", discretionary management is exposed to threats related to criminal offences of corruption and tax evasion.

In France, according to the data collected, asset management companies providing this discretionary management service as part of a more comprehensive wealth management offering have relatively few clients classified as high-risk, and even fewer PEP clients. Only about ten asset management companies state that they are in a business relationship with a limited number of clients established in a high-risk country (less than 0.7% of their clientele).

The money laundering threat is **MODERATE**. In contrast, the terrorist financing threat is low.

## Vulnerabilities

### Intrinsic vulnerabilities

The sector's vulnerabilities are mainly due to the nature of the investments decided on by the fund manager (listed versus unlisted financial instruments, cross-border transactions) and the proposed financial arrangements, which may be vehicles for opacification. The establishment of complex legal arrangements, corresponding to many specific needs (return on investment, tax optimisation, succession), prevents the fund manager from having a constant overall view of the client's activities and resources.

The vulnerabilities also depend on the clientele and its characteristics. Often represented by third parties or business finders, this demanding clientele may prove more reluctant to comply with all the requests made for justificatory documents. Politically Exposed Persons or foreign residents for tax purposes, established in countries with inadequate AML/CFT legislation, discretionary management clients are most likely to correspond to one or other of the high-risk factors.

The asset management sector has **HIGH** intrinsic vulnerabilities.

### Mitigation measures and residual vulnerabilities

The mitigation measures are the fact that the fund managers are subject to AML/CFT regulations, but also regulations based on MiFID 2. These two regulatory systems oblige clients to share with the fund manager all useful information, at the risk of not having access to the service wanted. By comparison with collective investment management, then, the discretionary management sector is characterised by a good knowledge of the customer and the business relationship. The fund manager (the agent) maintains close relations with its client (the principal), especially when the discretionary management service is supplemented by a more general offer of overall management of financial and/or real estate assets.

The regulatory measures relating to the exchange of information on tax matters also contribute to the fund manager's good knowledge of its client's profile.

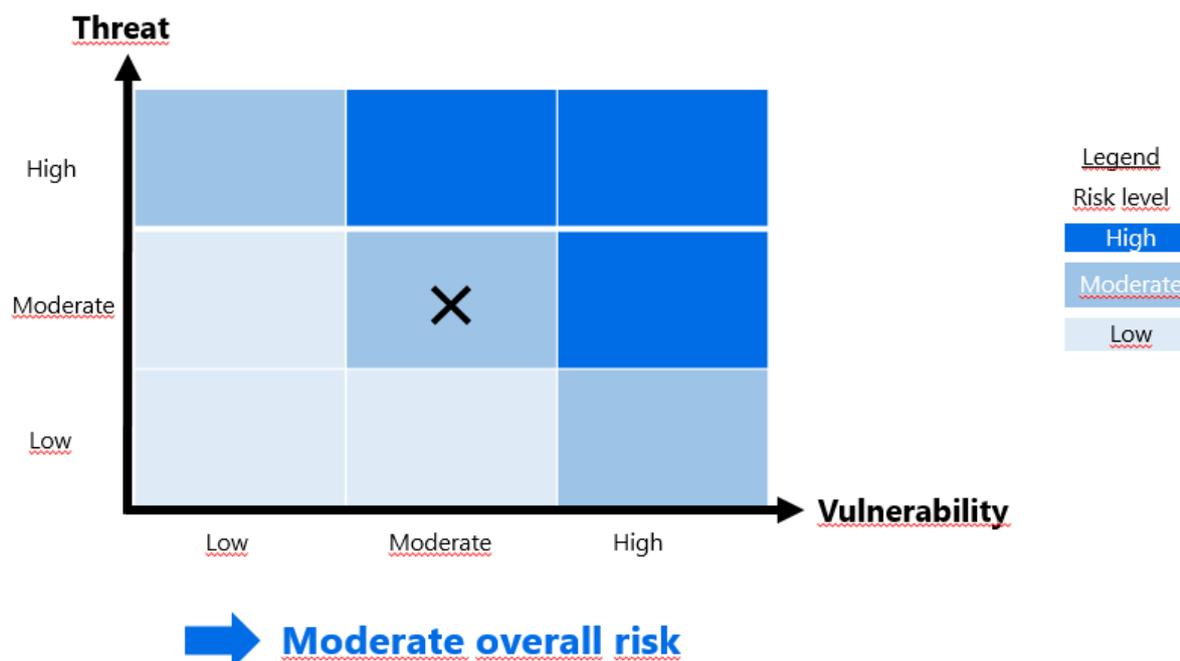
The intrinsic vulnerabilities are well known and identified by discretionary management professionals, who take this into account in their risk mapping, adapting their procedures and training their personnel as a consequence.

The residual vulnerability level is **MODERATE**.

## Risk rating

As a consequence, the combination of the threats and residual vulnerabilities after mitigation measures leads to a **MODERATE** ML/TF risk level for the discretionary management sector.

### Discretionary management



## 5. FINANCIAL INVESTMENT ADVISORS (FIA):

### Description of the sector

At 31 December 2018, 5,152 FIAs (individuals or legal entities) were registered with the ORIAS (organisation responsible for registering insurance, banking and finance intermediaries).

As a reminder, in accordance with Article L. 541-1 of the Monetary and Financial Code, financial investment advisors are “individuals and legal entities who/which provide the following services in the normal course of their business:

- 1° The investment advice referred to in paragraph 5 of Article L. 321-1;
- 2° (Repealed)
- 3° The advice relating to the provision of investment services referred to in Article L. 321-1;
- 4° The advice relating to the execution of transactions in miscellaneous property described in Article L. 551-1.”

FIAs can also, in accordance with II of Article L. 541-1 of the Monetary and Financial Code, “provide the service of third-party order reception and transmission, within the conditions and limits set by the General Regulation of the Autorité des Marchés Financiers, and perform other wealth management advisory activities.”

Depending on the services provided, the sector is divided among two main families of businesses:

- **Wealth management advisor (WMA) FIAs:** These are actors having a general wealth management advisory business which may be for private individuals or corporate clients (investment of cash holdings). For this business, the "WMA" FIA generally has other statutes in addition to FIA (insurance intermediary, "IOBSP" intermediary, "carte T" real estate licence, etc.). For sake of transparency, FIA platforms/groups intended of WMA FIAs are classified in this category (retail client base but multi-regulated). **This family comprises 94% of the FIA population.**
- **FIAs providing advisory services for institutional investors, investment management companies and other financial intermediaries:** This category covers FIAs who assist institutional investors (foundations, pension funds, insurance companies, etc.) in monitoring their investments (audits, invitations to tender, recommendations, etc.) but also those who provide investment recommendation services exclusively for asset management companies or funds, and also the actors in charge of advisors to other financial intermediaries (e.g. BtoB platform on structured products).

Of total declared FIA revenues of **€2.8 billion, €669m** concerns FIA activities, i.e. **24% of total revenues**. "Non-FIA" activities may concern activities performed within the framework of other statutes registered with ORIAS (organisation responsible for registering insurance, banking and finance intermediaries) or coming under other regulations (Hoguet Act, "carte T" real estate licence).<sup>31</sup>

The sector is highly concentrated, because the 50 leading firms account for 51% of FIA business, the following 500 33%, while the remainder (4,091 entities) account for 16% of FIA business.

The four professional associations authorised by the AMF are obliged to audit their members once every five years, and report on their audits to the AMF.

The AMF ensures that FIAs comply with the regulations by performing conventional audits (systematically including the AML/CFT system) and mass inspections (thematic), and by supervising the auditing of FIAs performed by the professional associations that it authorises.

### Exposure to the threat and description of use scenarios for ML/TF purposes

The FIA activity which consists in recommending financial investments (financial instruments or other) or investment services in itself offers few ways of laundering money. FIAs collect no funds other than those related to their remuneration.

On the other hand, the act of subscribing to an investment that has been recommended by an FIA in the normal course of their duties is a way to launder unlawful revenues, especially revenues evading taxation. The tax aspect is an important factor for most FIA clients.

In the case of regulated financial investments, a subscription involves other professionals: the financial instruments or investments that FIAs can recommend are those proposed by other entities in the financial sector (asset management companies, banking, finance and insurance institutions), and they can only be subscribed to by means of account-to-account transfers to accounts opened in other institutions that are likewise regulated.

In contrast, in the case of more atypical products, which are unregulated, the involvement of other professionals that are AML/CFT obliged entities is not verified.

---

<sup>31</sup> 91% of these firms declared having other statutes, namely:

- Insurance intermediary ("IAS"), statute registered with ORIAS;
- Intermediary in banking transactions and payment services ("IOBSP"), statute registered with ORIAS;
- Real estate ("carte T" real estate licence", statute registered with the prefecture and Chamber of Commerce).

Moreover, 45% of FIAs also declared that they had a "CJA" certificate of competence on legal matters, i.e. 1,962 firms (stable by comparison with the previous year).

The level of the threat to which FIAs are exposed can therefore vary greatly depending on the nature of their clients and the quality of their partners. It is **LOW** regarding terrorist financing, and **MODERATE** regarding money laundering.

## Vulnerabilities

### Intrinsic vulnerabilities

Anonymity is not possible in the close relationship which is established between an FIA and their client.

The vulnerabilities are therefore related to the characteristics of the clientele. Now, according to the AMF's information, the clientele of FIAs is domestic, and includes only a very small number of PEPs (less than two per thousand of the FIAs' total clientele).

Other vulnerabilities are due to the products recommended, depending on whether they are regulated CIUs authorised by the AMF, for which the subscription circuit uses French AML/CFT obliged entities, or more exotic products (foreign, declared and unregulated).

The financial investment advisor activity therefore has intrinsic vulnerabilities that are on the whole **MODERATE**.

### Mitigation measures and residual vulnerability

As AML/CFT obliged entities, FIAs are professionals with high AML/CFT awareness, supervised by the AMF and the four FIA professional associations (Association Nationale des Conseils Financiers ("ANACOFI CIF"), Chambre Nationale des Conseils en Gestion de Patrimoine ("CNCGP"), Chambre Nationale des Conseillers en Investissements Financiers ("CNCIF") and Compagnie des CGP-CIF).

In 2018, the FIA professional associations carried out audits on part of their members (each member being audited once every five years) in mainland France and overseas. For one-third of them, one or more breaches of AML/CFT obligations were noted. For its part, the AMF undertook 70 so-called "mass inspections" on FIAs spread over six regions, on precise regulatory aspects such as the collection of clients' funds. On the occasion of these thematic mass inspections, and for each FIA, the inspectors always read the latest audit report established by the professional association and ensure that the FIA has indeed taken measures to correct the shortcomings noted by the association. Seven conventional inspections concerned AML/CFT in particular.<sup>32</sup>

In 2018, 88% of FIAs questioned stated that they had prepared a risk classification. The training effort is continuing, with a further training obligation covering the themes of Instruction 2013-07, including AML/CFT. As of 1 January 2020, those entering the FIA profession will also all have to have AMF certification.

Moreover, in addition to the obligations of vigilance regarding their clients, FIAs are bound by numerous Know Your Customer obligations for the purposes of provision of the personalised recommendation as stipulated by MiFID II. These obligations concern clients' investment knowledge and experience in relation to the specific type of financial instruments, transactions or services, their financial position and their investment objectives, their ability to bear losses and their risk tolerance. The same regulations oblige them to abstain from recommending some transactions or products if clients or potential clients do not provide the required information.<sup>33</sup>

That said, and in light of the completeness of the information available to them, the reporting activity of FIAs remained at a low level in 2018, and is therefore not representative of the knowledge that these professionals have concerning the transactions they handle: a reminder of the reporting obligation seems essential.

---

<sup>32</sup> These inspections were able to identify potential scams or frauds which gave rise to transmission to the French fraud prevention authority (DGCCRF), TRACFIN or the Public Prosecutor's Office (see above: **threats of atypical products**).

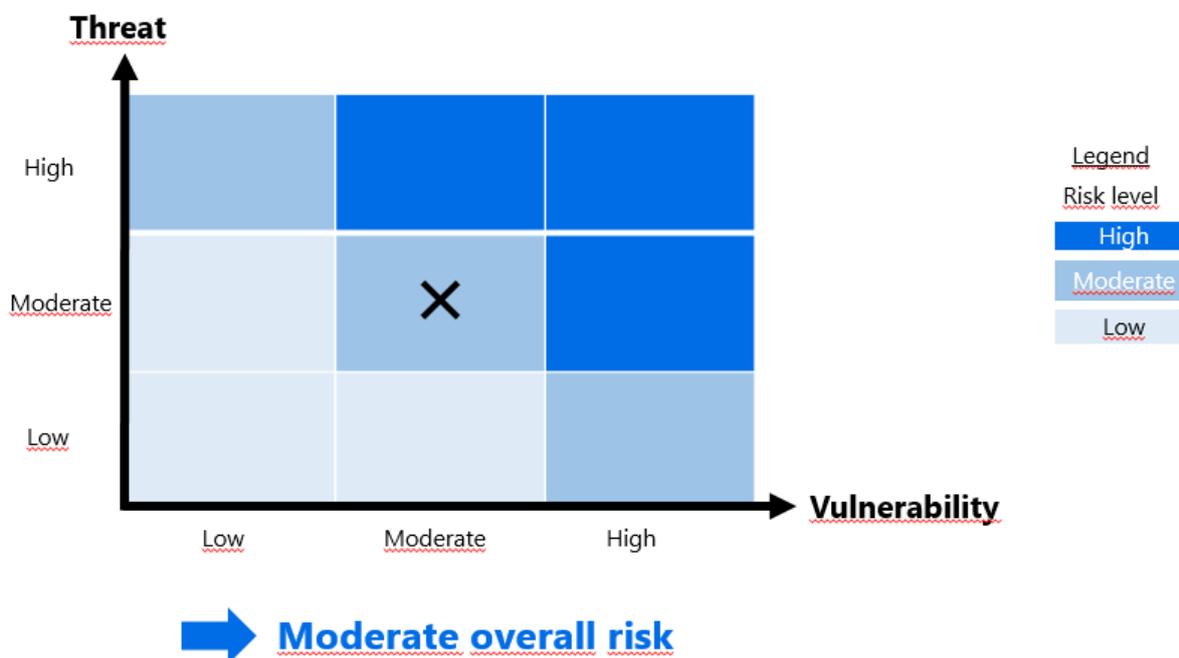
<sup>33</sup> Art. L. 541-8-1 4° of the Monetary and Financial Code.

The residual vulnerability level remains **MODERATE**.

### Risk rating

The combination of the threat and vulnerability levels leads to the selection of a **LOW** risk level regarding terrorist financing and a **MODERATE** risk level regarding the risk of money laundering.

### FIAs



## 6. CROWDFUNDING INVESTMENT ADVISORS (CIAs)

### Description of the sector

At 31 December 2018, 51 CIAs were registered and practising. In addition, there were three investment service providers (ISPs) which primarily or exclusively operate a crowdfunding business.

In 2018, CIA and ISP platforms financed 944 projects for a total amount of €324.8 million, i.e. a 63% increase relative to 2017. While the amount of reimbursed projects reached €83.2 million, up 117% from the previous year, the amount of financed projects that were in distress or in default also increased significantly, from €4.9 million to €20 million in 2018. The proportion of investors relative to the number of those registered remained stable, at around 25%: in 2018, 57,368 clients invested.

The market remains highly concentrated: 80% of the total funds were raised by about fifteen platforms, with two platforms accounting for 25% of the total amount of funds raised. Nine platforms even raised no funds in 2018.

Regarding the form of the fundraising, bond issuance outweighs investments in equity securities, accounting for 75% of the total funds raised by the platforms. The weaker success of equities is probably due to investors' moderate risk appetite and fears about the low potential for disposal of the securities.

The share of the real estate sector continued to grow in 2018, amounting to 62% of the total funds raised as at 31/12/2018, compared with 55% in 2017 and 50% in 2016. The AMF Board approved the first application for registration of a CIA specialised in rental real estate.

The combined total revenues of the platforms amounted to €26.9 million, or an average of €529,640 per platform, but only 15 platforms reported a net profit. Seven platforms had negative equity.

In 2019, the second professional association of crowdfunding firms, the AFCIM, ceased operations. 75% of CIAs are members of the Financement Participatif France association, which is now the only crowdfunding association with which the AMF can hold discussions.

### Threats and main scenarios of use for purposes of money laundering and/or terrorist financing

In its latest reports, TRACFIN regrets the lack of suspicion reports coming directly from CIAs (a single suspicion report in 2018): most suspicion reports come from payment institutions or credit institutions which are used by the platforms.

Due to the lack of liquidity of the securities, crowdfunding in equity capital is not very attractive for those who want to rapidly launder unlawful capital. However, one of the scenarios of use of crowdfunding platforms for purposes of money laundering would involve persons investing in projects which are promoted by themselves, or which are promoted by close relations (a disguised donation).

While case typologies have thus been identified, the threat of money laundering is still seldom materialised on the whole, and the sector does not represent a major financial weight. The threat level is **LOW**.

More specifically regarding the threat of terrorist financing, the fact that the amounts invested are small is not a decisive criterion. However, according to TRACFIN's research, the terrorist financing risks related to the crowdfunding sector primarily concern online kitty platforms, especially those designed to gather funds for associations of a radical nature or for funding communitarian projects.

As mentioned above, due to the relatively illiquid nature of the proposed investments and the purpose of the selected projects (62% real estate sector, 12% environment and energy), the CIAs under AMF supervision do not appear particularly exposed to this threat of terrorist financing. The threat level is **LOW**.

### Vulnerabilities

#### Intrinsic vulnerabilities

The operating model of the crowdfunding platforms suffers from inherent vulnerabilities:

- Remote access, which is liable to increase the risk of documentary fraud;
- The sharing of information relating to clients between the platform (experience and knowledge, investment objectives, risk appetite) and the underlying service provider possessing relevant information concerning the funds (source and destination), when it could be in the interest of both of them to have all the information.

Other vulnerabilities are due to the nature of the projects (potentially sensitive sectors of activity, acquisition of risky assets). According to the latest figures collected, it is in the real estate sector that the first platforms are concentrated.

There are grounds for selecting a **HIGH** level of intrinsic vulnerabilities.

### Mitigation measures and residual vulnerabilities

The main ML/TF risk mitigation measure was subjecting platforms to the CI and CIA regulated statutes. It is still recent. The platforms are assisted by TRACFIN in increasing their AML/CFT expertise.

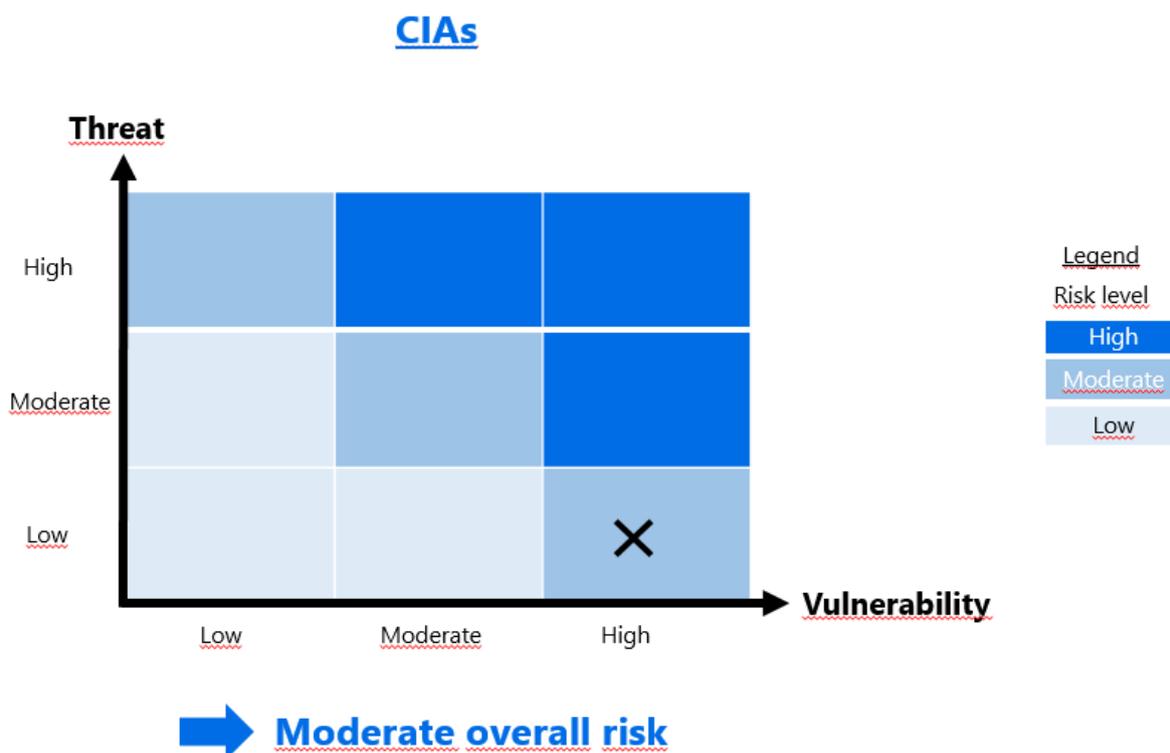
No CIA platform has been able to obtain authorisation unless the AMF has ensured the existence of AML/CFT procedures and a control system.

However, although some platforms backed up by banking groups benefit from their group's resources and expertise to effectively conduct due diligence on clients, most of the isolated platforms still face difficulties with the concrete implementation of their obligations and procedures.

The vulnerability level remains **HIGH**.

### Risk rating

The combination of the threat and residual vulnerability levels leads to the selection of a **MODERATE** risk level.



## 7. THE CENTRAL SECURITIES DEPOSITORY AND SECURITIES SETTLEMENT SYSTEM MANAGER: EUROCLEAR

### Description of the sector

The Central Securities Depository Euroclear France has a twofold role:

- as "notary", insofar as the Central Securities Depository lists securities when they are issued;
- as securities settlement system manager, thus enabling the circulation of securities between the participants.

Listings of securities with Euroclear France are subject to verification of the issuer's quality and to the issuer's agreement on the conditions of use of the Euroclear system. Depending on the type of security, the following are required in particular: the security prospectus, the issuance programme, the company's articles of association, the bond documentation, and the investment memorandum of the securities.

The securities settlement system operates with "central bank money", i.e. the participants' cash accounts are opened and kept by Banque de France.

The participants in the Central Securities Depository's securities settlement system are listed restrictively by the Monetary and Financial Code in Article L.330-1 II: Credit institutions and investment firms having their registered office or, failing that, their effective management, in a Member State of the European Community or another State party to the European Economic Area Agreement; credit institutions and investment firms in Europe or from third countries subject to certain conditions, central securities depositories, authorised interbank settlement systems and clearing houses in Europe or from third countries subject to certain conditions, and public and supranational organisations.

Euroclear France accordingly has **291 accounts opened for 140 participants**, the detailed list of which is provided to the authorities. The process of admission of participants entails procedures for verification of their quality (registration, authorisation, shareholders, managers), but also, depending on their statutes, verification of their submission to anti-money laundering regulations). It should also be noted that most of the participants also have a cash account opened with Banque de France, which is likewise subjected to due diligence by Banque de France.

By way of illustration, the total securities deposited with Euroclear France amount to €7,238 billion for a monthly settlement and delivery volume of €20,243 billion for slightly less than 5 million settlement and delivery instructions. Settlement and delivery instructions refer to the computer orders for securities transactions transmitted by each of the firms taking part in a transaction. In the light of such volumes, numerous settlement and delivery flows undergo netting to improve the fluidity of the settlement system. Regarding this, the clearing houses, downstream of the transactions performed on the markets, systematically net flows between their members in order to optimise risks.

#### Threats and main scenarios of use for purposes of money laundering and/or terrorist financing

**The CSD is relatively unexposed directly to the terrorist financing threat.** Being highly integrated into the financial ecosystem and offering only electronic exchange procedures which require the use of standardised communication systems that are hard to access (Swift), the CSD only handles securities swaps: cash settlements, for their part, are made via accounts opened with Banque de France. Inaccessible to individuals and not easily accessible to legal entities having no significant long-term securities settlement activity, the high level of investment required to obtain access to settlement systems makes the direct use of the central securities depository inappropriate for purposes of terrorist financing.

In its capacity as intermediary, **the CSD could be used as** a vehicle for spreading fraudulent operations, such as securities swaps at exchange values not really proportional to the assets' valuation.

Given these factors, the ML/TF threats faced by the CSD are considered as of a **LOW** level.

## Vulnerabilities

### Intrinsic vulnerabilities

Although the participants in the Central Securities Depository also subject their clients to their own AML/CFT systems, the participants' proprietary and third-party transactions, due to the complexity they may entail, are nevertheless a definite factor of vulnerability.

Regarding this, although all the flows are traceable, the fact that they may be netted with other transactions makes it difficult to identify possible suspicious behaviour. Accordingly, given the masses of instructions involved between participants, their possible netting and the variety of possible instructions, the CSD has no detailed view of the underlying strategies of the transactions going through its system. For example, insofar as the security collateral flows for a refinancing operation may be netted with securities buying and selling, it is impossible to identify which part of the flow of securities is covered by which transaction and at what price.

The same holds for the part of the instructions handled on account of the participants' clients, as the clients' operations are netted with one another in the same way.

The netting process, which ensures efficiency and security for all settlement systems managed by this type of infrastructure, obliges us to select a **MODERATE** intrinsic vulnerability level for money laundering risk.

### Mitigation measures and residual vulnerabilities

The first mitigation measure taken is to subject the CSD to AML/CFT to regulation, whereas Regulation No. 909/2014 (CSDR) provides for nothing in this respect. Monitoring of the French CSD's compliance with its AML/CFT obligations is incumbent on the AMF (Article L.561-36). Each year, the AMF receives and analyses the annual AML/CFT report which describes in detail, in particular, the number of personnel, the resources and the measures taken for AML/CFT monitoring, such as, for example, the establishment of alerts for transactions liable to be suspicious. Moreover, work has been performed to identify the obligations based on the FATF's recommendations for security management activities so as to consider what provisions are applicable within the framework of the French Central Securities Depository.

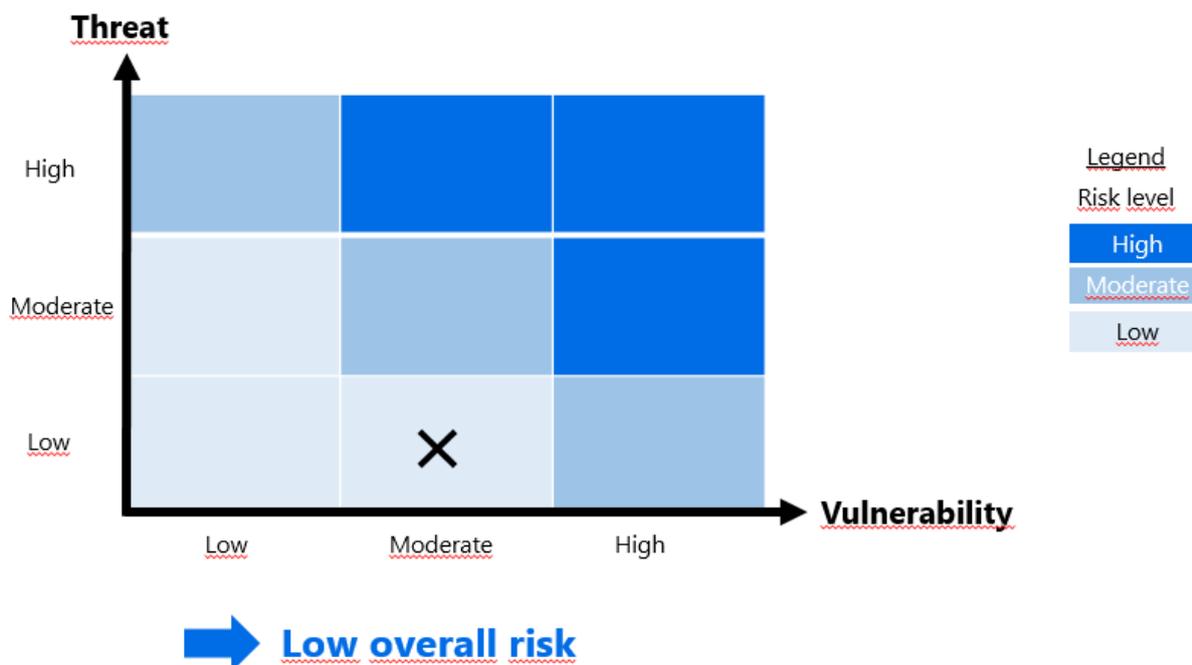
A second essential measure lies in the fact that **the CSD participants are themselves supervised entities, subject to AML/CFT**. In addition, the participants are subject to due diligence by Euroclear consisting of verifying compliance with the admission criteria (including submitting to an AML/CFT system) as a function of mainly geographic risk criteria.

However, these measures can cover the identified vulnerabilities, so that the residual vulnerability (after mitigation measures) is nevertheless still considered MODERATE for the Central Securities Depository,

### Risk rating

As a consequence, the combination of the threats and residual vulnerabilities after mitigation measures leads to a **LOW** risk level for the Central Securities Depository.

## EUROCLEAR



## 8. CRYPTO-ASSETS OR "DIGITAL ASSETS"

In France, since Act No. 2019-486 of 22 May 2019 on business growth and transformation (the so-called PACTE Law), crypto-assets are referred to as "digital assets". This term covers:

- Any digital representation of a security which is not issued or guaranteed by a central bank or by a public authority, which is not necessarily attached to a currency that is legal tender and which does not have the legal status of a currency, but which is accepted by natural or legal persons as a means of exchange and which can be transferred, stored or exchanged electronically;
- Tokens, defined as any intangible asset representing, in digital form, one or more rights that can be issued, registered, stored or transferred by means of a shared electronic recording system making it possible to identify, directly or indirectly, the owner of said asset.

For the SRA, a distinction should be made between risks related to digital-asset service providers ("**DASPs**") (8.1), and risks related to initial coin offerings (ICOs), (8.2).

### 8.1. DASPs

#### Description of the sector

The PACTE Law established a highly innovative specific framework for these digital assets. It defined ten digital-asset services which could be subject to an authorisation by the AMF on a voluntary basis. These services are as follows:

- **Custody of digital assets for third parties:** this activity involves providing custody of private cryptographic keys on behalf of clients with a view to holding, storing and transferring digital assets;

- **The buying and selling of digital assets for legal tender;**
- **The exchange of digital assets against other digital assets (broking);** this activity is mainly performed online (physical sales offices exist and plans have been reported for terminals for the physical withdrawal of digital assets);
- **The operation of a digital asset trading platform (stock exchange):** these platforms allow interaction of the participants with a view to buying or selling digital assets;
- **Other digital-asset services,** inspired by the investment services regulated by the European Union's Markets in Financial Instruments Directive ("MiFID") , such as the reception and transmission of third-party orders, third-party portfolio management, advisory services for investors in digital assets, underwriting, guaranteed placement and non-guaranteed placement (at present these services are not highly developed).

This is a sector that is at present not highly regulated worldwide: its actors are IT experts who are often not very familiar with the regulations, since digital assets circulate outside the conventional regulated payment systems and financial circuits. That said, in the past few years the AMF has met many of them, and has noted that the French actors currently in the business have come to grips with ML/TF risks, by imposing *Know Your Customer* procedures without waiting to be forced to do so by the regulations (before the transposition of the Fifth Directive by the PACTE Law), and by increasing the number of their staff devoted to compliance. Tools have also been developed, which are tending to come into widespread use, designed to assess ML/TF risk via an analysis of transactions and the history of digital assets.

Although in volume terms the crypto-asset sector is still marginal, in recent years it has experienced rapid growth to which the supervisors are paying very close attention.

#### Threats and main scenarios of use for purposes of money laundering and/or terrorist financing

As mentioned in the NRA, digital assets can be misappropriated and used for purposes of money laundering or terrorist financing. The business of conversion of digital assets into a currency that is legal tender is therefore extremely exposed to the threat of money laundering, since via a dual conversion operation (legal currency/digital assets/legal currency), it allows unlawful funds to be reintegrated into the banking and financial system. According to TRACFIN, the tendency to use foreign exchange platforms for laundering tax evasion proceeds is confirmed. In practice, however, the threat is contained, due to the AML/CFT controls performed by the banking institution which keeps the account in legal currency.

On the other hand, services which exchange digital assets for other digital assets, or other digital-asset services, are less exposed to this threat because they do not directly allow such reintegration.

As regards digital-asset trading platforms, the aspects discussed above should apparently apply likewise, depending on whether they propose to establish relations between buyers and sellers of digital assets for legal tender or digital assets for other digital assets. It has been noted that most transactions take place on so-called centralised platforms, which apply KYC procedures and transaction limits. On the other hand, the transactions performed on decentralised platforms offer fewer guarantees.

The sector is also exposed to other risks of fraud: price manipulation, cyberattacks on foreign exchange platforms or on users' computers (ransomware demanding ransoms payable in crypto-assets), and trade in unlawful products. In particular, the AMF has identified scams in the form of fake investments and has published blacklists of websites proposing investments in digital assets on fake platforms. These lists are updated regularly.

Identified but contained, the money laundering and terrorist financing threat is assessed as of a **MODERATE** level.

## Vulnerabilities

### Intrinsic vulnerabilities

The digital assets sector has specific features which could facilitate money laundering or terrorist financing.

- Anonymity is preferred: use of pseudonyms, public addresses, possibility of using "mixers" in certain blockchains to protect the anonymity of the participants and make it very hard to determine the source of the digital assets, or again, use of certain private blockchains which make it impossible to access transaction-related data or the addresses of the wallets used in these transactions;
- Relations almost exclusively "at a distance", and which have a cross-border aspect which makes it hard to identify the parties to the transactions;
- The possible stacking of several chains of transactions and actors making it difficult or even impossible to identify the parties to the transactions and the source of funds.

Accordingly, the intrinsic vulnerabilities of crypto-assets can be considered **HIGH**, with regard to both money laundering and terrorist financing.

### Mitigation measures and residual vulnerabilities

France is the first country in the world to have acquired a very comprehensive specific legislative and regulatory framework in the area of digital assets stipulating that the actors are subject to all the AML/CFT regulations, anticipating, moreover, the transposition of the fifth AML/CFT directive.

This innovative regulatory framework, established by the PACTE Law, provides for:

- **Mandatory registration with the AMF upon clearance by the ACPR**, for provision **(i) of the service of custody of digital assets** and for **(ii) buying/selling digital assets for legal tender**. The registration must be preceded by an investigation concerning the competence and integrity of key managers and shareholders, and verification of the internal AML/CFT system, and gives rise to a check by the ACPR on the service providers' compliance with these AML/CFT obligations. This mandatory registration is the measure transposing the requirements of the fifth money laundering directive (Directive (EU) 2018/843 of 30 May 2018); it is the ACPR which will be responsible for long-term monitoring in this area.
- An **optional authorisation issued by the AMF is also stipulated for these two services, and for the eight other digital-asset services** listed by the PACTE Law (including the service of operation of a digital asset trading platform). Authorisation requires the same due diligence regarding AML/CFT as mandatory registration, including verification of the competence and integrity of key managers and shareholders. It is the AMF which will be responsible for AML/CFT monitoring within this framework.

The AMF will publish on its website the white list of registered or authorised DASPs, which will enable investors to identify actors providing guarantees of trustworthiness, integrity and compliance with the regulations on combating money laundering and terrorist financing.

Under this system, **the biggest actors** will therefore be subject to AML/CFT regulatory requirements, and in particular those relating to the duty of vigilance concerning clients and their ultimate beneficial owners, insofar as:

- Those who only provide services involving merely optional authorisation are exceptions, since the actors in the sector usually propose a combination of services generally entailing the performance of services subject to mandatory registration;
- The first to apply for optional authorisations should be actors already subject to AML/CFT regulation as Payment Service Providers, portfolio managers or financial investment advisors, wanting to extend their range of services to digital assets.

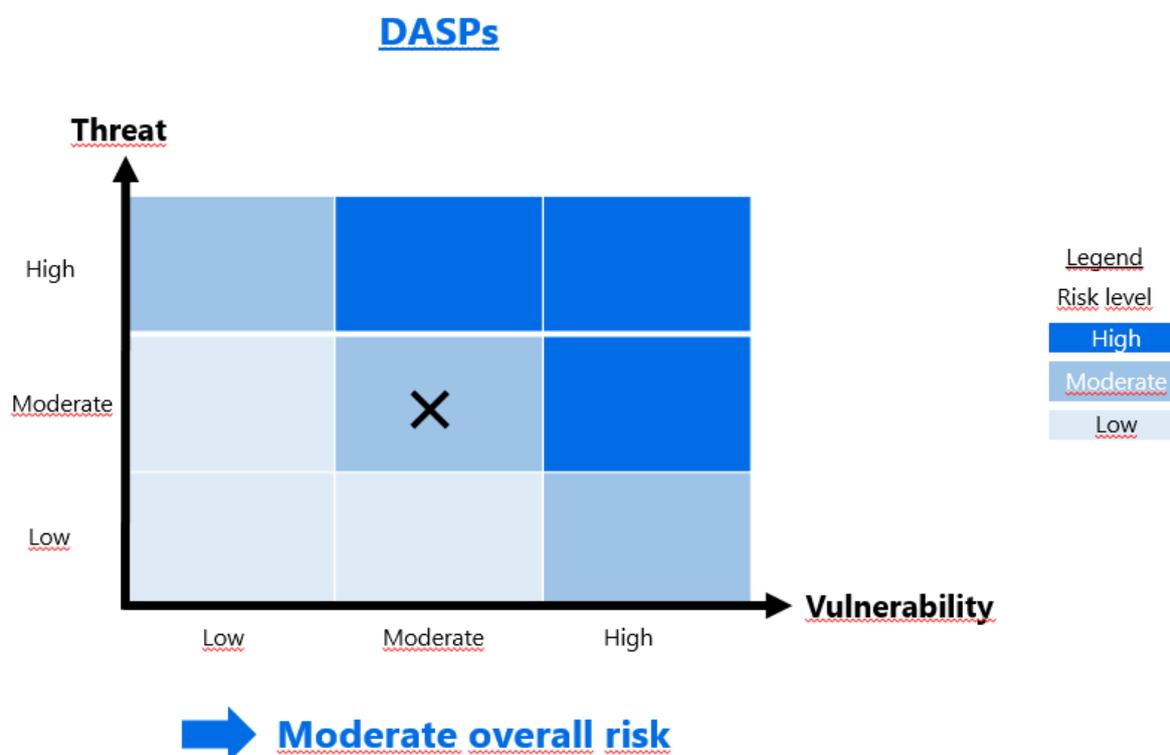
Authorisation has substantial advantages, not only in terms of credibility and reputation but also, very concretely, in that it means it is possible to do direct marketing and advertising for the French public in the form of banners.

Moreover, the existence in France of an authorisation similar to a quality label (open to the French and also to foreign companies on certain conditions) should be able to attract to France trustworthy actors wanting to provide guarantees for their clients and investors and thus create a sound ecosystem respectful of AML/CFT regulations.

Optional in its principle, but mandatory for the most sensitive activities, the innovative regulatory framework proposed by the PACTE Law allows us to consider a residual vulnerability of a **MODERATE** level.

### Risk rating

As a consequence, the combination of the threats and residual vulnerabilities after mitigation measures leads us to select a **MODERATE** risk level for the Digital-Asset Service Provider sector.



## 8.2. TOKEN ISSUERS (ICOs)

### Description of the sector

An Initial Coin Offering (ICO) is a fundraising transaction carried out through a distributed register system (or “blockchain”) and resulting in a token issue. These tokens can then be used to obtain goods or services, as the case may be.

After strong enthusiasm for this type of fundraising in 2016-2018, the number of ICOs effectively carried out fell in 2019. In any case, the amounts involved are very small compared with conventional funding channels.

## Threats and main scenarios of use for purposes of money laundering and/or terrorist financing

ICOs are exposed to the threat relating to their ecosystem: use of the blockchain and of other digital-asset service providers.

However, ICOs are not the main vehicles for money laundering:

- The tokens that can be subscribed to in an ICO can generally only give entitlement to a service or a product ("*utility tokens*");
- They are not very liquid, and are therefore not easily convertible into other digital assets or legal tender;
- There is a very high risk of total loss of the investment due to the relative immaturity of the issuer companies.

For these reasons the threat of money laundering or terrorist financing regarding ICOs is assessed as being **LOW**.

## Vulnerabilities

### Intrinsic vulnerabilities

The vulnerabilities of the ICO sector are also those related to their ecosystem: the use of technologies giving priority to anonymity, and relations that are exclusively at a distance and cross-border (see above).

Accordingly, the intrinsic vulnerabilities of the ICO sector can be considered as of a **HIGH** level.

### Mitigation measures and residual vulnerabilities

The PACTE Law introduced a specific system for initial coin offerings, providing for the possibility of obtaining approval of the AMF, and subjecting those token issuers who want AMF approval to all the applicable regulations regarding AML/CFT.

Thus, before granting its approval, the AMF is responsible for checking, among a number of requirements, that the token issuer has indeed established a system enabling it to comply with its obligations regarding anti-money laundering and combating the financing of terrorism. Unlike DASPs which, as actors, have a long-term obligation, token issuers are subject to AML/CFT obligations only for the duration of the ICO approved by the AMF and within the limits of the transactions with subscribers. For subscriptions of less than €1,000, the regulations do not require that issuers apply vigilance measures with regard to subscribers ("occasional clients" within the meaning of the regulations): however, the AMF recommends that token issuers identify all of their subscribers, whatever the amount of the subscription.

Like the authorisation granted for the performance of certain digital-asset services, approval is optional. Accordingly, only those ICO issuers who have applied for and obtained an AMF approval for their issue are subject to AML/CFT regulations. Issuers not applying for an approval can raise funds via ICOs without applying AML/CFT measures. This new system does not apply to the issue of tokens similar to financial securities (Security Token Offerings, or "STOs").

The approval provides a number of guarantees for subscribers, thereby providing a competitive advantage for issuers wanting to perform an ICO, which should constitute a strong incentive to obtain approval. The AMF will publish the list of ICOs that have obtained its approval.

An examination of the applications received shows that the issuers are often start-ups, which, by definition, are at an early stage of development. Unlike the actors traditionally regulated by the AMF, these young companies do not have the resources required to recruit employees qualified in the area of AML/CFT or enabling them to use external legal advisors. It is therefore stipulated that issuers may outsource all or part of their AML/CFT obligations to specialist external service providers: this possibility is recent and not highly developed. The AMF has also

published on its website the main AML/CFT measures applicable to token issuers, so as to enable these actors to better understand the main obligations incumbent on them.

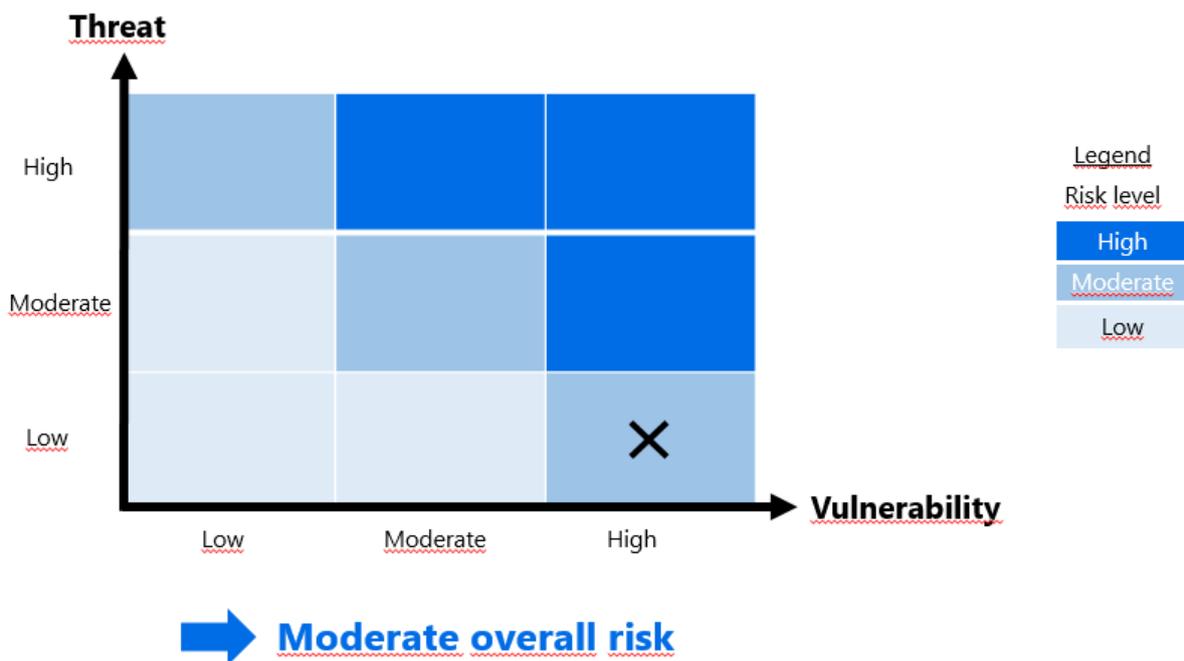
Although applications are currently being investigated, no approval has been granted or refused by the AMF to date, due to the system's novelty.

Although we are not yet able to measure the results of this new system, which is still in the test phase, there are grounds for considering that the vulnerabilities remain **HIGH**.

**Risk rating**

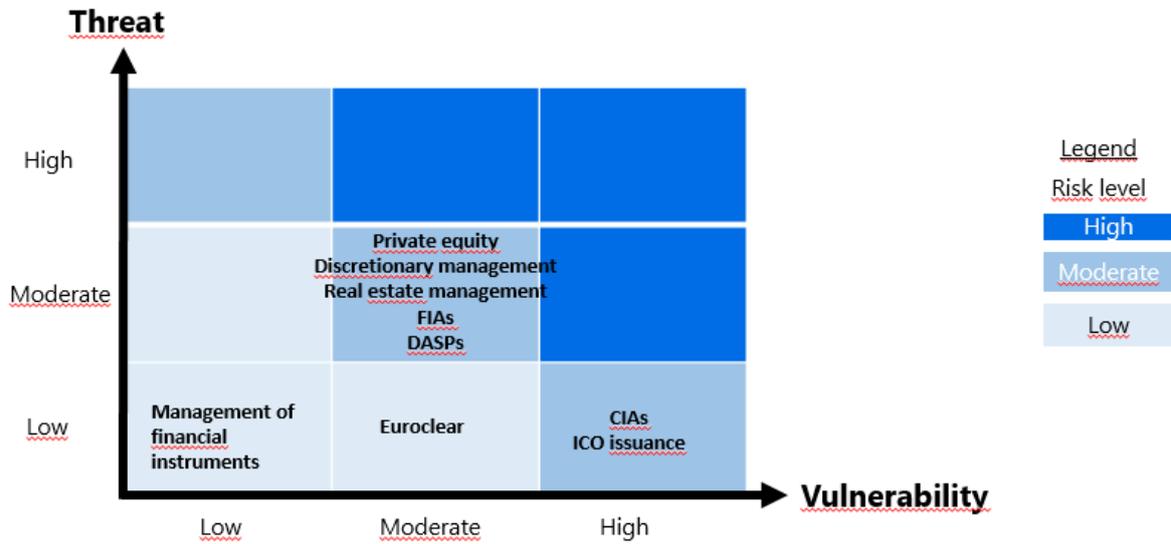
As a consequence, the combination of the threats and residual vulnerabilities after mitigation measures leads us to select a **MODERATE** risk level for the ICO sector.

**ICO issuers**



## 9. RECAP OF THE RATINGS

### AMF financial sector



➔ Moderate overall risk