JUNE 2024

# SECTOR RISK ASSESSMENT ON MONEY LAUNDERING AND TERRORIST FINANCING

amf-france.org

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

Table of contents

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

## SUMMARY


This money laundering and terrorist financing ***(ML/FT)*** sector risk assessment ***(SRA)*** is an update of the SRA published by the *Autorité des Marchés Financiers* ***(AMF)*** in December 2019[1].

It adapts, for the financial undertakings under the jurisdiction of the AMF in terms of anti-money laundering and countering terrorist financing ***(AML/CTF)***[2], the national risk assessment ***(NRA)*** published on 14 February 2023 by the *Conseil d'Orientation de la Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme* (Anti-Money Laundering and Countering Terrorist Financing Steering Committee) ***(COLB)***[3], which follows up on the NRA published by COLB in September 2019[4].

The purpose of this SRA is to help financial institutions under the AMF's AML/CTF jurisdiction to identify and map the risks to which they are exposed. It also helps to inform the AMF's AML/CTF supervisory and monitoring activities as part of its risk-based approach.

In particular, the SRA draws on the main findings of the NRA, the European Commission's supranational risk assessment[5] and the opinion of the European Banking Authority ***(EBA)*** on the ML/TF risks affecting the EU financial sector[6] to identify the main threats to the various services, products and activities of the financial sector, as well as the intrinsic vulnerabilities that may affect them and render them attractive to criminals. It assesses them on the basis of objective indicators, such as feedback from the AMF in terms of inspections and supervision.

The SRA also presents the existing mitigation measures (regulatory framework, AMF awareness-raising and inspection activities, the practices of the organisations concerned and the quality of their AML/CTF system) that make it possible to ascertain the level of residual vulnerability to which the financial organisations under the AMF's jurisdiction are exposed in terms of AML/CTF, reflecting the adaptation of mitigation measures to the intrinsic threats and vulnerabilities that are specific to them.

Finally, by combining the threats and residual vulnerability, the SRA identifies the overall level of risk associated with each sector or product, which is **now assessed using a four-level scale** (low, moderate, high or very high) in line with the NRA, compared with three levels (low, moderate, high) in the previous 2019 SRA.

The SRA first presents a reminder of the objectives set and the methodology used **(Section 1)**, as well as of the regulatory and institutional frameworks **(Section 2)**. It then looks at the cross-cutting issues applicable to the various sectors covered by the AMF's AML/CTF remit, which are in line with the main criminal threats at the root of money laundering identified in the NRA **(Section 3)**. It then details the risks of the main activities of the financial sector for which the AMF is responsible **(Sections 4 to 8)** and concludes with a summary of


[1] AMF, Sector Risk Assessment on Money Laundering and Terrorist Financing, December 2019 (available on the AMF website).
[2] Defined in Article L. 561-36, I, 2° of the Monetary and Financial Code.
[3] COLB, *Analyse nationale des risques de blanchiment de capitaux et de financement du terrorisme*, January 2023 [National money laundering and terrorist financing risk assessment], (available, in French only, on the website of the French Treasury, which provides the secretariat for the COLB).
[4] COLB, *Analyse nationale des risques de blanchiment de capitaux et de financement du terrorisme*, September 2019 [National money laundering and terrorist financing risk assessment], (available, in French only, on the website of the French Treasury, which provides the secretariat for the COLB).
[5] European Commission, Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, 27 October 2022 (COM(2022) 554 final and SWD(2022) 344 final), drawn up on the basis of Article 6 of Directive 2015/849. The European Commission's first supranational risk assessment was published on 26 June 2017, the second on 24 July 2019 and the third on 27 October 2022.
[6] EBA, Opinion on money laundering and terrorist financing risks affecting the EU's financial sector (EBA/Op/2023/08), 13 July 2023. This opinion follows up on the EBA opinion published on 3 March 2021 (EBA/Op/2021/04) and the Joint Opinion of the European Supervisory Authorities on the risks of money laundering and terrorist financing published on 20 February 2017 and 4 October 2019 (JC2019 59).

the overall risk ratings **(Section 9**). It should be emphasised that the AMF's AML/CTF jurisdiction does not include market operators and that this SRA therefore does not deal with the potential money laundering risks associated with the existence of insider networks.

- At the end of 2023, **the asset management sector** was comprised of 700 portfolio asset management companies ***(AMCs)*** representing total assets under management of €4,570bn at the end of 2022. This sector carries out a wide range of activities with varying degrees of exposure to the risks of money laundering ***(*ML*)*** and terrorist financing ***(TF***). The sector risk assessment shows an overall level of risk that is unchanged compared with 2019:
  - **Low** for the 'traditional' management of financial instruments; and
  - **Moderate** for private equity, discretionary management and real estate management.

- At the end of 2023, **the financial investment advisor** ***(FIA***) **sector** comprised 6,707 FIAs providing, in particular, investment advice, advice related to the provision of investment services and advice on the execution of transactions on miscellaneous property as their regular occupation. The SRA reveals a **moderate level of overall risk** for this sector.

- At the end of 2023, **the crowdfunding sector** was comprised of 45 crowdfunding service providers ***(CSPs)*** governed by Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business. Unlike crowdfunding investment advisers (CIAs), who existed under national law before the aforementioned Regulation came into force, CSPs are not currently subject to the AML/CTF obligations[7]. **As a result, this sector has not been rated in this SRA.**

- Among market infrastructures, **central securities depositories (*CSDs*)** and securities settlement system operators fall under the AMF's AML/CTF jurisdiction. In 2023, only one entity is authorized as CSD, for which the SRA shows an overall **low** level of risk, unchanged from 2019.

- In the **field of cryptoassets or digital assets**, the AMF is responsible for the AML/CTF supervision of those digital asset services providers ***(DASPs***) that have been granted optional authorisation by the AMF[8] and of issuers whose initial coin offerings (***ICOs***) have been granted optional approval by the AMF: to date, only one DASP has been authorised, and five ICOs have been approved between December 2019 and February 2024, of which only one approval was still valid on 1 May 2024. For this sector, the SRA shows a **high level of overall risk** for authorised DASPs and ICOs. However, it should be noted that, according to the SRA of the Autorité de Contrôle Prudentiel et de Résolution (ACPR), the competent authority for AML/CTF matters with regard to DASPs exercising one or more of the services referred to in 1) to 4) of Article L. 54-10-2 of the CMF, they present an overall risk that is considered to be **very high**.

[7] With the exception of those carrying out the activity referred to in Article L. 547-4 of the Monetary and Financial Code, which is not currently the case for any CSP.
[8] DASPs subject to mandatory registration are supervised by the ACPR in terms of AML/CTF and are rated in the SRA published by the ACPR.

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

# 1. SECTOR RISK ASSESSMENT OBJECTIVES AND METHODOLOGY

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

The first recommendation of the Financial Action Task Force ***(FATF)***[9] requires States to identify, assess and understand the money laundering ***(ML)*** and terrorist financing ***(TF)*** risks to which they are exposed (***ML/TF risks***). This recommendation has been taken up at European level by the 4th Anti-Money Laundering Directive[10].

The task of drawing up and regularly updating a national risk assessment (**NRA**) has been entrusted to the Steering Committee on the Fight against Money Laundering and Terrorist Financing (Conseil d'Orientation de la Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme - **COLB**)[11].

Thus, the COLB published an NRA on 21 September 2019, as well as an updated NRA in January 2023. This NRA takes into account and is in line with the supranational risk assessments drawn up by the European Commission[12] in application of the 4th Anti-Money Laundering Directive[13], as well as with the opinions on the ML/TF risks affecting the Union's financial sector, drawn up by the European supervisory authorities ***(ESAs)***[14] and later the European Banking Authority ***(EBA)***[15] in application of the aforementioned Directive[16].

As the national authority responsible for oversight of part of the financial sector, the *Autorité des Marchés Financiers* (***AMF***) is also required to contribute to the objective of a better understanding of the ML/TF risks to which the entities under its supervision are exposed. Thus, the AMF published an initial sector risk assessment ***(SRA)*** in December 2019[17].

Compliance with the requirement of having a better understanding of ML/TF risks imposed by the FATF's first recommendation was examined in depth by the FATF as part of its mutual evaluation of France, which was completed in May 2022. As stated in the FATF's mutual evaluation report on France, "*France has a good and very good understanding of the risks regarding* [money laundering] *and* [terrorist financing] *respectively, as reflected in the 2019 national risk assessment (NRA*) [...] *and certain sectoral risk analyses (SRAs)*"[18].

The 4th Anti-Money Laundering Directive[19] and the national provisions require that ML/TF risk assessments are regularly updated[20].

The purpose of this update to the AMF's sector risk assessment is to ensure an up-to-date identification, assessment and understanding of the ML/TF risks to which entities under the AMF's supervision are exposed, by sharing within the financial sector an overview of the ways in which these different risks materialise, their level and the objectives to be pursued within each sector and sub-sector.

---

[9] International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF Recommendations adopted by the FATF Plenary in February 2012 and updated in March 2022, available on the FATF website.

[10] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, as amended by Directives (EU) 2018/843 of 30 May 2018 and (EU) 2019/2177 of 18 December 2019 (the '***4th Anti-Money Laundering Directive***'), Article 7.

[11] Monetary and Financial Code, Articles D. 561-51 et seq.

[12] Reports from the Commission to the European Parliament and the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities (COM(2017) 340 final, June 2017; COM/2019/370 final, July 2019; COM(2022) 554 final, October 2022).

[13] Directive (EU) 2015/849, Article 6.

[14] Joint Opinion of the European Supervisory Authorities on the risks of money laundering and terrorist financing affecting the European Union's financial sector, JC2019 59, 4 October 2019.

[15] Opinion of the European Banking Authority on the risks of money laundering and terrorist financing affecting the EU's financial sector, EBA/Op/2023/08, 13 July 2023.

[16] Directive (EU) 2015/849, Article 6(5).

[17] AMF, Sector Risk Assessment on Money Laundering and Terrorist Financing, December 2019.

[18] FATF, Mutual Evaluation Report on France, 2022, summary, § 7.

[19] Directive (EU) 2015/849, Article 6(5): the EBA must therefore issue an opinion on ML/TF risks every two years.

[20] Monetary and Financial Code, Article D. 561-51, 4°, stating in particular that the COLB's purpose is *"to draw up and regularly update a national risk assessment".*

This sector risk assessment is intended:

- upstream, to adapt and feed into future thinking at the national level, within COLB;
- downstream, to support the entities supervised by the AMF in terms of AML/CTF, who will be able to adopt it and tailor it more effectively to their area of activity and business model, in their internal procedures and documents.

Finally, this SRA should also serve as a tool for the AMF to implement the risk-based approach on which its monitoring and inspection actions are based, in accordance with the requirements set out in the 4th AML Directive[21] and the EBA's guidelines on risk-based supervision for AML/CTF[22], with which the AMF complies[23].

Supervised entities may also usefully refer to the NRA, as well as to the sector risk assessment of the ACPR[24].

These documents provide guidance but do not replace the more detailed assessments that AML/CTF obliged entities are required to carry out, taking into account supranational and national risk assessments[25].

The overall ratings given by this SRA for a sub-sector do not preclude the distinction of different levels of risk when assessments are conducted at a more detailed level (for example, at the level of an operator or a product). This document endeavours to include the factors to be considered to this end.

However, an organisation may consider that an activity it conducts presents a level of inherent risk different from that assigned in the NRA or SRA, for example on account of the specific characteristics of the products it offers or its clients, in accordance with the risk-based approach. Consequently, with the exception of cases where applicable regulation require a high level of risk to be acknowledged, an organisation may, subject to justifying it by means of its own assessment, adopt a lower level of risk than the NRA or SRA. Symmetrically, the risk analysis specific to each organisation may also lead to a higher level of risk than that retained in the NRA or SRA.

[21] Directive 2015/849, Article 48.
[22] EBA, 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 under Article 48(10) of Directive (EU) 2015/849, amending the Joint Guidelines ESAs/2016/72 (EBA/GL/2021/16, 16 December 2021).
[23] AMF, Position DOC-2022-02.
[24] ACPR, *Analyse sectorielle des risques de blanchiment de capitaux et de financement du terrorisme en France*, published in December 2019 and updated on 29 June 2023 [Money Laundering and Terrorist Financing Sector Risk Assessment, only available in French] .
[25] Monetary and Financial Code, Article L. 561-4-1.

### 1.2. SOURCES USED

In order to carry out this risk assessment, the AMF used:

- the key figures for asset management in 2022, published in January 2024[26];
- the key figures for FIAs in 2022, published in December 2023[27];
- data collected in September 2023 in response to the anti-money laundering and countering terrorist financing questionnaire sent to asset management companies ***(AMCs***);
- the annual internal audit reports for AML/CTF (***RACI***) for 2022, submitted to the AMF at the end of April 2023[28];
- data contained in the annual fact sheets for the 2022 financial year, submitted to the AMF by AMCs in May 2023[29];
- the data in the annual fact sheets submitted to the AMF by FIAs for the 2022 financial year[30];
- the results of desk-based checks and on-site inspections carried out by the AMF.

Account was also taken of the reports published by the French financial intelligence unit (***FIU***), Tracfin, in particular the annual activity and analysis reports[31], certain information letters[32], and information communicated between Tracfin and the AMF under existing provisions[33].

Finally, this SRA naturally takes into account the supranational risk assessment produced by the European Commission[34] and the EBA's opinion on the ML/TF risks affecting the EU financial sector[35], as well as the NRA and the SRA of the ACPR.

### 1.3. METHODOLOGY

This SRA has been prepared using a methodology similar to that used for the NRA, of which it is one of the sector-specific versions. The NRA, drawn up in collaboration within the COLB, uses the methodology and principles defined by the FATF, which in particular require an analysis combining both threats and vulnerabilities in order to ascertain an overall level of risk. In this context:

- ML/TF **threats** are activities that could result in money laundering or terrorist financing offences, whether domestic or cross-border;
- **vulnerabilities** include factors that make it attractive to commit an infringement and the related money laundering or terrorist financing operation. In particular, they result from the practices and characteristics of the products used in a given sector of activity and make it possible to identify the areas, systems, factors and specific features of each sector or product that may lead to misappropriation for money laundering or terrorist financing purposes.

The **threat assessment** was based on the available quantitative data (sector size, number of reports) and a qualitative assessment of the ML/TF scenarios identified by the AMF or Tracfin.

---

[26] AMF, *Chiffres clés 2022 de la gestion d'actifs*, January 2024 [Key Figures for Asset Management 2022, only available in French].

[27] AMF, *Chiffres clés 2022 des conseillers en investissements financiers*, December 2023 [Key Figures for Financial Investment Advisors 2022].

[28] In accordance with the provisions of Articles 320-20, 8° and 321-147, 8° of the AMF General Regulation.

[29] In accordance with the provisions of Articles 318-37 and 321-75 of the AMF General Regulation.

[30] In accordance with the provisions of Articles 325-21, II and 325-42, II of the AMF General Regulation.

[31] In particular, its 2022 annual report, comprising three volumes: *AML/CFT: reporting entities activity - 2022 review* (Volume 1, published in May 2023), *Tracfin's activity in 2022* (Volume 2, published in July 2023) and *LCB-FT : état de la menace* [AML/CFT: State of the threat, only available in French] (Volume 3, published in October 2023), as well as Volume 1 of the annual activity report for 2023 (*LCB-FT : activité des professions déclarantes - Bilan 2023*), published in April 2024, [AML/CFT: reporting entities activity - 2023 review, only available in French].

[32] TRACFIN, AML/CTF industry newsletter, No. 20 of March 2022 on digital asset service providers.

[33] Monetary and Financial Code, Articles L. 561-27 *et seq.*

[34] Report from the Commission to the European Parliament and the Council on the assessment of risks of money laundering and terrorist financing risks affecting the internal market and related to cross-border activities (COM(2022) 554 final, 27 October 2022).

[35] Opinion of the European Banking Authority on the risks of money laundering and terrorist financing affecting the EU's financial sector, EBA/Op/2023/08, 13 July 2023.

Based on this assessment, **the exposure of each product or sector to the threat** has been **rated as one of four levels** (low, moderate, high or very high exposure). In order to ensure greater granularity and precision, and in line with the recommendations made by the COLB as part of its monitoring of the updating of sector and national risk assessments, **a four-level rating has been chosen** instead of the previous three-level rating used in the previous NRAs and SRAs published in 2019, making it possible, in particular, to avoid excessive recourse to categorisation in the 'moderate' tier.

**Vulnerabilities** were also assessed using a quantitative and qualitative assessment aimed at evaluating, for each product, service or operation, how its intrinsic characteristics could make it vulnerable to the threat of ML or FT. Vulnerability factors include:

- the potential for anonymity offered by the product or sector in question;
- the possibility of opacifying the transaction;
- the cross-border dimension;
- the complexity of the product; or
- sensitivity to document fraud.

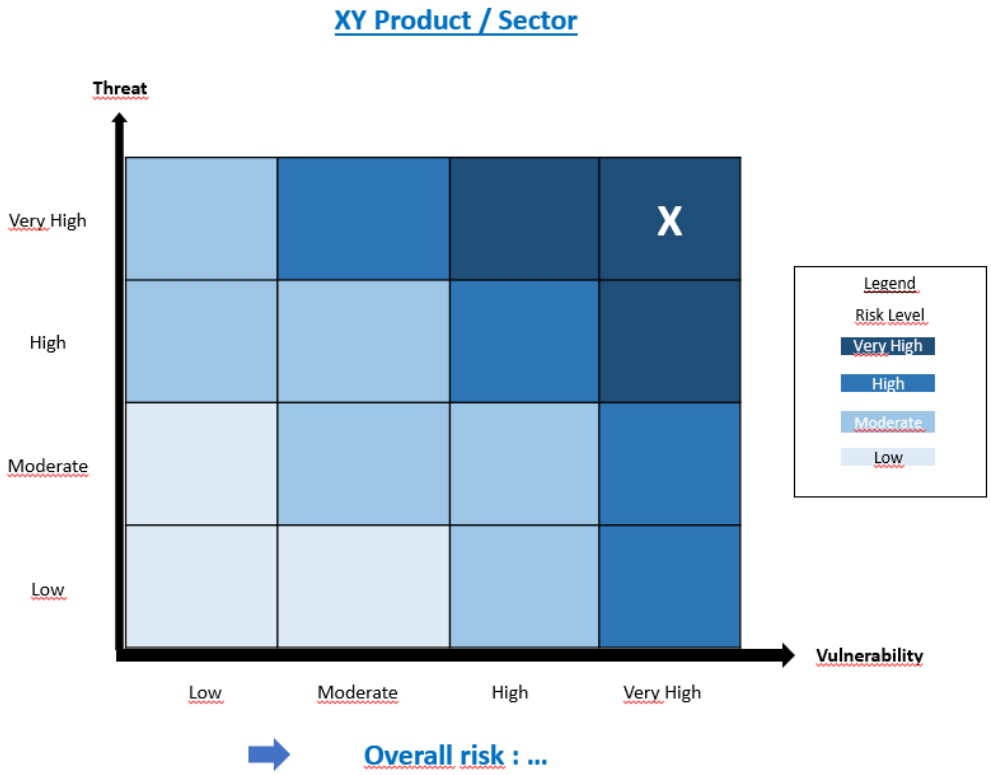
The adaptation of the mitigation measures to the threats and these 'natural' or 'intrinsic' vulnerabilities leads to the definition of a level of '**residual vulnerability**', presented for each product, service or operation, according to a four-level rating. This level of residual vulnerability takes into account the AMF's assessment of the following mitigation measures:

- the mitigation measures provided for by the AML/CFT regulations;
- the mitigation measures provided for by the law other than the AML/CTF regulations[36];
- the AMF's supervisory and awareness-raising activities;
- organisations' good practices, as identified by the AMF.

In this context, particular consideration is taken of the AMF's assessment of the quality of the AML/CTF framework of the obliged institutions, which is based on all available information (responses to annual AML/CTF questionnaires, annual AML/CTF internal audit reports, information sent to Tracfin, reports received, interviews, thematic reviews, inspections and on-site visits).

The combination of these threats and vulnerabilities, allows for the identification of the level of risk associated with each sector or product. At the end of this document, a grid comparing threat and residual vulnerability is used to summarise the **overall risk** level in the sector associated with each activity analysed, according to a four-level rating system, an example of which is shown below:

[36] For example: conditions for authorisation, obligations relating to organisation and good conduct, obligations relating to anti-tax evasion and fraud, etc.




Identifying a level of risk for the sectors or products identified does not mean that all the professionals involved are likely to commit money laundering or terrorist financing infringements. On the contrary, they are on the front line of ensuring that their profession is as exemplary and immune as possible to these criminal acts. The purpose of this analysis is to refine knowledge of the risks such that vigilance can be as effective as possible. As indicated above, it is intended as a guide and in no way replaces the more detailed assessments that the professionals subject to AML-CTF obligations must carry out.

Both the national assessment and this sector assessment endeavour to include the factors that the professionals subject to AML-CTF obligations must consider in order to conduct their own risk assessment. The intention is therefore not for these organisations to adopt the national and sectoral assessments as they stand, but for these assessments to feed into their own risk classification.

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

## 2.1. REGULATORY FRAMEWORK: EUROPEAN DIRECTIVES

France has played an active role in drafting the European AML/CTF legislation. The 4th Anti-Money Laundering Directive was transposed into French law by Order No. 2016-1635 of 1 December 2016[37], Decree No. 2017-1094 of 12 June 2017[38] and Decree No. 2018-284 of 18 April 2018[39].

The 5th Anti-Money Laundering Directive[40], which amends the 4th Anti-Money Laundering Directive, is also the result of an initiative led by France to make the European AML/CTF system more effective in the wake of the 2015 attacks. During the negotiations, France supported the **strengthening of transparency obligations relating to the register of beneficial owners** and the creation in all Member States of a **registry of bank accounts** making it possible to identify their holders, agents and beneficial owners. In addition, the 5th Anti-Money Laundering Directive **includes the digital assets sector in the scope of AML/CTF obliged entities** and strengthens the **additional due diligence measures to be carried out by obliged entities with regard to high-risk third countries**.

It came into force on 10 July 2018, and had to be transposed by 10 January 2020[41].

Law No. 2019-486 of 22 May 2019, known as '**PACTE'**[42], supplemented by two decrees[43], transposed its provisions relating to digital assets and authorised the Government to adopt the remaining necessary provisions by means of an order. Order No. 2020-115 of 12 February 2020 strengthening the national anti-money laundering and countering terrorist financing system, supplemented by two decrees[44], was thus adopted to finalise the transposition of the 5th Anti-Money Laundering Directive.

Under these provisions, AML/CTF obliged entities are subject to specific and material obligations, set out in Book V, Title VI, Chapters I and II of the Monetary and Financial Code, in order to prevent ML/TF risks. The main obligations entail:

- the implementation of robust organisation and internal control procedures capable of assessing risks and countering money laundering and terrorist financing;
- vigilance with regard to clients, whose identity must be ascertained and verified, as well as with regard to the beneficial owner(s);
- the application of enhanced and additional client and beneficial owner due diligence measures in the event of heightened risk factors (high-risk country, remote relationships, politically exposed persons ***(PEPs)***, etc.);
- the obligation to send suspicious transaction reports ***(STRs)*** to Tracfin, in order to flag up any suspicion transaction, failing which they may be held liable;
- the obligation to implement and comply with UN, European and national asset freezes;
- document retention.

The AML/CTF obligations are adapted according to the risk of the transaction. Enhanced due diligence obligations must therefore be implemented when the risk is deemed to be high, either by the legislator or by the obliged entity as a result of its own risk assessment. Conversely, simplified due diligence measures are permitted when the risk is considered to be low, either by the obliged entity itself or by the legislator.

---

[37] Order No. 2016-1635 of 1 December 2016 strengthening the French anti-money laundering and countering terrorist financing system.
[38] Decree No. 2017-1094 of 12 June 2017 on the register of beneficial owners of legal entities and legal constructions.
[39] Decree No. 2018-284 of 18 April 2018 strengthening the French anti-money laundering and countering terrorist financing system.
[40] 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 purpose of money laundering or terrorist financing and Directives 2009/138/EC and 2013/36/EU (the '**5th Anti-Money Laundering Directive'**).
[41] Directive (EU) 2018/843, Articles 4 and 5.
Law No. 2019-486 of 22 May 2019 on the growth and transformation of undertakings.
[43] Decree No. 2019-1213 of 21 November 2019 on digital asset services providers; Decree No. 2019-1248 of 28 November 2019 on the deadline for examining applications for the registration and authorisation of digital asset services providers.
[44] Decrees Nos 2020-118 and 2020-119 of 12 February 2020 strengthening the national anti-money laundering and countering terrorist financing system.

The AMF has incorporated the relevant provisions into its General Regulation in order to clarify the obligations of AMCs[45], CSDs[46], FIAs[47] and DASPs[48].

The AMF and the *Autorité de Contrôle Prudentiel et de Résolution* monitor obliged professionals' compliance with all the obligations to which they are subject, and jointly contribute to reducing these risks through the expertise of their staff.

### 2.2. INSTITUTIONAL FRAMEWORK: AML/CTF SUPERVISION OF THE FINANCIAL SECTOR SHARED BETWEEN THE AMF AND THE ACPR

Entities belonging to the financial sector are subject to the supervision and sanctioning powers of the ACPR[49] and the AMF[50].

In particular, the AMF is responsible for the AML-CTF supervision of[51]:

- 12,379 collective investment undertaking ***(CIUs)***;
- 700 AMCs;
- 6,707 FIAs;
- 1 DASP: Euroclear France;
- 1 digital asset services provider ***(DASP)***[52] which applied for and obtained optional authorisation;
- 5 digital token issuers whose offer has been approved by the AMF. As at the date of publication of the French version of this SRA, only one issuer had a current approval for its offer[53].

The AMF's AML/CTF jurisdiction may also apply to crowdfunding service provider **(CSPs**) in respect of their activities referred to in Article L. 547-4 of the Monetary and Financial Code only. However, as at 31 December 2023, no CSP was engaged in this activity.

'Registered' DASPs, i.e. those providing the digital services referred to in Article L. 54-10-2, 1° to 4° of the CMF[54] and, as such, subject to mandatory registration with the AMF, are supervised by the ACPR as regards compliance with the applicable AML-CTF obligations. As at 31 December 2023, 107 DASPs had been registered and not delisted.

The AMF ensures that the preventive AML/CTF rules are effectively implemented by the professionals under its supervision through ongoing supervision, both before they start business (notably as part of the authorisation process, and through checks on the good repute of managers and shareholders in the case of certain market participants under its supervision) and throughout their professional activity (monitoring). Its supervisory action follows a risk-based approach, in accordance with the EBA Guidelines on the characteristics of a risk-based approach to AML/CTF supervision, with which the AMF complies[55].

---

[45] AMF General Regulation, Articles 320-13 et seq. and 321-141-A et seq.
[46] AMF General Regulation, Article 560-9 et seq.
[47] AMF General Regulation, Articles 321-141, and 321-143 to 321-150 (with the exception of the provisions of Article 321-147 8° and 9°, and Article 321-149), in accordance with Article 325-22.
[48] AMF General Regulation, Article 721-1 et seq.
[49] Monetary and Financial Code, Article L. 561-36, I, 1°.
[50] Monetary and Financial Code, Article L. 561-36, I, 2°.
[51] Based on data as at 31 December 2023, presented in the AMF's 2023 Annual Report.
[52] AMF, List of authorised DASPs.
[53] AMF, List of Initial Coin Offering that have received the AMF approval, drawn up in accordance with Article 713-3 of the AMF General Regulation (as at 2 April 2024). This approval expired on 30 June 2024.
[54] Namely: 1° The service of custody of digital assets on behalf of third parties or providing access to digital assets, where applicable in the form of private cryptographic keys, with a view to holding, storing and transferring digital assets; 2° The service of buying or selling digital assets against legal tender; 3° The service of trading digital assets for other digital assets; 4° The operation of a digital asset trading platform.
[55] EBA, 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 under Article 48(10) of Directive (EU) 2015/849, amending the Joint Guidelines ESAs/2016/72 (EBA/GL/2021/16, 16 December 2021); AMF, Position DOC-2022-02.

Other financial sector professionals are subject to the AML/CTF powers of desk-based checks and on-site inspections, administrative policing and sanction by the ACPR[56].

# 3. MAIN THREATS AFFECTING THE FINANCIAL SERVICES SECTOR

## 3.1. THREATS IDENTIFIED AT THE NATIONAL LEVEL

As indicated by the COLB in the National Risk Assessment published in 2023, fraud (tax, social security and customs), drug trafficking and scams are among the main threats to which France is exposed[57]. This observation is corroborated by Tracfin, which notes that the laundering of the proceeds of scams is one of the main money laundering threats in France[58]. The AMF's inspections, particularly of FIAs marketing atypical products, also confirm this assessment.

### 3.1.1. Fraud and scams

The AMF plays its part in countering these threats through (i) oversight of the marketing practices for so-called atypical or unauthorised products, which may be employed by financial investment advisors under its supervision, and (ii) issuing alerts or warnings on its own website about the websites or individuals identified.

#### Marketing of atypical or unauthorised products by financial investment advisors (FIAs)

The AMF supervises and monitors FIAs using a risk-based approach, focusing in particular on the marketing of atypical products with a high risk of inappropriate marketing, as well as products that are not authorised for marketing in France.

In this context, the inspections of FIAs have brought to light scams involving certain atypical products (hotel products, real estate products, car parks, forests[59]) or the marketing by FIAs of products (miscellaneous assets or alternative investment funds) not authorised for marketing in France.

Working with the Banque de France, the AMF has drawn up an increasingly precise map of atypical products in France. These are characterised by:

- promises of high returns, often combined with guarantee mechanisms or promises of liquidity that are inconsistent with the nature of the investment vehicle (e.g. unlisted shares or equities);
- atypical underlying assets for mass-marketed products (see below - teak forests, hotels);
- atypical structures (e.g. investments in equity securities issued by structures of a different nationality to that of the underlying assets);
- the final destination of the funds is difficult to identify, or even opaque;
- schemes promising tax relief[60].

Through its FIA awareness raising and supervision activities, the AMF contributes to countering scams and fraud, which have been identified as threats at the national level.

[56] Monetary and Financial Code, Article L. 561-36-1. This applies in particular to credit institutions, payment institutions, electronic money institutions, investment firms, market undertakings, intermediaries in banking transactions and payment services, crowdfunding intermediaries and DASPs subject to compulsory registration that provide the services of custody of digital assets on behalf of third parties, the purchase and sale of digital assets against legal tender, trading digital assets for other digital assets or the operation of a digital asset trading platform.
[57] NRA 2023: *"In terms of money laundering, France is exposed to three major threats: fraud (tax, social security and customs), drug trafficking, and scams and theft."*
[58] TRACFIN, Operations and Analysis Report 2021.
[59] At the end of 2016, the AMF inspected and sanctioned an FIA for a regulatory breach of their professional obligations in the marketing of shares in a Panamanian company: 27 FIA clients invested a total of €1,047,735 by subscribing to an offer based on misleading information.
[60] Marketing of products that are similar to so-called 'Girardin', 'TEPA' or 'Dutreuil' products, but which do not meet the legal requirements for these.

Case 'A'

Between 2017 and 2018, an FIA marketed, for a total of €840,000, shares in partnerships limited by shares (*sociétés en commandite par actions*), which are classified as alternative investment funds ***(AIFs)*** and whose corporate purpose was to form and grow a portfolio of real estate assets through life annuity purchases, even though their marketing in France had not been authorised. The AMF Enforcement Committee fined this FIA in 2022 for breach of its professional obligations.

Other FIAs have also been inspected and sanctioned for marketing these products.

In a letter sent to FIA industry groups on 22 April 2022, and widely taken up by them, the AMF reminded FIAs of their professional obligations when issuing investment recommendations to their clients. The AMF has also published a news on its website reminding FIAs of their obligations regarding the marketing of AIFs[61].

### Monitoring fraudulent advertising and commercial practices[62]

The AMF and the ACPR work in collaboration, within a Joint Unit for Insurance, Banking and Retail Investment, on monitoring market participants that are not authorised to market their products or services in France, in order to alert the public to any fraudulent or dubious activities detected.

As part of this monitoring activity, an increase in financial scams has been observed in particular, mainly in the form of fake savings accounts, loans or financial investments, with an upsurge in identity or website theft.

The AMF and the ACPR regularly publish (particularly on the '*Assurance Banque Epargne Info Service*' ***(ABEIS)*** website[63]) alerts and warnings about the activities of market participants proposing investments in France, which are not authorised to do so in France, especially in Forex, digital assets or derivatives on cryptoassets, and continue to add to their blacklists of websites or entities not authorised to make offers to the public[64]. This and other information designed to inform investors and protect them against potential scams is also available on a dedicated website: *AMF Protect Epargne*[65].

Between 1 January and 31 December 2022, as part of their cooperation under the Joint Unit dedicated to this activity, the AMF and the ACPR added more than 1,320 names of unauthorised websites or market participants to one of the five blacklists published on the ABEIS website[66]. By the end of March 2024, over 1,400 names of unauthorised websites or market participants appeared on the AMF's four blacklists[67].

In response to the growth in websites offering **investments in cryptoassets**, a list, specifically naming websites offering cryptoasset derivatives without complying with the current regulations, was created in July 2018. The creation of this list stems from the AMF's assessment that platforms offering cash-settled derivatives on cryptoassets must comply with the regulations applicable to financial instruments. This assumes that platforms providing contracts for difference **(CFDs)** on cryptoassets, for example, are authorised as investment services providers. At the end of March 2024, 168 websites were on this list (excluding identity theft). More generally, the AMF draws up a list of market participants that appear on its blacklists, or have been the subject of a warning published by the AMF and/or are impersonating a regulated market

[61] AMF, 22 April 2022, *Obligations en matière de commercialisation des FIA par les CIF* [FIAs' obligations in terms of AIF marketing, only available in French].
[62] Excerpts from the ACPR and AMF Joint Unit for Insurance, Banking and Retail Investment 2022 Annual Activity Report, published in June 2023.
[63] https://www.abe-infoservice.fr/ [in French].
[64] https://www.amf-france.org/en/warnings/blacklists The AMF website thus provides the public with (i) four blacklists of persons or entities providing services or offering investments in binary options (332 listed), derivatives on cryptoassets (169 listed), miscellaneous property (404 listed) and foreign exchange (361 listed) respectively, (ii) a list of market participants who have been the subject of a warning published by the AMF and (iii) a list of market participants impersonating a regulated market participant (1,364 listed) (figures as at 29 April 2024).
[65] https://protectepargne.amf-france.org/ [in French].
[66] Concerning, respectively, offers of (i) loans, savings accounts, payment services or insurance policies, (ii) investments in Forex (foreign exchange market), (iii) derivatives on cryptoassets, (iv) binary options and (v) investments in miscellaneous property (diamonds, wine, cryptoassets).
[67] Concerning the offers referred in points (ii) to (v) above and excluding identity theft.

participant. Some sixty market participants or websites offering services based on digital assets without complying with the applicable provisions are included on this list.

### The risk of identity theft

The increase in digitalisation, leading in particular to the growth in relationships entered into remotely, constitutes a vulnerability that can be exploited for money laundering purposes, particularly as a result of fraud. This context is conducive to the growth of identity theft, whether at the level of the regulated professionals themselves or of the people with whom they are likely to establish business relations.

The AMF continues to observe that many platforms and websites fraudulently use the name or contact details of duly authorised or registered financial institutions, deliberately creating confusion that is detrimental to retail investors. To this end, it identifies cases, and publishes those of which it is aware through blacklists. At the end of March 2024, more than 934 names of fraudulent or dubious websites or players had been listed[68]. The AMF also regularly issues communications, where appropriate in conjunction with the ACPR, to warn the public against such practices[69]. Finally, the AMF's identity may also be stolen, which can likewise be a factor in misleading investors. To this end, it informs the public by means of press releases or dedicated blacklists[70 &71].

Professionals are obliged to increase their vigilance with regard to these risks of identity fraud on the Internet. The public is also encouraged to be extremely vigilant with regard to offers presented as risk-free, and in particular those offering yields well above what is usually offered by the market[72].

In addition, the growth in digitisation means that regulated players face increased risks in identifying and verifying the identity of their clients, as the increased use of new technologies and remote business relationships are likely to facilitate the misappropriation or falsification of the identity documents produced. In response, risk mitigation measures are being implemented at the European and national level[73]. The introduction of a digital identity in France and the use of remote identity verification service providers ***(PVID)***, five of which are now certified by the *Agence Nationale de la Sécurité des Systèmes d'Information (**ANSSI**)*[74], are helping to reduce these risks.

### 3.1.2. Tax fraud

With a developed economy that is open to international trade, France is particularly exposed to the threats related to tax fraud. Tax fraud, as defined by Article 1741 of the General Tax Code, consists of evading or attempting to evade tax by any means.

Although there is no exact measure of tax fraud, in 2022 the financial implications estimated in Tracfin's notes and analyses in terms of anti-tax, social security and customs evasion amounted to €1.5bn. In addition, in 2022, on-site tax inspections, mainly of firms, resulted in the recovery of €8.8bn in duties and penalties[75]. There are two main types of tax fraud:

- tax fraud involving commercial companies, mainly focusing on VAT and corporation tax, or even the taxation of dividends ('CumCum' and 'Cum-Ex' schemes);

[68] Blacklists of entities not authorised to offer financial products or services in France, accessible on the data.gouv.fr website [in French].
[69] AMF, press releases dated 29 September 2023 or 4 April 2024.
[70] AMF, press release dated 12 January 2023: The AMF warns the public about calls from fraudsters claiming to help recover funds.
[71] AMF, blacklist, AMF usurpation category.
[72] The AMF publishes very frequent warnings on its website for both the public and professionals.
[73] EBA Guidelines on the use of Remote Customer Onboarding Solutions (EBA/GL/2022/15), with which the AMF complies (AMF, Position DOC-2023-07).
[74] https://cyber.gouv.fr/en/actualites/publication-requirement-rule-set-remote-identity-verification-service-providers.
[75] Ministry for the Economy, Finance and Industrial and Digital Sovereignty, *Bilan de la lutte contre la fraude fiscale, douanière et sociale: une année record, les chiffres-clés de l'année 2022* [Assessment of anti-tax, customs and social security evasion: a record year, the key figures for 2022], press release dated 23 February 2023.

- tax fraud involving private individuals: this mainly concerns income tax, real estate wealth tax, and inheritance or transfer tax. Tax fraud entailing the concealment of assets abroad involves high net worth individuals in particular.

The growing exchange of information on tax matters between the authorities of different countries, which is based in part on information transmitted by AML/CTF obliged entities through the internal control systems they have put in place to identify clients, accounts and individuals in the context of countering tax evasion and fraud[76], increases the risk of sanctions linked to international tax fraud and helps to mitigate this threat.

### 3.1.3. Other threats

Some emerging or growing threats have also been the subject of specific reports. This is particularly true of the financing of proliferation and breaches of probity.

#### Proliferation financing

Proliferation financing is understood to mean the provision of financial or economic resources to entities contributing to the development of weapons of mass destruction ***(WMD)*** and includes dual-use goods and technologies used for non-legitimate purposes[77]. This financing can take several forms:

- direct financing entails the provision of funds or economic resources that can contribute directly to the development of the capabilities of a WMD programme (acquisition of a dual-use item useful in the development of a WMD, financing of a proliferating entity or state, etc.). France remains relatively unexposed to the risk of the direct financing of proliferation programmes, as all financial flows involving natural persons and legal entities from countries under international sanctions are closely monitored;
- indirect financing entails the provision of funds or economic resources that may contribute indirectly to proliferation through the interposition of a person, entity and/or State that maintains links with actors involved in WMD programmes (intermediaries and shell companies, for example).

In order to assess the threat and the level of residual risk in this area, a national risk assessment specifically dedicated to proliferation financing[78] was drawn up jointly by the COLB and the *Secrétariat Général de la Défense et de la Sécurité Nationale* ***(SGDSN)*** through the mobilisation of all the COLB stakeholders, French administrations and regulatory authorities involved in the fight against proliferation financing, as well as the private sector, which was consulted.

Following consultation with industry groups representing some of the private sector players that fall under the AMF's remit[79], all the organisations consulted considered the sector's exposure to the threat of proliferation financing to be low.

Finally, the national assessment of proliferation financing risks reveals the following with regard to the banking and financial sector: *"In the light of its specific characteristics (strong attractiveness due to French technological know-how, international integration, varied banking and financial products), it emerges from the expertise of the competent administrations and supervisory authorities that the banking and financial services sector presents* ***moderate intrinsic vulnerabilities****. Despite the vulnerabilities identified, banking and financial services guarantee a high level of traceability of fund movements and effective customer identification. […] The* ***residual vulnerability*** [of the banking and financial sector, after taking mitigation measures into account] *is considered to be* ***low***".

[76] Monetary and Financial Code, Article L. 564-2.
[77] The FATF guidance published in June 2021 on proliferation financing risk assessment and mitigation defines proliferation financing as: "*the risk of raising, moving, or making available funds, other assets or other economic resources, or financing, in whole or in part, to persons or entities for purposes of WMD proliferation, including the proliferation of their means of delivery or related materials (including both dual-use technologies and dual-use goods for non-legitimate purposes)*".
[78] *Analyse nationale des risques de financement de la prolifération* (NRA-FP), July 2022 [National proliferation financing risk assessment, only available in French].
[79] AMCs and FIAs.

### Probity breaches and corruption

Probity breaches refer to the regulatory breaches of the duty of probity identified in the Criminal Code: corruption, influence peddling, unlawful taking of an interest, misappropriation of public funds and favouritism.

The French Anti-Corruption Agency ***(AFA)***, a service with national competence created in 2016 and placed under the authority of the Minister of Justice and the Minister for the Budget, assists the competent authorities and those who come into contact with them to prevent and detect corruption, influence peddling, unlawful taking of an interest, misappropriation of public funds and favouritism. In November 2022, it published a national assessment of the risk of corruption[80], which shows that in France, in 2021, 800 offences of violation of probity were recorded by the police and gendarmerie. Between 2016 and 2021, these infringements increased by 28%, an average of 5% per year. The increase in probity breaches is linked in particular to corruption infringements (+46% over the period).

The AFA has also published recommendations, the latest version of which dates from January 2021, designed to help both public and private players to prevent and detect probity breaches, which are primary infringements whose proceeds can then give rise to money laundering operations.

Among these recommendations, the assessment of the integrity of the third parties recommended by the AFA can be taken into account in the implementation by obliged actors of their Know Your Client obligations, as set out in the Monetary and Financial Code.

The analyses and documents produced by the AFA are also useful for obliged actors insofar as they make it possible to identify certain roles exposed to risks of passive corruption: although these roles do not fall under the definition of politically exposed persons ***(PEPs***) as such, and therefore under the automatic application of the enhanced due diligence provided for by the regulations, they present a higher degree of risk, which varies according to the circumstances (nature of the functions, products, etc.)[81].

## 3.2. THREATS IDENTIFIED AT THE EUROPEAN LEVEL

In its latest opinion on the risks affecting the European Union's financial sector[82], the EBA identified the following cross-sectoral risks in particular:

- crypto assets;
- the new 'Fintech' and 'Regtech' technologies;
- terrorist financing;
- the risks associated with Brexit;
- 'de-risking': a practice whereby obliged firms terminate or restrict their business relationships with clients or categories of clients in order to avoid, rather than manage risk, in accordance with the FATF's risk-based approach, encouraging them to turn to unregulated financing channels where appropriate;
- legislative differences between Member States;
- differences in supervisory practices;
- crowdfunding platforms;
- tax infringements.

[80] AFA, *1ère étude statistique sur les atteintes à la probité enregistrées par la police et la gendarmerie*, November 2022 [1st statistical study of violations of probity recorded by the police and gendarmerie, only available in French].
[81] AFA, *1ère étude statistique sur les atteintes à la probité enregistrées par la police et la gendarmerie*, November 2022 [1st statistical study of violations of probity recorded by the police and gendarmerie, only available in French].
[82] Opinion of the European Banking Authority on the risks of money laundering and terrorist financing affecting the European Union's financial sector, EBA/Op/2023/08.

In terms of AML-CTF, the majority of obliged players (with the exception of FIAs) use **technological solutions and other external databases provided by Fintech and Regtech**[83], which are experiencing strong growth in France, mainly to 'filter' their clients and trace transactions involving digital assets. A few names of service providers and/or solutions arise repeatedly.

This possible concentration of the data market raises questions about:

- the quality of the data used;
- the lack of intellectual and personalised analysis;
- the intensification of de-risking.

The risk associated with Fintech and Regtech has therefore been clearly identified within the French financial sector, although it is not considered to be material.

According to data collected from AMCs, the practice of **de-risking** referred to by the EBA[84] is a reality in France. AMCs generally prefer not to enter into relationships with clients or invest in assets where the ML/TF or reputational risks exceed their risk appetite, or where the actual or expected cost of compliance exceeds the expected benefits.

## 4. THE ASSET MANAGEMENT SECTOR

### 4.1. OVERVIEW

With gross assets under management of almost €4,570bn by the end of 2022 (including €1,459bn under individual management), the asset management sector plays an important role in the French economy and its financing. Strongly integrated into the international and European financial systems, French individual and collective investment management ranks top in continental Europe, accounting for around 31% of this market.

Under the supervision of the AMF, **the asset management sector comprises 700 AMCs**, all of which are authorised to carry out collective investment management (of undertakings for collective investment in transferable securities ***(UCITS)*** and/or AIFs)[85]. Many of them are also authorised to provide investment services governed by MiFID II[86]:

- More than half are authorised to provide portfolio management services on behalf of third parties, also known as individual discretionary management;
- almost 10% are authorised to provide the service of reception and transmission of order on behalf of third parties; and
- almost all (over 95%) are authorised to provide investment advice (mainly in connection with the marketing of managed funds).

The asset management sector in France is **highly concentrated**: by the end of 2022, almost three-quarters of the market (71.6%) for discretionary management was held by the top five AMCs, representing €1,045bn in assets under

[83] These terms are respectively defined as follows in the Opinion of the European Banking Authority on money laundering and terrorist financing risks affecting the EU's financial sector, EBA/Op/2023/08:

- FinTech: means technologically enabled financial innovation that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services. Some examples of services provided via FinTech solutions: services enabling cash to be placed on a payment account; services enabling cash withdrawals from a payment account; execution of payment transactions; payment initiation services; account information services; e-money services;
- RegTech: means any range of applications of technology-enabled innovation for regulatory, compliance and reporting requirements implemented by a regulated institution (with or without the assistance of ICT third-party providers). Some examples of AML/CTF activities where RegTech solutions can be used: customer due diligence; customer risk assessment; ongoing monitoring of the business relationship; transaction monitoring.

[84] EBA, Opinion of the European Banking Authority on 'de-risking', EBA/Op/2022/01.

[85] As at 31 December 2022, 93% of AMCs were subject to at least one of the two sectoral directives (UCITS/AIFM), with the remaining 7% comprised of AMCs being below the thresholds of the AIFM Directive and falling under a national regime. These were mainly private equity companies.

[86] Directive 2014/65/EU of the European Parliament and of the Council on markets in financial instruments.

management. The level of concentration for collective investment management is slightly lower than for discretionary management, since the top five AMCs account for 41% of the market share, but for a higher level of assets under management, i.e. €1,275bn.

This concentration is accompanied by a wide variety of market participant profiles:

- 'entrepreneurial' companies[87], which operate mainly in private management, multi-management, real estate and private equity, account for more than 2/3 of the AMCs in France;
- almost a third of AMCs are subsidiaries of regulated banking, insurance or financial groups: they manage almost 90% of the total assets under management.

**The management sector is also highly regulated, with AMCs subject to the provisions arising from the transposition into French law of one or other, or even both, of the sectoral directives (AIFMs[88] and UCITSs[89]), while also complying with the MiFID II rules when providing investment services, such as discretionary management or investment advice.**

In addition, AMCs are prohibited from receiving deposits of funds or securities from their clients[90].

In addition to AMCs, asset management activites require the support of a number of professionals, including:

- the depositary: which is responsible for the safe-keeping of the fund's assets and verifies the lawfulness and correct execution of the AMC's decisions; its control is a bulwark against the risk of fraud or abuse that may be committed by the fund manager;
- the registrar, who may be delegated the task of keeping the register of fund units by the AMC or the fund if they do not carry out these tasks themselves;
    - either the units are held 'in registered form': the investors are registered in their own name;
    - or the units are 'in bearer form': the register does not contain the names of the investors, but rather those of the custodian-account keepers; the units or shares of collective investment schemes are registered in the name of the investors with the custodian account-keepers;
- the custodian-account keepers, whose business is to register financial securities in the name of their holders (i.e. to recognise the holders' rights to the said financial securities) and to keep the corresponding securities and assets. In this capacity, they hold the units or shares in collective investment schemes on behalf of their clients.

These professionals are authorised **credit institutions or investment firms** that are subject to AML/CTF obligations and are placed under the supervision of the ACPR.

Subject to AMF-supervised AML/CTF rules for all their activities, AMCs are themselves exposed to ML/TF risks that may vary depending on the products or services they offer, the distribution channels they use, the characteristics of their clients and the countries of origin or destination of the funds.

The risks have been assessed according to major business lines, strategies or assets.

[87] *i.e*. whose shareholders are not a credit institution, insurance company or investment services provider.
[88] Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on alternative investment fund managers ***(AIFM Directive)***.
[89] Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities ***(UCITS Directive)***.
[90] Monetary and Financial Code, Article L. 533-21.

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

### Sector description

The so-called 'traditional' asset management of financial instruments is carried out by the AMCs authorised to manage funds invested in transferable securities that are traded on the financial markets, and in particular in UCITSs. Under European regulations, listed equities, listed bonds and money market instruments are the preferred investment universe for UCITSs and, by extension, retail investment funds[91]. This investment management may also be carried out indirectly, through subscriptions to investment funds (CIUs) which themselves invest in these traditional financial instruments.

It encompasses the largest number of AMCs. More than 70% of them are authorised to select such instruments in their investment funds (UCITS or AIF) or management mandates.

With assets under management valued at €1,260bn[92], traditional asset management accounts for more than 60% of French collective investment management schemes.

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

While subscribing to units in collective investment schemes is, in theory, a means of reintroducing criminal funds into the financial sphere, the AMF has no conclusive evidence making it possible to prove and measure this threat.

Further, the collective investment management of financial instruments is also not exposed to the risk of terrorist financing.

The threat level is **LOW**.

### Vulnerabilities

#### *Intrinsic vulnerabilities*

As indicated above, the investment universe of traditional asset management funds is limited by strict eligibility rules: this universe is comprised of assets with a low risk of money laundering (transferable securities listed on a regulated market, money market instruments).

In France, traditional asset management is characterised by a high level of intermediation. The AMCs that manage the funds whose units are admitted to the operations of the central securities depositary (Euroclear France) are not able to know, in real time, the end investors of the funds[93] who hold their units or shares 'in bearer form', nor their identity, or the origin of the funds invested. In this sense, this intermediation could constitute a vulnerability. However, in this case, the custodian-account keepers (participants of the central securities depository) where investors hold their collective investment scheme units or shares are themselves subject to AML/CTF obligations.

As a result of this intermediation, but given the low asset-based risk, the intrinsic vulnerabilities of traditional asset management are **MODERATE**.

[91] A'*fonds d'investissement à vocation générale*': a kind of AIF subject to most of the constraints of a UCITS under French regulations.
[92] Assets under management in French UCITSs managed by French AMCs are estimated at €921bn. The assets under management of the French retail investment funds managed by French AMCs are valued at €339bn.
[93] Excluding the special case of 'dedicated' funds.

### *Mitigation measures and residual vulnerabilities*

In addition to the regulatory factors relating to the authorisation and supervision of AMCs, the mitigation measures relating to the quality of the professionals involved in the asset management ecosystem should also be taken into account.

As indicated, the fund's assets are held by a depositary, which monitors the regularity of the manager's decisions and instructions on the one hand, and cash flows on the other. With the status of a credit institution or investment firm, subject to AML/CTF rules, it is a bulwark against the risk of fraud.

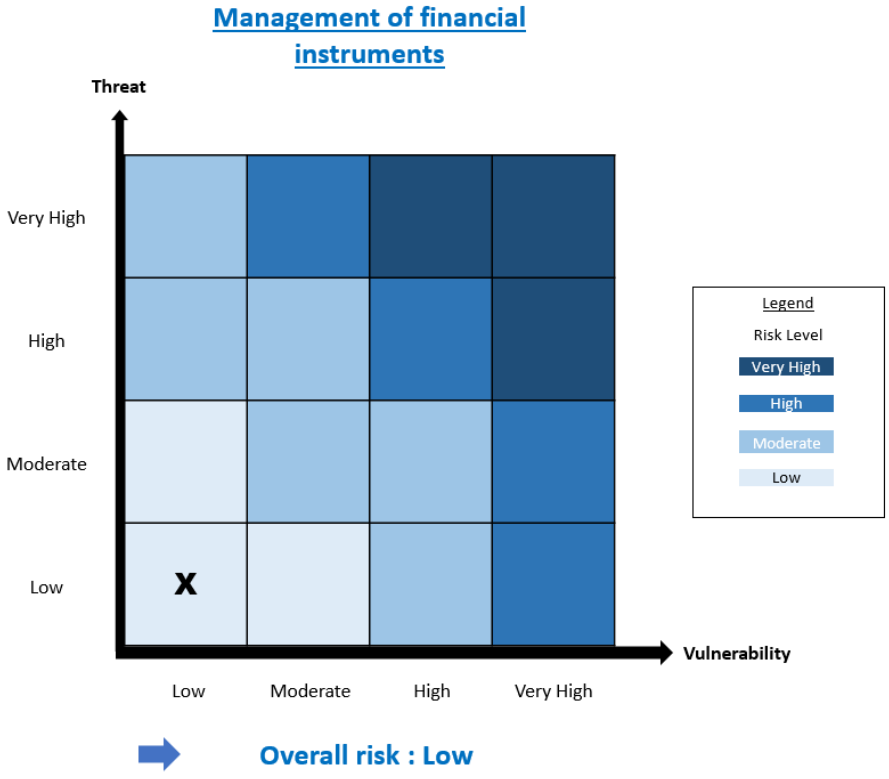
The vulnerability identified, which stems from the fact that the AMC (excluding dedicated funds) has no knowledge of its end investors when its units or shares are distributed through Euroclear, is considerably mitigated precisely by the interposition of Euroclear (see Chapter 7) and by the assurance that the unit subscription chain only includes AML/CTF obliged entities:

- insurance companies offering unit-linked investments;
- investment services providers (investment firms, AMCs or credit institutions authorised to provide investment services) providing investment advice, reception and transmission of orders on behalf of third parties or discretionary management services to their own clients;
- account keeper-custodians, also credit institutions or investment firms that receive funds directly or indirectly from clients known to them.

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

### *ML/TF risk rating*

The combination of the threat and vulnerability levels results in a **LOW** risk level.



## 4.3. PRIVATE EQUITY

### Sector description

This is a sector that continues to be buoyant: in 2023, the trend in terms of AMC setting up was characterised by the predominance of private equity and infrastructure projects (48%), followed by traditional asset management (30%) and real estate (22%). Assets under management at AIFs in the field of private equity also increased by 15% in 2022.

By 2022, the sums invested by private equity funds (excluding infrastructure) reached €24.7bn[94]. This sector had €97bn in net assets under management in 2021, rising to €112bn in 2023.

The AMCs operating in this sector exclusively manage AIFs:

- either in the form of funds with access conditions that are limited to professional or similar investors (professional private equity investment funds ***(FPCIs)*** or professional specialised funds ***(FPS)***). Where appropriate, they may also be authorised as European Long-Term Investment Funds (ELTIFs). The assets managed by these funds total more than €100bn;
- or in the form of AIFs open to subscription by the general public, some of which are eligible for tax relief. These funds may then take the form of retail private equity investment funds ***(FCPR)***, retail local investment funds ***(FIP***) or retail venture capital investment funds ***(FCPI)***. Where appropriate, they may also be authorised as ELTIFs. The assets under the management of these funds total almost €11bn.

In France, the majority of private equity investments are intended for institutional investors, which either invest on their own behalf or intermediate the investments of retail investors. This intermediation takes several forms: that of management mandate or unit-linked life insurance**,** within which an insurer (institutional client) can house professional private equity funds.

Of the €41.5bn in capital raised in 2022, 76% came from institutional investors: fund of funds (half of which were foreign), insurance companies, mutual insurers, pension funds and retirement funds. The proportion of funds invested by natural persons (including family offices) is around 16%.

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

By their very nature, private equity funds are not very attractive to criminals, due to the frequent existence of a lock-up period associated with each investment, which can be as long as 10 years for funds subscribed by retail investors[95]. This lock-up is often a condition for the granting of a tax incentive, which requires the client to provide proof of their tax liability, and requires that the units or shares be held in registered form in a register kept by the AMC or its delegate.

In this case, the risk of money laundering and terrorist financing arises more from the assets in which the fund invests:

- investment in companies that may be based in high-risk countries;
- investment in high-risk industrial sectors.

However, according to the data collected, private equity AMCs invest almost exclusively in French companies or those established in the EEA.

Having said this, it would appear that French private equity is attracting more and more foreign capital, which requires managers to be more diligent in terms of know your client and the origin of the funds.

Thus, while the data available in terms of volumes and cases identified means that the threat posed by fund assets can be put into perspective, the sector's exposure to foreign capital means that the threat posed by money laundering and terrorist financing is considered to be **MODERATE**.

---

[94] Source: France invest (Private equity activity in 2022).
[95] Professional investors can access investment funds with longer lock-up periods.

## Vulnerabilities

### *Intrinsic vulnerabilities*

The vulnerabilities are essentially linked to the nature of the assets, which are riskier than those of traditional asset management.

In contrast to traditional asset management, private equity AMCs have a direct relationship with their investors, as units in private equity funds are often held in registered form. As such, they are primarily responsible for the know your client-related obligations, without being able to rely on other professionals in the financial sector. Depending on the profile of the investor, whether institutional or retail, and whether based in France or abroad, this due diligence is more or less complex to carry out.

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

### *Mitigation measures and residual vulnerabilities*

Private equity is highly regulated: all so-called general public funds (FCPRs, FCPIs, FIPs; authorised as ELTIFs where applicable) are subject to prior authorisation by the AMF and to strict rules in terms of investment ratios. Other funds reserved for professional clients (or retail clients investing at least €100,000) are declared to the AMF. They all have an external auditor who audits the fund's financial statements, as well as a depositary who fulfils the function of custodian of the assets, as well as monitoring the regularity of management decisions and cash flows.

Another measure for mitigating asset-based risk is the regulatory requirement set out in Articles 320-22 and 321-149 of the AMF General Regulation, according to which: *"When it implements its investment policies for its own account or for third parties, 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."*

This mitigation measure is also specified in AMF doctrine[96], which requires, in particular that: "*Prior to the investments made by the collective investment management company, the latter shall collect the information that it will need to assess the money laundering and terrorist financing risk*" and also states that: "*With respect to the additional information to be collected, the AMF recommends that collective investment management companies follow the best practices below:*

*Before closing an investment in a company whose securities are not admitted for trading on a regulated market, the collective investment management company shall collect reliable information:*

- *the identity of the management and beneficial owners, for the purpose of identifying any politically exposed persons or persons on a list of frozen assets;*
- *financial data, to assess the consistency with the company's business.*

*Before subscribing for shares or units in a private equity fund, a specialised professional fund or a professional private equity investment fund or any other private equity vehicle registered in France or abroad, the collective investment management company shall collect and verify the information about said vehicle, as well as information about its asset management company: names of executives, shareholders and beneficial owners. The collective investment management company shall make inquiries about its co-investors*."

Generally speaking, discussions with private equity AMCs show that asset-based due diligence is extensive, both for ML/TF risk and for credit and reputation risk.

[96] AMF Position-Recommendation - DOC-2019-15 - Guidance on the risk-based approach to combating money laundering and terrorist financing.

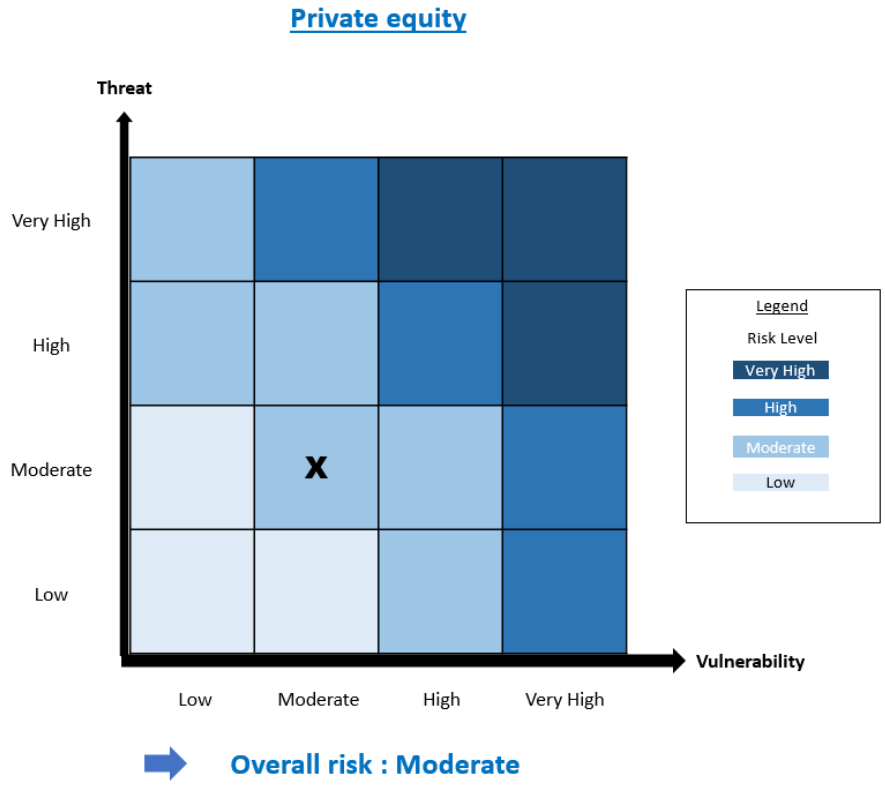
As a result of these requirements, French AMCs opt to invest mainly in France or in countries of the European Union or European Economic Area, rather than in third or high-risk countries.

As mentioned above, the risk associated with fund investors depends in particular on their nationality or domicile. Within the European Union, tax transparency regulations are helping to improve know your client work.

For these reasons, the residual vulnerabilities presented by private equity are **MODERATE**.

### Risk rating

The combination of the level of threat and the level of residual vulnerability results in a **MODERATE** risk for the private equity sector.



### 4.4. REAL ESTATE INVESTMENT

#### Sector description

Like private equity (see above), real estate is the most buoyant sector in which new AMCs are positioning themselves in France. Thus, in 2022, 26% of new AMCs were specialised in real estate, and real estate AIFs had increased their assets under management by 6%. By the end of 2023, 23% of French AMCs were authorised to select real estate assets.

At the end of 2023, the net assets of real estate funds totalled more than **€125bn**. These funds are held by institutional investors, mainly through professional real estate collective investment undertakings ***(OPPCIs)***. They are also held by the general public, through real estate collective investment undertakings ***(OPCIs***) (**€14.7bn**) and real estate investment companies (***SCPIs***) (**€54.3bn**).

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

As noted in the NRA, real estate acquisition and sales activities are exposed to a high threat of money laundering, due to the large sums involved and the relative security offered by this type of investment, which make the sector attractive to criminal groups.

According to the NRA, the luxury real estate sector, particularly in Paris, the Côte d'Azur and the French overseas territories, is more exposed than other sectors to threats linked to tax evasion, scams and drug trafficking. In particular, tax evasion can be based on schemes specific to the real estate sector, such as the 'Girardin social housing' scheme, which aims to reduce tax for investors in social housing in overseas France.

Tax evasion can also take the form of undervaluing the sale price and 'under-the-table' compensation in order to reduce the tax base.

The real estate investment sector, on the other hand, is more focused on real estate assets that are likely to generate regular rental income that is distributed to investors over a fairly long period (five years minimum for SCPIs). Luxury residential real estate is not the preferred investment target of real estate funds.

In addition, the real estate investment sector is also characterised by (i) the diversification of the assets of certain investment vehicles[97] and (ii) its concentration on certain real estate assets (commercial real estate in particular[98]), leading to less exposure to some of these threats.

As a result of these differences from the real estate sector in general, the exposure of the real estate investment sector to the threat of money laundering is lower, and at a **MODERATE** level.

It is not particularly exposed to the threat of terrorist financing. Because of their lower exposure to this threat, real estate acquisition, sales and rental activities have not been rated in the NRA.

[97] While SCPIs invest up to 100% in real estate assets, OPCIs generally invest between 51% and 65% in real estate, either directly or through other investment funds. The remainder of their assets is comprised of financial instruments and, residually, cash (5%).
[98] According to ASPIM data, 94% of SCPIs are invested in commercial real estate: offices and shops account for more than 88% of investments, of which more than half (53%) are located in Paris or the Paris region, areas in which the reporting activity of real estate obliged entities is one of the highest (see TRACFIN, AML/CFT: reporting entities activity - 2022 review); 69% of OPCIs and 64% of OPPCIs are also invested in offices and shops.

## Vulnerabilities

### Intrinsic vulnerabilities

The vulnerabilities of the real estate sector are essentially linked to the nature of the assets: prestigious real estate is more vulnerable to money laundering threats, due to the volatility of sale prices, the absence of a benchmark to check the consistency of prices and the often highly confidential nature of these transactions.

In the real estate investment sub-sector, the vulnerabilities are more closely related to the arrangements and structures for holding these assets, which meet specific tax needs, but can result in the identity of the company's actual beneficiary being obscured by the interposition of multiple shell companies: real estate management companies can thus be a vehicle for this opacification, but do not in themselves constitute a reason for alert.

The investor-client profile is also a risk factor: depending on whether they work in a sector in which cash circulates in large amounts (construction, catering, etc.), whether they are a PEP (risk of corruption) or on the grounds of their tax residence.

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

### Mitigation measures and residual vulnerabilities

On account of these vulnerabilities, the sector is heavily regulated. All real estate professionals are subject to AML/CTFobligations. AMCs operating in this sector are subject to two types of obligation:

- **under the supervision of the AMF**, in their capacity as AMCs managing real estate AIFs, as referred to in Article L. 561-2, 6° of the Monetary and Financial Code; and
- **under the supervision of the 'Direction générale de la concurrence, de la consommation et de la répression des fraudes' (DGCCRF)**, where applicable, in their capacity as real estate professionals referred to in Article L. 561-2, 8° of the Monetary and Financial Code, as carrying on the activities referred to in Article 1, 1°, 2°, 4, 5, 8° and 9° of law No. 70-9 of 2 January 1970 regulating the conditions governing the exercise of activities relating to certain transactions involving real estate and business assets (known as the 'Hoguet Law').

Real estate assets are valued by one (or more) independent valuers appointed by the AMC.

As in the case of private equity, real estate assets managers are subject to the asset-based AML/CTF due diligence requirements set out in Articles 320-22 and 321-149 of the AMF General Regulation, which state that: *"When it implements its investment policies for its own account or for third parties, 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."*

This mitigation measure is also specified in AMF doctrine[99], which requires, in particular, that:

- "*collective investment management companies specialising in the real estate sector (such as real estate investment companies, real estate collective investment undertakings, professional real estate collective investment undertakings) shall perform due diligence adapted to the nature of their target assets.*

  *Portfolio asset management companies specialising in real estate are therefore required to perform due diligence on the counterparties to their property acquisition and disposal transaction. The extent of due diligence is adapted to the counterparty's risk profile, the characteristics of the business relationship and/or the transaction based on the usual risk factors (product, country and client risks)*"; and

[99] AMF Position-Recommendation - DOC-2019-15 - Guidance on the risk-based approach to combating money laundering and terrorist financing.

- "*when the collective investment management company carries out the letting activity itself under the terms of a real estate transaction mandate referred to in Article 561-2 point 8° of the Monetary and Financial Code, the tenants it is searching for on behalf of the fund are clients of the collective investment management company which is therefore required to conduct due diligence regarding such tenants, provided that the monthly rent amounts to €10,000 or more, excl. tax*".

In addition, investment decisions are taken collectively, as a committee. Cash transactions are prohibited. They take a long time to conclude and involve many professionals alongside the AMC (lawyers, notaries), who are themselves subject to AML/CTF rules.

This robust sector regulatory framework and the efforts made by professionals in the sector have led to a **MODERATE** residual vulnerability.

### Risk rating

The overall level of risk associated with real estate investment is considered to be **MODERATE**.

## 4.5. DISCRETIONARY MANAGEMENT

### Sector description

Portfolio management on behalf of third parties, also known as individual management under mandate or, more simply, discretionary management, is a tailor-made service for managing a portfolio of financial instruments offered to clients by investment service providers, including AMCs.

This service is personalised, as it is adapted to the investor's situation (their knowledge and experience of investment, their financial situation, including their capacity to bear losses, and their investment objectives, including their risk tolerance and any preferences in terms of sustainability) and is entered into at the end of a know-your-client (KYC) process.

For these reasons, it is often intended for institutional investors (insurers, retirement funds, etc.) or retail investors with a certain level of resources and assets. For the latter, this activity frequently extends to a more general range of services linked to the overall management of financial and/or real estate assets, commonly grouped together under the term 'private management' or 'private banking'.

As previously indicated, assets under discretionary management amounted to €1,459bn at the end of 2022. More than half of French AMCs (354 out of 700) are authorised to offer discretionary management services, with the volume of business varying greatly depending on the type of AMC. The business of AMCs that are subsidiaries of credit institutions is more geared towards collective investment management than discretionary management (52% of assets under management and advice in collective investment management compared with 26.6% in discretionary management), while the business of subsidiaries of insurance companies, mutual insurers and investment services providers is highly concentrated on discretionary management, with assets under management of €565bn, i.e. 48.6% of total assets under management. For entrepreneurial AMCs, discretionary management represents only 3% of their total assets under management or advice.

The sector is also highly concentrated: at the end of 2022, almost three-quarters of the market share (71.6%) for this business was held by the top five AMCs, representing €1,045bn in assets under management.

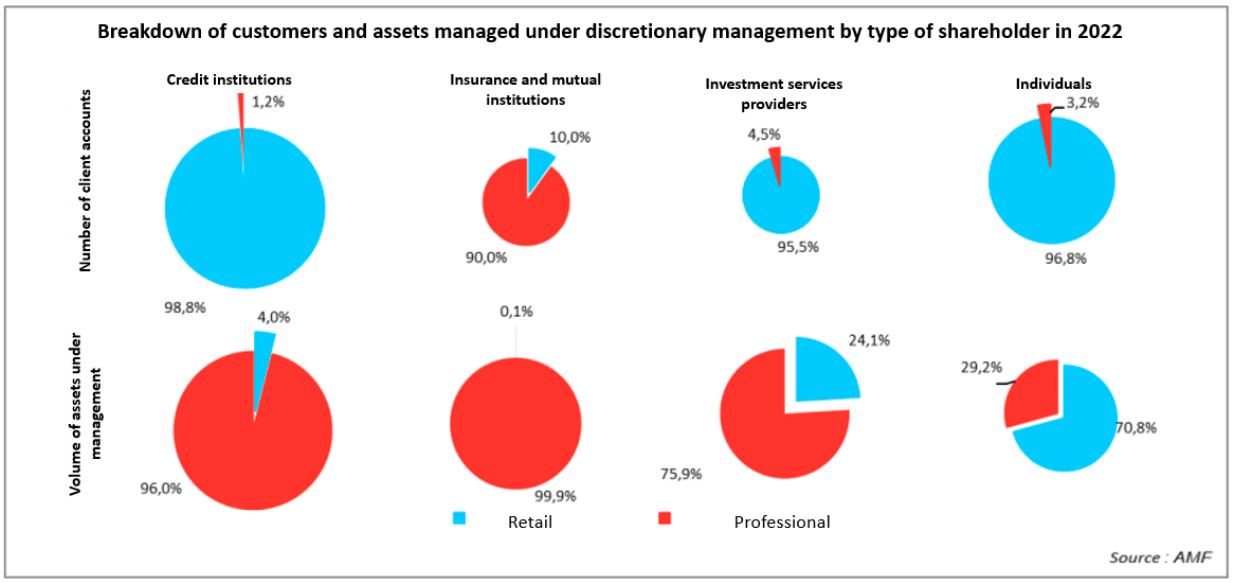
Depending on the type of shareholding, AMCs will invest their assets differently between in-house CIUs (managed by the same AMC or by an AMC of the same group), third-party CIUs (managed by third-party AMCs) or direct investments through securities. In 2022, assets under discretionary management were broken down as follows:

- 12.6% in in-house CIUs;
- 4.9% in third-party CIUs;
- 82.5% in directly-held securities.

In terms of clients, entrepreneurial AMCs primarily (97%) target retail clients, a proportion that is fairly similar for the subsidiaries of investment services providers (95.5%) and credit institutions (98.8%). By contrast, the subsidiaries of insurance companies and mutual insurers, which make less use of multi-management, tend to manage mandates on behalf of professional clients (90%).

Generally speaking, in terms of the number of client accounts, with the exception of AMCs that are subsidiaries of insurance companies and mutual insurers (which primarily manage assets on behalf of their shareholder insurance company), AMCs mainly cater to retail clients. Conversely, in terms of the volume of assets under management, excluding entrepreneurial companies, professional clients account for a much larger share[100].

[100] AMF, *chiffres clés de la gestion d'actifs 2022* [Key Figures for Asset Management in 2022, only available in French].




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

The discretionary management business, which consists of managing a portfolio of financial instruments on behalf of a client with a view to obtaining a return, may enable illicit income to be reintegrated into the legal economy.

Aimed at wealthy clients with high net worth or high incomes, who may not be resident in France and may originate from high-risk countries or be 'politically exposed persons', discretionary management is particularly exposed to the threats linked to corruption and tax fraud infringements.

In France, according to the data collected, AMCs offering this discretionary management service as part of a more comprehensive wealth management offer have relatively few clients classified as high risk, and even fewer PEP clients. Only around ten AMCs state they have business relations with a limited number of clients based in a high-risk country.

The threat of money laundering is **MODERATE**. Conversely, the threat of terrorist financing is **LOW**.

### Vulnerabilities

#### Intrinsic vulnerabilities

The sector's vulnerabilities are essentially due to the nature of the investments decided by the manager (listed versus unlisted financial instruments, cross-border transactions) and to the proposed arrangements, which can be vehicles for opacification. The set-up of complex legal arrangements to meet specific and multiple needs (yield, tax optimisation, inheritance) prevents the manager from having a continuous overview of the client's activities and resources.

Vulnerabilities also depend on the client and their characteristics. Often represented by third parties or business introducers, this demanding clientele may be more reluctant to respond to all requests for supporting documents. Comprised of a residual proportion of politically exposed persons or foreign tax residents, who may be based in countries with inadequate AML/CTF legislation, a portion of discretionary management clients are therefore more likely to present

one or other of the high-risk factors. However, this vulnerability is less pronounced in the case of clients who are professional 'by nature'[101], some of whom have regulated status and are subject to the AML/CTF provisions[102].

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

### Mitigation measures and residual vulnerabilities

The mitigating measures rely on the fact that AMCs are subject not only to the AML/CTF rules, but also to the rules arising from MiFID II. These two regulatory provisions require clients to share all relevant information with the asset manager, at the risk of not gaining access to the service they seek. Compared with collective investment management, the discretionary management sector is characterised by a good knowledge of the client and the business relationship. The manager (agent) maintains a close relationship with their client (the principal), especially when the discretionary management service is extended to include more general management of financial and/or real estate assets.

Regulatory measures relating to the exchange of information on tax matters also contribute to the manager's knowledge of their client's profile.

Intrinsic vulnerabilities are known and identified by discretionary management professionals, who take these into account in their risk mapping, adapt their procedures and train their staff accordingly.

The level of residual vulnerabilities is **MODERATE**.

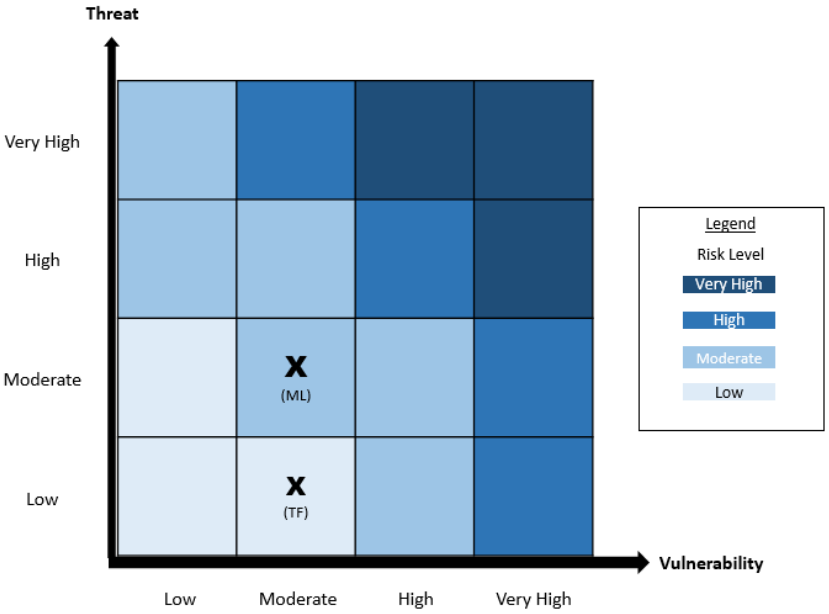
### Risk rating

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

[101] Defined in Article D. 533-11 of the Monetary and Financial Code.

[102] In particular those defined in 1 of Article D. 533-11 of the Monetary and Financial Code (credit institutions referred to in Article L. 511-9; investment firms referred to in Article L. 531-4; other authorised or regulated financial institutions; insurance and reinsurance firms referred to in the first paragraph of Article L. 310-1 and Article L. 310-1-1 of the Insurance Code respectively; insurance group companies referred to in Article L. 322-1-2 of the same code; mutual insurers and associations of mutual insurers governed by Book II of the Mutual Insurance Code; group mutual insurance associations referred to in Article L. 111-4-2 of the same code; prudential institutions and their associations governed by Book IX, Title III of the Social Security Code and social protection insurance group companies referred to in Article L. 931-2-2 of the same code, collective investments referred to in Article L. 214, I, and collective investment management companies referred to in Article L. 543-1; pension reserve funds referred to in Article L. 135-6 of the Social Security Code, occupational pension institutions referred to in Article L. 370-1 of the Insurance Code for their operations referred to in Article L. 370-2 of the same code, and legal entities administering an occupational pension institution referred to in Article 8 of order No. 2006-344 of 23 March 2006 on supplementary occupational retirement provisions; Persons whose principal activity consists of dealing on own account in commodities or commodity derivatives, referred to in Article L. 531-2, 2°, j; the *Caisse des Dépôts et Consignations* and other authorised or regulated institutional investors).

## Discretionary management




**Overall risk :**
**Moderate (ML) / Low (TF)**

## 5. FIAs

### Sector description

As at 31 December 2023, **6,707** financial investment advisors *(**FIAs***) were registered with ORIAS (the body responsible for registering insurance, banking and financial intermediaries).

As a reminder, under Article L. 541-1 of the Monetary and Financial Code, FIAs *"are persons carrying on the following activities as a regular occupation*:

*1° the investment advice referred to in Article L. 321-1, 5;*
*2° (Repealed)*
*3° advice on the provision of investment services as referred to in Article L. 321-1;*
*4° advice on carrying out transactions in miscellaneous property as defined in Article L. 551-1".*

In accordance with Article L. 541-1, II of the Monetary and Financial Code, FIAs may also "*provide the service of receiving and transmitting orders on behalf of third parties, under the conditions and within the limits set by the General Regulation of the Autorité des Marchés Financiers*[103] *and carry out other wealth management advisory activities."*.

Depending on the services provided, the sector can be divided into two main business lines:

- **FIA CGP** (**'wealth management advice'**): this category includes actors providing comprehensive wealth management advice to individuals or firms (cash investment). FIA platforms/groupings for FIA CGP are classified in this category. (Retail clientele, but multi-regulated) - **this line comprises 95% of the FIA population;**
- **FIA 'advice to institutional investors, AMCs and other financial intermediaries'**: this category includes FIAs who assist institutional investors (foundations, retirement funds, insurance companies, etc.) in monitoring their investments (audit, calls for tender, recommendations, etc.), but also those who work exclusively with AMCs or funds to make investment recommendations, or those players responsible for advising other financial intermediaries (for example, BtoB platforms for structured products).

Whether they operate as FIA CGPs or as advisors to institutionals investors and AMCs, FIAs may also provide services under other statutes (insurance intermediary (***IAS***), intermediary in banking transactions and payment services (***IOBSP***), statutes that are registered with ORIAS and subject to ACPR supervision. They may also hold a real estate transaction permit (*carte T*). This is particularly true of FIA CGPs. Only 5.7% of FIAs work under this status alone[104].

Of the total reported turnover of FIAs of **€4bn** in 2022**, €0.93bn** came specifically from financial investment advice, i.e. **23% of total business**. Non-FIA activities are those carried out under other statutes registered with ORIAS (insurance intermediation, banking intermediation and payment services) or under other regulations (Hoguet Law, *Carte T)*.

The sector is highly concentrated, with the top 50 players accounting for 50% of FIA business, the next 500 for 33% and the remainder (5,206) for 17% of FIA business.

Membership with one of the four professional associations authorised by the AMF is one of the conditions for obtaining FIA status. The four professional associations authorised by the AMF are required to audit their members at least once every five years, and report on their work to the AMF. As such, they are also subject to supervision

[103] In accordance with Article 325-32 of the AMF General Regulation, "*A financial investment adviser may agree to receive for transmission purposes an order for one or more units or shares in a collective investment undertaking that a client to whom it has provided an advisory service intends to subscribe for or sell*".
[104] 88.7% of these firms stated that they combine their FIA status with other statuses. Thus, 23% combine the statuses of FIA, IAS, IOBSP, *carte T* holder and holder of the appropriate legal qualification (CJA), while 24% combine the previous statuses with the exception of the CJA; 9.4% combine the statuses of FIA and IAS, and 9.6% combine the statuses of FIA, IAS and IOBSP.

by the AMF, and may be sanctioned by its Enforcement Committee if they commit regulatory breaches of their obligations to monitor the activities of their members.

The AMF also ensures that FIAs comply with the regulations by carrying out standard inspections (desk-based and on-site, including, in the vast majority of cases, of the AML/CTF system), mass inspections (desk-based and thematic) and by monitoring the inspections of FIAs carried out by the authorised professional associations.

### Threat exposure and description of scenarios of use for ML/TF purposes

The business of FIAs which consists of recommending financial investments (financial instruments or other more atypical products) or investment services, does not, in itself, offer many opportunities for money laundering. FIAs do not collect any funds other than their fees.

On the other hand, the act of subscribing to an investment recommended by an FIA in the normal course of their work is a means of laundering illegal income, in particular the proceeds of tax evasion. Tax is an important consideration for most FIAs clients.

In the case of regulated financial investments, other professionals are involved: the financial instruments or investments that FIAs are likely to recommend are those offered by other entities in the financial sector (AMCs, banking, financial or insurance institutions), and they can only be subscribed by means of account-to-account transfers opened at other institutions that are also regulated.

Conversely, in the case of more atypical, potentially unregulated products, the involvement of other professionals who are AML/CTF obliged entities is not verified. As a result, FIAs may be exposed to the threat of fraud involving false investments, scams or the risk of marketing products that are not authorised for distribution in France. In this respect, it should be noted that advice on 'other investment products' accounts for no less than 20% of the declared activity of FIA CGPs[105].

The level of threat to which FIAs are exposed is therefore likely to vary considerably depending on the nature of the products and the capacity of their partners. It has a **LOW** rating for terrorist financing and a **MODERATE** rating for money laundering.

### Vulnerabilities

#### Intrinsic vulnerabilities

Anonymity is not possible in the privileged relationship that develops between an FIA and their client.

Vulnerabilities are therefore more closely linked to client characteristics. According to data collected by the AMF from FIAs, their client base is essentially domestic, includes only a very small number of PEPs (less than two per thousand of the total FIA client base) and is almost entirely comprised of clients whose level of risk is estimated by the FIAs as being low (53%) or moderate (46%), with high-risk customers therefore representing 1% of their total client base, according to their estimates.

Other vulnerabilities relate to the products recommended and their wide diversity: depending on whether they are CIUs authorised by the AMF, whose subscription chain involves entities subject to French AML/CTF regulations, or more exotic products (foreign, declared and unregulated), FIAs' exposure to product risk is likely to vary considerably.

[105] Advice on 'other investment products' refers to advice on miscellaneous property as defined in Article L. 551-1 of the Monetary and Financial Code (the whitelist of which is available on the AMF website: https://geco.amf-france.org/Bio/BIO/BIO_PDFS/LISTE_PRODUITS_BIENS_DIVERS/produits_biens_divers.pdf) (in French), but also to all subscription offers not represented by financial instruments (e.g. subscription of company shares, tax exemption transactions) under the 'other wealth management advisory activities' referred to in L. 541-1, II of the Monetary and Financial Code.

In view of the above, the financial investment advisory business presents intrinsic vulnerabilities that are generally **HIGH** in terms of money laundering and **LOW** in terms of terrorist financing.

### Mitigation measures and residual vulnerability

Subject to AML/CTF rules, FIAs are professionals who are aware of the AML/CTF requirements, and are supervised by the AMF, and four professional associations (the *Association Nationale des Conseils Financiers* (ANACOFI CIF), the *Chambre Nationale des Conseils en Gestion de Patrimoine* (CNCGP), the *Chambre Nationale des Conseils en Experts - Patrimoine Financiers* (CNCEF Patrimoine) and *Compagnie CIF*, which are authorised by the AMF and of which FIAs are required to be members before they may carry on their business, and which are further responsible for supervising their activities.

Moreover, in addition to their client due diligence obligations, FIAs are bound by numerous know your client obligations for the purposes of providing personalised recommendations, as set out in MiFID II. These obligations relate to their knowledge and experience in terms of investment in relation to the specific type of financial instrument, transactions or services, their financial situation, including their capacity to bear losses, and their investment objectives, including their risk tolerance and any sustainability preferences. The same regulations oblige them to refrain from recommending any transaction or product if clients or potential clients do not provide the required information[106].

The implementation of these mitigation measures is, however, impacted by the resources available to FIAs to conduct their business in compliance with the different regulations to which they are subject due to the variety of their activities: with an average headcount per firm of three people (whereas AMCs have an average headcount of more than thirty people per AMC, for example), the sector has, compared to the asset management sector, very limited resources to carry out its business in a context marked by a constant increase in regulatory requirements (to which other sectors are also adapting), and this, even despite the increase in headcount declared by FIAs (8% increase in 2022).

In 2022, the FIA professional associations carried out inspections of some of their members (each member must be inspected at least once every five years) in mainland and overseas France. The associatiosn carried out 897 inspections in 2022.

These inspections led to the finding of at least one regulatory breach for 82% of the FIAs inspected. In almost half of the inspections (46%), one of the regulatory breaches found related to compliance with the applicable AML/CTF rules. With regard to AML/CTF, the associations noted in particular that:

- 19% (i.e. 168 FIAs) of the population inspected in 2022 did not have a risk classification (proportion stable overall compared with 2021: 20% or 205 FIAs);
- Five suspicious transaction reports were inventoried during the inspections, spread over three firms (14 reports in 2021 and seven reports in 2020).

These data show that while FIAs are indeed subject to AML/CTF obligations, the effective implementation of these obligations remains unsatisfactory for a significant proportion of the sector.

For its part, the AMF opened 50 ‘mass’ inspections of FIAs in six regions in both 2023 and 2022. During these mass inspections, and for each FIA, the inspectors systematically examined the most recent inspection report drawn up by the professional association and checked, where necessary, whether the FIA had taken steps to remedy the shortcomings identified by the association. Of these inspections, 21 were referred by the AMF to the FIA professional associations. It should be noted that the associations may be asked to inspect their members within a period shorter than five years if the referral is made following AMF inspections that reveal material findings.

[106] Monetary and Financial Code, Article L. 541-8-1 4°.

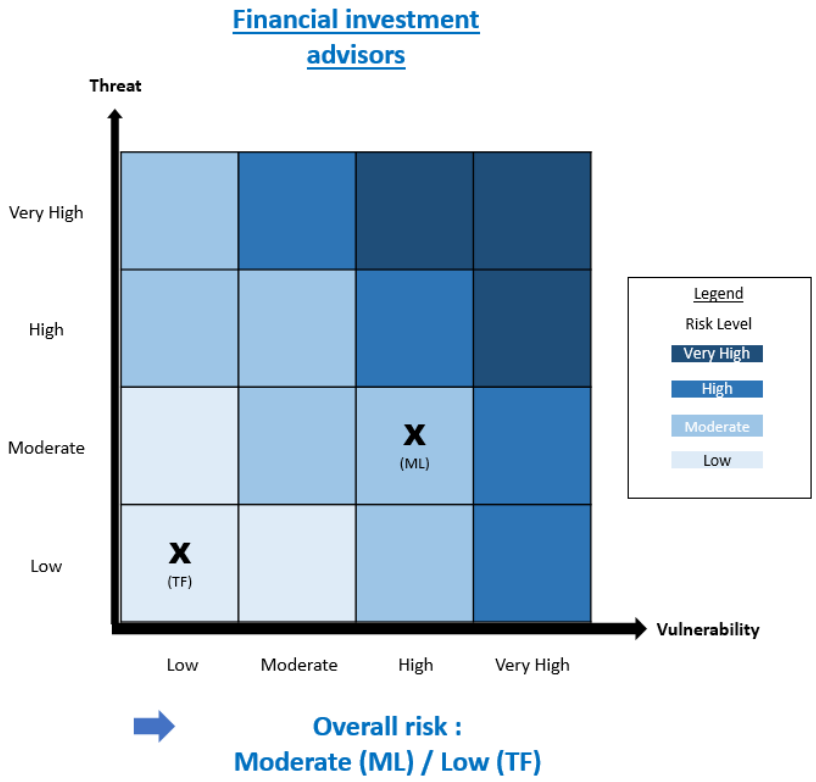
In addition, so-called 'traditional' inspections were also carried among FIAs (eight in 2022 and four in 2023, 10 of which focused on AML/CTF)[107].

Lastly, and in view of the completeness of the information available to them, the reporting activity of FIAs, although it has been steadily increasing for several years, remained low in 2022 (107 suspicious transaction reports recorded by Tracfin)[108], and therefore is unrepresentative of the knowledge that these professionals have of the transactions that they handle: a reminder of the reporting obligation therefore seemed necessary. To this end, in July 2023, a webinar dedicated specifically to FIAs was jointly organised by Tracfin and the AMF.

Taking into account all of the above, and after consideration of mitigation measures, the sector's residual level of vulnerability to money laundering is **HIGH** and to terrorist financing is **LOW**.

### Risk rating

The combination of the threat and vulnerability levels results in a **LOW** risk level for terrorist financing and a **MODERATE** risk level for money laundering.




[107] These inspections led to the identification of possible scams or fraud, which were passed on to the DGCCRF, TRACFIN or the Public Prosecutor's Office (see above: threats posed by atypical products).
[108] Tracfin, AML/CFT: reporting entities activity - 2022 review.

## 6. CROWDFUNDING

### Sector description

In general, crowdfunding refers to the activity carried out by online platforms that bring together project owners with financing needs and individuals or investors with financial capacity who are willing to invest in the proposed projects.

This sector was initially regulated by national provisions that led to the creation of the status of crowdfunding investment adviser ***(CIA)*** for financing in the form of financial securities or *minibons*, and crowdfunding intermediary ***(IFP***), for financing in the form of loans or donations. Today, crowdfunding is subject to a harmonised regulatory framework under Regulation (EU) 2020/1503 of 7 October 2020 on European crowdfunding service providers for business ***(CSP)***, which came into force on 10 November 2021 ***(Crowdfunding Regulation***), subject to a transitional period that ran until 10 November 2023 for platforms lawfully in existence on 10 November 2021.

Order No. 2021-1735 of 22 December 2021 modernising the framework for crowdfunding has adapted the French regulatory framework to the Crowdfunding Regulation. As a result, **the CIA status has been repealed**, the IFP status has been retained for activities outside the scope of the Crowdfunding Regulation and the CSP status has been incorporated into French law. A distinction must therefore be made between the entities covered by the different statuses:

- **CSPs**, encompassing platforms that put potential investors in touch with project owners raising funds in the form of loans for consideration and/or the issue of securities or instruments admitted for the purposes of crowdfunding and intended to finance projects with a commercial purpose, which are supervised by the AMF; and
- ***IFP*** is now dedicated to the activities of free loans and donations, including through online kitties, as well as financing in the form of certain loans for consideration (for example, the financing of certain projects sponsored by local authorities, and the financing of initial and ongoing training). This status falls under the supervision of the ACPR and is therefore dealt with in the ACPR's SRA[109].

Since 10 November 2023, only providers authorised as CSPs have been authorised to provide crowdfunding services falling within the scope of the Crowdfunding Regulation. Consequently, the risk rating for CIPs, which appears in the NRA published in January 2023, is not repeated here.

While CIAs and IFPs were subject to the AML/CTF regime[110], this is not the case for CSPs. **CSPs as such are not currently subject to the applicable AML/CTF provisions**, except where these are applicable in respect of their activities referred to in Article L. 547-4 of the CMF, i.e. in relation to projects involving certain company shares (*parts sociales*) as defined by decree[111]. No CSP currently engages in such activity, such that no CSP is currently subject to AML/CTF obligations in France.

**The part of the crowdfunding sector which falls under the jurisdiction of the AMF is therefore not the subject of any rating in this SRA.**

However, it should be noted that the European framework in this area is likely to evolve in the near future, with CSPs set to be included in the scope of market participants subject to AML/CTF obligations[112].

[109] ACPR, *analyse sectorielle des risques*, June 2023, §4.1 [Sector Risk Assessment].
[110] For IFPs: Article L. 561-2, 4° of the Monetary and Financial Code; for CIAs: Article 39, I of order No. 2021-1735 of 22 December 2021 modernising the framework relating to crowdfunding, as amended by Article 1 of order No. 2022-1229 of 14 September 2022.
[111] Monetary and Financial Code, Article L. 561-2, 6°.
[112] Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing - Confirmation of the final compromise text with a view to agreement, 13 February 2024, 2021/0239 (COD); see Article 2(14b).

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

## Sector description

In 2023, only one entity was authorised as a central securities depository ***(CSD***): Euroclear France.

The central securities depository has a dual role:

- of 'notary', insofar as the central securities depository admits securities when they are issued;
- as operator of the securities settlement-delivery system, thus enabling the circulation of securities between participants.

The admission of securities to Euroclear France is subject to verification of the issuer's status and the issuer's agreement to the conditions for use of the Euroclear system. Depending on the type of security, the following documents are required: the security prospectus, the issuing programme, the company's articles of association, the bond documentation and the securities information memorandum.

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

The participants in the central securities depository's securities settlement system are listed exhaustively in Article L. 330-1 II of the Monetary and Financial Code: European credit institutions and investment firms or those from third countries under certain conditions, central securities depositories, authorised European interbank settlement systems and clearing houses or those from third countries under certain conditions, public and supranational bodies, i.e. entities that are generally subject to AML/CTF obligations.

As at 31 December 2023, Euroclear France had **120 participants**, a detailed list of which is provided to the authorities. The process of admitting participants is subject to procedures to verify their capacity (registration, authorisation, shareholders, managers and also, depending on their status, whether they are subject to anti-money laundering regulations). It should further be noted that most participants also have a cash account with the Banque de France, which is likewise subject to due diligence by the Banque de France.

By way of illustration, as at 31 December 2023, the total deposits of financial securities with Euroclear France amounted to €9,400bn (excluding repurchase agreements with the Banque de France) for an annual settlement-delivery volume of €344,980bn. Settlement-delivery instructions are computerised orders for the movement of the securities issued by each of the institutions involved in a transaction. Given these volumes, many settlement-delivery flows are subject to netting to improve the fluidity of the settlement-delivery system[113]. In this respect, the clearing houses, downstream of the transactions carried out on the markets, systematically net the flows between their members in order to optimise risks.

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

**The CSD has little direct exposure to the threat of terrorist financing**. Highly integrated into the financial ecosystem and offering only electronic trading methods that require the use of standardised communication systems that are difficult to access (Swift), it only deals with the trading of securities: cash is settled through accounts opened with the Banque de France. The high level of investment required to access securities settlement-delivery systems makes the direct use of the central securities depository unsuitable for terrorist financing purposes, as it is inaccessible to natural persons and not very accessible to legal entities that do not have a significant securities settlement-delivery business over the long term.

[113] Euroclear France has indicated in this regard that in 2022 the number of cleared transactions was 35 million (Euroclear Annual Review 2022).

In its capacity as intermediary, **the CSD can be used** as a vehicle for the propagation of fraudulent transactions, such as the trading of securities for counter-values that are out of all proportion to the value of the assets.

In view of these factors, the ML/TF threats faced by the CSD are considered to be **LOW**.

### Vulnerabilities

#### Intrinsic vulnerabilities

Although participants in the central securities depository also subject their clients to their own AML/CTF systems, the complexity of the participants' own-account and third-party business is nevertheless a definite factor of vulnerability.

In this respect, although all flows are traceable, their possible netting with other transactions makes it difficult to identify any suspicious behaviour. Thus, given the large number of instructions at play between participants, their possible netting and the variety of possible instructions, the CSD does not have a detailed view of the underlying strategies of the transactions passing through its system. For example, insofar as the flows of securities that are collateral for a refinancing operation can be netted against purchases and sales of securities, it is impossible to identify which part of the securities flow is the subject of which transaction and at what price.

The same applies to the share of the instructions processed on behalf of participants' clients, as the clients' activities are similarly netted.

The netting process, which guarantees the efficiency and security of any settlement-delivery system managed by this type of infrastructure, dictates that a **MODERATE** rating of intrinsic vulnerability to the risk of money laundering must be given.

#### Mitigation measures and residual vulnerabilities

The first mitigating measure taken is that of making the CSD subject to AML/CTF rules, while Regulation No. 909/2014 on central securities depositories ***(CSDR)*** makes no provision for this. The AMF is responsible for ensuring that the French CSD complies with these AML/CTF obligations (Article L. 561-36 of the Monetary and Financial Code). Every year, the AMF receives and analyses the AML/CTF annual report, which gives details of the staffing levels, resources and measures implemented for AML/CTF control, such as the implementation of alerts for potentially suspicious transactions. An inventory of the obligations arising from the FATF recommendations for securities management activities has also been produced in order to consider which provisions are applicable in the context of the French central securities depository.

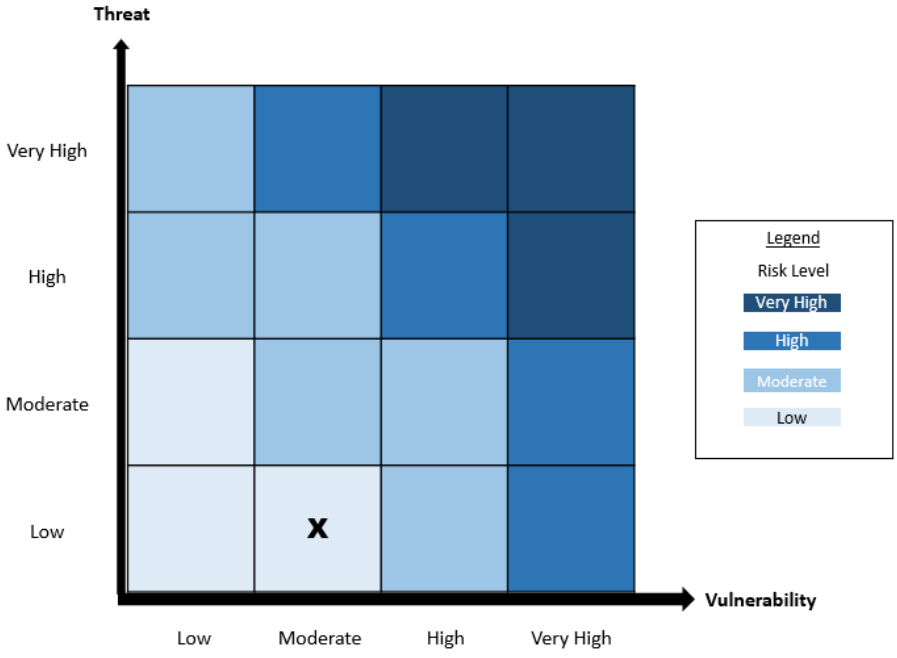
A second essential measure is that **CSD participants are, in principle, themselves supervised entities subject to AML/CTF obligations**. Participants are further subject to due diligence on the part of Euroclear France, which consists of verifying compliance with the admission criteria (including submission to an AML/CTF system) based on risk criteria, particularly geographical risk criteria.

While these measures do cover the identified vulnerabilities, the residual vulnerability (after mitigation measures) is still deemed to be **MODERATE** for the central securities depositary.

### Risk rating

Consequently, the combination of the threats and residual vulnerabilities after mitigation measures leads to a **LOW** level of risk for the central securities depository.

## Euroclear




**Overall risk : Low**

## 8. CRYPTOASSETS OR 'DIGITAL ASSETS'

In France, cryptoassets have been referred to as 'digital assets' since law No. 2019-486 of 22 May 2019 on the growth and transformation of undertakings (known as the 'PACTE Law'). These include[114]:

- any digital representation of a security which is not issued or guaranteed by a central bank or public authority, which is not necessarily attached to a legal tender and which does not have the legal status of money, but which is accepted by natural persons or legal entities as a means of trade, and which can be transferred, stored or traded electronically;
- tokens defined as any intangible asset representing, in digital form, one or more rights that can be issued, registered, kept or transferred by means of a shared electronic recording device enabling the owner of the asset to be identified, directly or indirectly.

As the ACPR's SRA points out, other definitions exist, in particular that of the European Markets in Crypto-Assets ***(MiCA)*** Regulation[115]. The latter, adopted by the European Parliament on 20 April 2023 and due to come into force in 2024, sets out a definition of cryptoassets based on their various uses[116].

As the NRA points out:

- In practice, the digital assets seen in circulation are based on blockchain-type technologies. Digital assets can be transferred in the absence of a trusted third party, linking users directly to one another;

- In principle, a digital asset is stored in an electronic wallet with which are associated, on the one hand, a private cryptographic key, held only by the owner, and, on the other hand, a public cryptographic key, used to identify the owner when carrying out a transaction on the blockchain. A wallet can be managed directly by its owner using software installed on their connection device (computer or telephone). This is referred to as a non-hosted wallet. Conversely, a user can entrust its management to a digital asset service proider (***DASP***). This is known as a hosted wallet;

- In particular, these DASPs provide services for the custody of digital assets, the purchase and sale of digital assets against legal tender or other digital assets, and the management of digital asset trading platforms;

- According to the COLB's assessment of the digital assets sector as a whole[117]:
  - *"While the threat is still relatively insignificant today, it could become significant in the medium term, given the patterns identified, and therefore requires very close monitoring. It is therefore very high in terms of both money laundering and terrorist financing"*;
  - "*The intrinsic vulnerabilities presented by digital assets can be considered to be high, both in terms of money laundering and terrorist financing"*;
  - "*The residual vulnerabilities presented by digital assets are considered to be high, both in terms of money laundering and terrorist financing";*
  - "*As a result, a combination of threats and residual vulnerabilities after mitigation measures leads to a very high level of risk for the digital assets sector"*.

With regard specifically to DASPs, supervision of AML/CTF obligations is split between the AMF and ACPR[118]: the AMF is responsible for those providers authorised under Article L. 54-10-5 of the Monetary and Financial Code, with the exception of the service providers referred to in Article L. 561-2, 7° bis of the same code, i.e. providers of

[114] Monetary and Financial Code, Articles L. 54-10-1, 2° and L. 552-2.
[115] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets (MiCA).
[116] Namely means of payment (cryptoassets such as bitcoin, ether and stablecoins), tokens that confer rights (utility tokens, non-fungible tokens) and financial instruments (security tokens).
[117] COLB, NRA 2023, Chapter 9, pgs 115 to 122.
[118] Monetary and Financial Code, Articles L. 561-36, I, 2° L. 561-36-1 and L. 561-2.

the services referred to in Article L. 54-10-2, 1° to 4°[119] of the Monetary and Financial Code, over which the ACPR has jurisdiction.

In terms of the SRA, a distinction should be made between:

- the risks associated with the **authorised DASPs falling within the remit of the AMF (8.1**);
- **the risks associated with token issues or 'ICOs' (8.2**).

### 8.1. DASPS

#### Sector description

The PACTE Law introduced a specific framework for DASPs. It has defined ten digital asset services, as follows[120]:

- **the custody of digital assets on behalf of third parties**: *this activity consists of managing, on behalf of a third party, the means of access to the digital assets registered in the shared electronic registration system and keeping a register of positions, opened in the name of the third party, corresponding to their rights to the said digital assets;*
- **the purchase and sale of digital assets against legal tender,** i.e. the conclusion of purchase or sale contracts on behalf of a third party relating to digital assets against legal tender, with, where applicable, the interposition of the service provider's own account;
- **the trading of digital assets for other digital assets:** this activity consists of concluding contracts providing for the trading of digital assets for other digital assets on behalf of a third party, with, where applicable, the interposition of the service provider's own account;
- **the operation of a digital asset trading platform:** this means managing one or more digital asset trading platforms, where multiple third-party interests in purchasing and selling digital assets for other digital assets or legal tender can interact in a way that results in the conclusion of contracts;
- **other services on digital assets**, inspired by the investment services regulated by MiFID II, such as the reception and transmission of orders for digital assets on behalf of third parties, digital asset portfolio management on behalf of third parties, advice to subscribers of digital assets, underwriting, guaranteed placement and unguaranteed placement in relation to digital assets[121].

Depending on the services they provide, DASPs may:

[119] Namely the following services: 1° The service of custody of digital assets on behalf of third parties or providing access to digital assets, where applicable in the form of private cryptographic keys, with a view to holding, storing and transferring digital assets; 2° The service of buying or selling digital assets against legal tender; 3° The service of trading digital assets for other digital assets; 4° The operation of a digital asset trading platform.
[120] Monetary and Financial Code, Article L. 54-10-2.
[121] These services are defined as follows in Article D. 54-10-1 of the Monetary and Financial Code:
*"5-1. The digital asset order reception and transmission service consists of receiving and transmitting orders for digital assets on behalf of a third party;*
*5-2. The service of digital asset portfolio management on behalf of third parties consists of the discretionary and individualised management of portfolios including one or more digital assets under a mandate given by a third party;*
*5-3. The service of providing advice to digital asset subscribers consists of providing personalised recommendations to a third party, either at the request of the third party or at the initiative of the service provider providing the advice, entailing one or more digital assets;*
*5-4. The digital asset underwriting service is the direct acquisition of digital assets from a digital asset issuer with a view to selling them;*
*5-5. The service of the guaranteed placement of digital assets consists of finding purchasers on behalf of an issuer of digital assets and guaranteeing the issuer a minimum amount of purchases by undertaking to purchase the digital assets not placed;*
*5-6. The service of the non-guaranteed placement of digital assets consists of finding purchasers on behalf of an issuer of digital assets without guaranteeing an acquisition amount".*

- be subject to registration with the AMF and supervision by the ACPR in terms of AML/CTF. In fact, the DASPs established in France or providing services in France that engage in (i) the custody of or access to digital assets on behalf of third parties, (ii) the purchase or sale of digital assets against legal tender, (iii) the trading of digital assets for other digital assets, or (iv) the operation of a digital asset trading platform, are subject to registration with the AMF with the approval of the ACPR. Registration is preceded by an examination of the competence and good repute of the managers and, for the first two categories of service provider, verification of certain aspects of the AML/CTF system. Once registered, DASPs are subject to all AML-CTF obligations, under the supervision of the ACPR;

- further apply for optional authorisation from the AMF, which entails additional obligations (e.g. IT security and prevention of conflicts of interest), under AMF supervision. The AMF also monitors authorised service providers' compliance with the AML/CTF provisions.

DASPs from the European Economic Area may provide services (i) to (iv) in France after registration with the AMF. They are mainly supervised by the authorities in their country of origin. However, the AMF may nevertheless delist them, either at its own initiative or at the ACPR's request, if they fail to comply with the obligations associated with registration.

As at 31 December 2023:

- **Only one DASP had been authorised by the AMF,** on 18 July 2023, for custody of digital assets, buying and selling digital assets against legal tender, trading digital assets for other digital assets, and receiving and transmitting orders for digital assets on behalf of third parties[122];
- **107 DASPs had been registered** and not delisted.

Four DASP delisting decisions have been made[123]. Two occurred in 2022, in the first case for cessation of activity, and in the second for non-compliance with the registration requirements (regulatory breach of the requirements set out in Article L. 54-10-3, 1° of the Monetary and Financial Code relating to the obligations of good repute and competence of managers, and regulatory breaches of the obligations relating to anti-money laundering and countering terrorist financing, and the freezing of assets referred to in Article L. 54-10-3, 4° of the Monetary and Financial Code). Two other delistings took place in 2023 and 2024, in both cases at the request of the players concerned, for reasons of restructuring or cessation of activity.

In 2023[124], the cumulative volume of purchases/sales of digital assets against legal tender represented €2.4 billion solely for those DASPs established in France (i.e. not including business done in France by DASPs established abroad). The total amount of digital assets held on behalf of their clients was €1.3 billion. Finally, the total volume of trades between digital assets amounted to a total of €41 billion.

While the cryptoasset sector was still marginal in volume terms a few years ago, in recent years it has experienced rapid growth and particular exposure to ML/TF threats which has attracted the full attention of the supervisors and led to the adaptation of the regulatory framework, in particular with the adoption of new regulations (MiCA Regulation[125] and the revision of the 'transfer of funds' regulation ***(TFR)***[126] leading to the inclusion, from the end of 2024, of cryptoasset service providers in the scope of AML/CTF obliged entities[127].

[122] AMF, list of authorised DASPs.
[123] See here.
[124] Based on ACPR figures from the AML/CTF questionnaires submitted by DASPs (covering 87% of DASPs covered by this reporting).
[125] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets.
[126] Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 ***(TFR Regulation)***.
[127] TFR Regulation, Article 38(2)(c), amending Article 3(19) to include cryptoasset service providers in the scope of AML/CTF obliged entities defined by the 4th Directive.

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

As indicated in the NRA, digital assets are susceptible to misappropriation and use for ML/TF purposes. Their exposure to the threat is particularly high on account of the transnational and virtually immediate nature of the transactions, the opacity of the trading channels and the volume of transferable values. Simply converting a currency into digital assets and then back into legal tender can be sufficient to conceal the illegal origin of funds.

According to Tracfin, cryptoassets are being used more and more, in particular for laundering funds derived from criminal activities (e.g. ransomware attacks), in tax fraud circuits and for terrorist financing[128].

Furthermore, as the ACPR points out in its SRA, digital assets are a prime vector for money laundering. They can be used to acquire or sell prohibited goods (drugs, weapons), illicit products or personal data (forged or false identity documents, credit card numbers), possibly from a site accessible on the darknet or the deepweb. They are also used as a vehicle for tax fraud and the laundering of its proceeds. Activities that are particularly vulnerable to money laundering threats are those that involve the purchase/sale of digital assets against legal tender via trading platforms, with rare cases of physical ATMs. Platforms offering services for trading in digital assets also play a major role in money laundering circuits by enabling digital assets based on traceable blockchains to be converted into digital assets based on less traceable blockchains guaranteeing the anonymity of the transactions. Digital assets can be the subject of financial scams such as bogus investment offers using websites or promotion by influencers on social media to attract money transfers from individuals, or through investment platforms operating in a context of high market volatility. Digital assets can also be used to collect and/or channel funds to a terrorist organisation. The use of cryptoassets can also be a means of circumventing asset freezing measures and other financial sanctions, which DASPs, like other institutions, must apply.

Given the rapid growth in the use of cryptoassets and the proliferation of the types of digital assets, the threat of their use for criminal purposes is considered to be **VERY HIGH** in terms of both money laundering and terrorist financing, and warrants very stringent monitoring.

### Vulnerabilities

#### Intrinsic vulnerabilities

The digital assets sector has specific characteristics that can facilitate money laundering or terrorist financing.

- Anonymity: use of pseudonyms, public addresses, the possibility of using mixers in certain blockchains to preserve the anonymity of participants, or the use of certain private blockchains that do not allow access to transaction data or the addresses of the wallets involved in these transactions, make it very difficult to ascertain the origin of digital assets

- By construction, digital assets offer the possibility of carrying out transactions without the intervention of a trusted third party or one subject to AML/CTF regulations, via so-called self-hosted portfolios that do not require any identification step

- More generally, digital assets are subject to complex infrastructures and can give rise to multiple conversions, which can contribute to the opacity of transactions

- These relationships are almost exclusively ‘remote’, with a cross-border dimension that makes it difficult to identify the parties to the transactions

[128] TRACFIN, Annual Report 2023, Volume 3.

- The sector lacks maturity in terms of AML/CTF, due to its recent emergence and the limited size of certain players.

As a result, the intrinsic vulnerabilities of cryptoassets can be considered to be **HIGH**, both in terms of money laundering and terrorist financing.

### Mitigation measures and residual vulnerabilities

France is one of the first countries in the world to have adopted an ad hoc legislative and regulatory framework in the field of digital assets, making all market participants subject to the full range of AML/CTF rules.

This regulatory framework, introduced by the PACTE Law, provides for:

- **compulsory registration with the AMF, with the approval of the ACPR**, for the provision of the services referred to in Article L. 54-10-2, 1 to 4 of the Monetary and Financial Code;

- an **optional authorisation issued by the AMF for all digital asset services**. Authorisation requires the same AML/CTF due diligence as compulsory registration, including verification of the competence and good repute of the managers and significant shareholders. Authorised DASPs are also subject to additional requirements compared with registered DASPs, particularly in terms of the resilience and security of their IT systems.

The AMF has published a whitelist of registered or authorised DASPs on its website, enabling investors to identify market participants that offer guarantees of a conscientious approach, good repute and compliance with anti-money laundering and countering terrorist financing rules.

Under this regime, **the largest players accounting for the greater part of this sector** are subject to AML/CTF regulatory requirements, in particular those relating to due diligence in respect of clients and their beneficial owners, and to AML/CTF supervision by the ACPR. For an assessment of the risks of these players, please refer to the ACPR's SRA.

To date, only one player has AMF authorisation. The volume of business represented by authorised DASPs is therefore presently very marginal compared with the volume of registered DASPs.

There are also additional guarantees attached to the status of authorised DASP compared with that of registered DASP. DASPs seeking AMF authorisation to carry on their activities must meet requirements in terms of financial resources, organisational rules and good conduct, for example. In particular, whatever the service provided[129], they must have **adequate security and internal control arrangements**, a resilient and secure IT system[130] and a system for managing conflicts of interest. They must provide the AMF with a programme of operations[131] detailing, in particular, the lists or categories of digital assets covered by their activities, the geographical distribution of their activities, the methods of marketing digital assets, the human and technical resources allocated to the various planned activities (**including those allocated to the internal control function**), as well as information on the **internal control and risk management systems** and details of the **systems for assessing and managing the risks of money laundering and terrorist financing**.

Finally, depending on the services they provide, they must satisfy specific conditions, including:

- for authorised DASPs providing a custody service: the setting-up of an asset custody policy, a system for segregating digital assets held on own account from those held on behalf of third parties, and the

[129] Monetary and Financial Code, Article L. 54-10-5, I.
[130] The AMF is responsible for verifying the security of the information systems of authorised service providers and may seek, to this end, the opinion of the *Agence Nationale de la Sécurité des Systèmes d'Information* (ANSSI) (Monetary and Financial Code, Article L. 54-10-5, i, in fine).
[131] AMF General Regulation, Article 721-3.

implementation of the means required to return digital assets as quickly as possible or to gain access to the digital assets held on behalf of their clients[132];

- for authorised DASPs providing services to buy or sell digital assets against legal tender or to trade digital assets for other digital assets[133] and for those providing a service to operate a digital asset trading platform[134], requirements liable to increase transparency and prevent abusive behaviour on digital asset markets;
- for DASPs authorised to provide digital asset portfolio management services on behalf of third parties or advice to digital asset subscribers[135], the obligation to obtain from their clients the information necessary to recommend digital asset services or digital assets suited to their situation, which may contribute to the implementation of the know your client obligations.

All of these additional requirements are measures that help to mitigate the high intrinsic vulnerabilities of the sector. The transition to 'enhanced' registration[136] introduced by the DDADUE Law, which aims to align the requirements applicable to the framework for the registration of DASPs with certain requirements applicable to authorisation, is also intended to mitigate these vulnerabilities.

Taken together, these factors suggest that the residual vulnerability of authorised DASPs is **MODERATE**.

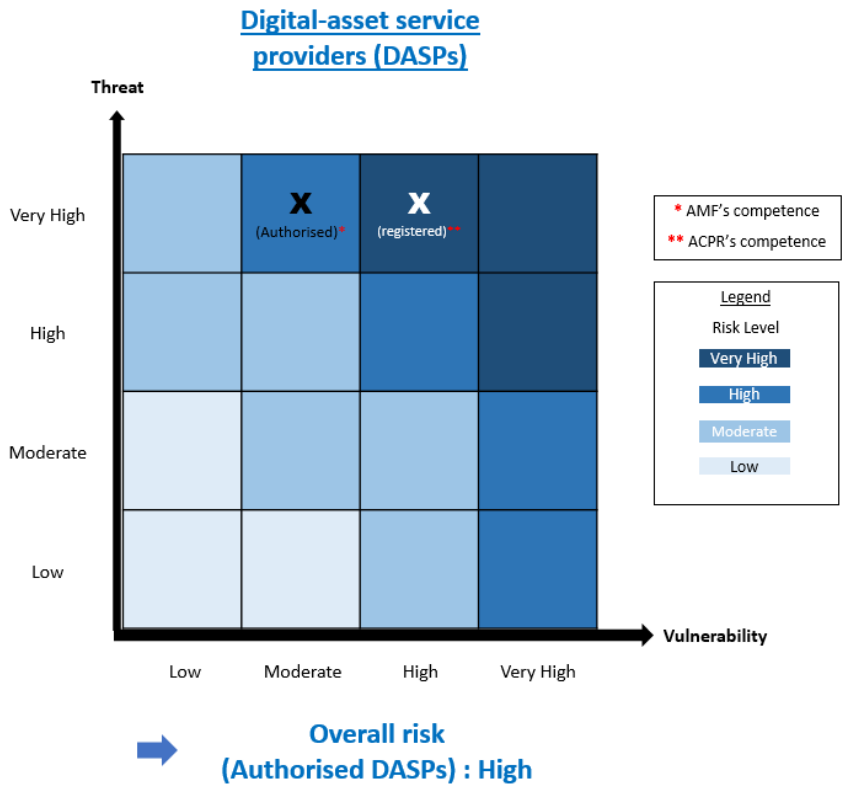
### Risk rating

Consequently, when the threats and residual vulnerabilities after mitigation measures are combined, the **overall** level of **risk** for the authorised DASP sector is **HIGH**, while that for registered DASPs is **very high** in the ACPR's SRA.

With regard to registered DASPs, it should be noted that the ACPR's SRA contains developments in their regard, which show in particular that:

- Given the rapid growth in the use of cryptoassets and the increase in the types of digital assets, the threat of their use for criminal purposes is considered to be **very high** in terms of both money laundering and terrorist financing, and warrants very stringent monitoring;
- The intrinsic vulnerability of digital assets is **high**, both in terms of money laundering and terrorist financing;
- Despite all the mitigation measures, the residual vulnerability of digital assets remains **high;**
- The combination of residual threats and vulnerabilities, after mitigation measures, leads to a **very high** level of risk of money laundering and terrorist financing in the digital assets sector.

[132] Monetary and Financial Code, Article L. 54-10-5, II.
[133] Monetary and Financial Code, Article L. 54-10-5, III (publication of a firm price for digital assets or a method for calculating the price of digital assets, publication of the volumes and prices for the transactions they have carried out, obligation to execute their clients' orders at the prices displayed at the time they are received).
[134] Monetary and Financial Code, Article L. 54-10-5, IV (introduction of operating rules ensuring fair and orderly trading; publication of the breakdowns of the orders and transactions concluded on their platforms).
[135] Monetary and Financial Code, Article L. 54-10-5, VI, 6° and AMF General Regulation, Article 722-21.
[136] Pursuant to the provisions of Article 8 of law No. 2023-171 of 9 March 2023 containing various measures for adapting to European Union law in the fields of the economy, health, employment, transport and agriculture (the DDADUE Law), DASPs that had submitted an application for registration on or after 1 July 2023 that the AMF deems to be complete in terms of the applicable laws and regulations are subject to 'enhanced' registration, the requirements of which are similar to those for DASP authorisation. To date, none of the DASPs registered by the AMF have been registered under the 'enhanced' registration regime.




## 8.2. TOKEN ISSUERS (ICOS)

### Sector description

An Initial Coin Offering (ICO) is a fundraising operation carried out via a shared electronic recording device (or 'blockchain') that results in a token issue that can then be used to obtain products or services, as applicable.

After much enthusiasm for this type of fundraising in 2016-2018, the number of ICOs actually carried out fell in 2019. In any case, these amounts are very small compared with traditional financing channels.

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

ICOs are exposed to the threat posed by their ecosystem: the use of blockchain and of other digital asset services providers.

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

- The tokens that can be subscribed to as part of an ICO can generally only grant entitlement to one service or product ('utility token');
- they are illiquid and therefore difficult to convert into other digital assets or legal tender;
- the risk of the total loss of the investment due to the low maturity of the issuing companies is very high.

For these reasons, the threat of money laundering or terrorist financing in connection with the ICOs approved by the AMF is assessed as **LOW**[137].

[137] In the absence of AMF approval, subscribers to an ICO are not subject to identity verification by the issuer. Such situations may allow a concealed transfer of funds from the subscriber to the issuer.

## Vulnerabilities

### Intrinsic vulnerabilities

The vulnerabilities of the ICO sector are also those linked to its ecosystem: the use of technologies that favour anonymity, and relationships that are exclusively remote and cross-border (see above).

As such, the intrinsic vulnerabilities of the ICO sector can be considered to be **VERY HIGH**.

### Mitigation measures and residual vulnerabilities

The PACTE Law introduced a specific regime for public offerings of tokens, providing for the possibility of obtaining AMF approval, and made token issuers seeking AMF approval subject to all applicable AML/CTF rules.

Before issuing its approval, the AMF is responsible for checking, among a number of other requirements, that the token issuer has put in place a system enabling it to comply with its anti-money laundering and countering terrorist financing obligations. Unlike DASPs which, in their capacity of market participants, have a long-term obligation, token issuers are only subject to AML/CTF obligations for the duration of the ICO approved by the AMF and within the limits of transactions with subscribers. For subscriptions of less than €1,000, the regulations do not require issuers to implement due diligence measures for subscribers ('occasional clients' within the meaning of the regulations). However, the AMF recommends that token issuers identify all their subscribers, regardless of the amount of the subscription.

Like the authorisation issued for the provision of certain digital asset services, the approval is optional. Thus, only those issuers of ICOs that have applied for and obtained AMF approval for their issue are subject to the AML/CTF rules. Issuers not seeking approval can raise funds through ICOs without implementing any AML/CTF measures. This regime does not apply to Security Token Offerings (STOs).

Approval provides a number of guarantees for subscribers, giving issuers wishing to carry out an ICO a competitive advantage, which should be a strong incentive to obtain approval. The AMF publishes the list of approved ICOs.

An examination of the applications received shows that 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 needed to recruit qualified AML/CTF staff or to call on external legal advice. It is therefore stipulated that issuers may outsource all or part of their AML/CTF obligations to specialised external service providers: this possibility is recent and not very developed. The AMF has also published the main AML/CTF provisions applicable to token issuers on its website to help them better understand their main obligations.

The number of approvals granted by the AMF is still very limited: Five approvals issued between December 2019 and February 2024, of which only one was still valid on 1 May 2024. It should also be noted that the AMF was also asked to approve a public offering of tokens by unscrupulous project owners, leading the AMF to issue a warning to the public[138].

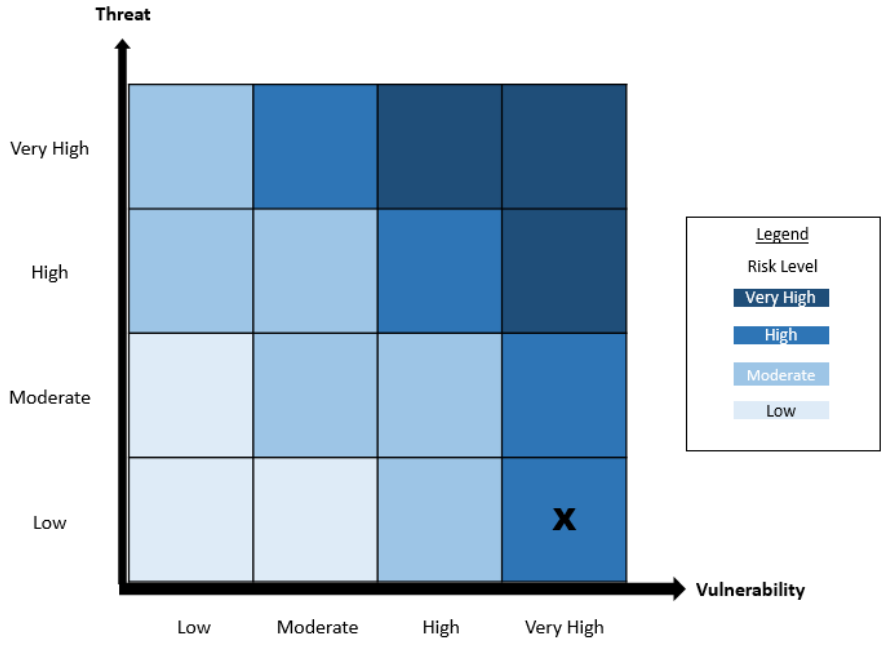
In view of the foregoing information, there are grounds to consider the vulnerabilities to still be **VERY HIGH**.

## Risk rating

As a result, the combination of the threats and residual vulnerabilities after mitigation measures results in a **HIGH** level of risk for the ICO sector.

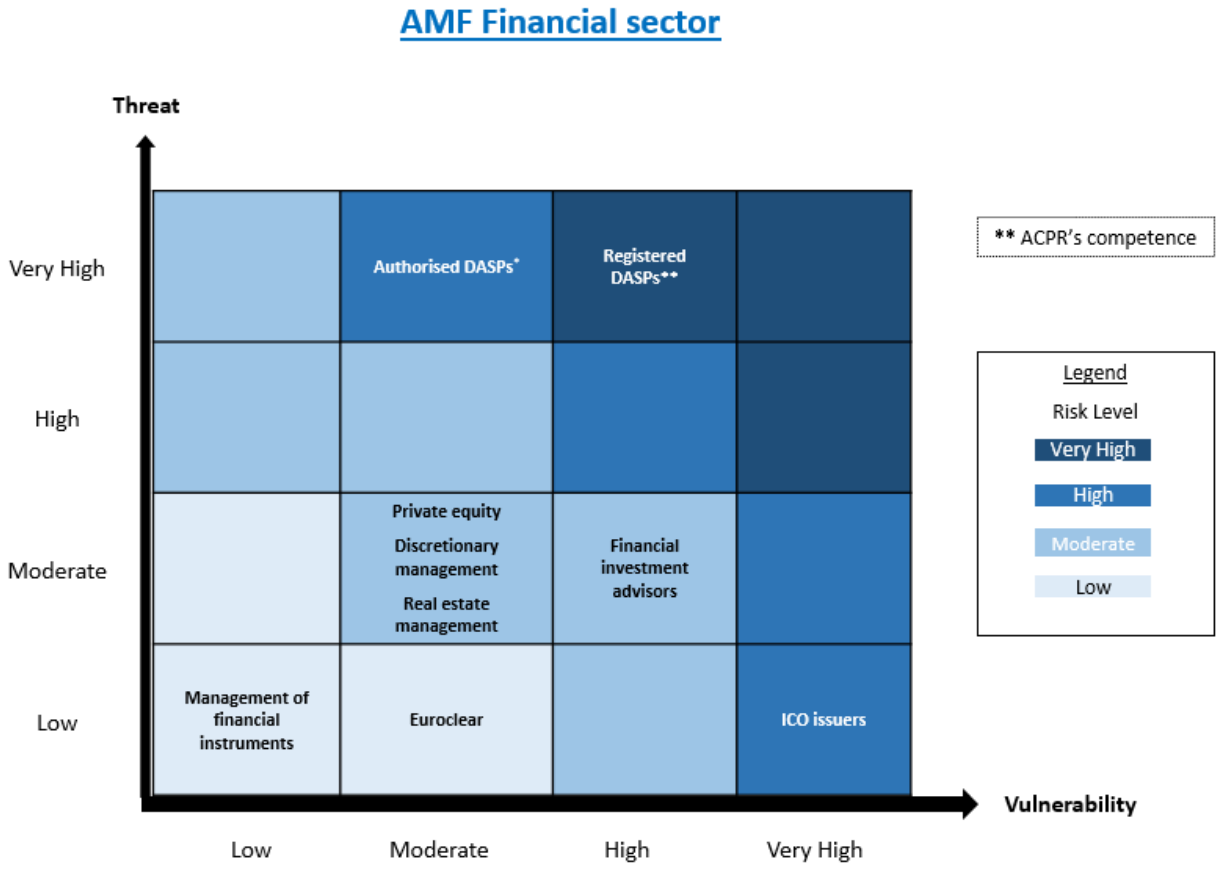
[138] AMF, press release dated 30 September 2021.

## ICO issuers




**Overall risk : High**

## 9. RATING SUMMARY




*Note: as at 14 May 2024, 103 PSANs were registered and 1 was authorised