National Risk Assessment on Money Laundering and Terrorist Financing

2026

Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias

Public version

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ECONOMÍA, COMERCIO Y EMPRESA

1. EXECUTIVE SUMMARY 3
2. INTRODUCTION 5
3. METHODOLOGY 6
4. THREATS OF MONEY LAUNDERING. 8
4.1. Organised Crime 8
4.2. Drug trafficking 17
4.3. Economic and financial crimes 23
4.3.1. Fraud offences 23
4.3.2. Tax offences 26
4.3.4. Corruption offences 27
4.4. Money Laundering by third parties and in relation to offences committed abroad. 29
5. MAIN THREATS FROM TERRORIST FINANCING 34
5.1. Terrorist Financing in Spain 36
6. MAIN VULNERABILITIES IN MONEY LAUNDERING AND TERRORIST FINANCING. 40
6.1. Vulnerabilities arising from the population 40
6.2. Vulnerabilities arising from geographical factors 40
6.2.1 Conducting operations in high-risk territories or with citizens/entities from those territories .. 40
6.2.2. Transactions with countries at higher risk of Terrorist Financing 41
6.2.3. Activities in the areas of Gibraltar and Ceuta-Melilla. 42
6.3. Vulnerabilities arising from the nature of the organisation or the activity carried out. 43
6.4. Vulnerabilities arising from the means of payment 44
6.4.1. Vulnerabilities arising from the use of cash and the informal economy. 44
6.4.1. Risks associated with the use of crypto-assets 45
6.5. Vulnerabilities arising from technological innovations in financial transactions 46
7. SECTORAL ANALYSIS 48
Sector: Credit Institutions 2026 48
Sector: Insurance and pension funds 2026 62
Sector: Securities 2026 69
Sector: Mutual Guarantee Societies 2026 78
Sector: Money transfers 2026 84
Sector: Other services provided by payment institutions 2026 97
Sector: Electronic money institutions 2026 106
Sector: Currency exchange 2026 115
Sector: Postal money orders 2026 122
Sector: Credit Institutions (CIs) and Lenders other than credit institutions, CIs and credit intermediaries 2026 ... 128
Sector: Credit intermediaries 2026 138
Sector: Property sector 2026 145

Sector: Auditors, external accountants and tax advisers 2026 153
Sector: Notaries 2026 161
Sector: Land, commercial and movable property registrars 2026 169
Sector: Lawyers 2026 178
Sector: Provision of corporate services to third parties 2026 187
Sector: Gambling: casinos, lotteries, slot machines and gaming venues, land-based betting, online gambling, sports and charity pools (quinielas) 2026 195
Sector: Jewellery, precious stones and metals 2026 211
Sector: Art and antiques 2026 217
Sector: Tangible assets 2026 224
Sector: Cash-in-transit 2026 230
Sector: Professional trade in other high-value goods 2026 237
Sector: Emissions rights 2026 243
Sector: Crypto-asset service providers 2026 250
Sector: Crowdfunding Platform Activities 2026 260
Sector: Multiple IBANs 2026 267
8. CONCLUSIONS 275
APPENDIX 1. Bibliography 277
APPENDIX 2. Collaborating public institutions and private sector organisations 278
APPENDIX 3. List of tables, charts and graphs 280
APPENDIX 4. Acronyms 282

1. EXECUTIVE SUMMARY

1. The aim of this analysis is to identify and assess the ML/TF threats, vulnerabilities and risk levels previously identified in the 2020 NRA and updated in the 2024 Addendum. To this end, quantitative and qualitative information has been used, drawn from official records, tip-off reports, financial intelligence reports, police and judicial investigations, as well as the operational experience of regulated entities and competent authorities.

2. The obligation to carry out a National Risk Assessment (NRA) was established by Directive (EU) 2015/849, recently updated by Directive (EU) 2024/1640 and Recommendation 1 of the FATF, which set out the principles of the Risk-Based Approach (RBA).

3. The **threats posed by Money Laundering** (ML) in Spain continue to be dominated by organised crime and drug trafficking, to which economic crimes – particularly fraud and large-scale VAT schemes – have been added with increasing prominence, whilst also bearing in mind the sharp rise in investigations into corruption offences. Organised crime demonstrates a high capacity for adaptation, with increasingly complex structures, functional specialisation (*'Crime as a Service*') and intensive use of digital technologies, crypto-assets and informal systems such as the *hawala*, which makes it difficult to trace funds. Drug trafficking, for its part, remains one of the main sources of illicit capital, with transnational networks operating across multiple territories and using various methods to introduce and move money into the formal economy. At the same time, economic crime has seen exponential growth since 2020, driven by digitalisation, the use of artificial intelligence and increasingly sophisticated fraud schemes, as well as complex tax fraud and corruption schemes involving significant sums of money. Taken together, these threats are characterised by their global scale, their high profitability, the combined use of traditional financial channels and new technologies, and their ability to infiltrate various economic sectors, thereby increasing their impact on the financial system and the economy.

4. **Threats relating to Terrorist Financing** (TF) are characterised by the growing decentralisation of terrorism, the prominence of lone actors and micro-cells, and the constant adaptation of their financing mechanisms. The main threat remains linked to jihadist terrorism, particularly to structures associated with Daesh. Terrorist organisations combine traditional methods, such as cash or the *hawala system*, with new technologies and digital tools, including crypto-assets, *crowdfunding*, *fintech* platforms, the use of video games and encrypted messaging, which facilitate the mobilisation of funds with greater levels of anonymity. Furthermore, the convergence between terrorism and organised crime persists, as does the risk of non-profit organisations being misused to channel resources towards terrorist purposes. Although the financial scale of the operations detected is usually small, the threat retains a high operational capacity and impact, particularly in digital environments and in processes of recruitment, radicalisation and logistical support.

5. Spain's **main vulnerabilities** in the area of ML/TF stem from demographic, geographical, economic and technological factors that facilitate the concealment and movement of illicit funds. These include, in particular, the increase in the foreign population and its concentration in cash-intensive sectors and the informal economy; operational exposure to high-risk jurisdictions and

sensitive geographical areas such as Gibraltar, Ceuta and Melilla; and certain particularly vulnerable activities and entities, such as payment institutions, crypto-asset service providers (CASPs), online gambling, the property sector, corporate services, lawyers and charitable organisations. Furthermore, there remains a high level of vulnerability associated with the intensive use of cash and the rise in the use of crypto-assets, whose operations—which can be made opaque through techniques designed for that purpose, and which are cross-border and highly technology-driven—make it difficult to trace funds when certain techniques are employed. Added to this is the impact of financial digitalisation, cybercrime and the use of artificial intelligence, which amplify the risks through complex fraud, the automation of operations, identity theft and the use of digital and decentralised platforms to move illicit funds quickly and anonymously.

6. The **sectoral analysis** shows that the highest levels of residual risk in relation to Money Laundering and Terrorist Financing are concentrated in certain financial, technology and professional sectors whose operational characteristics facilitate the concealment and movement of illicit funds. Of particular note are electronic money institutions and money transfer services, both of which present a high risk of ML due to the speed of their operations, the fragmentation of transactions and cross-border activity. Similarly, the property sector, the legal profession, online gambling and unregulated crypto-asset service providers (CASPs) present a substantial risk, particularly in relation to ML. In the field of crypto-assets, even regulated crypto-asset service providers (CASPs) remain significantly exposed due to the technological and cross-border nature of these operations. Credit institutions also retain a substantial level of risk due to the volume and complexity of international transactions, although this is mitigated by the existence of robust preventive controls. Finally, other sectors such as certain payment institutions, lenders and alternative financial services providers, or land-based casinos, also present significant exposure.

7. Sectors with low residual risk include mutual guarantee societies, postal money orders, tangible assets, cash-in-transit services, the professional trade in other high-value goods, and emission rights – either due to the high level of regulation to which the sector is subject, the small size and/or limited activity of the sector, or the extensive implementation of preventive measures.

8. Based on this sectoral risk analysis, the mitigating measures designed to address these risks are integrated in a coordinated manner into the National Strategy to Combat Money Laundering, which will be approved following this National Risk Analysis, and will also be incorporated into the 2020 update of the National Strategic Plan against Terrorist Financing (PENCFIT), in line with the National Counter-Terrorism Strategy (ENCOT) updated in 2023. This establishes a comprehensive framework for action that enables the strengthening of prevention, detection and investigation in the areas of greatest risk exposure.

2. INTRODUCTION

9. Article 7 of Directive (EU) 2015/849 laid down the obligation for Member States to identify, assess, understand and mitigate national risks of Money Laundering and Terrorist Financing (ML/TF) by drawing up and updating a national risk assessment, which was transposed into Article 44(2)(ñ) of Law 10/2010 of 28 April on the prevention of Money Laundering and Countering the Financing of Terrorism (AML/CFT), which confers the power to approve this assessment on the COPBLAC. This risk-based approach has been reinforced and updated by Article 8 of Directive (EU) 2024/1640, which emphasises the obligation to carry out the national risk assessment.

10. These principles were set out in the full version of the NRA published in 2020 and in the update that took place with the publication of Addendum 2024 to the NRA.

11. In this context, this NRA constitutes a comprehensive and complete assessment of the ML/TF risks affecting all regulated entities covered by Law 10/2010 of 28 April, which deals with Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT). Unlike previous exercises, which focused on partial or sector-specific updates – as the preliminary analysis indicated that there were no changes to the other risks – this analysis takes a comprehensive approach to the threats, vulnerabilities and risks associated with all sectors subject to preventive obligations, taking into account the evolution of criminal patterns, national and international regulatory changes, the impact of the digitalisation of financial services and the growing complexity of the structures and methods used to channel illicit funds. From a methodological perspective, whilst it builds on previous analyses, it seeks to strengthen the quantitative basis of the analysis and simplify it to ensure a better understanding of the risks.

12. Since 2020, events such as the COVID-19 pandemic, the war between Russia and Ukraine, the Israeli-Palestinian conflict, the increased risks associated with international financial sanctions, the expansion of crypto-asset service providers (CASPs), the development of new *Fintech* solutions and the growing use of advanced technological tools in the financial sector have created new challenges for authorities, institutions and regulated entities. At the same time, criminal organisations and Terrorist Financing networks have evolved their methods and operational mechanisms, exploiting vulnerabilities arising from financial globalisation, the international interconnection of markets and rapid technological innovation.

13. All of this requires the continuous updating of mechanisms for identifying, assessing and understanding risks, enabling the competent authorities and regulated entities to adapt their preventive systems to new types of crime, modus operandi and emerging risk factors. Consequently, this analysis is intended to serve as a strategic tool to strengthen the preventive and response capabilities of the national system for Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT), facilitating the adoption of mitigating measures proportionate to the identified risks, the adaptation of the regulatory framework, institutional strengthening and the improvement of national and international coordination, in both the preventive and enforcement spheres.

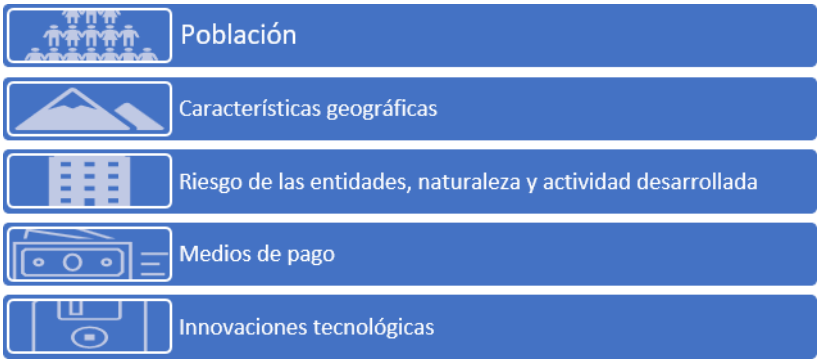
3. METHODOLOGY.

14. This update to the NRA was prepared in accordance with the FATF Guidelines for a National Money Laundering Risk Assessment (FATF 2024) and the FATF Guidelines for the Assessment of the Risk of TF (FATF 2019), as well as the Fourth Directive and its amendment by the Fifth Directive. The analysis drew on various national and international sources of information, and consultations were held with the relevant public authorities in each area and with representatives of the private sector. Annexes I and II contain the supporting documents used in the preparation of this analysis, as well as details of the participating institutions. Furthermore, Annex 3 provides a systematic overview of the regulatory and institutional framework underpinning the Spanish preventive system for the prevention of money laundering and TF. It details the main regulations in force and the competent bodies that form the structure for supervision, control and coordination at national level.

15. This analysis follows the methodology established in 2020 for determining country risks based on threats[1] and vulnerabilities[2] at national level. As set out in the previous NRA, in order to establish ML/TF risks, it is necessary to identify[3] : (i) the threats present in Spain, (ii) the vulnerabilities of the system and the country context that may be exploited by these threats to carry out their activities, and (iii) the sectors (economic and non-economic) and the types of entities and legal structures that may be used or exploited by these threats to perpetrate ML/TF activities by taking advantage of existing vulnerabilities.

16. This methodology was also used for the 2024 Addendum, which additionally took into account endogenous factors that influenced the risks arising from the economic and social circumstances that have affected the system in recent years. This is the case, for instance, with the effects of the COVID-19 pandemic and the war in Ukraine on ML/TF.

17. To identify the system's inherent vulnerabilities, various factors that could be exploited for the commission of illicit activities have been analysed. The following vulnerabilities have been taken into account:



[1] 'Threats' are those individuals, groups of individuals or their activities that pose a potential danger due to their capacity to to cause harm to the State, society, the economy or other fundamental aspects of a country's life.
[2] 'Vulnerabilities' are those situations and circumstances that may be exploited or used by organisations or individuals seeking to carry out Money Laundering or Terrorist Financing activities.
[3] The definitions set out in the previous NRA are adopted; these are based on the international standards promoted by the FATF for the identification of threats, vulnerabilities and risks, as well as the aspects to be taken into account when determining the vulnerabilities and risk factors indicated for the definition of inherent and residual risk.

18. Furthermore, an individualised analysis has been carried out of the impact that these vulnerabilities have on each of the different financial and non-financial sectors, their activities, corporate structures and other elements and operations that could be exploited by various threats for ML/TF purposes, leading to an assessment of the risk level for each of them.

19. Consequently, each chapter analyses the vulnerabilities associated with activities, sectors and types of institutions, taking into account the identified threats, characteristics and context, in order to determine the risk exposure of each. To this end, account is taken of vulnerabilities arising from the existence of endogenous[4] and exogenous[5] risk factors.

20. The result of this analysis is an assessment of the various types of risk affecting each sector, taking into account the type of natural or legal persons operating in that sector, the products it markets, the services it provides, the characteristics of its customers and the countries with which it operates. In addition to the specific nature of their operations and services, factors such as information gathered from supervisory experience, knowledge of the business gained through routine and ad hoc communications, and reports from external experts, amongst other sources, are assessed.

21. Specifically, for each sector, type of institution or activity, the inherent risk of them being used for ML/TF purposes is determined on the basis of their specific vulnerabilities and characteristics. The inherent risk is adjusted in line with the mitigating measures adopted at national level for that sector, taking into account, amongst other factors, its prudential regulation, level of supervision, criminal prosecution, the sector's understanding of risks, the extent to which ML/TF prevention measures are implemented, and the quality of its internal control procedures. It is these mitigation measures that make it possible to determine the residual risk of sectors, entities and activities being used for ML/TF-related purposes.

22. In accordance with the rating system set out in Article 12(3) of Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Anti-Money Laundering and Counter-Terrorism Authority, the levels of inherent and residual risk shall be classified as follows:

Low	Medium	Substantial	High

23. Whilst the levels of inherent and residual risk have been assessed taking into account the rating system set out in Article 12(3) of Regulation (EU) 2024/1620 of the European Parliament and of the Council, the analysis carried out for the purposes of this methodology has required the introduction of intermediate risk levels. These intermediate categories are intended to provide a more granular and proportionate assessment of risks, allowing for a more precise distinction between situations which, although falling within the same regulatory risk category, exhibit materially different risk characteristics.

Low/Medium	Medium/Substantial	Substantial/High

[4] 'Endogenous' risk factors are those that are intrinsic to the sector, arising from its nature and characteristics, which may enable or facilitate access to or control by criminals; for example, by setting up or acquiring an entity for the purpose of using it for ML/TF, or by recruiting an employee or agent.

[5] *'Exogenous'* risk factors are external factors associated with the potential misuse by third parties of the services, channels or products offered by the sector; for example, through a customer's use, for ML/TF purposes, of legitimately provided commercial or financial services.

4. MONEY LAUNDERING THREATS.

24. The main ML threats continue to be associated with organised crime, drug trafficking and, more recently, offences linked to large-scale VAT fraud schemes, despite the fact that suspicious transactions linked to economic crimes have grown exponentially since 2020 (particularly in relation to fraud) and that investigations arising from these incidents have also intensified.

25. These types of crime generate a significantly higher volume of illicit funds being moved, which increases their potential impact on the financial and economic system. All of this is discussed and analysed in greater detail in the following sections.

4.1. Organised Crime.

26. The trends in the indicators show that organised crime remains a significant threat in the area of ML. Although reports based on evidence rose significantly in 2022 and subsequently fell, active investigations continue to show a clear upward trend, indicating more complex and long-running cases.

27. The number of individuals under investigation for Money Laundering as their primary activity has fallen markedly, but the number of linked individuals remains very high, confirming the existence of extensive support networks utilised by international criminal organisations. The number of organised groups under investigation remains stable, particularly those linked to other offences, highlighting the cross-cutting nature of Money Laundering within criminal activity.

Table 1. Reports based on evidence, investigations, judgements and convictions relating to organised crime

	2020	2021	2022	2023	2024	2025
Reports received on suspicion of organised crime*	269	543	758	823	802	596
Number of active investigations into organised crime active at the end of the year**	1,017	1,103	1,764	2,131	2,276	2,583
Number of investigations into organised crime investigations initiated per year **	846	827	1,358	1,977	1,857	1,905
Number of people investigated for organised crime asa **	2,339	1,966	1,704	909	895	1,548
No. of people investigated as related activity **	12,493	15,293	12,289	12,269	11,060	9,886

Organisedinvestigated investigated as their main activity **	24	20	22	15	15	18
Organised groups investigated for activities linked to other offences **	185	187	170	183	176	145
Number of detainees by ML (as main activity) belonging to organised crime **	340	380	181	124	104	108
No. of people detained by ML (as related activity) belonging to organised crime **	2,580	3,099	2,290	2,082	2,026	1,526
Convictions relating to organised crime ***	10	22	27	31	34	-
Convictions relating to organised crime ***	6	10	20	25	26	-
Number of people convicted for organised rime ***	26	24	15	30	50	-

Source: *SEPBLAC; **CITCO; *** FGE Annual Report 2025

28. Arrests for ML linked to organised crime show a decline, consistent with greater operational sophistication or the use of intermediaries. In contrast, the number of people convicted of organised crime has risen in recent years, reflecting greater effectiveness in the judicial phase. Overall, the data paint a picture of an active and adaptable threat, against which investigative and judicial efforts continue to strengthen.

29. It should be borne in mind that the current model for this criminal activity centres on 'Crime as a Service' (CaaS), where there is specialisation in the execution of the various stages of the crime within the criminal organisation – and particularly with regard to ML – operating independently of the criminal organisation itself. Under this model, criminal organisations recruit experts from a range of disciplines and adopt advanced technologies that optimise the execution of each stage of the crime and make it more difficult to investigate. Organised crime has rapidly adapted to the use of digital tools and technological solutions associated with information and communication technologies (ICT), even going so far as to develop or fund specific software to bolster its illicit activities and expand its capacity to operate with greater impunity[6] .

30. Among the tactics employed by organised crime, the proliferation of commercial companies set up

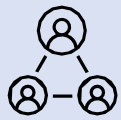
[6] See the National Strategy against Organised and Serious Crime 2025 https://www.dsn.gob.es/sites/default/files/2025-10/Estrategia%20Nacional%20contra%20el%20CO%20y%20la%20DG%202025.pdf

for the purpose of being exploited for committing crimes, acting as shell companies, without effective oversight of their promoters or directors.

31. In CaaS, communities have been identified that offer parallel **underground banking** services, without registration or supervision, enabling the informal international transfer of value (*hawala, fei chien,* etc.) with a high degree of opacity. This allows transfers to be made at a much lower cost than standard bank transfers and fees, and much more quickly, due to the absence of financial checks. Furthermore, the intensive use of stablecoins (USDT/USDC) for this purpose has been identified; this allows very large sums to be transferred in smaller amounts to other countries in a matter of seconds, without the risk of value fluctuations, at a very low cost and without the authorities' knowledge.

32. As regards undetected criminal activity, the State Security Forces and Bodies are aware that the data underestimate the extent of activity linked to organised crime, as there are trends in criminality that remain, to a certain extent, outside the scope of the authorities' surveillance. These identified trends are: the use of 'peer-to-peer' (P2P) payment methods, a significant increase in kidnappings and extortion linked to holders of crypto-assets, and the widespread use of encrypted communication systems**.** In short, undetected crime is not merely that which goes unreported or undetected, but rather that which is designed to leave no trace: delocalised, fragmented, encrypted and supported by digital infrastructures that dilute control points.

33. One of the main methods for channelling illicit flows is the splitting of cash. However, criminal organisations now tend to combine various methods of channelling funds with the aim of making them harder to trace. Table 1 sets out the methods identified, in addition to the aforementioned splitting of cash:

TABLE 1. Methods used by criminal organisations to channel funds	
Hawala 	The *hawala* system is not a new method, but it is the most common and widely used of the informal money transfer systems still in use today. It is not linked to organised crime per se, but it serves as a very useful tool for criminal organisations to move money, due to the lack of records for this type of transaction and the difficulty investigators face in tracing the money. These transfers have evolved to involve encrypted communication between the sender and recipient of the money, using codes known as *'tokens',* which usually correspond to the serial number of a legal tender banknote, ensuring that the amount transferred can only be handed over to the person holding that globally unique code. These transactions are completely opaque and operate in parallel to the conventional financial system, facilitating the concealment and transfer of funds to, for example, non-cooperative jurisdictions. The use of this method by Chinese organisations has been detected, combined with cash settlement or, more recently, evolved to include immediate settlement and transfer using crypto-assets.
Money in cash to CA, via 'money mules' 	The "mule" is a figure that has long been used by criminal organisations. Sometimes, the mule responds to a job advertisement, providing their personal details on a website advertised via social media, and is assigned the task of monitoring the operation of various payment systems. This monitoring involves receiving sums in *fiat* currencies into their account, which are then converted into CA and transferred to addresses specified by the criminal. The funds obtained may originate, for example, from a fraudulent online sale, and the proceeds of which are transferred to the money mule's account. Thus, the mule

	whether unwittingly or with intent (when acting in return for a commission), they are contributing to the illicit proceeds obtained by this criminal organisation. It has been observed that this is a system used in the CaaS model, where these *'crypto-mules'* convert illicit *fiat currency* into cryptocurrency to obscure both the origin and destination of the funds through multiple transfers. The types of organisations that generally use this method include cybercrime networks, online fraud rings and drug trafficking networks, which employ it primarily in the initial stages of money laundering to introduce and disperse illicit funds.
VAT Carousel 	A form of fraud carried out within a corporate network affecting several Member States, operating both in parallel and in a chain-like manner, and also involving several shell companies set up by large criminal organisations or by various internationally interconnected groups. The aim is to exploit loopholes in the existing VAT regulations governing intra-Community transactions. Thus, in accordance with current legislation, the movement of goods between Member States is exempt under the principle of taxation at the place of consumption, meaning that the chargeable event occurs at the place where the product is ultimately consumed, given the indirect nature of VAT. This situation not only prevents the collection of tax revenue but also affects free competition in the market, as companies that comply with their tax obligations are disadvantaged by those that evade tax.
Investment in property 	It enables large sums to be channelled into the formal economy and converted into assets that appear legitimate, particularly where there are links to drug trafficking offences. This is achieved through the acquisition of properties, commercial premises or land – either directly or via front men and shell companies – and by structuring payments through instalments, the use of cash or simulated financing. Manipulation of the declared price can be observed through overvaluation or undervaluation, unregistered property transfers or fictitious invoicing for renovations. Methods used to legitimise the capital include rental income or successive sales, generating lawful income and making it difficult to trace the origin of the money.
Channelling funds through the art and antiques market 	A method used both to launder the proceeds of criminal activity and to serve as a 'safe-haven asset' in which to invest those proceeds and keep them secure (given the enormous value of many works of art or antiques, and their minimal or non-existent depreciation). As this is a market in which price has a subjective component, it allows the works of art involved in ML operations to be significantly undervalued or overvalued. At the same time, it is a sector with a large number of intermediaries, which facilitates the anonymity of the beneficial owner of the traded items and in which informal channels or large amounts of cash are often used, making it easier to simulate transactions.
Trade-Base Money Laundering 	An alternative banking system used by large criminal networks, particularly those from Asia, where, through premises or establishments, they operate a clandestine system similar to the formal financial system, characterised by extensive use of cash. It is often combined with other systems such as *hawala* or the use of money mules, alongside over-invoicing or bulk shipments of goods.
Gift cards 	Cash is loaded onto this card and withdrawn in China or in other jurisdictions where the cash declaration threshold is higher than in Spain. They are used in particular by television and/or audio platforms, and large *retail* companies operating internationally.

34. Given the globalised nature of organised crime, it is difficult to pinpoint the jurisdictions involved in the movement of illicit funds. Police investigations have identified countries such as the United Arab Emirates, Türkiye, Ecuador, Bolivia, Mexico, Peru and Colombia.

35. Organised crime today is characterised by an increasing specialisation of its activities, offering highly professionalised illicit services that facilitate the commission of other offences, such as drug trafficking, human trafficking or smuggling. These organisations are operationally interconnected with terrorist networks, either through the provision of logistical or financial resources, or by exploiting the same routes used by these organisations to move funds or by interacting with the same clandestine structures. Furthermore, they systematically rely on corruption to remove obstacles, reduce risks and operate with greater freedom, thereby making it more difficult for the authorities to detect, trace and prosecute their criminal activities.

36. Table 2 sets out a categorisation of those organised crime groups identified as being active in Spain.

TABLE 2. Types of organised crime groups	
Groups of Latin American origin	Traditionally linked to illegal drug trafficking networks, they operate in Spain in cooperation with local networks that facilitate the smuggling and distribution of drugs. Certain South American countries are the main producers of cocaine, and nationals of those countries form part of groups specialising in the production and distribution of this substance. In these cases, there is a direct link between the predicate offences and ML activities. The drugs are smuggled into Europe, mainly via pre-established routes, many of which have their first point of entry into Europe in Spain. The linguistic and cultural characteristics of these criminals facilitate their integration in Spain, where there are communities of immigrants of the same nationalities, providing ideal cover to justify their ostensibly lawful activities. The funds generated are channelled into the financial system via an extensive network of individuals and establishments, including companies involved in the trade of goods and services with these countries, in relation to which it is relatively straightforward to justify sending transfers to those destinations. It is worth noting the facilities provided by payment institutions, whose operational centres, in some cases, and agency branches in others, enable funds to be received from and sent to the countries of origin, under the cover provided by the volume of remittances from migrants, many of which are incorporated into clearing operations used to settle commercial transactions between those countries and suppliers in the United States and Europe. The transport of money via 'human couriers' is also common. The methods employed are sophisticated and make use of the frequency of flights departing from Spain – mainly Madrid – to South American destinations, from where it is easier to reach the final destination country.
East Asian groups [7]	Generally of Chinese origin. For many years, the Chinese community has been engaged in commercial activity in Spain, through the establishment of wholesale distribution companies manufactured in China, as well as the sale of goods in the

[7] Between 2022 and 2024, €139,000,000 was identified in crypto-asset transfers alone, originating from premises located in the Grandland Chinese Business Park and linked to Asian criminal organisations.

	retail network, with an extensive network of specialist shops covering the whole of the country. Analyses and investigations have confirmed the existence of a complex and sophisticated network of commercial establishments covering all stages of production, distribution and sale, through which this community generates enormous sums of money that it either sends to China or invests in Spain by purchasing commercial premises – a sector in which this community is the leading foreign buyer. The illegal entry of goods into the EU is carried out by undervaluing purchase invoices, thereby reducing the customs value of the imported goods and, consequently, evading EU customs duties and Value Added Tax (VAT) in the country where the goods are consumed. The actual recipients of these goods in Spain (Chinese nationals) agree with a Spanish importer (based in the Netherlands or Germany) on a fixed price per container or customs clearance. The transport documentation and the purchase invoice are then falsified. The goods enter Spain in transit, with Portugal as their destination, meaning that VAT is not paid in Spain. However, they never actually reach Portugal; instead, they are stored and distributed to Spanish retailers. On other occasions, the goods are brought directly into Spain with a complete lack of transparency. The methods used by these criminal organisations to channel money generated in Spain to China have evolved as the activities of the Policía Nacional, the Tax Agency and the Public Prosecutor's Office have focused on combating the tax fraud perpetrated by them. Investigations carried out by the Special Anti-Corruption Public Prosecutor's Office have shown that, initially, the most common method involved the use of 'money couriers'. Traditionally, they would take advantage of the travel arrangements of many members of this large community, hire the services of third parties or use members of the organisation itself. As controls have become stricter, this method has been supplemented by others, such as the so-called 'compensation system', whereby a Spanish citizen, who has money deposited in overseas banks unknown to the Spanish tax authorities, makes a transfer from their overseas bank account to the organisation's accounts in China. In return, the money that the organisation has generated in Spain and which has not been declared is handed over in cash to the businessperson. The criminal organisation employs a number of intermediaries (advisers, economists, bankers, lawyers, etc.), who, in exchange for a commission, provide these clients in Spain with the cash they require. Police investigations have uncovered schemes involving the generation of large sums of cash that are channelled to China through complex transactions involving thousands of accounts from which transfers are ordered, under the guise of alleged commercial transactions for the purchase of goods to be sold in retail outlets. In reality, this is simply a means of sending money to China linked to activities constituting tax offences, as well as other offences relating to sexual offences, workers' rights, illegal drug trafficking, illegal gambling, etc. It has subsequently been established that the Chinese organisations have not only used a number of money transfer management companies, but have also set themselves up as agents for these transfer management firms. A further step has been to establish how the Chinese criminal organisation, in exchange for a commission, uses another (former Soviet) criminal organisation, which is dedicated to removing money from vehicles travelling to Spain and, on the same day, transporting it to another European country from where it is sent to China.

Groups from Eastern Europe	Criminal groups specialising in violent crime, as well as other activities linked to the illicit trafficking of vehicles and the fraudulent use of payment methods. These are groups, in some cases itinerant, which do not have a fixed abode in Spain, although they do have a certain infrastructure that ensures their discreet integration. They specialise in property offences, particularly burglaries at business premises and in private homes, as well as more violent offences against banks and establishments housing high-value goods: casinos, jewellers, art galleries, etc. Due to the very nature of the offences committed and the measures in place within the economic system itself, it is difficult for the proceeds to be channelled into the Spanish financial system; consequently, they are usually transferred to other territories – typically other EU countries – where they are deposited in financial institutions, offered for sale, etc. One of the most common offences in the EU is the fraudulent use of payment methods, particularly credit and debit cards. The weaknesses in the system and the number of fraud cases have led card-issuing organisations to develop complex systems to ensure the security of users, who are exposed to theft and the illegal copying of data. Groups specialising in these offences operate across all EU countries, distinguishing between the territories where cardholders reside, where data is skimmed, and where fraudulent use takes place. The proliferation of online platforms where users can purchase goods and services, place bets or participate in games of chance, etc., has introduced a factor that greatly facilitates the laundering of proceeds from these crimes. These groups specialise in property offences involving the use of violence and intimidation.
Groups originating in West Africa[8]	Spain is a country from which messages (postcards, telephone calls, emails, etc.) are sent to potential victims in countries across the rest of the world, mainly the most developed ones; it is also a country where a proportion of the funds obtained from this illegal activity is received. Police investigations have revealed links between these groups and individuals of other nationalities – mainly European, but also from certain South American and East Asian countries – as well as connections to other more serious offences, including those involving sexual exploitation. Through an extensive network of agents from payment service providers operating in Spain, and also via bank accounts—generally opened under false identities (mule accounts)—the funds sent by some of the victims are made available; the main purpose of these funds is to cover the infrastructure costs incurred by these groups in Spain. More recently, there has been a growing use of cryptocurrencies and informal transfer mechanisms to receive, move or convert funds.
Groups originating from North Africa	Generally of Maghreb origin[9] , they collaborate with local criminal networks. The region produces drugs that are mainly consumed in Europe; organised groups use Spain as a destination country and, above all, as a transit point to other European destinations, in coordination with local criminal groups. This has created a situation that affects the southern region of Spain most severely, particularly the Campo de Gibraltar area and the cities of Ceuta and Melilla.

8Several years ago, organisations specialising in the fight against crime coined the term WAOC to refer to a highly specialised form of criminal activity involving large-scale fraud, mainly through the sending of the original *'Nigerian* letters', the most notable feature of which was that the perpetrators came from one of the countries in the region, primarily those bordering or neighbouring Nigeria.

[9] Morocco is the country that contributes the largest number of foreign residents; this community is integrated into small towns or the outskirts of major cities, with a high rate of labour market participation. Many of its members have acquired Spanish nationality, and there are frequent cases of children born in Spain to Moroccan parents, or to parents who are Spanish by acquired nationality.

	This illegal trafficking generates sums of money which, for the most part, are exchanged on Spanish territory, or our country serves as a transit point to their final destination in North Africa. Within this scheme, the transport of cash by 'human couriers' is common, as are operations disguised as supposed commercial transactions.
Groups engaged in criminal activities in their own countries and bring illicit funds into Spain	Although the specific criminal acts are not carried out in Spain, the ML's operations are significant, having involved investments running into millions in the purchase of luxury goods and, in particular, in extremely high-value property. Groups from other European countries (mafia groups and others from the former Soviet republics) have been identified. The break-up of the Soviet Union gave rise to a criminal phenomenon whose consequences spread throughout Europe, with some organised groups establishing part of their infrastructure there; specifically, in the case of Spain, this included the place of residence – whether permanent or temporary – of some of their leaders and members. Law enforcement agencies have carried out operations whose investigations have uncovered serious criminal activity linked to offences of corruption, extortion and illicit trafficking carried out in other territories, but in respect of which significant ML schemes were being executed in Spain. These groups launder their illicit proceeds through complex corporate and commercial operations, utilising commercial companies registered in various jurisdictions – some of them in EU countries – with the initial banking transactions taking place in countries across all continents, including, in some cases, EU countries. These funds are used to cover the living expenses of the leaders and members of these networks; of particular significance are property investments in certain towns along the Mediterranean coast, which are financed through complex schemes involving frequent transfers of funds between three or more countries, and the use of law firms and consultants specialising in these markets.
Groups linked to political or financial corruption	These groups, whether national or international, engage in activities that have an impact across several countries, such that the country in which the criminal act of corruption (misappropriation of funds, bribery, fraud, etc.) or the corresponding financial offence takes place is different from the country of residence of the perpetrators, and also different from the country in which the funds are received or the assets – predominantly property – are acquired. Spanish groups involved in such activities carry out their criminal acts within the country, generally in connection with urban development and public services projects, and use foreign countries to maintain accounts and deposits and to register the commercial companies in whose name these accounts are held. For their part, foreign groups linked to these corruption offences choose Spain as a destination country for funds, through complex international transfer schemes involving two or more countries, and subsequently use these funds to purchase assets, generally luxury property in tourist areas, but also in upmarket neighbourhoods of major cities. The most significant cases detected involve authorities and senior officials from countries of the former Soviet Union, Africa (primarily Equatorial Guinea) and Latin America (primarily Venezuela).

37. To summarise, the following table sets out the main criminal specialities of each of these groups, and their preferred methods for laundering the proceeds of their illicit activities:

TABLE 3. Types of criminal groups		
Types of groups	Predicate offences	Methods selected for the ML
Latin America (in collaboration with local networks)	Illegal drug trafficking	Bank transfers Migrant remittances Cash transport Clearing operations Use of crypto-assets
East Asia	Tax, customs and commercial offences	Bank transfers Transport of cash Purchase of property Incorporation of companies with low turnover and activity Use of crypto-assets
Eastern Europe	Theft Fraud Cyber fraud Trafficking of drugs (Albania, Türkiye)	Cash transport Purchase of goods Online betting and gambling
West Africa	Fraud Sexual offences	Cash Payment service providers
Maghreb (in collaboration with local networks)	Illegal drug trafficking Human trafficking	Cash Cash receipts Clearing transactions
Groups with prior criminal offences committed outside Spain	Illicit trafficking Corruption	International transfers Purchase of property Luxury consumer goods Use of crypto-assets
National and international groups linked to political and/or financial corruption	Corruption (misappropriation of funds, bribery, fraud, tax offences, etc.)	International transfers Purchase of property Luxury consumer goods Use of crypto-assets

38. Among the emerging challenges facing the prosecution and investigation of organised crime, it is worth noting the advance towards post-quantum cryptography[10] , as this introduces a risk of 'sustained opacity' in illicit communications and transactions should these networks adopt the technology. The capabilities of post-quantum cryptography could permanently block key technical avenues for investigations, such as the interception of communications, the delayed decryption of stored data, or the exploitation of weaknesses in older keys or algorithms.

[10] Post-quantum cryptography (*PQC*) is a set of new cryptographic algorithms designed to withstand attacks from future quantum computers. PQC is based on mathematical problems which, according to current knowledge, would remain difficult to solve even for these advanced machines.
Its aim is to gradually replace the traditional mechanisms for encryption, digital signatures and authentication used on the internet, in banking, *blockchain* and secure communications. From the perspective of security and criminal investigation, PQC has two implications: it improves the protection of legitimate infrastructure and systems, but **it may also increase the technical difficulty of accessing communications and data when adopted by criminal actors**.

39. Similarly, the use of Artificial Intelligence (AI) by criminal organisations presents an emerging risk, as they exploit the technological capabilities of these tools to refine fraud schemes (*deepfakes*, voice cloning, etc.). Recently, warnings have even been issued regarding the possibility that some of these solutions have reached such a level of sophistication that greater security is required, as they are capable of detecting systemic errors in the security systems of all types of institutions, whether public or private.

4.2. Drug trafficking.

40. Drug trafficking in Spain is currently characterised by a growing trend **towards multi-criminality**. Networks involved in these activities are diversifying their sources of income by combining various forms of illicit trafficking, using less profitable substances, such as cannabis or synthetic drugs, to finance cocaine operations, or by turning to complementary activities such as human trafficking. Added to this dynamic are offences such as the illegal trafficking of arms, with investigations revealing an increase in the use of military-grade weapons to protect shipments and the proliferation of 'vuelcos'[11] between criminal organisations; corruption offences, which enable infiltration of public administrations and the recruitment of officials to facilitate criminal activity; and vehicle trafficking, both as a logistical tool and as a mechanism for moving illicit funds. Furthermore, there is evidence of a parallel criminal industry linked to the illicit supply of fuel and *VAT fraud schemes*, which highlights the diversification, specialisation and operational complexity of these networks.

41. At the national level, Andalusia—particularly the Costa del Sol, the Campo de Gibraltar and the mouth of the Guadalquivir—stands out as the main entry point for hashish from Morocco and an area where groups traditionally involved in this drug have expanded their activities to include cocaine, capitalising on their established structures. Meanwhile, the Levante region is emerging as a high-risk area due to the relocation of organisations from Andalusia and the expansion of cannabis cultivation in this region. Galicia retains its role as a hub for cocaine smuggling, facilitated by the complexity of its coastline and the existence of criminal networks that have endured for generations, whilst also incorporating new methods such as the use of semi-submersibles[12] . In the case of Catalonia, the cultivation and trafficking of cannabis[13] is considered one of the most significant strategic threats and one of the clearest risks to the establishment and growth of criminal organisations. Major ports such as Algeciras, Valencia, Barcelona, Málaga and Vigo constitute, due to their container volumes, critical hubs for international maritime trafficking.

42. At international level, Morocco remains the leading producer and exporter of hashish, whilst Latin America is the main hub for the production and export of cocaine to Europe. The Netherlands continues to play a central role in the manufacture and distribution of synthetic drugs such as amphetamines and MDMA, whilst Türkiye and Afghanistan remain key territories on the heroin routes to Europe. In addition to these traditional corridors, there are Atlantic regions such as the

[11] These are robberies – in many cases violent – carried out by criminals within the same illicit sphere. They are usually carried out using inside information or through the betrayal of members of rival organisations, with the aim of seizing resources such as drugs, money or weapons, whilst avoiding any form of commercial transaction.

[12] Operation Saona (Policía Nacional) led to the dismantling of a network that used semi-submersibles and the seizure of over 3,500 kg of cocaine.

[13] According to data from the EUDA (European Union Drugs Agency), Spain has become a producer of cannabis and cannabis derivatives

The Canary Islands, the Azores, Cape Verde, Martinique and the Gulf of Guinea act as intermediate hubs for the maritime and air transit of narcotics, reinforcing Spain's position as a key hub in global drug trafficking due to its strategic location and the diversification of methods employed by criminal organisations.

Table 2. Reports of suspected offences, investigations, judgements and convictions relating to drug trafficking

	2020	2021	2022	2023	2024	2025
Reports rep orts received regarding drug trafficking *	558	472	760	459	367	455
Number of investigations into drug trafficking **	556	448	507	447	442	465
No. arrested for drug trafficking***	24,114	27,141	28,678	30,814	29,693	-
Convictions relating to drug trafficking ****	31	29	29	50	38	35
Convictions relating to drug trafficking drugs ****	29	28	29	50	36	35
No. of people convicted of drug trafficking ****	150	204	120	168	253	193

Source: *SEPBLAC; **LEAs; ***Report on alcohol, tobacco and illicit drugs in Spain. Spanish Observatory on Drugs and Addictions; **** Special Anti-Drugs Prosecutor's Office.

43. Statistics on seized drugs show that, although the quantities of cocaine seized are lower than those of hashish, there has been a 236 % increase between 2020 and 2025[14] :

Table 3. Quantities of drugs seized

	2020	2021	2022	2023	2024	2025
Heroin (kg)	178	238	199	321	136	137
Cocaine (kg)	36,948	49,159	58,334	118,325	124,040	77,760
Hashish (kg)	473,925	676,182	324,709	375,290	205,991	279,962
Cannabis na (kg)	70,073	139,711	144,803	59,235	48,466	58,167
Ecstasy (no.tablets)	1,561,311	636,847	484,757	837,994	471,151	678,771

Source: CITCO

44. This may contribute to the strengthening of cocaine-related drug trafficking routes and dynamics, as well as an increase in the consumption of this substance amongst the Spanish population due to greater supply and access to it. Despite the decline in heroin use, the LEAs have noted an increase in consumption, based on the operations carried out by these police units. Furthermore, raids have been carried out on laboratories producing synthetic drugs and hashish.

[14] Source: Report on alcohol, tobacco and illegal drugs in Spain. Spanish Observatory on Drugs and Addictions

45. Based on the analyses carried out, it is estimated that seizures of cannabis, hashish, cocaine and heroin amount to around 1.76 trillion euros. It should be borne in mind that, at the operational level, investigations calculate the economic impact of trafficking using the price of the final product on the illicit market. This figure allows an estimate to be made of the potential funds that the criminal organisation would have generated or mobilised had the substance reached the distribution stage in its entirety.

46. If the quantities of liquid drugs seized are taken into account, this figure is lower because, in legal proceedings, liquid drugs are usually found in intermediate forms, dissolved or of low purity, of which only the fraction that is actually recoverable can be valued, using more conservative expert criteria. The table below shows that, although the figures in the initial table indicate an increase in operational detection data, seizures of liquid drugs declined up to 2023, having risen by 19 % compared with the previous year.

Table 4. Seized quantities of liquid drugs in euros

	2020	2021	2022	2023	2024	2025
Total amount	20,193,935	23,419,328	22,259,354	14,949,670	17,737,553	47,900,141

Source: Report on the activities of the fund for assets seized in connection with illicit drug trafficking and other related offences

47. With regard to confiscated assets, the annual reports of the National Drugs Plan show:

Table 5. Number of assets confiscated and values realised at auction

	2020	2021	2022	2023	2024	2025
No. Of seized assets	1,019	1,450	1,455	1,284	1,476	1,405
Proceeds from auction sales (euros)	12,832,737	15,854,473	851,392	8,949,261	4,025,132	5,248,704

Source: Report on the activities of the Fund for Assets Seized from illicit drug trafficking and other related offences

48. Data from the National Drugs Plan show significant fluctuations in the value of confiscated assets, peaking at 1,409 assets in 2022. The figures follow a similar pattern, falling from over 15 million euros in 2021 to just 850,000 euros in 2022, with a partial recovery in 2023 and a further decline in 2024.

49. This phenomenon may be explained by the fact that police investigations are identifying more cases linked to local distribution or upstream logistics, where large volumes are not always involved. At the same time, it must be borne in mind that criminal networks have adopted strategies of fragmenting shipments and diversifying routes, thereby reducing the transport of significant quantities in a single consignment to avoid losses. Consequently, whilst more criminal activity is being recorded, seizures of liquid volumes are lower.

50. The methods used to channel illicit funds are set out in the table below:

TABLE 4. Methods used to channel funds derived from drug trafficking	
Mules 	By opening accounts using borrowed and, at times, forged identities, or by moving cash via money transfer services to territories linked to drug trafficking. When using cash, it is common practice to split payments, dividing the money into multiple low-value transactions so as not to exceed established control thresholds. This method is used to smuggle cash into countries with less stringent controls, thereby preventing the funds from entering financial institutions and avoiding the formal financial system.
Hawala 	Through the use of trusted networks and the settlement of balances without the physical movement of currency[15] .
Crypto-assets 	The use of anonymity-focused methods in transactions provides an excellent means of obscuring cross-border transfers. The use of exchange platforms with little regulation or limited controls has been detected. Digital wallets and *mixing* services are also used to fragment the financial trail and make it difficult to identify the origin of the funds.
Wealth **Wealth** 	Through the acquisition of property, luxury goods or high-end vehicles.
Creation of business structures 	Through the setting up of companies with no real economic activity, used exclusively to issue false invoices and launder illicit proceeds. The creation of these structures is sometimes accompanied by the use of front men or intermediary companies, which allows the true ultimate beneficiary of the illicit cash flows generated to be concealed. These entities tend to have a high turnover of directors (front men), a total absence of employees, and fictitious accounts or a lack of bank statements.
International Electronic Transfers 	By sending funds abroad via transfers made through 'bank mules', intermediaries, or the creation of accounts using stolen identities. The role of the 'bank mule' is similar to that of a traditional mule.
Opening of retail businesses 	The opening of businesses (greengrocers, hairdressers or *retail* outlets, and the letting of hospitality premises to generate lawful income) which have characteristics that facilitate their use as money-laundering mechanisms: a high proportion of cash payments, difficulty in verifying the actual volume of activity, and the ability to inflate revenue, simulate sales or incorporate illicit cash into the daily takings without arousing suspicion.

[15] Operation KOPPU (Policía Nacional). The arrest of nine people in January 2025 led to the dismantling of a criminal organisation based in Spain, which provided a brokerage service for the movement of large sums of cash originating from other criminal organisations involved in drug trafficking.

51. Few sectors remain untouched by the criminal activities associated with drug trafficking. Thus, in the transport sector, the logistics and port sector plays a key role in the entry of narcotics via containers and major distribution 'hubs'; in the road transport sector, both parcel delivery companies and freight operators can be exploited to move shipments; and in the airline industry, although the illegal introduction of drugs is becoming increasingly difficult due to controls at Spanish airports, the use of drug mules to transport substances continues to be detected. For its part, the technology sector is playing an increasingly significant role through the use of encrypted communications and advanced tools (including artificial intelligence) that facilitate anonymity, planning and the operational coordination of criminal networks. Finally, although the banking sector has reduced its exposure thanks to tighter controls, other areas remain significantly vulnerable, such as the property sector—through investment—jewellery shops and the sale of luxury vehicles, which are frequently used to channel illicit capital into the formal economy.

52. From the reports received, the purchase of private hire vehicle licences by individuals and/or legal entities using funds whose origin is not substantiated by documentation has been identified as an emerging threat. It has been found that fictitious invoicing is being carried out through the use of TPS charged to these licences, as well as cash receipts of unknown origin presented as supposed payments from customers.

53. Investigations carried out by the LEAs have revealed that fuel supply companies have links to hashish trafficking in Spain. Furthermore, electricity supply companies are affected by illegal connections to the public grid by criminal organisations involved in the *indoor* cultivation of cannabis. The areas identified as being at highest risk in relation to drug trafficking show a convergence of geographical factors, strategic infrastructure and the adaptability of criminal organisations.

54. In connection with the territories mentioned above, the jurisdictions involved in the movement and concealment of funds derived from drug trafficking reflect the financial dimension of the phenomenon. Among these, the Netherlands and Belgium stand out, acting as logistical and financial hubs where the storage of drugs and the settlement of payments between European networks are concentrated. Spain, for its part, operates as a key hub for the receipt and integration of illicit capital, particularly through investments in the property sector and commercial structures that appear legitimate. Türkiye and the United Arab Emirates are establishing themselves as jurisdictions used for the asset management of criminal leaders and for Money Laundering associated with international commercial operations. In South America, countries such as Ecuador, Colombia, Brazil and the Dominican Republic continue to be strategic hubs both for the production and the channelling of financial flows linked to the global cocaine supply chain, given the need to move large sums of money without triggering alerts in formal banking systems. Taken together, these territories and jurisdictions form an operational and financial network that enables criminal organisations to sustain and expand their illicit activities on a transnational scale.

55. A distinction has been made between the groups involved in drug trafficking; however, these groups are not mutually exclusive – that is to say, they may operate jointly in carrying out the offence. Nevertheless, the groups that are of greater relevance to the ML, given their significance and impact, are those operating at an international level and those which, whilst local, establish links with international networks:

Table 6. Identification of groups involved in drug trafficking

Scope	Group of group	Drugs trafficked	Description	Objective
National	Local groups	Cannabis, speed, ecstasy, tusi, small amounts of cocaine	Neighbourhood networks, local sales points	Retail distribution and supply of micro-trafficking
National	Family networks	Cannabis, cocaine at regional level, hashish	Families living in margin alised urban or rural areas	Territorial control and local/regional distribution that is very stable
National	Structured criminal organisations	Cannabis, cocaine, hashish	Spanish groups with logistical infrastructure, drug-smuggling speedboats, grow houses	Import, storage and distribution at an intermediate scale; links with International networks
National	Groups linked to other offences	Cannabis, cocaine, hashish	Gangs also involved in burglary, weapons and human trafficking	Diversification of income and violent protection of shipments (including "carjackings")
International	Networks synthetic opioids	Fentanyl, nitazenes (a minority in Spain)	Source: diversion from the legal supply chain	Low current impact in Spain; emerging risk
National/inte rnational	Crime as a Service	Not necessarily their own drugs; they provide services for hashish, cocaine and cannabis	Fuel supply networks fuel, drug-smuggling boats, security	Provide logistics, fuel, transport and protection to other networks
International	Transnational organisations	Cocaine, hashish, heroin, synthetic drugs	Groups with multinational logistics	Bringing drugs into Spanish territory and redistributing them to Europe
International	Latin American cartels	Cocaine (main), as well as emerging synthetic drugs	Sinaloa, Jalisco Nueva Generación	Control of maritime routes, shipment of large consignments and establishment of alliances
International	Maghreb crime	Hashish, cocaine	Dominates the port of Algeciras; Magh reb/Dutch origin	Smuggling of hashish and logistics management of Containers of cocaine
International	Albanian and Turkish	Cannabis, heroin	Balkan and Turkish groups	Large-scale cannabis production; control of heroin routes

International	'Ndrangheta, Russian mafias	Cocaine	Italy (Calabria), Russia	Smuggling cocaine and money laundering via the property

4.3. Economic and financial crimes.

56. This section addresses fraud, tax offences and corruption offences, as they pose significant threats to Spain's ML.

4.3.1. Fraud offences

57. Fraud offences are the sub-category of economic crimes reported to SEPBLAC that has seen the greatest increase, with the figure for 2024 being almost three times higher than that for 2023. The main drivers are the use of artificial intelligence to create fake content and personalised scams, and the rise in phishing and identity theft in online shopping and job offers.

Table 7. Reports based on evidence and investigations linked to fraud offences

	2020	2021	2022	2023	2024	2025
Reports based on evidence received regarding crimes relating to fraud *	2,323	2,654	2,954	3,673	10,026	6,520
No. investigations into crimes involving fraud **	4,513	4,710	4,549	5,489	6,036	5,922

Source: *SEPBLAC; **LEAs

58. The digitalisation of society and the increased use of digital channels for financial transactions have facilitated the carrying out of these fraudulent schemes. Furthermore, investment fraud has intensified due to a combination of lower returns on financial products and growing technological complexity, with retail savers being particularly vulnerable to fictitious high-yield offers. Social Security fraud has evolved into organised schemes involving fictitious companies, the wrongful claiming of benefits, the misuse of rights and the forgery of documents for the illegal regularisation of foreign nationals. An analysis of fraud-related threats estimates that the volume of funds involved in the operations reported by regulated entities amounts to 5,255 million euros, whilst ongoing investigations relate to a total of 83.6 million euros. It is particularly noteworthy that, from 2024 onwards, there has been a significant increase in the funds affected by fraudulent operations, suggesting greater sophistication in the schemes used and an increase in the economic impact associated with this type of unlawful conduct.

59. As regards the methods used to channel funds derived from fraud, there has been an increase in transactions that combine both the traditional financial system and emerging technological solutions:

TABLE 5. Methods used to channel funds derived from fraud	
Mule accounts 	Opened in the names of third parties, either by recruiting vulnerable individuals or using identities obtained through *phishing* and social engineering techniques, which enables the receipt and movement of illicit funds, making them difficult to trace.
Crypto-assets and exchange platforms 	These facilitate the immediate conversion of fiat currency and the cross-border transfer of funds with a lower degree of transparency. There has been a growing trend in the use of ***stablecoins*****,** particularly for **asset** diversification**,** due to their ability to freeze funds if suspicious activity is detected.
Digital payment platforms and non-bank financial services (Fintech) 	These enable international transfers, currency exchanges or the opening of accounts with multiple IBANs (such as *neobanks*), which introduces additional layers of opacity. In complex scams, the victims themselves may be tricked into carrying out transactions via their own accounts or opening profiles on *exchange platforms*, whilst in smaller-scale frauds a wide variety of mechanisms — such as prepaid cards or online gambling — are used to quickly launder the proceeds of crime. The proliferation of providers based outside the country often necessitates the use of international judicial cooperation instruments, such as European Investigation Orders or letters rogatory, which adds complexity to the reconstruction of financial flows and the identification of ultimate beneficiaries.

60. Various types of actors and organisations involved in the commission of fraud offences have been identified. Table 6 sets out those identified in investigations and intelligence analyses:

TABLE 6. Types of organisations linked to fraud offences	
Criminals individual and small-scale online fraudsters	They operate in isolation and without any organisational structure. These individuals commit scams with a low economic impact: fake online sales, rental scams, insurance fraud, 'nazareno' scams, etc. They benefit from the anonymity digital and instant messaging platforms provide.
Organised groups operating at regional or national level	They have structures with a division of roles (recruitment, social engineering, payment management) and specialise in frauds involving a high volume of victims: the *'child in distress'* scam*,* bank fraud, fake utility contract switches, etc. They often use money mule accounts and rapid fund transfers to make them harder to trace.
International criminal organisations specialising in financial fraud	These organisations are usually structured like businesses, with support, advisory and operations departments. They also have *call centres* with hundreds of operators dedicated to recruiting victims in Europe and North America. They typically specialise in fake investments, *trading*, crypto-assets or purported financial products, and are frequently based in Eastern Europe and Indochina, operating under the guise of legitimate companies.

BEC (Business Email Compromise).	Organisations that manipulate business communications to divert payments, requiring the use of traditional bank accounts to maintain the appearance of legitimacy. The money is immediately withdrawn or redistributed to avoid being frozen and to make it difficult for the police to trace.
Groups involved in investment fraud of varying sophistication	Depending on their region of origin, their funds are channelled through money mule networks: i) Eastern Europe: more elaborate methods (fake websites, professional telephone intermediation) and ii) Asia: less complex schemes, based on direct contacts, messaging groups and pyramid schemes or *'pig-butchering*'.
Ransomware and cyber-extortion groups	130[16]active groups have been identified and monitored, with victims since 1 January 2025. These groups operate as criminal organisations or as part of them, and specialise in compromising systems and demanding payments. *Ransomware* operates through *'Crime-as-a-Service'* structures, in which cyber-attackers join a platform that provides them with the technological means required to carry out the attack (*malware)* and make contact with victims. Each platform typically specialises in a specific 'family' of *ransomware* (the term it uses) or criminal group, which are created *specifically for this purpose*. The platform facilitates 'negotiations' between the attacker and the victim to agree on the ransom amount for restoring the system and decrypting the data, with payments made via obfuscated cryptocurrencies (such as Monero). Investigations within the framework of EUROPOL are carried out on the basis of the identified *ransomware* 'families', with working groups being set up under the auspices of EC3 and J-CAT (Joint Cybercrime Action Taskforce)[17]. Furthermore, scams such as *lovestortion, sextortion* and fake pimps have been identified; these do not require a high level of technical sophistication and are primarily carried out by organisations based in countries with low levels of cooperation in ML/TF.
Transnational operating under the guise of legitimate companies	These organisations simultaneously carry out various types of fraud (investment scams, fake technical support, crypto-asset scams) and use technology such as Artificial Intelligence and advanced digital tools to optimise recruitment, social engineering and victim targeting. They comprise members in different countries, coordinated to maximise profits and hinder investigations. They present a corporate image, websites, customer service and marketing materials.

61. Fraud is closely linked to other categories of crime. The proceeds from fraud can fund other criminal activities, such as drug trafficking, arms trafficking or human trafficking. Although there is no single pattern linking it to a specific criminal typology in Spain, digital globalisation and the standardisation of criminal methods mean that the same modus operandi are used across multiple jurisdictions, ranging from complex frauds to traditional schemes exported to other countries.

62. The jurisdictions involved in the illicit movement of funds linked to fraud vary depending on who is behind the crime. Transnational criminal organisations combine multiple jurisdictions and movements via *blockchain* prior to the final conversion in jurisdictions with less stringent regulatory requirements.

[16] Data from the Basque Cybersecurity Agency (Cyberzaintza).

[17] The Policía Nacional is currently working in nine task forces, focusing on nine families of ransomware.

These organisations use networks and structures in different countries to fragment and conceal the financial trail. Nevertheless, the following classification has been drawn up:

TABLE 7. Types of jurisdictions linked to fraud offences
Funds linked to individual perpetrators or national groups tend to remain and be spent in Spain. In more sophisticated corporate fraud schemes, funds are transferred to non-cooperative jurisdictions via intermediary companies.
Jurisdictions frequently involved in frauds operated via online payment platforms or services include Malta (particularly significant due to the use of the *Openpay* platform, employed to convert assets into crypto-assets); or Ireland, Lithuania, Estonia and Cyprus, where numerous European of payment services are based.
Countries used as transit points or destinations for illicit funds: the United Kingdom, France, Italy, Portugal, Germany, Poland, Hungary, Croatia, the United States, Hong Kong, China, the United Arab Emirates, Nigeria and Benin.
Offshore jurisdictions or those with lax regulatory regimes: the Cayman Islands, the Seychelles, the British Virgin Islands, Gibraltar, Delaware (US).

63. As regards the technologies used to carry out these attacks, the use of artificial intelligence stands out, enabling the creation of masking tools, automated *bots* and *deepfakes*, which are even sold on the *dark web*. Furthermore, there are various forms of *phishing, smishing and vishing,* which involve creating websites, messages or calls that mimic legitimate organisations in order to obtain personal data or banking credentials. Remote control programmes (such as *TeamViewer* or *AnyDesk*) are also becoming increasingly prevalent; these are used to take control of victims' devices and carry out unauthorised operations, as *is ransomware-associated malware,* which encrypts business systems to demand payments, usually in cryptocurrencies. In investment scams and romance scams, criminals use fake platforms, AI-generated *bots* and fake social media profiles to lure and manipulate victims. At the same time, the use of crypto-assets has become widespread in the most sophisticated scams and is the sole means of payment in schemes such as *ransomware*.

4.3.2. Tax offences

64. In terms of the amount defrauded, there has been a significant increase in tax offences in Spain in recent years, driven mainly by the expansion of domestic VAT fraud schemes in the hydrocarbons sector.

65. Despite this sector's increased prominence, investigations have uncovered offences relating to intra-Community VAT fraud linked to trade in electronic components, mobile phones, high-end vehicles, trade with Asia and alcoholic beverages. Whilst investigations continue in more traditional areas (such as corporation tax fraud or cases of tax avoidance), the complexity and high profitability of fuel fraud have focused investigative efforts on this area.

Table 8. Reports based on evidence and investigations linked to tax fraud

	2020	2021	2022	2023	2024	2025
Reports received on the basis of evidence *	1,515	1,458	2,088	2,746	2,728	2,447
No. of investigations **	625	701	661	565	632	685

Source: *SEPBLAC; **LEAs and AEAT

66. The estimated volume of funds linked to tax fraud amounts to 8,675 million euros in 2025, according to information derived from the operations reported by the regulated entities. Large-scale tax offences linked to major VAT schemes, both nationally and internationally, are usually carried out by criminal organisations that operate on a global scale and set up corporate structures designed to facilitate the fraud and subsequently channel the proceeds through money-laundering networks. These networks maintain links in various EU Member States (Portugal, France, Germany and the Czech Republic in the case of intra-Community VAT fraud) as well as with third countries involved in the smuggling of goods (China, Vietnam) or tobacco (Poland, Bulgaria, Ukraine). In this context, illicit funds are often channelled through financial routes involving offshore jurisdictions, combining shell companies and low-tax territories to conceal assets and make it difficult to trace the international movement of assets linked to fraud.

67. As regards the profile of organisations involved in tax fraud, it is common to find groups comprising nationals from East Asian countries (particularly China) linked to VAT fraud, smuggling, customs offences and opaque commercial activities. At the same time, organisations comprising citizens of European Union member states, including Spain, tend to be more closely associated with subsidy fraud, tax offences and intra-Community VAT schemes. In the latter area, recent investigations by the European Public Prosecutor's Office have identified a high level of involvement by nationals of Germany, Portugal and Italy in complex VAT fraud schemes, with groups comprising citizens of Romania, Estonia, France and Belgium ranking second in terms of volume and intensity, primarily involved in fraud relating to European subsidies.

4.3.4. Corruption offences

68. Corruption in Spain constitutes a complex phenomenon that affects the proper functioning of the public administration. Its most widespread manifestation is the manipulation of public procurement procedures, where rigged tenders, unjustified cost overruns, tailored tender specifications and the instrumental use of subcontracting allow public resources to be diverted towards private interests. Added to this are acts of embezzlement and fraud involving subsidies and grants, carried out through fictitious projects, beneficiaries selected in a targeted manner, or corporate networks created to channel illicit funds. At the same time, local town planning remains a well-established source of illicit income, facilitated through irregular planning permissions, ad hoc rezoning and tailor-made town planning agreements. This network is reinforced by the irregular financing of political parties, characterised by opaque donations, fictitious campaign invoicing or exchanges of favours linked to contract awards, keeping the public perception of risk very high despite the dismissal of some recent cases.

69. In this context, the most common offences in corruption schemes (influence peddling, embezzlement, abuse of office and bribery) are typically linked to discretionary decisions taken by authorities and officials in the awarding of works contracts, services and licences. Tracing these incidents reveals a series of associated practices that facilitate the generation and concealment of illicit gains: the issuing of false or inflated invoices, the payment of 'kickbacks' in cash or in kind, and the use of corporate structures to conceal the actual control of

contract awards. Alongside this, other offences are emerging, such as document forgery, corruption in business dealings, breach of fiduciary duty, fraud, as well as planning and environmental offences.

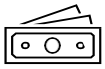
70. The number of reports received from regulated entities doubled in 2024 compared with the previous year. Data provided by the LEAs for the period 2020–2025 shows that investigations into corruption offences have risen sharply, with the figure for 2025 being almost three times higher than that for 2020.

Table 9. Reports based on evidence and investigations relating to corruption offences

	2020	2021	2022	2023	2024	2025
Reports received on the basis of evidence*	130	119	232	171	379	126
Number of corruption investigations	163	194	410	365	411	421

Source: *SEPBLAC; **LEAs

71. The methods used to channel illicit flows generated by corruption in Spain between 2020 and 2025, as identified in the investigations, are as follows:

TABLE 8. Methods used to channel illicit funds from corruption	
Agreed commissions 	Use of kickbacks as a percentage of the contract or grant. These are disguised as payments for consultancy or intermediary services, backed by false invoices issued by shell companies with no real business activity.
Use of cash 	A central mechanism fuelled by split withdrawals, cash discrepancies or parallel accounts that generate a 'slush fund', used for direct bribes to public officials or intermediaries.
Complex corporate structures 	Use of networks of shell companies and frontmen, who receive funds, issue fraudulent invoices and redistribute payments via bank transfers, fictitious loans or apparent commercial transactions, thereby obscuring the trail of the money.
Bank transfers to jurisdictions 	Bank transfers to offshore jurisdictions or those with more lenient tax controls.
Investment funds 	Use of investment funds for large-scale projects or emerging markets. This is used as a means of channelling capital and giving it the appearance of legitimate returns.
Crypto-assets 	A novel method detected during the period analysed.

72. Although the funds generated by corruption are, for the most part, channelled as cash flows, investigations reveal that a range of safe-haven assets

intended to conceal, preserve and channel illicit funds derived from kickbacks and the misappropriation of public resources:

TABLE 9. Types of assets used to channel funds derived from corruption	
Property	The primary vehicle for the covert accumulation of wealth, whether through direct purchases, acquisitions via front companies, or by including such assets in personal holdings through sham transactions.
High-end goods	The purchase of high-end vehicles, luxury goods and art enables cash to be converted quickly.
Financial products	Traditional financial products that enable transactions to be broken down and diversified in order to obscure the trail of illicit funds.

4.4. Money Laundering by third parties and from offences committed abroad.

73. There are two types of foreign criminal organisations that use Spain for ML:

    - Criminal organisations based in Spain that invest money of illicit origin obtained by or on behalf of foreign criminals.
    - 'Active' criminal organisations that carry out their criminal activities in our country.

74. International cooperation is an essential pillar in the processes of identifying, freezing and recovering assets linked to cross-border crime, as it enables action to be taken against criminal structures that disperse their funds across multiple countries and ensures a consistent response to international asset concealment.

75. The following tables (10 and 11) set out the requests for international cooperation processed by Spain within the framework of the National Office for Asset Recovery (O.R.A.) under the Ministry of Home Affairs [18]relating to predicate offences during the period 2020–2025. The data show an upward trend in requests relating to economic crimes and Money Laundering, which highlights the greater complexity and transnational dimension of these investigations. In this context, mutual legal assistance is an essential tool for cooperation between law enforcement agencies in different states, enabling the exchange of information to locate and identify assets, obtain evidence and, consequently, implement precautionary measures or confiscations which are subsequently authorised by court order. Its purpose is to ensure a coordinated and effective response to criminal organisations operating across multiple jurisdictions, thereby strengthening the capacity for asset recovery and the fight against organised and financial crime.

[18] *In the asset recovery process, CITCO establishes an international network of collaboration with international networks focused on locating these assets, working alongside other asset recovery networks – Asset Recovery Interagency Networks (ARINs) – such as the GAFILAT Asset Recovery Network (RRAG) or the European Asset Recovery Office (ARO). It also responds, on an ad hoc basis, to requests received under bilateral agreements, with the ARINs serving as our main channel for mutual assistance.*

Table 10. Number of formal or informal requests for international cooperation in criminal cases. Estimated value of funds involved (ORA CITCO).

	2020	2021	2022	2023	2024	2025
Received	440	529	617	1,060	1,397	827
Estimate	42,259,971	262,938.11	380,916.44	163,305.15	187,097,12	49,566,258
Issued	88	99	63	133	186	216
Estimate	2,897,005	9,263,336	3,665,670	41,076,201	5,094,123	15,584,219

Source: CITCO

76. Requests for and responses to international cooperation are a key element in advancing investigations involving cross-border movements of assets, particularly in ML, economic crime and drug trafficking. The volume of these communications reflects the growing need for mutual support between jurisdictions to identify hidden assets and ensure their recovery. The requests received show that economic crimes are the criminal activities most frequently involved in such collaboration, with an exponential increase in the number of requests received since 2023. The rise in the number of requests made is due to actions undertaken by CITCO to promote and raise awareness of the use of these channels amongst LEAs.

Table 11. International cooperation under the O.R.A. by predicate offence. Requests received.

	2020	2021	2022	2023	2024	2025
Money Laundering	276	309	336	464	524	318
Economic offences	121	129	305	766	812	698
Drug trafficking	137	165	171	210	205	140

Source: CITCO

77. As regards requests made from Spain, particular attention should be paid to those concerning organised crime and, as was the case with the requests received, to requests for cooperation relating to economic crime.

Table 12. International cooperation under the O.R.A. by predicate offence. Requests processed.

	2020	2021	2022	2023	2024	2025
Money Laundering	55	48	46	110	124	158
Organised crime	41	47	28	73	100	120
Economic offences	11	26	29	89	196	141
Drug trafficking	26	16	14	26	17	28
Terrorism	0	0	0	1	0	1

Source: CITCO

78. The regional police forces, through EUROPOL, INTERPOL and the SIRENE Bureau, process formal requests for international cooperation, which help to streamline cross-border investigations. Within this framework, property offences are the most significant across all cooperation systems, accounting for the largest number of international cooperation cases processed.

79. Among the requests made and forwarded within the framework of international cooperation in response to judicial requests are the operations carried out by ORGA, which plays a key role in the processes of identifying, seizing and recovering assets linked to crimes with a cross-border dimension.

Table 13. International cooperation within the framework of the O.R.G.A.

	2020	**2021**	**2022**	**2023**	**2024**	**2025**
Received	25	60	23	30	44	99
Issued	84	41	61	96	130	115

Source: Ministry of Justice

80. As can be seen, the number of requests for and referrals of international cooperation is lower, but it should be emphasised that these are carried out by court order and that ORGA's involvement is restricted to those cases in which the requesting State does not expressly include the offence of Money Laundering in its request.

81. Despite this restriction, Table 14 below shows that the number of cases relating to Money Laundering handled by ORGA for the period 2021–2025 is on the rise, particularly those of an international nature. This reflects the increase in international cooperation in identifying global threats that affect several countries across the board.

Table 14. Trend in cases relating to Money Laundering (2021–2025) handled by ORGA

Year	**2021**	**2022**	**2023**	**2024**	**2025**
Total number of cases	45	23	30	34	73
National cases	14	9	18	23	15
International cases	31	14	12	11	58

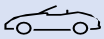
Source: Ministry of Justice

82. With regard to the funds involved in these requests for international cooperation, in cases handled by the Policía Nacional alone, the period under review saw 4 requests relating to drug trafficking, with an estimated value of funds involved of 5,071,000 euros; 7 requests relating to organised

crime, with an estimated value of assets involved of 250,000 euros; and 32 requests relating to economic crimes, for which the value of assets involved has been estimated at 3,770,000 euros.

83. Furthermore, the value of assets traced by ORGA is estimated at 180,018,679.89 euros in 2025, reflecting the economic scale of the assets linked to criminal activities that are subject to tracing and recovery.

84. These figures reflect the scale of illicit flows generated by drug trafficking, despite the lower volume of requests for international cooperation. The channelling of illicit funds from crimes committed on an international scale and the global nature of transaction flows have led to the identification of various methods used to introduce these monetary flows into our country.

TABLE 10. Methods used to channel illicit funds derived from international crime into Spain	
Fictitious international trade 	Use of falsified invoices or fictitious shipments to justify transfers from abroad to Spain.
Property investment 	Channelling illicit funds into Spain through property purchases (common on the Costa del Sol, the Levante coast, the Balearic Islands, the Canary Islands and in major cities), with a high likelihood of the use of shell companies or frontmen.
Acquisition of movable and luxury goods 	Channelling of capital through art, watches, vehicles or high-value movable assets, which are subsequently resold to give the appearance of legitimacy.
Crypto-assets 	Use of crypto-assets, particularly *stablecoins,* for international fund transfers with reduced traceability and the possibility of using *'professional* providers' of ML.
Split transfers (*smurfing*) 	Inflow of funds via multiple small transactions to circumvent monitoring thresholds and obscure the foreign origin.
Complex corporate structures 	Use of front men, shell companies, *holding companies* or *trusts* based in various jurisdictions to conceal the ultimate beneficial owner and facilitate the inflow of illicit funds into Spain under the guise of legality.

85. The inflow of illicit funds into the country affects the following economic sectors, which are impacted by the commission of this international offence:

- The property sector: a key tool for criminal organisations due to the high volume of transactions, Spain's appeal to foreign investors and the ease with which prices can be manipulated or intermediaries used to obscure the traceability of funds.
- Logistics system: increased activity is being detected in the port sector. Consequently, the high level of commercial activity in Spanish ports and the large flow of containers increase the likelihood of illicit goods being concealed.

- Economic and financial sector: despite the reduction in legal limits on cash payments, money smuggling remains a significant risk, particularly in cross-border movements detected at customs, ports and airports.
- Emerging sectors and financial digitalisation: crypto-assets, investment platforms, Fintech and associated operations (*phishing, smishing, malware*) present vulnerabilities due to their rapid evolution, the technical difficulties in tracing them and the limited supervisory capacity to keep pace with innovation.

86. In short, although economic crime is the type of criminal activity with the highest volume of requests processed and received, it must be borne in mind that crimes such as drug trafficking can, with fewer operations, involve a greater volume of illicit funds.

5. MAIN THREATS FROM TERRORIST FINANCING

87. Currently, the terrorist group with the largest number of supporters in Spain is Daesh, linked to 66 % of operations and 68 % of those arrested in 2025 for jihadist terrorism, to the detriment of Al-Qaeda (AQ), which continues to exert influence.

88. Both organisations share the ultimate objective of establishing, through the use of violence, a Caliphate in Muslim lands (which they consider to include virtually the whole of Spain), in which the only sources of law would be those derived from the Qur'an and the Islamic Sunnah (tradition), in accordance with the precepts applied in the most radical forms of Salafism.

89. The LEAs have detected a surge both in the consumption and dissemination of Hamas propaganda and in the intention of Spanish radicals or those resident in Spain to travel to Gaza and the West Bank to join pro-Palestinian groups, a trend that has intensified following the conflict between Israel and Hamas. Furthermore, the threat posed by organisations linked to Hezbollah remains active, as demonstrated by the operation carried out in 2025 against a logistics network dedicated to acquiring components for the manufacture of drones used in attacks against Israel. Moreover, investigations have been carried out into plots linked to Daesh and its ISKP (Islamic State in the Khorasan Province) branch, whilst at the same time there has been an increase in *crowdfunding* campaigns aimed at financing Hamas, capitalising on growing social sensitivity regarding the Palestinian-Israeli conflict and channelling contributions from both donors aware of the funds' final destination and others unaware of how the funds are actually being used. In this context, there is a growing presence in Europe of networks of Central Asian and Caucasian origin linked to ISKP, which carry out logistical and financing functions and, in some cases, maintain links with organised crime structures, particularly in areas such as arms trafficking.

90. The modus operandi of terrorist organisations differs significantly between Europe and North Africa, a context of particular relevance to Spain given its strategic position. In Western Europe, low-sophistication attacks using bladed weapons, vehicle-ramming attacks, homemade explosives and improvised weapons predominate, whilst in the eastern part of the continent there is a more frequent use of military-grade weapons. The perpetrators are predominantly lone actors, although small cells providing logistical or financial support also operate. In North Africa, police pressure has reduced jihadist activity, limiting it to isolated individuals or autonomous cells, whilst in the Sahel more complex attacks persist, such as ambushes, attacks using homemade devices and raids on infrastructure, alongside a growing use of drones and cryptocurrencies. At the national level, the dissemination of jihadist propaganda translated into Spanish is also noteworthy, as it broadens its reach and accessibility.

91. In relation to these operational dynamics, opportunities for collaboration between terrorism and organised crime can be observed, whereby both phenomena benefit mutually through lucrative activities such as property crime, arms trafficking, document forgery, people smuggling, human trafficking, drug trafficking and extortion. Furthermore, terrorist organisations resort to the misuse of non-profit organisations, crowdfunding campaigns and fraud to raise funds. Added to this is the adoption of new technologies, which facilitate both online radicalisation and communication, as well as the mobilisation of financial resources through crypto-assets and Fintech platforms, thereby expanding their capabilities for financing and anonymity.

92. The main areas of terrorist conflict are concentrated in the Sahel, currently the global epicentre, alongside Somalia, Afghanistan, Syria and Iraq, where affiliates of Daesh and Al-Qaeda operate. In Europe, there is no

There are areas under terrorist control, although some neighbourhoods such as Molenbeek (in Brussels) and Saint-Denis (in Paris) have high levels of radicalisation. In Africa, in addition to the Sahel and Nigeria, hotspots persist in the Lake Chad basin and the Horn of Africa, whilst in Latin America there are certain links (albeit not posing a high risk) between Hezbollah and the tri-border region of Argentina, Brazil and Paraguay, as well as border areas of Venezuela and Colombia. All of this coexists with a globalised threat model based on micro-cells and lone actors, which facilitates the spread of the phenomenon across various countries.

93. The threat in Spain is predominantly endogenous in nature (based on processes of self-radicalisation), with these cells and lone actors constituting the main terrorist threat in Spain; the growing role of the online environment in recruitment and indoctrination processes is particularly noteworthy. Furthermore, account must be taken of the risks associated with the return of foreign fighters, not only from Syria, but also from Daesh and Al-Qaeda affiliates; foreign fighters not only from Syria and Iraq, but also from Daesh affiliates in the Sahel, West Africa, Somalia and Khorasan, as well as from Al-Qaeda in Yemen.

94. Of particular note is the diversity of profiles among aspiring jihadists, such as young people of Maghrebi origin, minors, converts, and individuals of Caucasian and Central Asian origin who are also present on national territory. It should be noted that, amongst the systems used for recruitment, indoctrination and radicalisation, the online sphere stands out most prominently, followed by the prison environment and, to a lesser extent, places of assembly and worship.

95. The following chart shows the counter-terrorism activity carried out by the LEAs in 2025, with Catalonia standing out in terms of the number of people arrested for terrorist activities. As regards terrorist criminal activities detected in investigations into jihadism in Spain in 2025, the vast majority of arrests can be linked to illegal activities involving indoctrination, self-indoctrination and terrorist recruitment, carried out via the internet, social media and instant messaging apps, although there are cases where indoctrination takes place in person, particularly among young people.

96. In terms of trends, there is evidence of the involvement of women and minors in jihadist activities, with 8 women and 15 minors arrested in 2025. The figures support the strategy of '*the rejuvenation of* jihadism', a strategy employed in particular by Daesh and specifically aimed at recruiting minors and involving them in terrorist activities at an increasingly early age.

Figure 1. Counter-terrorism activity carried out by the LEAs in 2025



Source: LEAs

5.1. Terrorist Financing in Spain

97. In the Spanish context, data on TF in Spain for 2022 showed a peak in both reports of suspicious activity and confirmed investigations and convictions linked to terrorism. In 2024, although the number of reports of suspicious activity and investigations carried out by the LEAs has stabilised compared with previous years, However, the number of people convicted has increased compared with previous years. This shows that TF is a persistent threat, with fluctuations in detection, prosecution and judicial impact; these fluctuations do not allow for inferring causality beyond the observed trends, nor do they bridge gaps or differences in scope between data series.

Table 15. Reports based on evidence, investigations, detainees, sentences and those convicted of TF offences

	2020	2021	2022	2023	2024	2025
Communications by report received*	223	205	308	167	216	231
No. of research projects TF**	57	59	100	94	65	76
Number of detainees held by TF***	20	4	2	14	11	-
Judgments relating to TF	18	18	11	9	23	-
Related convictions to TF***	12	12	11	7	4	-
Number of people convicted of TF***	0	8	13	10	14	-

Source: *SEPBLAC; **LEAs; ***CENDOJ

98. The channelling of illicit funds for the purposes of TF is most commonly seen through the use of cash, fragmentation and the use of irregular banking systems. However, investigations carried out by the LEAs have highlighted the use of a combination of methods to commit the offence. These funds are summarised in Table 9.

***TABLE 11. Methods used to channel illicit funds linked** to TF*	
Payment platforms 	Use of **online payment platforms** to send or collect funds: PayPal, also utilising bank accounts with virtual IBANs and crowdfunding campaigns. These payments are made via intermediaries or individuals linked to the financial networks used by terrorist groups
Cryptocurrencies 	Growing use of **cryptocurrencies,** particularly on decentralised platforms that promote anonymity, are difficult to trace and enable swift transactions. Exploitation of anonymisation techniques, such as *mixers*, services in non-cooperative jurisdictions, VPNs, *the dark web*, *the deep web* and encrypted messaging. As well as the use of *stablecoins* as an alternative to prepaid cards, allowing funds to be loaded or transferred via QR codes, and the inclusion of other digital assets, such as **NFTs,** through direct purchase by supporters or by handing them over to the organisation for sale.
Donations 	**Requests for donations via cryptocurrency addresses** publicised in **terrorist** propaganda**.**
Cash-in-hand parcels 	Use of traditional methods, such as ***hawala*** and **cash couriers,** to move money without leaving a banking trail.
Purchase of goods 	**Logistical structures** designed to procure goods for terrorist activities (for example, drone components), **using methods similar to those employed in Money Laundering**: front companies, intermediaries or the simulation of legitimate business transactions.

99. The mobilisation of funds for TF requires the use of intermediary territories presenting varying levels of risk at both national and international levels. In Spain, although this type of crime can occur anywhere in the country, activity is particularly concentrated in the peninsular Mediterranean arc (Catalonia and the Levante region), along with Ceuta, Melilla and Madrid on the one hand, and the Basque Country on the other.

100. At the international level, investigations identify the greatest risks in the Middle East: in Syria and Iraq; in Africa: the Sahel (Mali, Niger and Burkina Faso), Nigeria and Somalia; and in Asia: Afghanistan, Pakistan, the Central Asian and Caucasian republics. However, it is necessary to highlight other jurisdictions and border areas with the countries mentioned above where elements providing logistical, financial or media support to terrorist organisations persist, despite the counter-terrorism measures taken by their security forces: the Maghreb countries; the northern regions of the Gulf of Guinea countries (Benin, Ghana, Côte d'Ivoire and Togo); Egypt; Ethiopia; Türkiye; South Africa; Lebanon; Jordan; Gaza and Iran; the Maldives; the Philippines; and Indonesia.

101. Furthermore, the Maghreb countries must be taken into account, not from the perspective of the establishment of stable cells (although there is a call from Daesh to revive its activities in that

that region, which could alter this situation), but as countries of origin for terrorist fighters travelling to conflict zones.

102. Furthermore, the operational analysis shows that, although these areas constitute the main risk points, the international movement of funds also involves jurisdictions posing an indirect risk, such as Germany, the United Kingdom, Denmark, the United States, Canada, the United Arab Emirates and Qatar, which feature in various investigations. Similarly, there is evidence of the recurring involvement of Belgium and France within the European Union, as well as Morocco and Algeria outside the EU.

103. Estimates of the volume of illicit funds channelled through TF in Spain show that, with a few isolated exceptions, most investigations do not involve large sums, which is consistent with the fact that the offence does not require a minimum financial threshold. Although in 2023 a single case involving 4 BTC was seized (which would represent a current value of approximately 226,326.18 euros)[19] , the total value of the funds cannot be determined due to ongoing investigations and the difficulty of identifying which part of the money handled by those under investigation is actually linked to terrorism. Taking into account only cases with final judgements, the attributable amount totals approximately 11,000 euros[20] .

104. TF maintains a link with underlying categories of crime, which provide financial or logistical support for the activities under investigation. These include, notably, property offences, including theft and violent conduct, alongside offences against the socio-economic order, document forgery, offences against public health and against the rights of foreign nationals, forming a network in which Terrorist Financing is integrated into the dynamics of organised crime, facilitating the diversification of income sources and the concealment of the origin of the funds.

105. The objectives of TF are varied and have evolved in line with the organisations' operational context. Although in some cases the aim is to channel funds directly to terrorist groups in third countries, in practice most of the resources are directed towards sympathisers or small local cells to cover basic needs such as accommodation, rent, living expenses, food, travel or the purchase of devices, rather than the acquisition of weapons or dual-use materials. This pattern has changed particularly following the territorial defeat of *Daesh*, at which point the priority shifted from supporting active fighters to focusing on the wives and children of jihadists held in camps such as Al Roj or Al Hol, where the funds act as a form of *'false charity'* intended to maintain the organisation's internal cohesion, facilitate escapes or guarantee a support structure similar to an internal social security system. However, there are still operations in which money is sent directly to the terrorist organisation or to former fighters, either for their personal upkeep or to cover the logistical needs of the organisation.

106. As set out in TF's Sectoral Risk Analysis (SRA) on NPO organisations[21] (2025), TF in Spain has identified a number of cases of fraudulent use of charitable channels and private crowdfunding campaigns, where the transfer of funds was disguised as humanitarian aid but was in fact directed at members of Daesh, their families or radicalised women in refugee camps, thereby ensuring the cohesion of the terrorist group. Investigations have also uncovered evidence of the misuse of NPO

[19] Source: Policía Nacional
[20] Source: Guardia Civil.
[21] https://www.tesoro.es/sites/default/files/publicaciones/file/SRA%20OSFL_V.PUBLICA.pdf

organizations, with the diversion of funds for terrorist purposes, particularly through property purchases, non-bank international remittances such as *hawala*, and links with organisations based in conflict zones. This pattern, observed in various police operations and intelligence communications, demonstrates that certain NPO organisations can become vulnerable vehicles or be exploited to channel resources to jihadist structures.

107. Finally, with regard to the use of new technologies in TF, crypto-assets have become firmly established and expanded exponentially across all stages of the process, becoming one of the main means of transferring funds. There has been a noticeable trend amongst DAESH members towards the use of stablecoins, particularly USDT due to its liquidity, as it avoids fluctuations in value and transaction fees are low. Furthermore, the use of private-key cryptocurrencies such as Monero has been detected when they have launched fundraising campaigns on their propaganda channels.

108. Although artificial intelligence and online gaming have not been used to any significant extent for financing purposes, their use has been detected for purposes such as recruitment, through platforms such as Discord [22] . In this regard, *streaming* and *gaming* platforms are currently being exploited by terrorist groups to facilitate the recruitment, indoctrination and radicalisation of jihadist sympathisers in the West. These platforms also offer opportunities for making micro-payments via their virtual tokens, which can be used to raise funds for terrorist purposes whilst obscuring their traceability. Their importance for TF in terms of volume would be lower than that of other channels, as they are less profitable. As regards the use of artificial intelligence, techniques have been observed whereby criminal networks evade the *onboarding* controls of financial institutions. Despite this threat being recognised, no evidence of such micropayment operations has been detected in Spain.

109. The nationwide crypto-asset operations identified during the investigations involve sending small payments to cryptocurrency addresses that form part of TF campaigns and are published or shared via social media or messaging apps alongside the organisation's own propaganda. During the period analysed, there were 8 investigations [23]in which the use of crypto-assets as a method of financing was identified, confirming their central role in this form of criminal activity. With regard to the Policía Nacional's operations, out of the 25 operations investigated in 2025, crypto-assets were detected in 10 of them.

110. In conclusion, although Spain has maintained a high level of anti-terrorism alert since 2015, the TF shows that the volume per transaction is steadily decreasing. This is a consequence of the changing international terrorist landscape, where large sums directed towards structured organisations are no longer required, but rather smaller amounts intended for the basic sustenance of individual actors or small cells. This scenario is reinforced at national level, where the activity detected is mainly linked to self-radicalisation and indoctrination, as well as recruitment – phenomena that require less funding and take place primarily in digital environments. Overall, the threat remains high, but its financial impact has diminished, reflecting an operational transformation in contemporary terrorism.

[22] A free platform for voice, video and text communication, designed to create communities ('servers') and chat in real time.
[23] Figures from the Guardia Civil's Information Directorate.

6. MAIN VULNERABILITIES IN Money Laundering AND Terrorist Financing.

111. The 2024 Addendum identified the following vulnerabilities:

A. Vulnerabilities arising from the population.
B. Vulnerabilities arising from geographical factors: i) transactions involving high-risk territories or their citizens/entities; ii) transactions involving countries with a significant presence of organisations/citizens linked to jihadist terrorism; and iii) transactions in the area of Gibraltar and Ceuta–Melilla.
C. Vulnerabilities arising from the nature of the organisation or the activity carried out.
D. Vulnerabilities arising from payment methods; (i) the use of cash and the informal economy; and (ii) the use of crypto-assets
E. Vulnerabilities arising from technological innovations in financial transactions

6.1. Vulnerabilities arising from the population.

112. Vulnerabilities arising from the population are reflected in the increase in the foreign population in Spain, which in 2025 will account for 14.07 % of the total, compared with 13.37 % recorded in 2024. This group is diverse in composition, with nationals from Morocco (14 %), Colombia (10 %), Romania (9 %), Venezuela and Italy (5 % each), the United Kingdom and Peru (4 % each), as well as China and Ukraine (both at 3 %)[24] .

113. Employment among these nationalities is mainly concentrated in the services sector (73 %), whilst men have a strong presence in agriculture (77.56 %), industry (69.98 %) and, in particular, construction (96.66 %). These sectors (particularly agriculture, construction, hospitality and domestic services) traditionally exhibit higher levels of the informal economy and intensive use of cash, facilitating practices such as informal hiring, a lack of transparency in financial flows and the employment of workers in situations of administrative or financial vulnerability.

114. In this context, the increase in the foreign population, combined with its concentration in sectors where cash is used extensively, can be exploited by criminal networks to channel illicit funds through cash payments, the use of identities for opaque business structures, the use of intermediaries in exchange for a commission, or the proliferation of cash couriers to carry out fraudulent operations involving the splitting of cash.

6.2. Vulnerabilities arising from geographical factors.

6.2.1 Conducting transactions with high-risk territories or with citizens/entities from those territories.

115. Transactions carried out with high-risk territories or with citizens and entities linked to them present vulnerabilities in terms of ML, particularly with those jurisdictions

[24] Source: INE

considered non-cooperative, given the lower level of AML/CFT supervision and financial transparency in many of these jurisdictions.

116. An estimate has been made of the exposure of Spain's operations to those jurisdictions considered non-cooperative[25] . For this exercise, the estimated volume of funds reported in ad hoc reports[26] and systematic reports[27] received by SEBPLAC during the period 2020–2025 has been analysed.

117. The result of this analysis is that it is estimated that only 4 % of the total volume of funds reported on an ad hoc basis explicitly refers to non-cooperative jurisdictions, whilst 46 % of the funds reported in systematic reports to SEPBLAC are related to these high-risk territories. The weight given to systematic reports is consistent, as the majority of these reports relate primarily to the transfer of funds to high-risk territories and the channelling of funds through money laundering intermediaries.

118. The percentage attributed to the estimated volume of funds in suspicious activity reports reflects the suspicious transactions detected by regulated entities in which there are indications of activity involving these countries.

119. This duality highlights, on the one hand, the vulnerability inherent in analysing flows with high-risk jurisdictions, given their capacity to hinder traceability and facilitate asset concealment schemes.

6.2.2. Transactions with countries posing a higher risk of Terrorist Financing.

120. Spain has a limited level of vulnerability in relation to TF linked to transactions with higher-risk countries, but there are geographical and operational factors that increase its exposure. Its geographical position makes Spain a point of entry and transit for migration flows from North Africa and the Sahel – areas where terrorist activity is present – which introduces a risk associated with support networks or family and community links among displaced persons in Spain.

121. However, Spain does not act as a significant financial route for the transfer or receipt of funds linked to terrorist organisations, partly thanks to controls on payment transactions both within the country and at its borders, and to the banking sector's robust preventive system, which reduces the likelihood of operations linked to the financing needs of terrorist organisations in Spain (as explained in section 2.1 of this report).

122. Even so, investigations reveal links with jurisdictions such as Morocco, Algeria, Türkiye (particularly in areas bordering Syria) and European countries such as France and Belgium, which are used for travel or as hubs for logistical support.

[25] https://www.boe.es/buscar/act.php?id=BOE-A-2023-3508

[26] The volume of funds reported in the communications received is calculated, taking into account the countries included in the list set out in Order HFP/115/2023 of 9 February, and applying the following criteria for counting a country: the nationality, residence or place of birth of each person involved in the case, and the country indicated in the case by the analyst.

[27] The volume of funds reported in the communications received is calculated, taking into account the countries included in the list set out in Order HFP/115/2023 of 9 February, and applying the following criteria for determining a country: the country of origin or destination of the transaction; the country of nationality or birth of the parties involved; and the country of residence of the parties involved.

123. Furthermore, certain Gulf States, such as the United Arab Emirates or Saudi Arabia, feature in schemes involving the triangulation of transactions or investments, with these countries being used as financial conduits to areas of terrorist conflict.

124. With regard to routine reports, an analysis has been carried out of the information submitted by regulated entities to SEPBLAC, and an estimate has been made by jurisdiction in terms of terrorist risk[28] . It is estimated that 10 % of these reports relate to a factor associated with jurisdictions posing a terrorist risk: either the country in question is mentioned, or there is a party involved whose nationality, residence or place of birth is linked to the case in question for the period 2020–2025.

125. As regards the systematic reports received by SEPBLAC, 2 % of the volume of funds covered by these reports includes information on the country of origin or destination of the DMO (Monthly Statement of Transactions, Declaración Mensual de Operaciones) transaction, the country of nationality or birth of the parties involved, or the country of residence of the parties involved.

126. Therefore, the main vulnerability for Spain does not stem from it being a financial centre for terrorist financing, but rather from the risk associated with migratory flows of people, links due to geographical proximity, and connections with third countries where there is indeed a higher risk of TF due to their role as intermediaries in the financial route.

6.2.3. Activities in the Gibraltar and Ceuta-Melilla area.

127. The area presents specific vulnerabilities arising from its geostrategic position, which is highly exposed due to the intensity of maritime and commercial traffic in the Strait, making it a high-risk area for illicit activities and ML operations by opaque corporate structures that exploit the high volume of financial and logistical traffic.

128. For their part, Ceuta and Melilla exhibit vulnerabilities specific to their land border with Morocco, which makes them critical areas for irregular migration and the potential infiltration of radicalised individuals or those linked to terrorism, as well as constituting high-risk areas for cross-border organised crime and the trafficking of illicit goods, people and funds.

129. As regards data on declarations at border payment points, the significance of the Gibraltar area is evident from the percentage of declarations for both entries and exits for the period 2020–2025.

130. The amounts (in euros) declared for the period 2020–2025 are set out in the following table:

Table 16. Declarations and amounts declared (euros) for the period 2020–2025 at customs.

	IMPORTS		OUTBOUND	
	Total amount	Declarations	Total amount	Declarations
GIBRALTAR	791,583.52	30.00	7,944,559.16	295.00
ALGECIRAS	92,855,081.08	3,162.00	101,864,046.52	4,340.00
CEUTA	15,473,799.25	662.00	2,855,597.44	88.00
MELILLA	19,666,331.46	789.00	135,700.00	6.00

[28] Jurisdictions identified as being at risk of TF, based on the findings of the Sectoral Analysis of Terrorist Financing Risks through Non-Profit Organisations, 2025.

TOTAL 4 AREAS	128,786,795.31	4,643.00	112,799,903.12	4,729.00
SPAIN	**1,963,461,466.90**	**37,501.00**	**1,471,582,199.65**	**38,053.00**

131. Analysing the figures in percentage terms, we can see that, during this period, imports and exports accounted for 12 % of declarations out of the total number of declarations made at all customs offices in Spain.

Table 17. Percentages of declarations and amounts from customs offices in the Gibraltar Area in relation to the total declared at Spanish customs offices.

	IMPORTS		OUTBOUND	
	Total value %	Declarations %	Total value %	Declarations %
GIBRALTAR	0.04%	0.08%	1%	1%
ALGECIRAS	4.73%	8.43%	7%	11%
CEUTA	0.79%	1.77%	0.19%	0.23%
MELILLA	1.00%	2.10%	0.01%	0.02%
TOTAL 4 AREAS/ TOTAL SPAIN	6.56%	12.38%	8%	12%

Source: AEAT

132. As regards customs data on smuggling operations, tobacco is the commodity that has been seized most frequently by customs authorities in terms of the number of packets. Nevertheless, there has been a 65 % decrease since 2020, from almost 2.8 million packets seized in 2020 to 9.1 million packets in 2025[29] .

133. In conclusion, drug trafficking and organised crime are the threats most closely linked to the geographical vulnerabilities of the Gibraltar, Ceuta and Melilla area.

6.3. Vulnerabilities arising from the nature of the organisation or activity carried out.

134. Based on the 2020 and 2024 NRA, as well as the 2025 SRA for NPO organisations, a number of sectors and types of entities were identified whose nature and operations place them among those most exposed to ML and TF risks. On this basis, this section provides a specific analysis of the vulnerabilities associated with these entities and links these vulnerabilities to the specific threats that may materialise, depending on the type of threat analysed in this report.

135. Credit institutions, particularly in the private banking and correspondent banking sectors, exhibit high levels of vulnerability due to the volume of transactions, the complexity of their products and their capacity to mobilise international funds. These characteristics make them particularly susceptible to being exploited both by organised crime—which seeks to channel large illicit profits through complex financial circuits—and in economic crimes, where banking products are used through document forgery and international transfers

[29] Tax Administration Reports (published by the Ministry of Finance)

or complex products located abroad to conceal funds derived from criminal activities linked to corruption. In the context of terrorism and TF, correspondent banking and cross-border transfers amplify the risk as they allow small amounts to be moved between jurisdictions in fragmented transactions.

136. Payment institutions and electronic money institutions have vulnerabilities arising from high transaction speeds, digital operations, the ability to split transactions and reduced face-to-face interaction with customers. This operational framework makes them particularly vulnerable to threats linked to drug trafficking and organised crime, which use these channels to move proceeds via micropayments or successive transfers. In turn, they are highly vulnerable to financial fraud, both due to the ease of identity theft and the possibility of moving funds without sufficient traceability. These characteristics also make them susceptible to TF, where the fragmentation of amounts and the use of electronic platforms are consistent with the funding patterns of terrorist cells or sympathisers.

137. Currency exchange businesses are vulnerable due to the use of cash and the fragmentation of transactions, which can facilitate both TF operations and cross-border fund transfers by criminal organisations.

138. Entities providing gambling services via online platforms are vulnerable to the channelling of illicit funds, particularly those obtained through fraud, with deposits and withdrawals designed to simulate legitimate winnings. Digital operations and the fragmentation of payments facilitate the use of false identities and rapid transfers. These same characteristics enable small contributions intended for TF to be channelled.

139. Activities that rely heavily on assets and legal structures, such as the property sector, corporate services and the legal profession, exhibit vulnerabilities linked to a lack of transparency regarding beneficial ownership, the possibility of laundering funds or using shell companies, and the difficulty in identifying ultimate beneficial owners. These vulnerabilities are directly linked to threats such as ML stemming from organised crime, drug trafficking and tax offences. In the case of the property sector and special-purpose vehicles, the risk is heightened in cases of corruption, where property acquisitions are used to conceal illicit enrichment.

140. Finally, certain religious organisations, given their humanitarian and charitable nature, are vulnerable to TF primarily due to the nature of donations, which are fragmented and made in cash. This vulnerability is exacerbated when they act as recipients or distributors of funds to third countries.

6.4. Vulnerabilities arising from means of payment.

6.4.1. Vulnerabilities arising from the use of cash and the informal economy[30] .

141. In Spain, there is no problem with access to banking services, as the ownership and use of current accounts is almost universal (98 %)[31]. However, according to the **Report on the Monitoring of Financial Inclusion in Municipalities with More Than 500 Inhabitants. Updated June 2025**: as at 31 December 2024, there were 61 municipalities with more than 500 inhabitants without a banking access point.

[30] Source: *Study on cash usage habits 2022*, Banco de España.
[31] Data for 2024. https://www.worldbank.org/en/publication/globalfindex/report/accounts-saving-borrowing-payments

142. According to the Banco de España's 2025 Study on Cash Usage Habits[32], 57 % of consumers continue to use cash as their primary means of payment for purchases in physical shops, and 55 % of the population use it on a daily basis. The use of cash is most widespread amongst those aged 55 and over and people with basic education, with convenience, habit and control over spending being the main reasons for choosing it.

143. Although bank cards remain the second most common means of payment in physical shops, used by 27 % of the population, mobile devices represent the method that has seen the greatest increase, with 15 % of the population now using them as their primary means of payment. As for transactions between individuals, *Bizum* ranks second, used by 37 % of the population, behind cash.

144. In the retail and hospitality sectors, 43 % of establishments receive the majority of their payments by card or other means, whilst 30 % rely mainly on cash.

145. Finally, with regard to cash withdrawals from ATMs, as reported by the Banco de España[33], in 2025 the number of withdrawal transactions fell by 4.47 %, but the volume of withdrawals increased by 1.37 % compared with 2024. This may be an indicator of a reduction in the practice of splitting cash withdrawal transactions during 2025.

146. In conclusion, despite high levels of banking penetration and the rise of digital payment methods, the widespread use of cash (particularly amongst certain demographic groups and in sectors such as small retail and the hospitality industry) continues to pose risks associated with this payment method. The persistence of cash as the primary means of payment and the increase in the volume withdrawn from ATMs, despite the fall in the number of transactions, suggests that it remains an attractive tool for criminal organisations, fraud networks, tax offences and corruption schemes due to its ability to obscure financial traceability.

6.4.1. Vulnerabilities associated with the use of crypto-assets[34] .

147. The regulation of the use of crypto-assets as a means of payment in Spain presents a fundamental vulnerability linked to a lack of transparency regarding the holding and use of this instrument, as well as the potential for opacity and pseudo-anonymity arising from the use of techniques designed for this purpose, which makes it difficult to identify the actual originator of the funds.

148. The methods used to circumvent transparency highlighted by the authorities include the use of VPNs and proxies, the use of *mixers*, *cross-chain* transactions, the use of DEXs without the possibility of carrying out know-your-customer checks, and the use of *exchanges* in non-cooperative jurisdictions to conceal the actual location of the transaction and the user's true identity, complicating traceability in rapid, cross-border transactions that can be used to move illicit capital without leaving a verifiable trail. This makes crypto-assets an attractive tool for circumventing traditional financial controls in peer-to-peer payments, e-commerce and instant transfers.

[32] Source: https://www.banco-de-espana.es/f/webbe/INF/MenuVertical/BilletesYMonedas/Estudios_e_informes/Estudio_sobre_habitos_efectivo/Informe_Ejecutivo_EHUE_2025_es.pdf

[33] https://www.banco-de-espana.es/webbe/es/estadisticas/temas/sistemas-pago.html

[34] Source: *Study on cash usage habits 2022*, Banco de España.

149. Vulnerability increases when the use of different types of crypto-assets is factored in. Private cryptocurrencies or those with strong privacy mechanisms (such as wallets designed to obscure transactions) pose a high risk by enhancing anonymity and reducing traceability, thereby hindering investigative work into digital payments.

150. For their part, *stablecoins,* which are widely adopted for international payments and transfers, introduce additional risks by enabling value to be moved in a stable and rapid manner outside the banking system, which can circumvent operational limits and cross-border controls. The EBA warns that the expansion of these assets is increasing the European financial system's exposure to money laundering risks due to the growing interconnection between crypto providers and traditional financial institutions.

151. Finally, the existence of crypto-asset service providers without adequate controls and in the process of adapting to the MiCA framework increases the inherent risk associated with the use of crypto-assets as a means of payment. Although the CNMV has assumed supervisory responsibility since December 2024, vulnerabilities remain during the regulatory transition period.

6.5. Vulnerabilities arising fromtechnological technological in financial operations.

152. According to the 2025 State of the Digital Decade Report[35] , Spain ranks second in terms of fibre-optic coverage, reaching 95 % of households and 86.3 % in rural areas, well above the European average, which stands at just 58.8 % of households in rural areas. As regards 5G technology, coverage reaches 95 % of the population, and 8 out of every 10 people living in rural areas. This information underlines the digital transformation of society. The rise in digital activity has coincided with a sharp increase in cybercrime: in 2023, 472,125 cybercrimes were reported in Spain, 26 % more than the previous year, with 90.5 % of these being cases of computer fraud, cementing digital fraud as the main threat to citizens and organisations. In 2024, these figures saw a slight decline, but remain at levels similar to those of 2023[36] .

153. The main vulnerabilities identified in Spain stem from society's heavy reliance on digital technology and the increasing sophistication of attacks. In terms of impact, cybercrime in Spain primarily affects individuals, who account for the majority of recorded incidents (350,795 in 2024). Businesses, for their part, are most affected by technically complex attacks (such as *ransomware*, *BEC* or *DDoS*), which result in significant financial losses and data breaches, particularly in sectors such as ICT, professional services, retail and critical infrastructure.

154. The widespread use of AI exacerbates this vulnerability, as it helps to create more credible and large-scale attacks. Furthermore, the use of AI can circumvent the *'Know Your* Customer' (KYC) barriers of fintech companies and electronic money institutions, whilst instant *cross-border* payments enable microtransactions that bypass regulatory thresholds. Criminal AI, utilising *deepfakes* and large language models (LLMs), amplifies the recruitment of digital money mules via social media, breaking down geographical barriers and

[35] https://digital-strategy.ec.europa.eu/es/library/state-digital-decade-2025-report
36https://www.interior.gob.es/opencms/es/archivos-y-documentacion/documentacion-y-publications/publications/downloadable-publications/periodicals-yearbooks-and-journals/report-on-cybercrime-in-spain/

cultural aspects in schemes such as *'pig butchering*'. Such innovations lead to the fragmentation of information and impact the fulfilment of due diligence obligations.

155. In addition to the above, the use of artificial intelligence also enables the automation of transactions, particularly in the field of cryptocurrencies, allowing for the scheduling of movements that hinder traceability during investigations.

156. Finally, the expansion of crypto-assets and DLT technology has created new challenges due to their pseudonymous nature and the speed of transactions. The growing use of DeFi platforms and the tokenisation of real-world assets creates security gaps in identity and governance that criminal organisations exploit to launder money. The main vulnerability stems not only from the technology itself, but also from the lack of regulation capable of keeping pace with its evolution. Added to this is increased opacity through mixers, *tumbling* services and the systematic use of *proxies* and *VPNs* – tools that make it difficult to trace transactions and link them to specific individuals or devices.

    In conclusion, cyber activity linked to the rise in digital payments – sometimes facilitated by non-financial platforms that are not governed by Law 10/2010 of 28 April – makes it easier for financial flows to be linked to criminal activities such as organised crime, drug trafficking and terrorist groups, and to be transferred more quickly and anonymously. Social engineering, the use of AI and techniques involving crypto-assets that facilitate opacity make it possible to divert funds and operate across borders, turning cybercrime into a direct multiplier of national threats posed by ML and TF.

7. SECTORAL ANALYSIS[37]

Sector: Credit Institutions 2026

Activity and context

157. Credit institutions are obliged entities under Article 2.1(a) of Law 10/2010 of 28 April.

158. Credit institutions are entered in the Banco de España (Banco de España) register, subject to authorisation by the ECB, as part of a procedure handled by the Banco de España using documentation provided by the institution and a mandatory report from SEPBLAC on the adequacy of its procedures for the prevention of ML and TF. The total number of credit institutions in Spain, as of December 2025, stands at 186[38]. Most of these institutions belong to the Spanish Banking Association (AEB), the Spanish Confederation of Savings Banks (CECA) and the National Union of Credit Cooperatives (UNACC), which act as a link between credit institutions and public authorities and have been playing a very significant role in the implementation of measures to prevent ML and TF.

159. The trend in the number of institutions registered with the Banco de España is shown in the following table:

ENTITIES	2020	2021	2022	2023	2024	2025
Banks	51	48	48	47	46	43
Savings banks	2	2	2	2	2	2
Credit unions	61	61	61	61	61	60
Branches of EU credit institutions	75	79	78	74	74	78
Branches of non-EU credit institutions	3	4	4	4	4	3
TOTAL	**192**	**194**	**193**	**188**	**187**	**186**

160. By activity, the sectoral breakdown of credit institutions entered in the Banco de España's register for the year 2024, based on the sectoral risk analysis carried out by SEPBLAC this year, is as follows:

[37] The colour codes in the tables throughout this document indicate the ratings assigned, in accordance with the rating system set out in Article 12(3) of Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024, establishing the Anti-Money Laundering and Counter-Terrorism Authority. The levels of inherent and residual risk shall be rated as follows:

Low	Medium	Substantial	High

Whilst the levels of inherent and residual risk have been assessed taking into account the rating system set out in Article 12(3) of Regulation (EU) 2024/1620 of the European Parliament and of the Council, the analysis carried out for the purposes of this methodology has required the introduction of intermediate risk levels. These intermediate categories are intended to provide a more granular and proportionate assessment of risks, allowing for a more precise distinction between situations which, although falling within the same regulatory risk category, exhibit materially different risk characteristics.

Low/Medium	Medium/Substantial	Substantial/High

[38] The ICO is not included

grouped into 5 sectors[39] : 10 significant institutions[40], 94 institutions engaged in commercial banking[41] , 12[42] private banking institutions, 2[43] 6 institutions classified as 'financing institutions' whose sole activity is essentially the granting of loans, particularly consumer credit, and 43 classified as 'other institutions' specialising in other activities (custodial services, corporate banking, etc.).

161. **Banks** are commercial credit institutions, generally incorporated as public limited companies. Their activities usually cover a very broad spectrum. From an AML/CFT perspective, this more diversified nature entails a risk ranging from medium to high (depending on the specific activities carried out), due to the high volume of transactions, the sophistication of their product range and their presence across multiple jurisdictions.

162. **Savings banks** currently tend to operate through banking foundations or as shareholders in banks established following the restructuring of the financial sector. Historically, they have maintained strong regional ties and a dual mission, combining financial activities with social welfare work. Although the AML/CFT risk profile is generally lower than that of banks due to the predominance of retail customers, the governance model, geographical concentration and the potential presence of vulnerable groups necessitate a nuanced supervisory approach.

163. **Credit cooperatives**, also known as rural savings and credit cooperatives, are organised as cooperative societies and are owned by their members, who exercise democratic control. Their business is predominantly retail-based and of low complexity, which in principle translates into a lower AML/CFT risk. However, the close relationship between staff and customers — which may give rise to a risk of familiarity — and the potential technological limitations of some institutions require careful attention in supervision.

164. In summary, banks are characterised by their commercial approach and broad diversification; savings banks by their social and regional focus; and credit unions by their cooperative model and proximity to customers. These elements, combined with the type of business each carries out, determine clearly differentiated AML/CFT risk profiles.

165. The sector's balance sheet totals 3.1 trillion euros, with banks – at 2.7 trillion euros – being the type of institution with the greatest weight within the sector as a whole. With regard to the sector's integration into the financial system, it should be noted that the level of financial inclusion in Spain stands at 99%[44]. 92 % of the population live in municipalities with two or more bank branches, and less than 3 % live in areas without physical access to a bank branch.

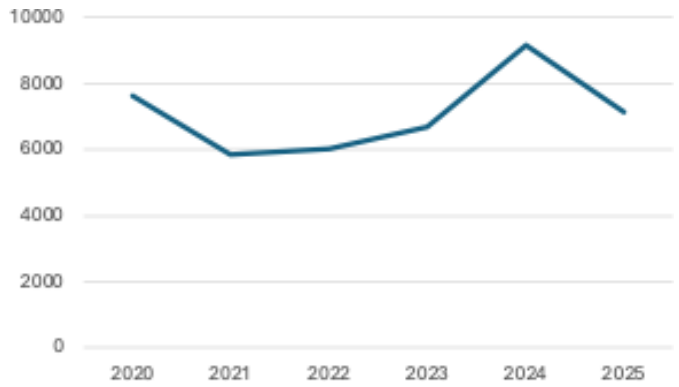
Threats

166. The credit institutions sector forms the core of the Spanish financial system and channels the vast majority of domestic and international economic flows. This central role, combined with its enormous volume of business, diversity of products, breadth of customer base, and use

[39] This classification includes banks, savings banks, credit unions, branches of EU credit institutions and branches of non-EU credit institutions.
[40] 9 Spanish banks and 1 credit union group.
[41] 59 credit unions, 20 Spanish banks, 13 branches of EU credit institutions, 6 branches of non-EU credit institutions and 2 savings banks.
[42] 8 branches of EU credit institutions, 1 branch of a non-EU credit institution and 3 Spanish banks
[43] 22 branches of EU credit institutions, 3 Spanish banks and 1 branch of a non-EU credit institution
[44] Report on Financial Inclusion in Spain 2024 (AEB, CECA and UNACC).

The intensive use of digital channels, cross-border exposure and a high level of interconnection with other regulated sectors place credit institutions amongst the sectors with the greatest exposure to the threats of Money Laundering and Terrorist Financing in Spain.

167. Since 2020, the indicators reported by the sector are shown in the following chart:



Source: SEPBLAC

168. Of these reports, 44 % related to general money laundering offences, followed by fraud-related offences (24 % of the reports) and tax offences (20 % of the reports received). Between 2020 and 2025, 78,065 reports were recorded in which the credit institutions sector was mentioned, although the majority were submitted by institutions within the same sector regarding other credit institutions, payment institutions, notaries and registrars. The associated offences correspond to those typically detected in reports issued directly by the credit institutions sector, with fraud offences rising to 26 % of the identified cases.

169. The most significant specific threats to the sector are detailed below.

Organised crime and banking channels as a gateway to the financial system

170. Chapter 4 identifies organised crime as a persistent threat that uses bank accounts, transfers, loans, digital banking and money mules to channel and disperse illicit funds. Credit institutions, due to their ability to operate across multiple jurisdictions and manage highly liquid products, constitute the main channel for: i) placing illicit funds into current accounts with apparently legitimate activity, ii) moving funds via international transfers, iii) creating financial structures linked to shell companies, iv) facilitating the conversion of cash into deposits, and v) exploiting digital operations for rapid dispersal. Their widespread involvement in almost all criminal investigations — including fraud, drug trafficking, human trafficking and cybercrime — confirms the centrality of this risk.

Economic crimes, large-scale fraud and 'mule accounts'

171. According to the NRA, economic and digital fraud is one of the threats that has seen the greatest increase since 2020, particularly in relation to: i) investment fraud, ii) digital scams, ii)

phishing/vishing/smishing, iii) SIM-swap fraud, iv) BEC scams, v) organisational and corporate fraud, and vi) the widespread use of money mule accounts. Industry data confirms this threat: in 2024, reports of suspected fraud accounted for almost 80 % of the total reported by credit institutions, driven in particular by *neobanks*, which saw their reports increase sevenfold compared with 2023. Bank accounts are the main channel for: receiving fraudulently obtained funds, their immediate dispersal across different jurisdictions, their subsequent withdrawal and conversion, and the concealment of their origin through micro-transactions.

Political and financial corruption and complex corporate structures

172. Chapter 4 identifies offences such as embezzlement, bribery, influence peddling and international tax fraud as significant threats, in which credit institutions may act as a conduit for: opening accounts for shell companies, moving funds between various corporate layers, concealing the beneficial owner in companies with cross-shareholdings, financing property and asset transactions linked to PEPs, or receiving illicit donations, payments or kickbacks. The sector reports that complex corporate clients, non-residents and PEPs represent a high risk, particularly in private banking and corporate banking.

Drug trafficking and transnational criminal economies

173. The 2026 NRA confirms that drug trafficking makes extensive use of: transfers, crypto-assets, operational accounts held by frontmen, cash deposits—sometimes involving *'smurfing'* or splitting transactions—loans to simulate economic activity, and the use of international clearing networks. Credit institutions are the main channel for: splitting funds derived from drug trafficking, transferring funds to suppliers in Latin America, Africa and Asia, and channelling logistical payments for criminal networks. The wide availability of banking products facilitates the integration of these funds into the formal system.

Terrorist Financing and international micropayments

174. The NRA highlights that the current threat of TF is characterised by, amongst other things: small transfers, sometimes disguised as donations; informal banking systems; digital platforms and fintech with weak controls; the use of multiple financial intermediaries; scattered micropayments; and international transactions to high-risk countries. Credit institutions may channel these transactions through accounts held by: non-resident individuals, NPOs, or companies with indirect links to sensitive countries, via recurring low-value transfers. The scale of the sector makes early detection difficult in the absence of additional indicators.

Breaches of international sanctions

175. In the current context of growing geopolitical fragmentation, sanctions are no longer limited to direct prohibitions on countries or individuals, but include complex mechanisms of indirect evasion, risks of secondary sanctions and the use of intermediary jurisdictions to channel commercial and financial transactions. Parties subject to sanctions use indirect and sophisticated structures to conceal the true origin, destination or beneficial owner. The sanctioned entities typically operate through: shell companies, holding companies in multiple jurisdictions, trust companies, *nominee shareholders* and/or hidden beneficial owners.

176. The factors most frequently exploited by threats in the credit institutions sector are as follows:

Factors most frequently exploited by threats	
International transfers and correspondent banking	The level of exposure associated with international transfers is particularly high, given that their total volume amounts to 5 trillion euros; 2.2 % of these involve countries on the FATF list; large groups hold thousands of correspondent accounts; and the speed and relative opacity of these flows facilitate the dispersal of funds. Chains of intermediaries make it difficult to verify the origin and destination of funds, which is consistent with the NRA's patterns relating to: i) illicit trade networks, ii) transnational organisations, iii) the financing of foreign groups, and iv) activities linked to proliferation. The risks centre on the triangulation and fragmentation of payments into separate orders designed to hinder or prevent full traceability.
Crypto-assets, technological opacity and links with CASPS	The banking sector is experiencing an expansion of services under MiCA, partnerships with crypto-asset service providers and greater exposure to crypto flows. Although proprietary trading is limited, flows between bank customers and crypto-asset service providers reached 2,540 million euros in 2024, representing a 24 % increase in outflows and a 91 % increase in inflows compared with 2023. The NRA warns of: i) relative anonymity, ii) opacity of wallets, iii) hybrid crypto–digital banking schemes, iv) high risk in significant institutions and commercial banking. This channel represents a growing exposure, particularly to fraud, drug trafficking and TF.
Identity theft, digital banking and instant payments	The NRA notes that the widespread digitalisation of the financial sector has given rise to new threats due to: remote account opening, theft of credentials, social engineering, immediate transactions (instant payments), and the use of fintech intermediaries. By 2024, 63 % of transactions were already being carried out via remote channels. This facilitates: i) the immediate dispersal of stolen funds, ii) the concealment of the origin through multiple transactions, iii) identity theft in remote account openings, and iv) the use of poorly regulated intermediary platforms.

Risk factors due to inherent vulnerability

177. The following sets out the factors relating to inherent vulnerability analysed to determine the inherent risk of credit institutions:

Sector Characteristics	
Size of the sector and turnover.	As of 31 December 2024, the sector had 157,000 employees, some 19,000 branches and 111 million customers. The high volume of business in the sector, the number and diversity of customer types and institutions, and the variety of transactions routinely carried out make this sector highly attractive and vulnerable to the concealment of ML/TF operations.
Level of complexity of the sector's structure.	In Spain, there were 10 consolidated banking groups as of 31 December 2024, including significant institutions that account for 75 % of the sector's activity, concentrating 76 % of employees, 77 % of branches, 67 % of the number of customers and 70 % of the number of accounts[45]. Concentration is particularly high among the four largest significant institutions, which account for approximately 50 % of all credit institutions' activity. The combination of a high degree of concentration in the banking sector, together with the existence of large groups with *cross-border* structures, subsidiaries, branches and outsourced services, creates a significant structural vulnerability in terms of ML/TF prevention. The organisational complexity of the largest institutions hinders supervision and increases the likelihood of gaps in the consistent application of controls, whilst their dominant position within the system amplifies the potential impact of any failure.
Level of integration with other regulated sectors.	The sector is closely linked to investment firms, insurers, *fintech* companies and payment service providers. This interconnection broadens the scope of risk. It should be borne in mind that, apart from their core business, credit institutions carry out, either directly or through subsidiaries, the lion's share of other financial activities: - approximately 70 % of life insurance activity in 2023 is accounted for by insurers integrated into banking groups[46]; - credit institutions, following a process of absorbing the securities firms that were their former subsidiaries, receive more than 87 % of commissions for investment services[47]; - securities firms that remain subsidiaries of banks accounted in 2022 for 80 % of the total assets of securities firms and around 16 % of the income received by such entities; - management companies of collective investment schemes that are owned by banks manage, as of 31 December 2023, 86 % of the assets of Spanish investment funds[48];

[45] Metrics established in accordance with the R.I.E.
[46] Activity measured by the volume of annual premiums. Source: ICEA
[47] CNMV. Annual Report on the Securities Markets and its Activities 2024.
[48] Association of Collective Investment Schemes and Pension Funds. Statistics on the management of collective investment schemes and pension funds by financial groups (December 2023).

	- the same percentage of 86 % represents the assets of pension funds managed by subsidiaries of credit institutions as a proportion of the total[49] ; Approximately 50 % of the gross lending by credit institutions as of 30 June 2023 was attributable to subsidiaries of credit institutions[50].
The geographical location of the institution, including the geographical scope of the sector's operations.	Banks operate across multiple jurisdictions, some of which are higher-risk. From a global perspective, there are two main players with a strong international presence, whose assets account for 59 % of the total. Overall, credit institutions' overseas business accounts for between 40 and 45 % of their total business. Savings banks and co-operatives have local operations with lower exposure, but overall the sector maintains significant activity in countries with varying levels of risk. Some 3 % of institutions are classified as high-risk due to having branches in tax havens (including the parent company)[51] and 24 % of institutions are classified as medium-high risk due to this factor. On the other hand, 90.91 % of institutions have a low inherent risk or have no subsidiaries or branches abroad, or their activity is very limited, although their share of total assets is not particularly significant. As regards the domestic geographical position, 9 % of institutions have offices in high-risk cross-border areas and 14 % in medium-to-high-risk areas.
Nature of the products and services provided by the sector	
Level derived from the complexity of the products, due to their impact on anonymity or the limited information available on clients.	Taking into account the sectoral breakdown by volume of activity, private banking institutions, characterised by their high complexity, concentrate 88 % of their assets under management in activities strictly linked to private banking, relative to their total assets under management. This percentage stands at 14 % for institutions engaged in commercial banking and 20 % for the 10 significant institutions. With regard to private banking institutions, the use of complex corporate structures and products makes it difficult to correctly identify beneficial owners. Furthermore, the diversification of investments across entities within the financial group – some of which are established in countries with limited cooperation in this area – makes it difficult to ascertain the origin of the funds and the amounts actually under management. As for the volume of transactions involving crypto-assets, given their impact on anonymity, significant institutions account for an average of 80 % of all crypto-asset transactions across all credit institutions. If we compare the proportion of crypto-asset activity relative to both outgoing and incoming customer transfers, outflows to CASPS would account for 10 % of outgoing transfers and 12 % of incoming funds from transfers across all credit institutions.

[49] Association of Collective Investment Schemes and Pension Funds. Statistics on the management of collective investment schemes and pension funds by financial groups (December 2023).
[50] Source: Banco de España.
[51] Three are branches of Chinese parent companies and two are domestic banks with branches/subsidiaries in high-risk countries

Level at which specific products and services offered are linked to intelligence reports and/or national ML or TF investigations.	The banking sector is the main source of reports based on indications in terms of volume and its cross-cutting presence in almost all economic activity. Its exposure to predicate offences is high due to its role as a gateway to the financial system. In 2024, regulated entities submitted 76 % more suspicious activity reports than in the previous year, rising from 13,854 to 24,320. This increase is widespread, although it is concentrated primarily within the financial sector, particularly among so-called *neobanks,* which have increased their submissions from 1,152 suspicious activity reports in 2023 to 7,595 in 2024. With regard to the potential underlying criminal activities identified in the analysis of communications based on suspicion, 2024 was characterised by communications linked to fraud and so-called 'mule accounts', categories which have driven the rise in the total number of communications. Thus, the percentage of communications falling within this category was close to 80 %, 20 percentage points higher than in 2023[52]. In 2025, there were 21,667 communications based on suspicion, 12 % fewer than in 2024. Reports from credit institutions totalled 12,105, representing a 38 % reduction on the previous year. This decline was influenced by new instructions issued to institutions to submit aggregated reports in cases involving money mules and fraud involving the same modus operandi.
Nature of the customer	
This is determined by the nature of the business relationship with customers, based on the duration (ongoing, transactional or occasional) and frequency of transactions.	Generally speaking, an ongoing relationship with customers predominates, characterised by stable and sustained interaction over time across the entire sector. Despite this, there is a certain percentage of occasional transactions. The institutions reported that as of 31 December 2024 (i) 12 % of customers had not carried out any transactions in the past year (88 % of whom had been with the institution for more than one year) and (ii) 20 % of accounts had not been active in the past year (82 % of which had been open for more than one year).
Level derived from the client's status (natural person v. legal entity, national v. foreign, high-net-worth clients, PEP, amongst others).	The presence of complex corporate clients, non-residents, private banking clients and PEPs significantly increases the sector's inherent vulnerability. According to the structured information questionnaire, as at 31 December 2024 - 89 % were individuals, of whom 0.08 % were PEPs - 89% Spanish nationals, 5% EEA nationals, 7% other nationalities - 98% resident in Spain - 0.5% private banking clients With regard to the potential use of complex corporate structures, the institutions reported that, as at 31 December 2024, they knew the beneficial owner of 91 % of corporate clients (74 % in the case of institutions in the 'financing' sector, which accounts for 5 % of the sector's corporate in the sector).

[52] Source: 2024 Annual Report (SEBPLAC)

	In conclusion, based on the sectoral classification of institutions, the subsectors with the highest risk are those classified as private banking and other specialised institutions, whilst those with substantial risk include significant institutions, commercial banks, and institutions classified as 'financing' due to the nature of their activities.
Level derived from the client's occupation or type of business.	The level of financial inclusion in Spain stands at 98 %. 92 % of the population live in municipalities with two or more bank branches, and less than 3 % live in areas without physical access to a bank branch. However, it should be borne in mind that this 3 % usually have access to financial inclusion measures such as: the deployment of mobile bank branches, agreements between financial institutions and the Post Office to facilitate basic banking transactions, or the installation of cash machines. Furthermore, the labour force stands at 51.1%[53],with 13.7% of this population being self-employed and the unemployment rate at 9.9%. The diversity of occupations within the labour force makes it impossible to assess risk in generalised terms. The risks that can be identified are those associated with customers at the highest and lowest ends of the income scale. The former, due to possible links with tax havens to avoid taxation, and the latter because they are more economically vulnerable, more likely to deal in cash, and more susceptible to being used as intermediaries by criminal organisations.
Geographical scope of the sector's activities	
A level of risk derived from specific countries of interest frequently linked to the sector.	The sector operates primarily with neighbouring countries, but there are interactions with countries of greater ML/TF sensitivity that cannot be ignored, as well as customers with cross-border operations, which raises the risk from low levels to an intermediate level. Spain's geographical and cultural/historical profile presents specific characteristics and involves flows of funds to higher-risk regions such as North Africa or Latin America.
Level derived from the nature of interactions or transactions involving countries identified by the FATF.	2.2 % of international transfers sent or received in 2024 were destined for or originated from countries included on the FATF lists during 2024 (111 billion euros). 99.97 % of these transfers involved a country on the grey list, although it is not possible to determine whether the country was on the list at the time of the transfer.
Level derived from the nature of the interactions or transactions involving countries subject to financial sanctions [54]	The FP Sectoral Risk Analysis determined that the inherent risk for credit institutions was Substantial/Medium, due to the threats identified regarding the opening of bank accounts such as clearing accounts, particularly those linked to Iranian activities. With regard to North Korea, there is no evidence of direct transactions, although there are transactions with countries allied to the regime.

[53] Source: INE

[54] This factor was rated as medium-substantial.

Nature of distribution channels	
A rating derived from the complexity of the channels, given their impact on anonymity or the limited information available on customers.	Some products allow for greater structural complexity (investment instruments, trust arrangements, foreign trade). Although regulations reduce anonymity, the risk remains significant. 71 % of the institutions' customers were acquired through branches, 13 % through remote channels (internet and telephone banking) and the remaining 16 % through third parties or other means. However, customer acquisition channels have undergone a significant change in recent years. Looking at the figures for customers acquired in the last year, 33 % of the institutions' customers were acquired through branches, 23 % via remote channels (online and telephone banking) and the remaining 44 % through third parties or other means.
A level resulting from the use of new technologies or payment methods.	Digitalisation, instant payments and new *Fintech* solutions speed up the movement of funds and may increase the risks of identity theft and rapid transactions. The presence of non-financial intermediaries interacting with the sector increases the inherent risk, as the customer's business relationship with the credit institution is, in these cases, partially mediated by these third parties, which reduces direct visibility of the end customer and makes it difficult to verify identity and trace transactions. By 2024, 63 % of customer transactions were carried out via remote channels.

Conclusion on the sector's inherent risk: Substantial-high for ML and substantial for TF

178. The credit institutions sector presents a **high-substantial** inherent risk to the ML and **a substantial** TF risk due to its central role in the financial system, its diverse range of products and the breadth of its customer base. The individual assessment of the risk level for each factor ranges from substantial to high, depending on the factor analysed. From the perspective of size and structure, the sector handles a very high volume of transactions and maintains complex corporate structures, particularly within large banking groups with an international presence. This increases exposure to risks arising both from cross-border activity and from interaction with other regulated sectors, such as investment firms, insurers and payment service providers. By contrast, savings banks and credit unions have more limited structures and a narrower geographical focus, which partially mitigates this vulnerability, though without eliminating it.

179. With regard to the nature of products and services, the sector offers everything from simple retail products to sophisticated solutions in corporate banking, private banking, foreign trade and investment. The complexity associated with certain products can lead to a lack of transparency and facilitate more elaborate forms of money laundering, particularly where there is the possibility of relative anonymity, complicated corporate structures or international transfers involving high-risk jurisdictions. The sector is also one of the main sources of suspicious transaction reports, reflecting both its cross-cutting exposure and its detection capabilities.

180. Analysis of the customer base reveals considerable diversity: ranging from low-risk retail customers to multinational corporations, non-resident customers, PEPs and high-net-worth individuals. This broad profile increases the inherent risk, particularly due to the presence of economic activities classified as high-risk and due to interaction – albeit residual – with clients located in or linked to countries with higher levels of exposure to money laundering or subject to international sanctions.

181. In terms of geographical scope, banks conduct operations and maintain correspondent banking relationships in multiple jurisdictions, some of which – albeit to a limited extent – have been flagged by the FATF, are subject to sanctions, or have deficiencies in their AML/CFT systems. This represents a high level of risk in relation to international transactions, foreign trade and cross-border payments. Although savings banks and cooperatives operate mainly at a local level, they are not exempt from risks arising from external customers or transactions.

182. Distribution channels also contribute to vulnerability: the combination of branches, digital banking, mobile apps and new payment methods results in a broad operational footprint. Digitalisation and the immediacy of payments increase exposure to risks such as identity theft or the rapid dispersal of funds, even when institutions have sophisticated risk mitigation systems in place.

183. In summary, the credit institutions sector presents a set of inherent risks which, due to their volume, complexity and international scope, place it amongst the sectors most exposed to ML and TF.

184. Among the threats identified, economic crimes are particularly noteworthy, especially fraud and 'mule' accounts used as a mechanism for moving illicit funds.

185. When categorising the registered credit institutions by sector, according to the sectoral risk analysis carried out by SEPBLAC, the inherent risk would be as follows:

SUBSECTOR	RISK BY CHARACTERISTICS	RISK BY PRODUCT	RISK BY CUSTOMERS	GEOGRAPHICAL RISK	RISK BY DISTRIBUTION CHANNELS	INHERENT RISK ML	INHERENT RISK TF
Commercial banking	High	High	Substantial	Medium	Substantial	**Substantial/ High**	**Substantial/ High**
Private banking	High	High	High	High	Substantial	**High**	**Low**
Significant entities	High	High	Substantial	High	Substantial	**Substantial/ High**	**Substantial/ High**
Funding	High	Medium	Substantial	Medium	Substantial	**Substantial**	**Medium**
Other specialised	High	Medium	High	High	Substantial	**Substantial**	**Medium**
Total sector	**High**	**Substantial**	**High/Substantial**	**Substantial**	**Substantial**	**Substantial/ High**	**Substantial**

Risk factors relating to the effective implementation (or lack thereof) of controls

186. An analysis of residual risk requires an assessment of how existing controls are implemented within the sector and to what extent those controls are effective. The following section presents an analysis of the factors used to determine the residual risk of credit institutions.

Risk factors relating to the effective implementation (or lack thereof) of controls	
Level of regulation in the sector.	The credit institutions sector is subject to strict regulation and close supervision by the Banco de España and/or the ECB.
Extent to which unauthorised institutions may be operating operate.	The carrying out of activities reserved for credit institutions by unauthorised persons ('unauthorised practice') is subject to continuous monitoring by the Banco de España. The penalties imposed by the Banco de España for unauthorised practice during the period 2020–2025 amounted to €2.6 million.
Extent of any direct or indirect control over the institution or its management by money laundering networks.	The acquisition of significant shareholdings in a credit institution is always subject to an administrative authorisation process by the Banco de España, during which the suitability and good repute of the acquirers are assessed. As part of the authorisation process, SEBPLAC issues a report on matters relating to AML/CFT.
Level of regulation of anti-ML and TF (AML/TF).	Credit institutions have been subject to AML/CFT regulations since 1993. The regulations set out specific provisions relating to many specific aspects of their activities.
Level of supervision.	The credit institutions sector – and in particular significant institutions and the largest non-significant institutions – has been subject to intensive scrutiny over recent years due to its central role in preventing ML crises. To date, with more than 90 institutions having been reviewed over the last five years by SEBPLAC and Banco de España, the institutions most relevant in terms of risk or size have been reasonably thoroughly analysed. Within the framework of the Single Supervisory Mechanism (SSM) – a system comprising the ECB and the national supervisory authorities of the participating countries – the ECB directly supervises significant institutions (10 consolidated groups as at 1 January 2026), whilst the less significant institutions (73 institutions as at 1 January 2026) are supervised directly by the Banco de España under the oversight of the ECB.
Level of sanctions imposed on institutions in the sector.	For several years now, a significant number of sanctions have been imposed on credit institutions, which has led to a generally high level of compliance. Between 2020 and 2025[55], sanctions were imposed on 31 credit institutions (12 significant institutions, 12 commercial banks, 5 private banks, 1 specialised in financing and 1 classified as 'other specialised institutions'), involving 98 infringements, of which 93 were serious and 5 very serious.
Level of the professionalism of Managers and Executives of the institution.	It is currently considered that all directors and senior managers of credit institutions are fully aware of the importance of correctly implementing AML/CFT measures, and there are specific training and refresher programmes for them in the most significant. Furthermore, authorisation for the registration and provision of activities requires verification of the

[55] Year in which the sanction was imposed

	new institution's solvency, the suitability and professionalism of its shareholders and directors, and the existence of an adequate administrative and control structure. Once authorisation has been obtained and once incorporated, the institution must be entered in the Register of Institutions and its senior officers in the Banco de España's Register of Senior Officers.
Level of awareness and understanding of its obligations regarding anti-ML and counter-terrorist financing (AML/CTF).	Inspections have confirmed that credit institutions always communicate their prevention procedures to their staff.
The institution's level of commitment to policies and measures for ML/TF prevention policies and measures.	In general, credit institutions demonstrate a high level of commitment to implementing AML/CFT measures.
Level of professional qualifications of staff and their training in ML and TF.	The inspections carried out have confirmed that credit institutions provide training to their staff to a generally satisfactory standard and comply with the relevant regulatory requirements. There have been no penalties for non-compliance with the obligation to provide staff training during the 2020–2025 period for credit institutions. A total of 86 inspections were carried out during this period, and no credit institution was penalised on this ground.
Level of internal monitoring by institutions of their employees' compliance.	The inspections carried out have confirmed that, in general, institutions monitor their employees' compliance with their AML/CFT obligations. However, in some cases, it is considered that internal audit work should be strengthened.
Level of compliance with preventive measures, particularly DDC/KYC	With regard to formal identification, the overall level of compliance is very high. In the case of ongoing monitoring of business relationships, differences are apparent between institutions, such that in some cases compliance is very good, whilst in others – albeit fewer in number – there are significant shortcomings. During the inspections carried out at credit institutions in the period 2020–2025, 44 breaches were detected due to breaches of due diligence obligations.
Level of identification and reporting of suspicious transaction reports (STRs).	The credit institutions sector is by far the one that has consistently submitted the highest number of suspicious activity reports to SEBPLAC. For example, of the total of 21,667 suspicious activity reports received by SEBPLAC in 2025, more than 55 % came from credit institutions (12,105 reports). The average rating for the significance of reports based on evidence for the period 2022–2025 was 5.75. This category, introduced in 2021, enables the relative importance of reports to be assessed on the basis of their link to factors such as their connection to serious crimes, the emergence of new types of risk, the detection of criminal structures or criminal networks and/or the involvement of large sums of money.

Conclusion on the sector's residual risk: substantial for ML and medium/substantial for TF

187. The generally sound implementation of preventive measures and the strict supervision of their activities by the regulator mean that the residual risk is considered to be **substantial** for ML and **medium/substantial** for TF.

188. However, taking these measures into account for each credit institution classification, the residual risk would be determined as:

SUBSECTOR	RESIDUAL RISK ML	RESIDUAL RISK TF
Commercial banking	Medium/Substantial	Medium/Substantial
Private banking	Substantial/High	Low
Significant institutions	Substantial	Substantial
Funding	Medium	Low
Other specialist	Medium	Low/Medium
Total sector	Substantial	Medium/Substantial

Sector: Insurance and pension funds 2026

Activity and context

189. Insurance companies and insurance brokers operating in the life insurance sector, as well as pension fund management companies, are obliged entities under Article 2.1(b) and (e) of Law 10/2010 of 28 April.

190. The insurance sector's vital role in the economy justifies a high level of regulation and public intervention aimed at protecting policyholders, insured persons, beneficiaries and third parties who may suffer loss under private insurance contracts, which involve the exchange of a present and certain payment – the premium – for a future and uncertain payment – the indemnity.

191. Insurance business may be carried out by entities organised as public limited companies, mutual societies, cooperatives and social welfare mutuals; however, it is important to note that around 60 % of the sector's volume is accounted for by entities that form part of a banking group.

192. In Spain, the authority responsible for the registration and supervision of entities belonging to the insurance sector, in general, is the Directorate-General for Insurance and Pension Funds (hereinafter the DGSFP), which reports to the Ministry of Economy, Trade and Enterprise; this is without prejudice to the fact that brokers whose scope of activity is limited to a single autonomous community may be registered with the relevant regional register, with this information reflected in the Single Information Point. In order to commence operations, insurance entities require a mandatory report from SEPBLAC. Insurance companies and insurance brokers, when acting in relation to life insurance or other investment-related services, and pension fund management companies are obliged entities in the field of ML/TF prevention pursuant to Law 10/2010 of 28 April.

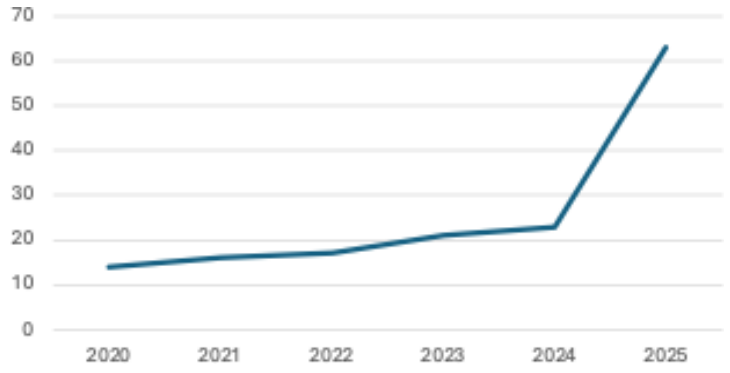
193. As of 31 December 2024, there were 172 entities listed in the Administrative Register of Insurance Companies, of which 79 operate in the life insurance sector. The number of brokers registered with the DGSFP as of 31 December 2024 stood at 3,689, of whom 1,799 have declared that they manage their clients' funds; of these, 1,650 have declared that they have brokered life insurance premiums totalling 1,498 million euros. With regard to the 386 tied intermediaries (348 tied agents and 38 bancassurance operators) registered with the DGSFP as at 31 December 2024, the information provided by 319 tied intermediaries required to submit an annual declaration shows that they handle €44,949 million in brokered premiums, of which 265 have brokered life insurance premiums worth 33,273 million euros. Most of the insurance companies in the sector are members of the Spanish Union of Insurance and Reinsurance Companies (UNESPA), which accounts for 96 % of the business. According to statistics from the DGSFP, gross premiums written at the end of 2024 stood at 75,109 million euros, of which 28,832 million corresponded to the life insurance sector.

194. With regard to pension fund managers, of the 53 active managers, only 31 are stand-alone managers, accounting for 536 million euros; the remainder (22 life insurance companies authorised to act as fund managers) are included in the balance sheet of their respective insurance company.

Threats

195. The threats would stem mainly from the areas of economic crime and tax evasion; no terrorist threats linked to these activities have been detected.

196. The following chart on reports based on suspicious activity shows an upward trend in such reports from the insurance sector over the period analysed. Between 2020 and 2024, a gradual and sustained increase can be observed, rising from 14 to 23 reports during that period, suggesting a progressive improvement in detection systems and in the sector's awareness of AML/CFT matters. In 2025, there is a very significant increase, reaching around 63 reports, due to a progressive improvement in detection systems and in the sector's awareness of AML/CFT.



Source: SEPBLAC

197. The indications detected in the communications received were mainly related to generic ML activities; in 2024 and 2025, this category of offence accounted for 50 % of the reports received. ML requires a high level of knowledge of the sector and of related products that could facilitate anonymity, such as unit-linked insurance policies. As regards terrorist financing (TF), the scenario is less likely, and the knowledge and planning required to exploit the sector for such purposes, as well as the lack of immediate availability, make its use for terrorist purposes largely unfeasible, although a few isolated operations have been detected.

198. Nevertheless, there are certain risk factors that must be taken into account when analysing the sector in question. The most common classification divides these into three types of risk (those associated with policyholders, those associated with premiums and those associated with employees), with single-premium life insurance and unit-linked policies being identified as the main products posing a risk; these risks can be mitigated by the due diligence measures applied within the sector.

Emerging threats	Taking out 100% digital insurance policies without a physical presence facilitates identity theft.
	The use of complex corporate structures to conceal the policy's beneficial owner.
	The evolution of the insurance sector in Spain in relation to Insurtech since 2016. According to NTT DATA's latest Insurtech Global Outlook 2025 report, the insurance sector is no longer talking solely about disruption, but about systemic transformation. Three major drivers explain this: i) hyper-personalisation (HYPER-X), ii) the integration

	of insurance into 'always-on' ecosystems (INSUREVERSE) and the technological revolution based on AI and advanced analytics (AI-SSURANCE).
	Hyper-personalisation and the intensive use of data can hinder traceability and encourage opaque segmentation if not balanced by robust data governance; the integration of insurance into 'always-on' digital ecosystems blurs the boundaries between insurers, technology providers and other service providers, creating risks associated with outsourcing and dependence on platforms that are not uniformly supervised; and whilst AI and advanced analytics enhance the detection of suspicious patterns, they also introduce risks of bias, models that are difficult to explain, and automated processes that may be exploited by sophisticated criminal organisations.

Risk factors due to inherent vulnerability

199. The following sets out the factors relating to inherent vulnerability analysed to determine the inherent risk in the insurance and pension funds sector:

Sector Characteristics	
Size of the sector and turnover.	Although the sector's turnover figures are not negligible, they do not, in themselves, make it a particularly attractive sector for concealing ML/TF operations compared with other entities in the financial sector.
Level of complexity of the sector's structure[56]	The main complexity arises with *unit-linked* products, as they allow for large contributions and early redemptions. Complex changes in ownership can make it difficult to identify the ultimate beneficiary.
Level of integration with other regulated[57]	Around 60 % of the sector's volume relates to the activities of institutions that are part of a banking group.
Level of concentration of the entity, including the geographical scope of the sector's operations[58].	The specific elements of geographical risk in the sector (cross-border policies or the application of banking secrecy to insurance policies) do not apply in our jurisdiction. However, the cross-border purchase of *'unit-linked'* products linked to life insurance policies must be subject to special monitoring.
Nature of the products and services provided by the sector	
Level derived from the complexity of the products, due to their impact on anonymity or on the reduced information about customers.	The greatest exposure lies in insurance contracts (both single-premium and regular-premium), with a high financial component and a low insurance component, in which the agreement essentially provides for the repayment of capital and interest. In cases where the capital is paid in advance by the policyholder, the risk is moderate.

[56] This inherent vulnerability factor is rated as low/medium.
[57] This inherent vulnerability factor is rated as low/medium.
[58] This inherent vulnerability factor is rated as low/medium.

The extent to which the specific products and services offered are linked in advertising and/or national ML or TF investigations[59].	The number of tip-off communications and/or national ML or TF investigations is low.
Nature of the customer	
Level derived from the nature of the business relationship with customers, based on duration (ongoing, transactional or occasional) and frequency of transactions[60].	The parties to insurance contracts, whatever their status or role, must be fully identified by means of the authentic documents specified for each case. Given the nature of the product being sold, the relationship is generally ongoing. However, there may be changes to the designation of the beneficiary that are not duly identified until the benefit is paid out.
Level derived from the client's status (natural person v. legal person , domestic v. foreign, high-net-worth clients, PEP, amongst others)	The majority of the portfolio consists of natural persons, who are nationals and whose financial and operational profiles are consistent with the products taken out, which reduces the complexity and opacity of business relationships. Whilst there are clients who are classified as PEPs, they represent a limited percentage and are subject to enhanced due diligence measures; no evidence has been detected of the use of insurance products for ML or TF purposes. Furthermore, the limited presence of complex legal entities, high-risk foreign clients or sophisticated asset structures significantly limits the inherent exposure associated with this factor, enabling effective risk through existing controls.
Level derived from the client's occupation or type of business.	There is no significant presence of complex, cash-intensive or difficult-to-verify economic activities, and the declared professional profiles are diverse and consistent with the products taken out.
Geographical scope of the sector's activities	
Level derived from specific jurisdictions/countries of interest frequently associated with the sector.	The specific elements of geographical risk in the sector (cross-border policies or the application of banking secrecy to insurance policies) do not arise in Spain. However, the taking out of cross-border *'unit-linked'* products linked to life insurance policies must be subject to particular monitoring.
Level derived from the nature of the interactions or transactions involving countries identified by the FATF.	In the insurance sector, transactions involving countries identified by the FATF are rare.

(59) The rating for this inherent vulnerability factor is low/medium.
(60) The rating for this inherent vulnerability factor is low/medium.

Level derived from the nature of the interactions or transactions involving the countries subject to international financial sanctions.	There is no evidence of transactions with countries subject to international financial sanctions.
Nature of distribution channels	
A measure derived from the complexity of the channels, based on their impact on anonymity or on the reduced information on customers.	Contracts concluded through agents and/or brokers may pose a risk if they lack adequate training in AML/CFT matters. The channels used for the mobilisation of funds are conducted in fiat currency and via credit institutions through transfers.
Level derived from the use of new technologies or payment methods[61].	The risk arising from taking out a product such as insurance or pension funds via electronic means is low, although, as can be seen from the DGSFP data, the uptake via electronic means is limited, but on an upward trend.

Conclusion on the sector's inherent risk: Low/medium for ML and TF

200. The insurance and pension funds and schemes sectors generally have low inherent risks, although these may be moderate in relation to certain specific products, particularly single-premium life insurance policies and international unit-linked investments; consequently, the conclusion is that the inherent risk level is low to medium.

Risk factors arising from the effective (or lack of) implementation of controls

201. To analyse residual risk, it is necessary to assess the implementation of existing controls within the sector and the extent to which these controls are effective. The following section presents an analysis of the factors used to determine residual risk in the insurance and pension funds sector.

Risk factors relating to the effective implementation (or lack thereof) of controls	
Level of regulation in the sector.	The sector is subject to comprehensive and detailed regulation, which stipulates that it is subject to prudential supervision by the DGSFP and requires prior administrative authorisation to operate.
Level of possible existence of Entities not Authorised to operate.	Entities in the sector are subject to a strict authorisation regime. In this regard, controls are in place to prevent unauthorised entities or individuals from operating in the sector.
Level of potential control, whether direct or	In the insurance sector, the use of companies with a is rare. Law 20/2015 of 14 July on the regulation, on the Supervision and Solvency of Insurance

[61] The rating for this inherent vulnerability factor is low/medium.

indirect, of the entity or its management by money-laundering networks.	and Reinsurance Undertakings stipulates, as a requirement for authorisation and the conduct of insurance business, that those exercising effective management or forming part of the board of directors must meet criteria of commercial and professional integrity, as well as competence (in particular, Articles 22 and 38). Royal Decree 1060/2015 implements Law 20/2015 of 14 July and specifies the content and scope of the assessment of good repute and competence.
Level of regulation of anti-money laundering and counter-terrorist financing (ML/TF).	Entities in the sector are obliged to comply with ML and TF (AML/CTF) requirements under Law 10/2010 of 28 April.
Level of supervision.	The sector has for several years been subject to inspections and/or requirements regarding the prevention of ML/TF by the DGSFP (whose supervisory activity is increasing), SEPBLAC and the COPBLAC. The DGSFP draws up an annual risk matrix relating to AML/CFT. This matrix includes and assesses the main indicators affecting life insurers in relation to AML (size, materiality, turnover, type of products and clientele, alerts generated). The data included in this matrix provides relevant information for the purposes of drawing up the annual inspection plan for life insurers. The insurance sector has been encouraged not to apply merely formal compliance models, but rather to allocate resources according to actual risk: to step up due diligence measures and prioritise the monitoring of certain transactions (*unit-linked products*, savings-linked life insurance, high-value contributions, surrenders, PEP clients, and high-risk intermediaries). During the period analysed (2020–2025), 24 inspections were carried out on insurers and 3 on insurance brokers.
Level of sanctions imposed on entities in the sector.	During the period analysed, 11 sanctions were imposed on entities in the sector, all of which were classified as serious. Given the sector's materiality, the risk is low. In addition, 12 entities were required to rectify deficiencies, which led to the implementation of remediation plans covering 35 AML/CFT procedures.
Level of the Professionalism of the organisation's administrators and managers.	The directors and senior managers of insurance undertakings have received appropriate training. Law 20/2015 of 14 July on the regulation, supervision and solvency of insurance and reinsurance undertakings, stipulates, as a requirement for authorisation and the conduct of insurance business, that those exercising effective management or forming part of the board of directors must meet criteria of commercial and professional integrity, as well as competence (in particular, Articles 22 and 38). Royal Decree 1060/2015 of 20 November, which implements Law 20/2015 of 14 July, specifies the content and scope of the assessment of good repute and fitness and propriety.
Level of awareness and understanding of their obligations for the prevention of ML and TF.	There are legal obligations regarding the existence and dissemination of manuals setting out internal policies and procedures. Inspections by the supervisory bodies have confirmed that the dissemination activities and the level of awareness amongst the entities' staff regarding ML/TF prevention are, in general, adequate.

Level of the institution's commitment to ML/TF prevention policies and measures.	In general, insurance companies are committed to complying with ML and TF measures. Authorisation to provide services requires, in addition to the DGSFP's assessment of the established requirements, the issuance of a preliminary report by SEPBLAC regarding the suitability of the ML/TF bodies and procedures that the entity being incorporated intends to implement.
Level of professional qualifications of staff and their training in ML/TF prevention[62]	Generally speaking, and particularly in recent years, the professional qualifications of employees in the sector regarding prevention have improved significantly. However, the scale of the sales network and the large number of employees who require specific qualifications due to their responsibilities in the area of prevention are areas for improvement that affect the level of risk of the network being used for ML and TF purposes. The scale of the distribution networks remains a challenge for the on-site implementation of preventative measures.
Level of internal monitoring by organisations of staff compliance.	Inspections and requests reveal that institutions have control mechanisms in place to verify employees' compliance with their obligations.
Level of compliance with obligations regarding preventive measures, particularly CDD/KYC[63].	Institutions have put in place measures to block new business if a customer fails to comply with CDD/KYC measures. During the period analysed, five sanctions were imposed for non-compliance with due diligence measures.
Level of identification and reporting of suspicious transaction reports (STRs)	During the period analysed, there has been an increase in the number of suspicious transaction reports (STRs) from the sector, suggesting a gradual improvement in detection systems and in the sector's awareness of AML/CFT. The number of STRs in the sector is not high, owing to the sector's limited exposure to AML/CFT operations. The average rating for the significance of suspicious activity reports for the period 2022–2025 was 6.12. This category, introduced in 2021, enables the relative importance of reports to be assessed based on their link to factors such as the connection to serious crimes, the emergence of new types of risk, the detection of criminal structures or networks, and/or the existence of large sums of money.

Conclusion on residual risk in the sector: Low for ML and TF

202. The main risk lies in the activities of employees and intermediaries. Although there are legal obligations in this regard, and there is constant monitoring within the sector of the actions of employees and intermediaries. The residual risk is characterised by the existence of robust regulation, accompanied by the corresponding control and supervision, both in the prudential sphere and in the area of ML/TF. Furthermore, the sector has a high level of awareness of both its obligations regarding prevention and potential high-risk transactions, through, amongst other things, the documents issued by the regulator.

[62] This inherent vulnerability factor is rated as low/medium.
[63] This inherent vulnerability factor is rated as low/medium.

Sector: Securities 2026

Activity and context

203. Investment services firms, management companies of collective investment undertakings, venture capital fund management companies and venture capital firms are regulated entities under Article 2.1(c), (d) and (f) of Law 10/2010 of 28 April.

204. Investment services are provided by Investment Services Firms (ISFs), by credit institutions (the latter being by far the main providers of investment services) and, to a lesser extent, by SGIICs.

205. Within the category of Investment Services Firms (ISFs), a distinction is made between Securities Firms (SVs) and Securities Agencies (AVs), or Securities Firms and Agencies (SAVs) considered collectively (which are equivalent to *dealers* and *brokers* in financial terminology), on the one hand, and financial advisory firms (FAFs), on the other.

Number of entities	2020	2021	2022	2023	2024
Securities Firms and Agencies	96	91	95	99	99
Financial Advisory Firms	134	138	140	139	131
Investment Services Firms	230	229	235	238	230
Credit institutions (including EU branches)	135	136	136	133	133

206. The figures relating to investment services – in terms of assets under management, the number of clients to whom investment services are provided, revenue from the provision of investment services, and assets held in custody (belonging to clients) – indicate that credit institutions account for more than 90 % of these variables in relation to investment services activity.

207. Collective investment is organised through open-ended and closed-ended vehicles, which may take the form of funds or companies. Among the open-ended vehicles, investment funds predominate, whilst the closed-ended ones include Venture Capital Funds (VCF), Venture Capital Companies (VCC) and Closed-End Collective Investment Institutions (CECII), as well as certain specialised European vehicles. Management is primarily carried out by SGIICs (for both open-ended and closed-ended vehicles) and SGEICs (for closed-ended vehicles). Some companies may be self-managed, although these are few and far between. Marketing is carried out mainly by credit institutions and, to a lesser extent, by investment services firms.

208. As regards collective investment undertakings, SGIICs manage 98 % of the assets held by clients of these collective investment undertakings. Collective investment undertakings account for 483 billion euros, compared with 47 billion euros for private equity vehicles.

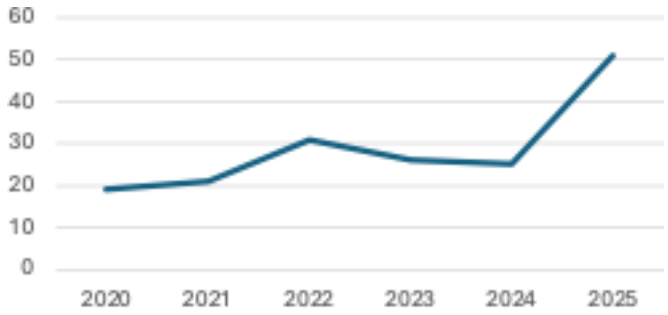
Number of entities	2020	2021	2022	2023	2024
SGIIC. Number of UCITS Management Companies	123	123	123	117	119

SGEIC. Number of closed-end fund management companies	119	122	135	150	158
Self-managed companies	44	45	47	51	51

209. ESI and collective investment undertakings require prior authorisation and registration by the CNMV, the authority responsible for their prudential supervision. The granting of such authorisation also requires a mandatory report from SEPBLAC on the suitability of the Money Laundering bodies and procedures established by the undertaking.

Threats

210. The sector has limited data regarding investment services and investment management activities. Since 2020, the figures reported by the sector are shown in the following chart:



Source: SEPBLAC

211. Of these reports, 53 % related to general money laundering offences, followed by fraud-related offences (20 % of the reports) and tax fraud (17 % of the reports received).

212. Between 2020 and 2025, 30 reports based on indications were recorded in which the securities sector was implicated; the majority of these were submitted by credit institutions, registrars and payment institutions. Although the number of reports based on indications submitted by the sector is low, this does not reflect the sector's true exposure, due to its extensive interconnection with other financial intermediaries (mainly banks), which channel a large part of the final transactions or detect signs linked to investments managed outside their direct scope.

213. The associated offences correspond to those typically detected in reports issued directly by the investment services and collective investment sector. Notably, two indicators relating to possible cases of corruption were identified, highlighting the potential use of the securities market as a channel for concealing or circulating funds of illicit origin.

214. The factors underpinning these threats are the technical complexity of the products, the global interconnection of capital markets, and the presence of sophisticated corporate structures

and operational reliance on credit institutions for the marketing, custody, deposit and execution of transactions.

215. These characteristics coincide with numerous threats identified in Chapter 4: economic and financial crimes, investment fraud, the use of opaque structures, international flows and corruption.

Economic crime, financial fraud and investment manipulation

216. At national level, the growth of complex economic crimes stands out as a priority threat, including investment fraud, market abuse, the use of shell companies, mass scams and Ponzi schemes. The securities sector is particularly exposed to:

    - The marketing of complex financial products (*hedge funds*, structured products, *unit-linked products*, exotic derivatives).
    - The use of omnibus accounts that obscure the identity of the end investor.
    - The delegation of functions (management, custody, administration) which hinders traceability.
    - Operations involving international funds with cross-shareholdings.
    - Capital flows between interconnected vehicles, which may conceal accounting or tax fraud.

217. Industry data show that 53 % of reports based on indications relate to general ML offences and 20 % to fraud.

Organised financial crime and the use of investment vehicles as money-laundering structures

218. Criminal groups with an economic profile use investment funds, venture capital firms, EICCs and alternative investment structures as mechanisms for layering and converting illicit funds, exploiting:

    - the multi-tiered capital structure of these vehicles,
    - the international diversion of assets,
    - the high volume of subscription and redemption transactions,
    - the involvement of multiple intermediaries.

Corruption and concealment of assets

219. Through investment structures that may be based in the securities sector via closed-end funds or VCCs, where it is possible to conceal the origin of illicit gains through contributions that are not sufficiently traceable; international investment structures that mix lawful and illicit capital; and fund holdings acquired through shell companies that make it difficult to identify the beneficial owner.

220. The sectoral analysis specifically highlights the emergence of indicators associated with corruption, demonstrating the potential use of the securities market as a channel for the circulation of illicit funds under the guise of investment.

Tax fraud, aggressive tax planning and the use of collective investment schemes for opaque restructuring

221. Collective investment vehicles, particularly closed-ended funds, enable funds to be moved between different jurisdictions, which can be used to: i) obscure the origin of assets, ii) justify illicit increases in wealth, and iii) fragment tax evasion schemes. This risk is reflected in the indications of tax fraud detected (17% of STRs).

Terrorist Financing

222. The threat of TF was assessed as low due to the asset-based nature of the products, the need to tie up funds for prolonged periods, and the limited practical utility of financial investments for the logistical operations of terrorism. However, certain patterns of TF detected in the NRA (micropayments, triangulation, use of front organisations) could, in specific scenarios, be exploited:

- closed-end funds with little trading activity,
- holdings via special purpose vehicles,
- investments channelled from third countries.

223. Although exposure is limited, this is considered a significant threat in complex cross-border vehicles.

224. The factors most likely to be exploited by threats in the securities sector are as follows:

Factors that are frequently exploited by threats	
Cross-border exposure and exposure to high-risk jurisdictions	The securities sector is, by definition, highly internationalised. Both ESI and asset management firms maintain operational relationships with: • European and non-EU markets, • Luxembourg, Irish or *offshore* vehicles, • non-European counterparties, • custodians and administrators located in third countries. Interaction with high-risk jurisdictions is a moderate but structural factor, particularly in complex vehicles and in institutional investments.
Complex products and omnibus accounts to make it difficult to identify the beneficial owner	The inherent opacity of certain products such as: *hedge funds*, structured funds, *unit-linked* products, derivatives with multiple counterparties, omnibus accounts, or closed-end funds with multiple layers of ownership. These instruments may: i) temporarily conceal the identity of the beneficiaries, ii) make it difficult to trace the origin of the assets, or iii) allow funds to flow in from companies acting as intermediaries.
Digitalisation, Fintech and the risk of 'financial fly-by-night operations'	At national level, there has been an exponential growth in: • unregistered online platforms, • cross-border lenders with no physical presence, • fraudulent investment schemes based on *apps* and social media. This factor particularly affects FAFs and small intermediaries.

Risk factors based on inherent vulnerability

225. The following sets out the factors relating to inherent vulnerability analysed to determine the inherent risk in the securities sector:

Sector Characteristics	
Size of the sector and turnover.	The high turnover in the sector and the diversity of operator types, transactions and services make this sector attractive for concealing ML operations.
Level of complexity of the sector's structure[64]	Due to the high diversity of entities and functions, the multiplicity of vehicles with distinct regulatory frameworks, and the delegation and outsourcing of management, administration and marketing activities.
Level of integration with other regulated sectors[65]	In the case of investment services, there is a direct dependence on credit institutions, which act as the main distributors; and, in the case of UCITS, credit institutions act as custodians of the assets. The operation of investment vehicles also requires the involvement of regulated market infrastructures (such as central counterparties and settlement systems) and coordination with other ESIs that execute orders, provide custody services or channel investments.
The entity's geographical level, including the geographical scope of its operations within the sector.	The location of certain branches in high-risk areas – either due to the significant presence of high-risk groups or the nature of the clientele's main business activity – may have a significant impact on the institution's risk rating.
Nature of the products and services provided by the sector	
Level derived from the complexity of the products, due to their impact on anonymity or the reduced amount of information about customers.	Among the products offered by the sector, there is a wide variety of complex products of different types that can be used for illicit purposes; despite the measures in place, these continue to represent a risk exposure factor for ML operations that must be taken into account.
The extent to which specific products and services offered are linked to tip-off communications and/or national ML or TF investigations	Between 2020 and 2025, 30 reports based on indications of suspected wrongdoing involving the securities sector were recorded; the majority of these were submitted by credit institutions, registrars and payment institutions.

[64] The rating for this inherent vulnerability factor is medium/substantial.
[65] The rating for this inherent vulnerability factor is medium/substantial.

Nature of the customer	
Level derived from the nature of the business relationship with customers, based on the duration (ongoing, transactional or occasional) and frequency of transactions.	These relationships are typically ongoing and focused on portfolio management, advisory services and fund investments, which involve frequent trading and large-value transactions. Professional clients or qualified investors tend to diversify across complex products, trade through various intermediaries and make frequent subscriptions and redemptions, which makes it difficult to detect unusual changes in their investment patterns. Retail clients do not fit this description, having a more conservative investment profile and an ongoing business relationship.
Level derived from client status (natural person v. legal entity, national v. foreign, high-net-worth clients, PEP, among others)	Due to the diversity of profiles accessing its services, which includes both natural and legal persons, nationals and non-residents, as well as high-net-worth clients and institutional investors.
Level derived from the client's occupation or type of business.	This depends on the type of client (retail, professional or eligible counterparty), as this will determine their level of sector knowledge and financial capacity for investment.
Geographical scope of the sector's activities	
Level derived from specific countries of interest frequently associated with the sector.	The securities sector primarily operates within Spain, with a very limited presence in other jurisdictions and few non-resident clients. As regards financial products, the marketing of Irish and Luxembourg investment funds to Spanish residents is of some significance; in all cases, these are funds subject to the UCITS Directive, not alternative investment funds.
Level derived from the nature of interactions or transactions involving countries identified by the FATF.	The relationship with other markets and jurisdictions in which the securities investment services provider operates, or to which it is otherwise exposed – whether through its own activities or those of its clients – is a factor that must be taken into account. Given the global interconnectedness of the financial system, interaction with high-risk jurisdictions, offshore centres or intermediaries that do not meet European AML/CFT standards constitutes a risk arising from the transnational nature of operations.
Level derived from the nature of interactions or transactions involving countries subject to financial sanctions International.	Direct links with sanctioned countries are limited or non-existent.
Nature of distribution channels	
Level derived from the complexity of the	In the investment services sector, there is little connection with the use of cash as a distribution channel.

channels due to their impact on anonymity or the reduced amount of information available on clients.	Remote operations in the investment services sector present a level of complexity similar to that of sectors such as credit institutions, particularly given the high proportion of investment services activity channelled through credit institutions. However, this risk is largely mitigated by the regulatory requirements arising from MiFID II, which impose strict obligations on firms regarding know-your-customer (KYC) procedures, suitability and appropriateness assessments, as well as the collection and continuous updating of information on their clients. In practice, this translates into the use of enhanced digital identification procedures, structured questionnaires, investor profiles, traceability of interactions and automated control systems.
Level resulting from the use of new technologies or payment methods.	The use of new technologies and payment methods – largely associated with fintech companies – increases vulnerability to ML insofar as they make it more difficult to ascertain the identity of the investor's beneficial owner and the origin of the funds invested.

Conclusion on the inherent risk of the sector: substantial for ML and low for TF

226. The inherent risk of investment services being used for ML activities is substantial, owing to the very purpose of generating financial returns on the funds invested and to the existence of various vulnerabilities arising from the types of investment products and investment channels, which can help to conceal the origin of the funds and the identity of the beneficial owner.

227. Unlike ML risks, the very nature of this type of service – which is linked to the financial returns on products – makes it more difficult and less attractive to use for TF purposes and reduces the exposure to such use; consequently, the inherent risk is considered to be low.

Risk factors relating to the effective implementation (or lack thereof) of controls

228. Analysing residual risk requires an assessment of the implementation of existing controls within the sector and the extent to which these controls are effective. The following section presents an analysis of the factors used to determine residual risk in the securities sector.

Risk factors relating to the effective implementation (or lack thereof) of controls	
Level of regulation in the sector	The sector is subject to comprehensive and detailed regulation[66].
Level of potential presence of unauthorised entities	Entities in the sector are subject to an authorisation regime, as previously analysed, and the presence of unauthorised entities operating in the sector is of very little significance. However, the use of new technologies

[66] The securities sector is extensively regulated at both national and European level, both from a prudential perspective and in terms of conduct of business rules, through various laws (and implementing regulations). In particular, Law 6/2023 on the Securities Market, Law 35/2003 on Collective Investment Undertakings, and Law 22/2014 on Venture Capital Firms. Among other requirements, participants in this sector must obtain authorisation to operate, are obliged to comply with Money Laundering regulations, and are subject to supervision by the CNMV.

authorised to operate.	and online channels for contracting services provided by these regulated entities have contributed to the rise in 'financial fly-by-night operations'.
Level of potential control, direct or indirect, over the entity or its management by ML networks	Law 6/2023 and Royal Decree 217/2008 establish strict authorisation and supervision requirements for investment firms, including the assessment of the good repute and suitability of shareholders with significant holdings, directors and senior managers, as well as the analysis of direct or indirect control structures that may hinder effective supervision or facilitate the infiltration of ML/TF networks.
Regulatory framework for ML/TF prevention measures	Entities in the sector have been subject to AML/TF obligations for many years under Law 10/2010 of 28 April (Article 2.1(g)). Entities have extensively developed policies, procedures and internal controls (KYC, transaction monitoring, training, supervisory bodies), reflecting a high degree of maturity in the management of these risks.
Level of supervision	The sector is subject to inspections by supervisors in the area of ML/TF prevention. Despite this, the size of the sector, its number of customers, the volume of transactions and deposits, and, above all, the nature of the transactions make this sector vulnerable to money laundering activities. The number of inspections carried out in this sector is limited. However, the proportion of activity carried out by credit institutions must be taken into account. The prudential supervisor has set up a specific ML prevention unit, which is expected to have a positive impact on supervisory activities targeting this sector. Between 2020 and 2025, 64 inspections were carried out in the sector, the majority of which targeted investment firms.
Level of sanctions imposed on entities in the sector.	Since 2020, one investment services firm has been sanctioned following the identification of shortcomings in the training provided and in the external expert's report.
Level of professionalism among the entity's directors and senior management.	There is a high level of professionalism in this sector, underpinned by very strict regulatory measures. However, if these firms were managed by directors or senior managers who were unprofessional or lacked commitment to ML/TF prevention measures, this would render the firms highly vulnerable.
Level of awareness and understanding of their ML/TF obligations.	There are legal obligations in this regard, and inspections by the supervisory bodies have found that, although awareness-raising activities are in place, the level of knowledge amongst employees of these institutions regarding the prevention of ML and TF cannot always be considered satisfactory.
The institution's level of commitment to ML/TF prevention policies and measures.	Knowledge of prevention policies, awareness and commitment, whilst varying considerably within the sector, are high. However, the potential conflict between the commercial division and the AML/TF division is particularly significant in this sector.

Level of professional qualifications of staff and their training in AML and CFT.	Training and, consequently, the qualifications of employees in the sector regarding ML/TF, whilst having increased significantly, cannot be considered fully satisfactory, given the sanction imposed on the aforementioned institution in 2020.
Level of internal monitoring by organisations of employees' compliance employees.	Although there are legal obligations, some supervisory reviews have revealed that the level of monitoring of staff compliance in this area is inadequate, which increases the risk of ML/TF activities.
Level of compliance with obligations regarding preventive measures, particularly CDD/KYC	There are stringent legal requirements regarding know-your-customer (KYC) procedures, which require institutions to apply due diligence measures to a high standard. However, the existence and marketing of complex investment products and funds that make it difficult to identify individuals, the large number of clients in the sector, and the need to implement measures—particularly for clients who were already on the books before the regulatory requirements came into force—all contribute to the existing ML/TF risk. Despite the risks involved in the use of omnibus accounts, as noted in previous sections, it should be pointed out that this is a distribution mechanism in which there is always a final intermediary who identifies the beneficial owner, as provided for in the concept of nominee accounts (*"nominee* account") as set out in recital 131 of Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for ML and TF.
Level of identification and reporting of suspicious transaction reports (STRs)	Since 2020, 173 reports based on evidence have been submitted, with 2025 being the year in which the highest number of reports were received, totalling 51. The average rating for the significance of reports based on indications for the period 2022–2025 was 6.37. This category, introduced in 2021, enables the relative importance of reports to be assessed based on their link to factors such as their connection to serious crimes, the emergence of new types of risk, the detection of criminal structures or criminal networks and/or the involvement of large sums of money.

Conclusion on the sector's residual risk: Medium for ML and low for TF

229. The regulation and supervision of these services, the awareness amongst sector entities regarding the implementation of ML/TF prevention measures, and the mitigation measures outlined to control the activities of such entities serve to reduce the residual ML risk, which should be classified as **medium**, depending on the product and the profile of their customers.

230. The residual risk associated with the use of securities investment services, the financial services provided by managers of collective investment schemes and securitisation fund management companies for TF activities is considered to be **low**.

Sector: Mutual Guarantee Societies 2026

Activity and context

231. Mutual Guarantee Societies (MGSs) are non-profit organisations whose aim is to facilitate and reduce the cost of access to credit for small and medium-sized enterprises by providing guarantees (sureties or other forms of guarantee, other than surety insurance). Article 2.1(g) of Law 10/2010 includes MGSs among the entities subject to the law.

232. Generally, they operate at a regional level and across multiple sectors and are made up of two types of members: participating members, who are the SMEs benefiting from the guarantees offered, and protective members, which are institutions that provide resources to the MGSs. The latter typically include public administrations, chambers of commerce, associations and credit institutions.

233. MGSs are supervised by the Banco de España and are subject to the legal regime governing mutual guarantee societies, including its various amendments and implementing regulations. MGSs are members of the Spanish Confederation of Mutual Guarantee Societies (CESGAR), which is responsible for coordinating, cooperating with, defending and representing the interests of its members, whilst also promoting all kinds of agreements with public or private institutions, both domestic and foreign, and providing advisory and technical assistance services.

234. As of 31 December 2025, the Banco de España's Special Register listed 18 Reciprocal Guarantee Societies, which reported total assets of 2,000 million euros and a turnover of 107 million euros. However, due to the merger by absorption that took place during 2025, the Santander Mutual Guarantee Society (SOGARCA, M.G.S.) was struck off the register on 2 January 2026; consequently, the number of mutual guarantee societies listed in the Banco de España's Register now stands at 17.

Threats

235. MGSs products do not allow for anonymity, do not handle cash, do not operate internationally and require full identification; consequently, the ML/TF threats associated with organised crime, drug trafficking, corruption or terrorist financing have a very limited impact.

236. The most significant threats relate to economic crimes and document fraud, and stem mainly from SMEs or self-employed individuals who may falsify financial information, submit manipulated documentation or use simple corporate structures to obtain guarantees improperly. This is in line with the types of corporate fraud outlined in Chapter 4 (punishable insolvencies, document forgery, instrumental use of companies).

237. In addition, other factors that may be exploited by threats within the MGSs environment include:

Factors that could be further exploited by threats	
Companies with opaque operations or indirect links to higher-risk sectors	Although the appeal to organised crime is very low, there is a residual risk that companies operating in sensitive sectors (cash-intensive trade, construction, transport) may seek guarantees to bolster their creditworthiness or access bank financing for undeclared purposes.
Clients with sensitive profiles (PEPor complex corporate structures)	The level of exposure to this threat can be considered low, but there is a possibility that some applicant companies may include PRPs or structures with high director turnover, which necessitates enhanced controls, although supervision and identification requirements significantly mitigate this threat.

Risk factors due to inherent vulnerability

238. The following section sets out the factors relating to inherent vulnerability analysed to determine the inherent risk of the MGS sector.

Characteristics of the sector	
Level of size of the sector and volume of business	The sector's turnover figures are not significant. In December 2025, the sector was concentrated in 18 MGSs, which reported a balance sheet total of 2,000 million euros and a turnover of 107 million euros.
Level of complexity of the sector's structure	The structure of the sector has been well-established for years and does not present any significant complexity, with no recent substantial changes.
Level of integration with other regulated sectors	The sector is fully integrated with other highly regulated institutions, such as credit institutions; however, given the nature of the sector, its activities do not affect the risk profile of credit institutions.
Level of the organisation's geographical location, including the geographical scope of the sector's operations	Entities in the sector operate exclusively within Spanish territory, with their scope of operations being regional in most cases.
Nature of the products and services provided by the sector	
Level derived from the complexity of the products, due to their impact on anonymity or the limited information on provided to customers.	The products offered by the sector, which consist of guarantees, are straightforward and highly transparent.
The extent to which specific products and services offered are linked in communications by Indication and/or national ML or TF investigations.	The products offered by the sector make it difficult to use them to conceal ML or TF operations.
Nature of the customer	

Level derived from the nature of the business relationship with customers, depending on its duration (ongoing, transactional or occasional) and frequency of transactions	The business relationship with customers in the sector is stable and long-standing.
Level derived from the customer's status	The client base is predominantly made up of Spanish legal entities, mainly SMEs and the self-employed. The majority of these clients operate within the formal economy, are subject to tax and company law supervision, and generally have a clearly identifiable ownership structure, which reduces the risks of a lack of transparency and misuse of the financial system. The limited presence of non-resident clients, high-net-worth individuals or PEPs further mitigates exposure to the AML/CFT risk.
Level derived from the client's occupation or type of business [67]	These activities are usually carried out in traditional economic sectors, with varied business purposes and subject to tax, labour and commercial supervision, which promotes the transparency and traceability of funds. Furthermore, there is no significant presence of activities classified as particularly vulnerable to AML/CFT. However, the sectoral diversity inherent in the SME sector and the possible existence of cash-intensive businesses or those with simple suggests a greater vulnerability.
Geographical scope of the sector's activities	
Level derived specific jurisdictions/countries of interest, frequently associated with the sector.	Entities in the sector operate exclusively within Spanish territory.
Level derived from the nature of the interactions or transactions involving countries identified by the FATF.	Entities in this sector operate exclusively within Spanish territory.
Level derived from the nature of the interactions or transactions involving countries subject to international financial sanctions.	Entities in the sector operate exclusively within Spanish territory.
Nature of the distribution channels	
Level derived from the complexity of the channels due to their impact on anonymity or on	Clients in the sector must provide full identification in order to become participating members. The transfer of funds takes place when, thanks to the guarantee provided by the *MGSs*, a credit institution grants a loan, policy or other financial instrument to the participating member. In this case, the funds are disbursed directly from the financial institution to the

[67] This inherent vulnerability factor is rated as low/medium.

less information about customers.	customer, with the MGSs acting as guarantor of the transaction; therefore, there is no impact on anonymity.
Level derived from the use of new technologies or payment methods.	The sector does not operate using innovative payment methods or high-risk financial technologies, but rather those integrated into the regulated banking system.

Conclusion on the sector's inherent risk: Low for ML and TF

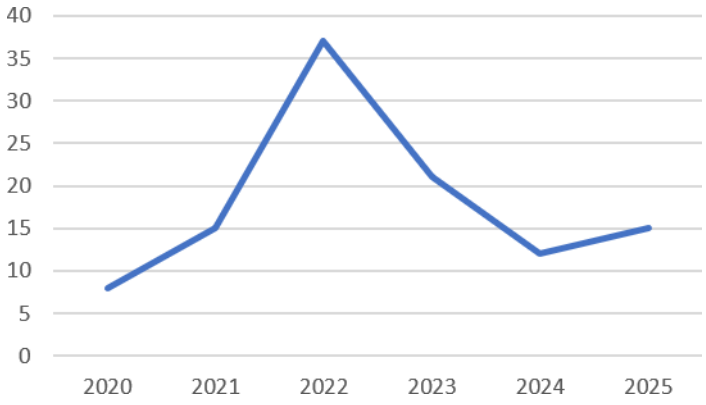
239. Given the nature of the business (the provision of guarantees to SMEs and the self-employed) and the low volume of assets with which the sector operates, the inherent risk is considered low. Whilst lending activity generally involves risks, the internal requirements and controls imposed by MGSs in order to grant guarantees for loans – such as the need to become a member – limit any potential threat's access to funds for ML/TF purposes.

Risk factors relating to the effective implementation (or lack thereof) of controls

240. To analyse residual risk, it is necessary to assess the implementation of existing controls within the sector and the extent to which these controls are effective. The following section presents an analysis of the factors used to determine the residual risk in the sector of other services provided by MGSs.

Risk factors relating to the effective implementation (or lack thereof) of controls	
Level of regulation in the sector	The sector is subject to extensive and detailed regulation.
Extent to which unauthorised non- e entities may be operate.	Entities in the sector are subject to a strict authorisation regime in order to operate as MGSs.
Level of potential direct or indirect control over the entity or its management by or networks involved in money laundering	The sector's structure is entirely transparent, and the regulations require very strict control measures regarding the conditions for operating.
Level regulation of ML and TF measures	Entities in the sector have been subject to ML/TF prevention for many years and also have specific guidelines in place.
Level of supervision[68]	The sector is subject to ML and TF (AML/TF) inspections carried out by SEPBLAC, which cover all institutions. One of the key issues to be addressed is the sale of foreclosed assets following the call on guarantees.
Level of sanctions imposed on institutions in the sector. [69]	No sanctioning proceedings have been brought against the sector, but given the materiality and inherent risk, the risk level assigned to this factor is considered appropriate. Between 2020 and 2025, three inspections of the sector were carried out.

[68] This inherent vulnerability factor is rated as low/medium.
[69] This inherent vulnerability factor is rated as low/medium.

Level of the professionalism of Administrators and senior managers of the organisation.	Regulation of the sector requires very strict controls on the suitability of applicants and their directors and senior managers.
Level of awareness and understanding of their obligations regarding ML/TF prevention.	There are legal obligations for institutions to disseminate information on ML/TF.
The organisation's level of commitment to policies and measures for AML/CFT	Three inspections were carried out during the period under review, and an acceptable level of commitment to AML/CFT measures was observed.
Level of professional qualifications of staff and regarding their training in ML/TF prevention.	There are legal obligations to provide training on ML/TF prevention to employees of financial institutions, and no significant issues were identified during the inspections carried out.
Level of internal monitoring by organisations of employees' compliance.	The quality of the internal control systems and procedures for the prevention of ML and TF has been assessed using self-assessment forms, the external expert's evaluation and information from the Banco de España in its capacity as prudential supervisor; no any significant breaches having been detected.
Level of compliance with obligations regarding preventive measures, in particular with regard to CDD/KYC	The sector's AML/CFT regulations require these due diligence obligations, and no significant breaches were detected during the inspections carried out.
Level of identification and reporting of suspicious transaction reports	The SRGs issued 15 notifications based on indications in 2025 and 14 in 2024, which demonstrates that the control system is functioning properly, highlighting the organisation's ability to identify and analyse potentially suspicious transactions and to diligently fulfil its reporting obligations. This volume of reports is consistent with the organisation's risk profile and does not reflect any failings in the system, but rather an adequate level of vigilance and internal awareness.  Source: SEPBLAC The average rating for the relevance of reports based on evidence for the period 2022–2025 was 5.93. This category, introduced in

	2021, makes it possible to assess the relative importance of reports based on their link to factors such as the connection to serious crimes, the emergence of new types of risk, the detection of criminal structures or networks, and/or the involvement of large sums of money.

Conclusion on the sector's residual risk: Low for ML and TF

241. Given that the sector's regulatory environment is sound, thanks to the high level of regulation and supervision in the area of ML/TF to which it is subject, as well as the transparency and stability that characterise it, the residual ML/TF risk in the sector is considered to be **low**. Nevertheless, risk monitoring is carried out in cases involving partners with complex structures, higher-risk economic sectors or guarantees of a significant value.

Sector: Money Transfers 2026

Activity and context

242. Payment institutions engaged in money remittance activities are obliged entities under Article 2.1(h) of Law 10/2010, of 28 April.

243. Money transfers to or from abroad are provided by payment institutions and are commonly known as remittances. A payment service is considered a 'money transfer' when it takes place without the involvement of any payment account held in the name of the payer or the payee. In this case, the recipients of the funds may receive them directly or via correspondent institutions established at the destination.

244. Payment institutions are subject to authorisation by the Banco de España, following a mandatory report from SEPBLAC regarding the suitability of their governance structures and anti-money laundering procedures. Once authorisation has been obtained, and following registration in the Commercial Register, the payment institution will be entered in the Special Register of Payment Institutions, in which its agents and branches must also be listed. The Banco de España is responsible for the prudential supervision of compliance with and maintenance of the conditions of the authorisation.

245. The sector comprises 51 payment institutions[70] based in Spain, to which must be added 10 EU payment institutions operating in Spain through their own agent networks, such as Western Union and MoneyGram. However, not all payment institutions carry out money transfers. The money transfer business is concentrated amongst 32 remittance operators[71], of which three (RIA, Western Union and MoneyGram) stand out in terms of the concentration of activity. The turnover figures are very significant: in 2025, 37 million transfers were made totalling 9,829 million euros, alongside 3.7 million payments received amounting to 1,029 million; in December alone, 3.36 million transfers and 896 million euros were recorded. Market concentration is high: the three largest remittance providers account for 79 % of remittances and 94 % of payments received; this, combined with the granular nature of the transactions and the extensive network of agents (around 7,200, of whom 6,800 work for two or more entities), constitutes a sector of considerable economic importance and high inherent risk.

246. The sector is represented by the Association of Payment Institutions (AENPA), which has 17 members, 16 of which are payment institutions, and one is a bank; the majority are engaged in money transfers, and among them are those with the highest volume of assets. AENPA maintains a Register of High-Risk Agents (RAAR), the purpose of which is to prevent agents of member institutions who are listed in the RAAR from acting as intermediaries in the provision of money transfer services on behalf of a member institution; there are currently 1,109 agents listed, who are removed from the register after 10 years if they have not been subject to any further entries.

[70] Figures as of 31/12/2025

[71] Figures as of 31 December 2025

Threats

247. The money transfer sector operated by payment institutions is one of the areas most exposed to the threats of ML/TF within the Spanish financial system, due to a combination of structural, operational and geographical factors that facilitate its use by criminal organisations and transnational networks. The activity is based on account-less transactions, with high levels of cash usage, small-value cross-border transfers, occasional customers, inconsistent identification procedures, and a vast network of agents whose supervision presents significant challenges. These characteristics align fully with several risk vectors identified at national level: organised crime, drug trafficking, large-scale fraud, opaque international fund flows, informal economies, and micropayments used for TF.

Organised crime and international money-transfer networks

248. The threats referred to in section 4.1 indicate that organised crime makes extensive use of rapid transfer systems as a means of fragmenting illicit proceeds, laundering funds and transferring them to jurisdictions with less oversight. Organisations involved in drug trafficking, human trafficking, extortion or fraud use the remittance sector to: break down large sums into multiple small transfers ("pitufeo"), use real, borrowed or forged identities; move funds to countries with significant informal economies or low levels of supervision; or rely on actively collaborating agents (up to 80–90 % of investigated cases have involved agents, according to the sector). The direct link to countries considered high-risk, the speed of transactions, the lack of documentary trail, and the high degree of fragmentation make the threat posed by organised crime one of the most significant for this sector.

Drug trafficking and associated criminal economies

249. Remittances are used by networks linked to drug trafficking to: disperse proceeds from local micro-sales; send payments for logistics to Morocco, Latin America, West Africa or other routes identified by the LEAs; and finance transport and storage through low-value transfers. The cross-border nature of remittances and the prevalence of destination countries that coincide with drug trafficking routes heighten the threat.

Financial fraud, cyber fraud and the recruitment of money mules

250. The threats referred to in section 4.3 highlight the exponential growth of digital and economic fraud, where illicitly obtained funds need to be transferred quickly and without being fully traceable. Remittances facilitate: the immediate dispersal of defrauded sums; the use of money mules recruited through deception; cross-border transfers of small amounts that conceal the scale of the fraud; and the recurring operations of businesses that mix lawful and unlawful funds. The most commonly detected types of fraud include: investment fraud, phishing, BEC, online trading scams, and schemes targeting migrant populations.

Terrorist Financing via micropayments and informal channels

251. The threats referred to in section 5 indicate that current TF primarily utilises small payments, discreet transfers, simulated humanitarian aid operations, and scattered remittances to areas with a jihadist presence. Remittances enable: low-value transfers that are difficult to distinguish from legitimate family support; triangulation via third countries; and links to *hawala* networks or hybrid digital-informal systems. This positions the sector as a channel historically utilised in TF investigations, particularly involving migrant communities with links to conflict zones.

252. Furthermore, other factors that may be exploited by threats within the money transfer sector include:

Factors most frequently exploited by threats	
Informal economies and exposure arising from customer profiles	The sector mainly serves customers who: deal in cash, work in sectors considered to be higher risk (hospitality, construction, agriculture) [72] , have fewer formal financial links, and send money to countries that may have limited supervision or banking penetration. These factors make it easier for funds derived from local illicit activities to be diluted amongst legitimate remittances.
Cross-border flows to high-risk jurisdictions	The concentration of business in corridors across Latin America, North Africa, sub-Saharan Africa and certain Asian countries entails: the risk of sending funds to jurisdictions on FATF lists; the use of multiple correspondent institutions with varying levels of control; and the inflow of funds from countries with vulnerable financial systems. National threats confirm that these routes are used by organised crime, fraud networks and terrorists alike.
Use of agent networks as a primary risk vector	The sector relies on thousands of agents, many of whom have varied levels of training, work simultaneously for several entities, are subject to limited supervision, and are under investigation for collaborating with or facilitating illicit operations. Agents appear to be the main point of infiltration for criminal networks, manipulating data, simulating transfers, fragmenting transactions or permitting the use of fraudulent identities.
Digitalisation, remote identification and integration with new technologies	The threats referred to in section 4 highlight that the expansion of digital payments, remote identification, multi-channel approaches and the use of apps increases vulnerabilities. In the remittances sector, there are instances of the submission of falsified documentation, identity theft, links to unsupervised digital payment platforms and the use of crypto-assets for conversion or withdrawal.

[72] These sectors are considered because they involve extensive use of cash and based on the analysis in the Quarterly Report on Foreign Nationals and the Labour Market from the Labour Force Survey published by the INE, which indicates that these are the main sectors of employment for the foreign population.

Risk factors due to inherent vulnerability

253. The following section sets out the factors relating to inherent vulnerability analysed to determine the inherent risk of the remittance sector.

Characteristics of the sector	
Size of the sector and turnover	The size of the sector and the turnover in 2025 point to a very high level of activity: 37 million transactions totalling over 9,800 million euros, as well as 3.7 million payment transactions totalling over 1,029 million. This massive volume, combined with the high frequency of low-value transactions, naturally increases the inherent risk, as it makes it easier for illicit transactions to be concealed within large legitimate flows. Activity is concentrated among 16 organisations, three of which account for the majority of remittances and virtually all incoming payments (they handle 79 % of remittances and 94 % of incoming payments); this means that any operational shortcoming or control failure at these major remittance providers would have a significant impact on the sector as a whole. Their size, reach and network of agents (around 7,200, of whom 6,800 work for two or more organisations) enable them to process large volumes of transactions in a short space of time; whilst this is operationally efficient, it reduces the capacity for individualised analysis and increases exposure to money-laundering patterns based on in systematic division or repetition.
Level of complexity of the sector's structure	Due to a high degree of fragmentation, in which a few dominant operators coexist alongside thousands of agents, creating a multi-layered structure that is difficult to supervise. Added to this is the presence of heterogeneous business models (brick-and-mortar agents, networks in call shops, distributors, referral agents, *Fintech firms* and hybrid structures). Payment institutions specialising in remittances operate through extensive external networks, in many cases comprising small-scale establishments with inconsistent controls, which increases operational and supervisory complexity. These networks can change rapidly, incorporating new agents or ceasing operations without immediate notification, making it difficult to ensure comprehensive monitoring and the traceability of transactions. In practice, this structural complexity facilitates vulnerabilities such as split transactions, identity fraud, or the channelling of funds to transnational criminal organisations .
Level of integration with other regulated sectors	Money transfer services are characterised by operating without an associated payment account, which reduces their operational interconnection with other traditional financial products. Even so, the level of integration is not low, as payment institutions need to maintain operational accounts with banks (escrow accounts, *nostro* accounts for settlement and correspondent banking) and rely on the banking infrastructure to execute international payment orders. This interdependence with the banking sector creates a significant level of indirect exposure, particularly with regard to the quality of correspondent banking relationships and the risks arising from compliance of obligations such as those set out in Regulation (EU) 2023/1113 on fund transfers. Finally, there is a progressive

	interaction with *fintech* companies, technology providers and other market participants, both regulated and unregulated.
Level of the organisation's local presence, including the geographical scope of the sector's operations	The level of vulnerability is high due to the convergence of several structural factors. On the one hand, activity is concentrated in urban areas with a high proportion of migrant populations, where the majority of operators are based. The structure of the sector (with payment institutions based in Spain but closely integrated into global settlement and distribution networks) amplifies the risk arising from this geographical concentration. The autonomous communities of Madrid and Catalonia have the highest concentration of agents and money transfer outlets, primarily due to their large migrant populations. Furthermore, it should be borne in mind that in Spain a single agent may operate on behalf of several payment institutions, which increases the location-related risk for these institutions, as any customer visiting such an establishment can carry out transactions through all the institutions with which the agent has agreements. This feature increases operational and supervisory complexity, as it multiplies the potential operational flows.
Nature of the products and services provided by the sector	
Level derived from the complexity of the products, due to their impact on anonymity or the limited information available on customers.	Money transfers are carried out without an associated payment account, which reduces the amount of information obtained and retained about the customer. This increases the risk of anonymity and the use of documentation that can be easily forged. Furthermore, the very design of the service—which is based on the execution of low-value, high-frequency transactions with a strong international focus—facilitates the occurrence of split transactions and patterns that are difficult to distinguish from the legitimate behaviour of remittance users, thereby increasing the risk of illicit funds being concealed. The reliance on extensive networks of agents making extensive use of cash—which, in many cases, are small establishments with limited preventive knowledge—reinforces the incidence of anonymity.
Level at which specific products and services offered are linked to intelligence-based communications and/or national ML or TF investigations	The remittance sector is one of the most frequently cited in actual cases, investigated patterns and reports received by SEPBLAC on the basis of suspicious activity. Remittances frequently feature in operations linked to informal transfer networks, split-payment schemes, the use of third parties, illicit trade, human trafficking and cash movements linked to criminal organisations. Money transfers repeatedly feature in police and judicial operations, including cases of ML linked to drug trafficking, hybrid *hawala* networks, document fraud, the financing of illegal movements of persons, and transnational criminal organisations. In this regard, the sector consistently ranks among the most frequently cited in risk typologies and suspicious patterns identified by European FIUs. Recent investigations confirm the continued use of money transfer services by criminal groups, both in their face-to-face form via agents as through international networks of global operators.
Nature of the customer	
Level derived from the nature of the relationship	This activity is based primarily on occasional or transactional relationships. Money transfers by payment institutions are a

offered to customers, depending on the duration (ongoing, transactional or occasional) and frequency of transactions	— typically used on an ad hoc basis or within limited relationships, where the provider does not maintain a long-term financial relationship with the customer. This significantly reduces the quantity and quality of information available to analyse user behaviour over the long term, thereby increasing the sector's vulnerability when it comes to detecting anomalous patterns, as well as identifying structures involving split remittances, the use of money mules or coordinated actions between different intermediaries.
Level derived from the customer's status	The predominant profile consists of foreign individuals. Most users come from Latin America, North Africa and Asia, figures that correspond to the percentage of foreign nationals in Spain by nationality (14 % Moroccans, 10 % Colombians, 5 % Venezuelans, 4 % Peruvians and 3 % Chinese). Although the sector has little exposure to high-net-worth clients, it does occasionally serve sensitive profiles, such as foreign PEPs. Finally, the presence of legal entities is marginal, but when they do appear, they may be linked to opaque structures or international trade activities that are difficult to trace.
Level derived from the client's occupation or type of business	A significant proportion of users work in cash-intensive sectors, such as hospitality, construction, agriculture or domestic services. These profiles face greater difficulties in providing proof of income, stable financial patterns or verifiable employment documentation, which increases the opacity surrounding the origin of the funds. This dynamic is accentuated in the case of irregular migrants working in the informal economy. Similarly, certain professional groups are subject to investigations on the basis of circumstantial evidence, such as small retailers acting as money transfer agents where there is a high volume of cash transactions.
Geographical scope of the sector's activities	
This level relates to specific jurisdictions/countries of interest frequently associated with the sector.	The main remittance corridors from Spain are to Latin America, Africa (North and sub-Saharan) and Asia. These jurisdictions frequently feature in reports based on indications and in police investigations relating to the use of remittance agencies as a channel for the cross-border transfer of illicit funds. Furthermore, the speed of the service and the turnover of customers make it difficult to obtain comprehensive information on the origin of the funds and to apply enhanced due diligence measures in a timely manner. The fact that agents operate on behalf of several payment institutions increases the level of vulnerability, as these jurisdictions end up receiving flows whose actual traceability is distorted at source.
Level arising from the nature of interactions or transactions involving countries identified by the FATF.	Thirteen % of foreign nationals in Spain come from countries identified by the FATF as being at risk of ML/TF. This proportion of the population increases the likelihood that remittances to such jurisdictions are exposed to vulnerabilities associated with ML/TF, particularly if local intermediaries are involved in receiving remittances.
Level derived from the nature of the	There is no evidence of remittance flows to the (DPRK) or Iran. However,

interactions or transactions involving countries subject to international financial sanctions.	in the PF Risk Analysis, mention was made of the use of intermediaries as channels to increase opacity and facilitate the movement of funds linked to these jurisdictions.
Nature of distribution channels	
Level derived from the complexity of the channels due to their impact on anonymity or reduced customer information.	Money transfers provided by payment institutions allow transactions to be carried out without the need for an account, which in itself introduces a structural lack of customer information. This service, combined with the widespread use of cash, facilitates opacity in the transfer of funds and the use of mules who act, for a commission, on behalf of criminal organisations. The large number of agents in the network – who manage the sending and receiving of remittances – increases vulnerability due to the greater operational complexity this introduces into the channels, which facilitates anonymity and may undermine the availability and quality of customer information. The small size and fragmentation of transactions facilitate *'structuring'*: criminal networks can split large illicit sums into multiple small transfers to evade alerts, taking advantage of the fact that each transfer has a low average value (below 300 euros). By its very nature, this product facilitates the transfer of funds with minimal documentation, particularly in transactions involving small amounts, high frequency, or in corridors with a strong informal economy. This characteristic, combined with the use of basic data and manual processing by agents, makes it more difficult to identify anomalous patterns and enables individuals linked to criminal networks to conceal their identity or use that of third parties.
Level arising from the use of new technologies or payment methods.	The sector is undergoing increasing digitalisation, with the emergence of platforms that allow transfers to be initiated electronically, integrations with mobile applications and new payment solutions that speed up the transfer of funds. Whilst these advances improve the user experience, they also reduce the number of in-person checkpoints and enable individuals with illicit intentions to carry out transactions without physical interaction with an agent. This environment facilitates identity theft, the manipulation of digital documents and the emergence of opaque platforms operating from abroad – factors which significantly increase the inherent risk. Furthermore, new technologies make it possible to link traditional remittances with emerging instruments, such as certain crypto-assets, which allow for greater decentralisation and faster transfers. These characteristics make it difficult to identify the true origin of the funds and complicate international coordination between authorities, particularly when providers based in jurisdictions with limited oversight are involved. Although payment institutions have made progress in automated controls and biometric solutions, gaps remain in the traceability and verification of the authenticity of digital transactions.

Conclusion on the sector's inherent risk: High for ML and TF

254. The factors analysed reveal a significant accumulation of structural vulnerabilities. Money transfers are, by definition, account-less transactions that are highly decentralised, based on networks of agents who may act on behalf of various entities, and involve a high degree of cross-border activity towards high-risk jurisdictions. This architecture facilitates high levels of anonymity or limited customer information, the systematic fragmentation of transactions below the threshold of €3,000 per calendar quarter (which triggers the application of customer due diligence) and the use of real or fictitious identities to channel illicit funds. Added to this are the scale of the sector (almost 10,000 million euros sent and 37 million transactions in a single year) and the concentration in a small number of entities operating through thousands of agents subject to varying levels of oversight. Furthermore, the supervisory cycle strategy, previous NRA assessments and the inspections carried out confirm that these patterns persist: the use of agents as the main vectors of risk, the ease with which funds can be concealed through fragmentation, and increasing digitalisation.

Risk factors relating to the effective implementation (or lack thereof) of controls

255. To analyse residual risk, it is necessary to assess the implementation of existing controls within the sector and the extent to which these controls are effective. The following section presents an analysis of the factors used to determine the residual risk in the 'other services' sector, specifically the money remittance sector.

Risk factors relating to the effective implementation (or lack thereof) of controls	
Level of regulation in the sector	The money transfer business is subject to a strict and specialised regulatory framework, which includes prior authorisation from the Banco de España, the mandatory report from SEPBLAC and compulsory registration in the Special Register of Payment Institutions, together with the identification of all agents and branches. The applicable regulations—Law 10/2010, its implementing regulations, payment services legislation, electronic money regulations and the enhanced due diligence obligations set out in Article 19 of the Regulation— create a legally demanding environment that requires money transfer operators to implement due diligence controls, robust monitoring systems and robust identification procedures.
Extent to which unauthorised entities may be operating.	The regulatory framework governing remittances establishes a very strict authorisation and registration system which significantly reduces the likelihood of unauthorised entities operating, making it difficult for an informal provider to operate under the guise of legality within the formal sector. Furthermore, the activity requires operational infrastructure, agreements with international payment providers and compliance with regulatory obligations that are not easily replicated outside the authorised system, which significantly mitigates this risk. The Spanish money transfer sector must compete with other regulated payment institutions in the European Union operating under the freedom to provide services (FPS), such as *Wise* and *Remitly*, and with other entities engaging in unauthorised practice as they do not hold a licence to operate in Spain. However, the nature

	The sector remains to some extent vulnerable: the existence of hundreds of establishments acting as agents, their and the coexistence with non-financial activities (such as telephone kiosks or small shops) encourage unauthorised practice.
Level of potential direct or indirect control over the institution or its management by money-laundering networks	The strict regulatory framework considerably limits the possibility of money-laundering networks exercising direct or indirect control over the institution or its management. Authorisation by the Banco de España requires a thorough assessment of the governing bodies and prevention procedures, accompanied by a prior report from SEPBLAC on suitability and governance; furthermore, registration in the Special Register of Payment Institutions entails ongoing supervision and the obligation to report any relevant corporate changes. These mechanisms significantly reduce the risk of a criminal network infiltrating the entity's ownership structure or formal management, as any change in shareholding, the appointment of directors or a substantial change in control must be notified to and assessed by the supervisory authority. However, there may be attempts to exert indirect influence through agents or establishments linked to criminal networks, particularly at points of sale managed by individuals from communities where organisations engaged in illicit activities operate.
Level of regulation of ML/TF prevention measures	They are entities subject to the provisions of Law 10/2010, of 28 April.
Level of supervision	During the period 2020–2025, 13 inspections were carried out on payment institutions, including those engaged in money transfer activities and the provision of other payment services. Of these, one institution whose main activity was remittance transfers was referred to the penalty proceedings.
Level of sanctions imposed on entities in the sector.	Between 2020 and 2025, six serious sanctions were imposed on two payment institutions that sent remittances. One of them ceased to provide services in Spain.
Level of professionalism of the entity's directors and senior management.	In order to be authorised, remittance companies must have directors and senior managers who have undergone a suitability assessment by the Banco de España and SEPBLAC, which acts as a significant barrier to candidates lacking the necessary qualifications. However, there is marked heterogeneity: alongside large, highly professionalised companies, there are smaller entities whose technical capacity, internal resources and management experience in the area of controls may be more limited. Furthermore, the complexity of the agent-based model requires management to implement supervision and ongoing training mechanisms, which are not always applied with the necessary rigour, leading to gaps in the quality of internal control.
Level of awareness and understanding of their obligations regarding the prevention of ML and TF.	Although payment institutions are required to have formal prevention policies and procedures in place, as well as to provide regular training to their staff and agents, supervisory experience shows that the actual level of awareness of these obligations varies. The structure of the sector — based on a network of agents, many of

	These small businesses or establishments that carry out several activities simultaneously make it difficult to ensure that training is delivered consistently across all points of sale. Inspections have revealed recurring shortcomings in basic tasks such as the correct identification of customers, the verification of documents, the application of DDR (Due Diligence) or the detection of split payments, which shows that, despite the training programmes, the practical implementation of these obligations remains limited in parts of the network. Furthermore, high staff turnover in many of these establishments, the presence of agents working simultaneously for several remittance companies, and the frequent existence of language barriers hinder the assimilation of training content. Larger payment institutions have more robust programmes, but even in these cases significant gaps persist when the agent network is extensive and diverse. The finding that a significant proportion of the shortcomings identified by SEPBLAC are due to insufficient knowledge or incorrect application of regulatory obligations justifies the residual risk being classified as substantial, as the effective dissemination and understanding of prevention requirements remains one of the most vulnerable aspects of the operational model of the remittances.
The organisation's level of commitment to ML/TF policies and measures.	Large remittance firms demonstrate a more visible commitment, with well-established compliance departments, up-to-date manuals, designated internal officers and relatively structured control mechanisms. However, this commitment does not always extend uniformly across the entire organisation, particularly in smaller firms or those whose operations rely on extensive networks of agents with varying levels of training, engagement and understanding of the controls. Inspections show that, despite formal documents and statements, there are some shortcomings in practical implementation: incomplete procedures, insufficient internal supervision, a lack of monitoring of agents, and failures in detecting money-laundering patterns or in the correct application of enhanced due diligence (EDD). This indicates an uneven level of commitment amongst senior management, internal teams and agents on the ground, which limits the actual effectiveness of the policies and justifies the residual risk being classified as medium, given that there are solid elements of institutional commitment, but practical implementation remains insufficient at critical points in the operational chain.
Employees' level of professional qualification and their training in the prevention of ML and TF.	The level of professional qualifications among staff varies considerably, particularly amongst the network of agents, which constitutes the most critical link in the model. Many of these agents are small businesses with high staff turnover and a business-oriented focus. The majority of operations are carried out through agents, who represent the main source of risk, as investigations and inspections have shown that up to 80–90 % of money laundered via remittances has involved agents, rather than ordinary customers.

	Inspections show that a significant proportion of the shortcomings detected — incomplete identification, incorrect document verification, failure to apply the DDR, and failure to detect fragmentation — stem from training gaps or an insufficient understanding of the risks associated with the product. Even when institutions provide regular training, its actual impact is diluted by the highly fragmented nature of the network and differences in the educational background, experience and availability of staff working at points of sale. Although some institutions, particularly the larger ones, have strengthened their training programmes, significant differences persist between agents, which limits the ability to detect suspicious transactions and apply preventive measures with the required rigour.
Level of internal monitoring by organisations of staff compliance.	Internal monitoring of compliance by employees and agents has significant limitations due to the sector's decentralised structure. Although organisations have manuals, procedures and control tools in place, effective supervision of thousands of agents — many of whom are self-employed, with high staff turnover and varying levels of training — is difficult to implement consistently. Inspections have shown that a significant proportion of recurring breaches stem precisely from a lack of effective control over agents' day-to-day activities. The decentralised nature of the model, the use of premises that carry out multiple activities simultaneously, and the high volume of small-scale transactions mean that internal supervision systems, whilst in place, fail to systematically detect or correct malpractice at source. Furthermore, the organisations' capacity to carry out on-site inspections, periodic internal audits or comprehensive remote checks is constrained by the wide geographical spread and by the large number of points of sale.
Level of compliance with obligations regarding preventive measures, in particular CDD/KYC	Compliance with due diligence obligations is one of the most sensitive issues in the remittance sector, as operations rely on a massive volume of one-off transactions, customers with highly diverse documentation and profiles, and an extensive network of agents acting as the first point of contact. SEPBLAC inspections have revealed shortcomings in customer identification and verification, inadequacies in the application of due diligence procedures for transactions exceeding the threshold, and poor detection of transaction splitting. These shortcomings are not due to a lack of regulations, but rather to practical difficulties in implementing them correctly in establishments with high staff turnover, commercial pressure and limited training resources. Furthermore, the presence of agents operating simultaneously for several remittance companies, the coexistence of non-financial activities, and the language or cultural barriers faced by some customers further complicate the correct application of due diligence obligations.
Level of identification and reporting of suspicious transaction reports	The money transfer sector already faces, in itself, structural difficulties in identifying suspicious transactions due to the massive volume of transactions, the diverse nature of customers and the widespread distribution of the agent network. SEPBLAC's inspections have

	consistently revealed that many institutions fail to adequately detect patterns of transaction splitting, inconsistencies in customer information or red flags linked to high-risk jurisdictions. These shortcomings are exacerbated in practice because much of the initial identification falls to agents with varying levels of training and, in many cases, without the technical capacity to correctly interpret risk indicators. As a result, the number of reports is often lower than might be expected in a high-risk sector, and many suspicious transactions only come to light following an inspection or external review. Compounding this situation is the presence of agents working for criminal networks who deliberately conceal their illicit operations within legitimate business activity, by manipulating customer data, cleverly splitting transactions or camouflaging illicit funds within the normal flow of remittances. These agents, being familiar with the internal monitoring mechanisms and alert criteria, adjust their behaviour so as not to generate detectable signals, which greatly hinders the work of the organisation's internal audit and compliance units. This operational infiltration, combined with the difficulty of carrying out frequent on-site checks across such an extensive network, means that even advanced monitoring systems are insufficient to detect fraud at source. The average rating for the relevance of reports based on evidence for the period 2022–2025 was 5.64. This category, introduced in 2021, enables the relative importance of reports to be assessed based on their link to factors such as the connection to serious crimes, the emergence of new types of risk, the detection of criminal structures or networks, and/or the involvement of large sums of money.

Conclusion on the sector's residual risk: Substantial for ML and TF

256. The set of factors assessed indicates that, although the money transfer sector operated by payment institutions has a robust regulatory framework, with strict authorisations, active supervision and formal compliance structures, the mitigation achieved is only partial. The nature of the product —cash-based transactions, high fragmentation, networks of agents that are difficult to control, high-risk cross-border destinations and the ease with which transactions can be split up—mean that the inherent vulnerabilities remain very high. The various existing controls show average levels of implementation (regulation, supervision, formal commitment, managerial professionalism), whilst others demonstrate substantial shortcomings (frequent sanctions, uneven dissemination of obligations, insufficient training, limited internal monitoring, difficulties with due diligence). The identification and reporting of suspicious transactions—particularly affected by agents who collude with criminal networks and conceal their activities within legitimate operations—even reaches a high level of residual risk. Overall, the measures implemented reduce some of the risk, but do not fully compensate for the structural weaknesses of the model.

257. The presence of agents exhibiting irregular behaviour or who are directly infiltrated, inconsistencies in training, the uneven application of due diligence, insufficient internal monitoring capacity and the high rate of disciplinary proceedings resulting from inspections carried out reveal that risk mitigation, whilst significant, is incomplete.

A comprehensive analysis of all these factors confirms that the final assessment of residual risk must be classified as **'substantial'**, as there remains a significant degree of exposure that necessitates maintaining intensive supervision, strengthening training, improving the consistency of controls and closing the operational gaps identified.

Sector: Other services provided by payment institutions 2026

Activity and context

258. Payment institutions that carry out payment services other than money remittance are regulated entities under Article 2.1(h) of Law 10/2010, of 28 April.

259. Payment institutions are those authorised to provide one or more payment services, such as cash deposits and withdrawals from payment accounts, transfers, direct debits, card payments, the issuance or acquisition of payment instruments, as well as other services linked to payment operations. These institutions are subject to significant restrictions, as they may not take deposits or issue electronic money, and their activity is limited to the provision of payment services.

260. Within this sector, and expressly excluding money transfers, the services introduced by the PSD2 Directive are also included[73] which do not involve direct transfers of funds by the institution, in particular the following services: (i) payment initiation, which enables the provider to initiate payment orders from accounts held by the customer with other institutions, subject to prior consent; and (ii) account aggregation, which consists of consolidating information on balances and transactions across different accounts held by the same customer.

261. These services do not involve the management of funds; when they act solely as initiators or aggregators, they do not manage payment accounts but merely access the necessary information with the customer's consent. All these entities are subject to authorisation, registration and supervision by the Banco de España. According to data from the register of entities managed by the Banco de España, in December 2025 there were 51 registered payment institutions in Spain, 10 branches of payment institutions (of which 2 have been deregistered since 2024) and 7 entities authorised to provide services as account information service providers.

262. In addition, there are 14 registered exempt payment service providers, which may, to a limited extent, provide one or more services included within the scope of the Payment Services Directive (PSD2), without the need to obtain full authorisation as a payment institution, provided that: their payment services activity is limited and they meet specific conditions regarding volume, business model or operational risk, for example, collections and payments linked to their own commercial activity.

263. Furthermore, as of 31 December 2025, the EBA's EUCLID[74]register lists 201 authorised payment institutions operating in Spain under the EU passport scheme for the freedom to provide services. There are 39 account information service providers.

264. With regard to the sector's activity in Spain, payments are predominantly made by credit institutions or with their involvement. Collection and payment services provided by payment institutions – with the exception of money transfers mentioned in the previous section – account for a minority of the market, although they have been expanding in recent years due to their speed and lower cost.

[73] https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex%3A32015L2366
[74] https://euclid.eba.europa.eu/register/

Threats

265. The other services provided by payment institutions are exposed to a range of threats directly linked to their digital nature, rapid expansion, the emergence of new business models, the entry of new players via the EU passport, and the presence of occasional and diverse users.

266. This environment may give rise to threats identified at national level, particularly in relation to fraud and organised crime, as well as rapid transfer methods, digital payments, remote identification, identity theft, the use of opaque technologies and the exploitation of *Fintech* channels for ML and TF. The multitude of providers (both domestic and those operating under the freedom to provide services), limited physical presence, operations based on micro-transactions, and the possibility of dealing with customers who are not fully linked to traditional institutions all increase the sector's exposure to these risks.

Cyber fraud, identity theft and the use of accounts for the rapid transfer of funds

267. The threats referred to in section 4 may be exacerbated in the payments sector by:

- high-speed digital transactions,
- online registrations using scanned documentation,
- identity theft in remote processes,
- the use of cards and digital *wallets* with multiple unverified payers,
- low-value, high-frequency transactions, which make it difficult to detect fraud.

268. Payment service providers can act as a channel for dispersing fraudulently obtained funds before they can be blocked by traditional financial institutions.

Organised crime and the use of payment providers as a channel for money laundering

269. Organised crime —particularly that linked to drug trafficking, human trafficking, economic fraud and transnational networks— seeks fast, decentralised and low-friction platforms. The sector may be exposed through:

- multiple free-service payment service providers (FSPs) operating from jurisdictions with varying AML standards,
- payment accounts used as intermediary layers,
- massive fragmentation of transactions,
- immediate international transfer of funds,
- embedded business models (marketplaces, apps, wallets) that allow illicit funds to be channelled under the guise of commercial payments.

270. The growing use of these types of services creates an environment conducive to the layering and dispersal of illicit funds.

Economic crimes and tax fraud involving digital payments and complex structures

271. With regard to the threats identified in section 4, payment services could facilitate:

- channelling revenue from shell companies,
- making cross-transactions that are difficult to trace,
- embedding illicit funds within legitimate commercial transactions,
- handling collections and payments for companies with no financial history,
- receiving cash deposits which are then dispersed via digital payments.

272. The factors most frequently exploited by threats within the context of other services provided by payment institutions are as follows:

Factors that are frequently exploited by threats	
Exposure cross-border and operational with higher-risk countries	In the payments sector, the level of exposure increases in: • frequent international transactions, • communities of non-resident users, • PSPs authorised in jurisdictions with less stringent supervision, • the use of payment accounts or payment orders to non-EU countries, • payments linked to cross-border e-commerce with limited traceability.
Digital, scalable and rapidly expanding business models	This exposure is associated with: • rapid growth without a commensurate adaptation of controls, • compliance teams that are understaffed, • process automation vulnerable to widespread abuse, • 'embedded' operations where the organisation does not know the actual customer, • outsourcing of critical processes. The use of such regulated entities may "make it difficult to identify the actual customer and the economic origin of the funds". Furthermore, customers "without a documented economic activity" may increase the level of exposure.
Cash, cards and micro-transactions	Although many services are digital, the following still exist: • cash deposits and withdrawals, • top-ups via cards from multiple payers, • small-value payments that facilitate payment in instalments, • hybrid physical/digital operations. This corresponds to NRA classifications relating to 'pitufeo', the commingling of funds, and manual operations without adequate traceability.
Remote identification and false documents.	One of the most significant risk factors is remote verification: • high exposure to forged documentation, • identity theft to open payment accounts, • automated processes vulnerable to manipulation, • international customers without a physical presence. The lack of a physical presence and remote verification increase the risk of fraudulent or impersonated transactions.

Micropayments and payment initiation services	In relation to the threats identified in section 4, payment services, particularly payment initiators and digital PSPs, may facilitate: • small cross-border transfers that are difficult to detect, • rapid transactions involving multiple intermediaries, • transfers to sensitive jurisdictions without the use of traditional bank accounts. Although the sector does not present the same level of exposure as remittance companies, it does constitute a significant channel for low-value TF.

Risk factors due to inherent vulnerability

273. The following sets out the factors relating to inherent vulnerability analysed to determine the inherent risk of the sector of other services provided by payment institutions:

Sector Characteristics	
Size of the sector and turnover	Although not particularly high, the sector's turnover figures may make it attractive for concealing ML and TF operations. The digitalisation of the economy has contributed to the growth of this type of service.
Level of complexity of the sector's structure	The widespread use of the EU passport, which allows for the free provision of services, increases the number of different market participants, the complexity of supervision and the burden of complying with national regulations.
Level of integration with other regulated sectors	It relies on banks for settlement and operational accounts, and on international networks with varying regulations, which introduces cross-border and technological risks that increase the inherent risk.
The extent to which the organisation is localised, including the geographical scope of the sector	As these services are provided mainly via digital payment platforms, the entity's location within the national territory is not necessarily a risk factor. However, there is a possibility that entities based in countries with fewer preventive controls may provide this type of payment service in Spain.
Nature of the products and services provided by the sector	
Level derived from the complexity of the products, due to their impact on anonymity or the limited information available on customers.	Other payment services, such as executing transfers or initiating payments, have a product structure that requires customer identification. However, where the service is provided through the use of omnibus accounts [75] , the complexity of the product may give rise to a higher level of anonymity and reduced operational visibility of the underlying customer. This circumstance may hinder the direct identification of the end customer within the operational flow and affect the individual traceability of transactions, thereby increasing the risk associated with the product's complexity.

[75] An omnibus account is one in which a financial intermediary groups the assets of multiple customers under a single account holder and carries out transactions on behalf of those customers under that same account.

The level at which specific products and services offered are linked in communications by reference and/or domestic ML or TF investigations	During the period analysed, there were 1,674 reports based on suspicious activity submitted by other regulated entities in which the payment institutions sector was implicated; however, not all reports relate to other services provided, but may also include money transfer activities.
Nature of the customer	
Level derived from the nature of the business relationship with customers, based on the duration and frequency of transactions	Commercial relationships may vary in nature: they range from ongoing relationships with regular customers to transactional or occasional relationships linked to one-off transactions. In cases where the relationship is occasional or low-frequency, the customer's pattern of service use may be more limited, which increases the risk associated with one-off use of the service.
Level derived from the customer's status, taking into account the type of person, their origin and their characteristics	These services are provided to both individuals and legal entities. This breadth may result in a diverse range of client types, including individuals with straightforward financial profiles or legal entities of varying size and complexity.
Level derived from the client's occupation or type of business	The other payment services provided by payment institutions may be used by customers with different occupations or types of business, which introduces significant diversity into the associated risk profiles. Certain economic activities, by their very nature, may involve a higher volume of transactions, variable cash flows or less standardised business models, which can make it difficult to define an expected pattern of service usage.
Geographical scope of the sector's activities	
Level derived from specific jurisdictions/countries of interest frequently related to the sector.	In Spain, there is a very high number of resident foreign individuals, as well as legal entities operating in various economic sectors, such as those linked to foreign trade. This entails a high number of international transactions, often of a regular nature and relating to trade or investment.
Level derived from the nature of the interactions or transactions involving countries identified by the FATF.	The high number of international transactions and the presence of communities of foreign residents and legal entities incorporated in third countries – which are sometimes countries identified by the FATF – may involve a significant volume of fund transfers and remittances to these countries, which could potentially be linked to ML and TF activities.
Level derived from the nature of the interactions or transactions that involve countries	There is no evidence of these services being used to evade international financial sanctions. However, the SRA for PF identifies the use of *Fintech*-type intermediaries, such as payment gateways, as an emerging threat, with the ultimate aim of evading sanctions.

entities subject to internation financial sanctions.	These intermediaries, would be the payment institution's end customer, which contributes to a lack of transparency in identifying the customer and the transaction.
Nature of distribution channels	
Level derived from the complexity of the channels due to their impact on anonymity or the limited information available on customers.	The growing use of online platforms for payment transfers may result in less customer information and traceability, as it facilitates remote transactions and increases the risks associated with such transactions. The accumulation of low-value transactions can add complexity to monitoring; combined with the use of cash, a lack of rigour in online registration, or payments made via bank cards belonging to unknown third parties, this would increase the risk. The use of cash takes the form of prepaid cards used as an electronic means of payment for the execution of payment orders.
Level arising from the use of new technologies or payment methods.	Use of payment technologies where transactions are difficult to trace. Digitalisation reduces in-person checks and facilitates identity theft or document tampering. Foreign platforms or links to crypto-assets may be used, which make tracing transactions more difficult.

Conclusion on the sector's inherent risk: Substantial in ML and TF

274. The payment institutions sector offers a wide range of services, some of which present very high inherent risks. These risks are heightened in cases involving digital identity verification, which facilitates the use of false or forged documentation. The monitoring of transactions is often insufficient. The lack of qualified staff and understaffed compliance teams, combined with the widespread use of the EU passport for the freedom to provide services, increases the complexity of supervision and reduces the capacity for effective oversight. Added to this are multi-layered business models (*marketplaces*, embedded services), which make it difficult to identify the actual customer and the economic origin of the funds.

275. The use of payment accounts opened and operated in digital environments, as well as the possible involvement of third-party intermediaries and prepaid cards – which are non-nominal and receive split cash deposits – can hinder the effective identification of the beneficial owner and the traceability of funds, thereby increasing the risk of these services being used for Money Laundering and Terrorist Financing. Consequently, the risk inherent in the execution of payment orders is **high** for both ML and TF.

276. In the case of payment initiation services, the **average** inherent risk of ML and TF stems mainly from the speed with which transfers are executed, the possibility of split cross-border payments, and their role as intermediaries in these transactions. Account aggregation services present a **low** risk of ML and TF, as they are limited to the collection and display of customers' financial information, without involving the execution of transactions or the safekeeping or transfer of funds. This nature significantly reduces their potential for use in channelling illicit flows. Furthermore, access to information is granted with the customer's express consent and within the framework of payment services regulations, which provides additional safeguards in terms of traceability and control. Whilst there may be indirect risks associated with the misuse of aggregated information or potential integration with other services, these are not inherent to the service's core functionality; consequently, the level of risk is considered low. Account aggregation services, by being limited to the aggregation and display of

information—without executing transactions or holding funds—present a **low** risk of ML and TF.

277. In credit and debit card issuance services, there is a direct contractual relationship with the customer and a link to credit institutions that are also regulated entities. However, the widespread and transactional use of cards can facilitate misuse, as they are an easily obtainable instrument for the movement of funds; consequently, the risk of ML and TF is **substantial**.

Risk factors relating to the effective implementation (or lack thereof) of controls

278. To analyse residual risk, it is necessary to assess the implementation of existing controls within the sector and the extent to which these controls are effective. The following section presents an analysis of the factors used to determine the residual risk in the sector of other services provided by payment institutions.

Risk factors relating to the effective implementation (or lack thereof) of controls	
Level of regulation in the sector	The sector is subject to comprehensive and detailed regulation.
Extent to which unauthorised entities may be operating.	Entities in the sector are subject to a strict authorisation regime. Controls are in place to prevent unauthorised entities or individuals from operating in the sector. The provision of payment services without the required authorisation breaches the reservation of activity established in Royal Decree-Law 19/2018 and is punishable under the regime set out in Law 10/2014, which classifies this type of conduct as a very serious offence.
Level of potential direct or indirect control over the entity or its management by money-laundering networks	The regulations require control measures in this regard; however, the potential management or control of the management of small electronic money institutions, even if indirect, with the aim of carrying out ML/TF activities, poses a risk that must be taken into account.
Level regulation of measures to prevent ML and TF	Payment institutions providing these services and electronic money institutions are obliged entities under Law 10/2010[76].
Level of supervision	The sector is subject to ML and TF inspections by SEPBLAC, covering all institutions within it. However, as there are low barriers to entry in terms of capital requirements, the large number of institutions makes supervision difficult. Since January 2022, Royal Decree-Law 7/2021 has introduced a requirement for payment institutions and electronic money institutions to report their payment accounts to the FTF, thereby strengthening the supervision of these institutions through the reporting of accounts.

[76] Payment institutions and electronic money institutions are obliged entities under Law 10/2010 on Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) (Article 2.1(h) and (i)), as well as its implementing regulations, in particular Royal Decree 304/2014, which approves its Regulations. This framework comprehensively regulates obligations relating to customer due diligence, internal controls, transaction reporting and supervision, which is considered sufficient to adequately mitigate the ML/TF risks associated with these services. Consequently, the classification of the regulatory level of ML/TF prevention measures as 'low risk' is justified.

	In the period 2020–2025, 13 inspections were carried out on payment institutions, including those engaged in money remittance and the provision of other payment services.
Level of sanctions imposed on entities in the sector.	During the period under review, six sanctions were imposed on the sector, all of which were classified as serious. These sanctions account for 38 % of the infringements identified among the entities inspected. These sanctions have heightened the perception of regulatory risk and the consequences of non-compliance. This effect reinforces senior management's commitment and encourages the adoption of more robust controls, embedding compliance within day-to-day operations.
Level of professionalism of the organisation's directors and senior managers.	The authorisation of payment institutions is subject, in accordance with Law 19/2018 and its implementing Regulations approved by Royal Decree 736/2019, to compliance with commercial and professional integrity requirements by the persons who effectively manage the institution and by holders of significant shareholdings.
Level of awareness and understanding of on the prevention of ML and TF.	Although the need for training in this area is particularly important for this sector, awareness of the sector's ML/TF obligations has grown significantly, especially in recent years, when there has been a marked increase in the sector's culture of prevention.
The organisation's level of commitment to ML/TF policies and measures.	Growth in the customer base is not always accompanied by a commensurate effort in the development of policies and measures, which highlights certain limitations in the organisations' ability to adapt. Nevertheless, it is observed that, generally speaking, compliance frameworks are in place and operational, albeit with shortcomings in terms of development and scalability.
Level of professional qualifications of staff and their training in ML/CFT prevention.	Although the need for training in this area is particularly relevant to this sector, in general – and especially in recent years – the professional qualifications of employees in the sector regarding ML/TF prevention have improved significantly.
Level of internal monitoring by organisations of employees' compliance.	There are legal obligations in this regard and there is increasing scrutiny within the sector regarding employees' conduct, as employees may enjoy a considerable degree of freedom of action which has a very significant impact on the risks associated with ML/TF operations.
Level of compliance with obligations regarding preventive measures, particularly CDD/KYC	Substantive inconsistencies have been detected in matters relating to remote identification, identification of the beneficial owner, the purpose of the business relationship and the monitoring of that relationship.
Level of identification and reporting of suspicious transactions suspicious transactions	Within the financial sector, payment institutions are the second-largest group of organisations in terms of the number of reports submitted on the basis of indications. During the period analysed, more than 14,000 reports were submitted based on indications, representing an increase of over 300 % since 2020.

	The average rating for the significance of reports based on indications for the period 2022–2025 was 5.64. This category, introduced in 2021, enables the relative importance of reports to be assessed based on their link to factors such as the connection to serious offences , the emergence of new types of risk, the detection of criminal structures or networks, and/or the involvement of large sums of money.

Conclusion on the sector's residual risk: medium/substantial for ML and TF

279. The ability to execute payment orders and access the SNCE, which enables the creation of payment accounts, poses a risk of these accounts being used for ML and TF activities. Although credit institutions are the main issuers of payment accounts, the use of such accounts by payment institutions and electronic money institutions is increasing, leading to the view that these services present a **substantial** residual risk of being misused (abused) for ML/TF purposes.

280. On the other hand, the residual risk associated with payment initiation operations is **low to medium**, as it relates solely to acting as an intermediary in the payment for goods or services without managing the customer's funds. In other words, once the instruction to initiate the payment has been received, they simply check whether there are sufficient funds in the payer's payment account specified by the payer to proceed with the payment, and, if there are, inform the seller that the payment has been initiated.

281. As for the activities of account aggregators, their residual risk could be classified as **low**, as they do not act as intermediaries in any payments and merely consolidate information previously analysed by the account managers who, as obliged entities, are subject to the ML/TF preventive framework. Nevertheless, they are entities that hold a large amount of aggregated financial information on customers and their funds, and can play an important role in detecting ML/TF-related activities that are not detected by the other obliged entities managing the accounts.

282. Finally, with regard to payment institutions that issue credit and debit cards, their residual risk could be classified as **medium**, as they generally operate with funds originating from other regulated entities (via direct debits). However, as in the previous case, these institutions hold a great deal of information on customers and the destination or use of their funds, and can play an important role in detecting ML/TF-related activities that are not detected by the other obliged entities managing their main accounts.

Sector: Electronic money institutions 2026

Activity and context

283. Electronic money institutions (EMIs) are obliged entities under Article 2.1(h) of Law 10/2010 of 28 April.

284. EMIs are those authorised to issue electronic money that is accepted as a means of payment by entities other than the issuing institution. They may issue, distribute and redeem electronic money – defined as monetary value stored electronically and accepted by third parties – and may also provide payment services relating both to the electronic money issued and to other funds, without the need for additional authorisation as a payment institution, in accordance with Law 21/2011 and its implementing regulations.

285. The procedure for EMIs from other EU Member States to open branches and freely provide services in Spain is subject to the Banco de España receiving notification from the supervisory authority of the EMIs' country of origin; therefore, the mandatory report from SEPBLAC is not required.

286. According to data from the register of institutions managed by the Banco de España, in December 2025 there were 12 EMI institutions registered in Spain. There are also 9 registered EMI branches, 5 of which have been registered since 2024. The EBA's EUCLID register lists 278 entities authorised to provide electronic money services, the majority of which operate under the EU passport scheme for the freedom to provide services. With regard to the sector's activity, the 12 registered EMIs had total assets of 1,100 million euros as at June 2025.

Threats

287. The EMI sector is one of the most exposed to ML and TF threats within the financial sector, due to the digital nature of its products, the high speed of transactions, its limited physical presence, its intensive international operations and the possibility of carrying out a large number of low-value transactions in a fragmented manner. These factors align with several of the identified national threats, particularly digital fraud and transnational criminal networks, amongst others.

288. EMI operators operate in business segments that are critical due to their technological vulnerability: cross-border payments, high-frequency digital transactions, payment initiation, contactless services and the acquisition of international users. These factors make the sector susceptible to exploitation by criminal networks, all with less friction than in the traditional banking system.

289. The specific threats of greatest relevance to this sector are described below.

Organised crime and international money-transfer networks

290. Organised crime poses a strategic threat characterised by a strong capacity to adapt to technological developments, the intensive use of encrypted communications, the splitting of funds ('smurfing') and alternative systems such as *hawala*, digital platforms or money mule networks. EMI platforms are particularly attractive to these networks due to the speed of transactions, the ability to operate without a physical presence, the massive fragmentation of payments, cross-border operations and the acceptance of non-resident users. Furthermore, the existence of EMI platforms

licencesed in other EU Member States, with varying identification standards, allows criminal organisations to use EMI with more lax controls as a point of entry.

Digital fraud, phishing, BEC and mass scams

291. There has been a significant increase in digital fraud and social engineering scams (*phishing, smishing, vishing, pig butchering*, investment fraud, mule accounts), which represent one of the greatest threats to the Spanish economic system. EMI platforms can serve as a channel for: receiving funds from victims, rapidly dispersing them across multiple jurisdictions, moving small amounts under the radar, and operating with identities created or verified online.

292. The massive volume of low-value transactions, combined with remote identification, increases the sector's appeal to networks channelling illicit proceeds from complex fraud schemes.

Drug trafficking and the use of digital remittance services

293. Drug trafficking groups use digital payment platforms, money mules and express delivery services to move funds derived from drug trafficking. Express delivery services can be used by these networks to: i) fragment proceeds from local micro-sales, ii) send funds to suppliers in Latin America, Africa or Asia, iii) use borrowed or unverified identities, and
iv) channel payments linked to logistics services and illicit transport. Exposure to this threat is particularly high when the following factors converge:

- recurring international payments,
- non-resident users,
- heavy use of cash at top-up points,
- online sign-ups with minimal documentation.

TF and cross-border micropayments

294. TF has evolved towards micropayments, small-scale donations, the use of online payment platforms, and cryptocurrencies. EMI services can be used to: send small amounts to countries where terrorist groups are active; raise funds through structures that appear to be humanitarian in nature; incorporate anonymised or untraceable payments by mixing illicit funds with legitimate ones; and use hybrid methods (EMI ↔ crypto-assets ↔ prepaid cards). Their cross-border operations make it difficult to determine whether the final recipients are located in high-risk jurisdictions.

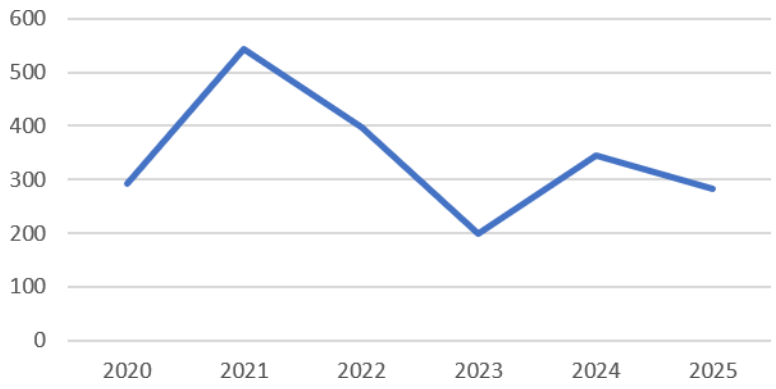
Economic crime, tax fraud and the use of shell companies

295. Tax fraud, VAT carousels and networks of shell companies frequently require digital accounts to move funds quickly. EMI are vulnerable to:

- newly formed companies,
- companies with no real business activity,
- structures with multiple directors,
- corporate clients domiciled in third countries,
- recurring payments without economic justification.

296. The ability to process large numbers of transactions without a physical presence facilitates the introduction and dispersal of fraudulently obtained funds.

297. In addition, other factors that may be exploited by threats in the EMI environment include:

Other factors frequently exploited by threats	
International flows, migration and intensive cross-border use	As a result of flows with high-risk countries, whether for migration reasons, commercial activity or remittances, the following is observed in the case of EMI: • there is a very high volume of international transactions, • users resident in Spain send funds to jurisdictions posing a ML/TF risk, • Part of the business involves foreign clients or companies registered in third countries, • the high mobility of funds between EU Member States creates gaps in supervision.
Crypto-assets, conversion and hybrid use with DeFi platforms	Among the vulnerabilities identified is a sharp increase in the use of crypto-assets for both fraud and ML. EMI may be used as: • a point of entry or exit between fiat currency and crypto-assets, • a channel for digital payments prior to conversion on *exchanges*, • a platform for mixing funds with proceeds from unverified *wallets*. The purchase of cards, top-ups or reloads linked to cryptocurrency significantly amplifies the threat. As regards the trend in reports based on evidence, the following chart shows a stable trend, albeit lower than in previous years such as 2021. Fraud and scams, associated with economic crimes, are the predominant criminal category in the evidence contained in the reports submitted  Source: SEPBLAC

Risk factors by inherent vulnerability

298. The following section presents the factors relating to inherent vulnerability analysed to determine the inherent risk of the EMI sector.

Sector characteristics	
Size of the sector and turnover	Although it is not the largest sector within the financial system, its growth in recent years – driven by financial digitalisation – must be taken into account. Turnover figures are not particularly high. However, the fact that it is a fundamentally digital sector makes it attractive for concealing ML and TF operations.
Level of complexity of the sector's structure	The widespread use of the EU passport, which allows for the freedom to provide services, increases the complexity of supervision and compliance with national regulations.
Level of integration with other regulated sectors	The mobilisation of funds links them directly to credit institutions, which provide them with escrow accounts and the necessary infrastructure to load, unload and transfer electronic money. Furthermore, as with crypto-asset service providers, who rely on them as payment platforms to convert fiat to crypto (and vice versa), a continuous operational cycle is generated between the banking sector, EMI and the crypto sector.
Location of the institution, including the geographical scope of the sector's operations	The location of certain branches in high-risk areas – whether due to the significant presence of high-risk groups or the nature of the clientele's main business activity – can have a significant impact on the risk rating of the institution's various branches. The level of exposure arises from EMI operations that establish themselves in countries where fewer requirements are imposed for setting up a business and which operate in Spain under the freedom to provide services. The lack of a physical presence in Spain heightens the reliance on digital channels and third parties for the identification and movement of funds, which may increase exposure to heterogeneous operational environments, differences in internal control standards and technological vulnerabilities.
Nature of the products and services provided by the sector	
Level derived from the complexity of the products, due to their impact on anonymity or on the reduced amount of information available about customers.	The use of these services to obtain cash in transactions in other countries entails an extremely high risk of their being used for ML/TF operations. The lack of a physical presence and the consequent difficulty in verifying the user's identity has been mitigated through regulations and the requirement for various customer identity verification measures that hinder potential ML/TF operations carried out under these circumstances.
The extent to which specific products and services offered are linked to intelligence-led communications and/or national ML or TF investigations	1 % of reports based on evidence are made by this sector.
Nature of the customer	
Level derived from the nature of the relationship	Difficulty in monitoring, as most transactions are below the breakdown level.

commercial with customers, depending on duration (ongoing, transactional or occasional) and frequency of transactions	
Level derived from the customer's status	The customer profile is highly varied. This heterogeneity, combined with the high number of customers and EMI, increases the complexity of adequately segmenting customer types and, consequently, identifying anomalous patterns. Furthermore, the predominantly non-face-to-face nature of operations introduces additional challenges, as the lack of physical contact makes it difficult to directly verify the user's identity, thereby increasing the exposure to identity theft, fraudulent documentation and misuse of digital services.
Level determined by the customer's occupation or type of business	Customer activity and how it aligns with transactions is key to risk assessment. The fragmentation of the customer base makes this a challenge, as it hinders our understanding of the activities carried out by customers.
Geographical scope of the sector's activities	
A level derived from specific jurisdictions/countries of interest frequently associated with the sector.	The high number of international transactions and the presence of communities of foreign residents and legal entities incorporated in third countries – which are sometimes countries posing a ML/TF risk – may result in a high volume of fund transfers and remittances to these countries, which could entail significant exposure to potential links with ML/TF operations.
Level derived from the nature of interactions or transactions involving countries identified by the FATF.	The rise of EMI and the fact that, in many cases, they operate as *neobanks* in these jurisdictions has significantly increased cross-border flows into environments with greater vulnerabilities. This expansion is most notable in countries with low levels of banking penetration, where EMI have become the main channel for accessing digital financial services, increasing the volume and frequency of transactions that may involve customers with less standardised documentation, heterogeneous legal frameworks or weaker control infrastructures. The volume of transactions to and from countries designated by the FATF creates an environment in which risk profiles are more varied and the detection of unusual patterns is more complex, thereby increasing the vulnerability of this sector.
Level arising from the nature of interactions or transactions involving countries subject to international financial sanctions.	There is no evidence that the sector is being used to channel funds to Iran or the DPRK. However, the FP Risk Analysis mentions the use of intermediaries as channels to increase opacity and facilitate the movement of funds linked to these jurisdictions. Therefore, given the sector's digital operations and its use as neobanks, the possible channelling of funds to intermediary countries must be considered.
Nature of distribution channels	
Level derived from the complexity of the	The accumulation of operations of under amount may add complexity when it comes to monitoring, coupled with the use of cash

channels due to their impact on anonymity or the limited information available on customers.	through the topping up of prepaid cards, a lack of rigour in online registration or payments via bank cards belonging to unknown individuals, multiple payers would increase vulnerability. Furthermore, the existence of EMI offering crypto-asset services within their platform increases exposure to the use of channels for channelling illicit funds.
Level arising from the use of new technologies or payment methods.	Use of digital payment technologies where transactions are difficult to trace.

Conclusion on the sector's inherent risk: High for ML and TF

299. EMIs present a high inherent risk of ML/TF due to their digital, cross-border and predominantly remote operations.

300. The high inherent risk rating for electronic money institutions is fully justified when considering a weighted assessment of the factors analysed, in which the elements with the greatest potential for exposure to ML/TF (primarily the nature of the products and services, the distribution channels and the geographical scope) present high or substantial levels of risk and carry greater relative weight in the analysis. Added to this is the cumulative effect arising from the combination of digital, non-face-to-face operations, high fragmentation of transactions, international exposure and difficulties in identifying and monitoring customers, which significantly increases the complexity of detecting suspicious transactions. Consequently, the final assessment is not based on a simple quantitative criterion, but on a qualitative approach based on the materiality and interdependence of risks, consistent with a risk-based supervisory model.

Risk factors relating to the effective implementation (or lack thereof) of controls

301. To analyse residual risk, it is necessary to assess the implementation of existing controls within the sector and the extent to which these controls are effective. The following section presents an analysis of the factors used to determine the residual risk in the sector of other services provided by EMIs.

Risk factors relating to the effective implementation (or lack thereof) of controls	
Level of regulation in the sector	The sector is subject to comprehensive and detailed regulation under the Electronic Money Act (Law 21/2011). The process of establishing EMI entities requires, amongst other things: a minimum registered share capital of 350,000 euros, a registered office within Spanish territory, and professional and commercial integrity. Spanish EMI must obtain a preliminary report from SEPBLAC assessing the suitability of the proposed governing bodies and procedures, based on the documentation submitted regarding the ML and TF structure and procedures they intend to apply once operational.
Level of potential existence of entities	EMIs are subject to a strict authorisation regime. There are controls in place to prevent unauthorised organisations or individuals from

without authorisation.	operating in the sector. The regulatory framework applicable to electronic money institutions, based on Directive 2009/110/EC and Law 21/2011, establishes these controls, which include, in particular, the legal reserve for the activity, the requirement for prior administrative authorisation from the Banco de España, registration in official public registers, compliance with prudential and organisational requirements, as well as ongoing supervision and the system of sanctions. Furthermore, the supervision of agents and the regulation of the EU passport reinforce these requirements. However, whilst not considered to be entities without authorisation to operate, there is a growing number of intermediaries who contract the service from a licensed entity, acting themselves as clients rather than those who are the beneficial owners of the transactions.
Level of potential direct or indirect control over the entity or its management by money-laundering networks	Regulation already requires control measures in this regard; however, the potential management or control of the management of small EMI entities, even if indirect, with the aim of carrying out ML/TF activities, poses a risk that must be taken into account.
Level of regulation of AML/TF prevention measures	Electronic money institutions are obliged entities under Law 10/2010 of 28 April, Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) (Article 2.1(i)), as well as its implementing regulations, in particular Royal Decree 304/2014, which approves its Regulations. This framework comprehensively regulates obligations relating to customer due diligence, internal controls, reporting of transactions and supervision, which is considered sufficient to adequately mitigate the ML/TF risks associated with these services.
Level of supervision	The sector is subject to inspections as part of SEPBLAC's ML/TF by SEPBLAC, covering all institutions within the sector. Since 2021, seven inspections have been carried out (three of which are still ongoing as part of the 2025 plan), resulting in one disciplinary proceeding. The sector has also been monitored through the distribution of a structured information questionnaire.
Level of sanctions imposed on entities in the sector.	During the period analysed, there were no sanctions or formal notices issued to the sector.
Level of professionalism of the organisation's administrators and senior managers.	The professionalism of EMI directors is expressly regulated under Spanish legislation, which requires that those holding such positions possess commercial and professional integrity, adequate experience and managerial competence. Law 21/2011 on electronic money and its implementing provisions in Royal Decree 778/2012.
Level of awareness and understanding of their obligations regarding the prevention of ML and TF.	There are legal obligations regarding the existence and dissemination of manuals setting out internal policies and procedures. The level of knowledge among the institutions' staff regarding ML/TF varies depending on the type of institution.
Organisation's level of commitment to ML and	Awareness and commitment amongst institutions in the sector and their directors and senior management is high. However, it should be borne

TF policies and measures.	in mind that the fragmentation of the sector has contributed to the emergence of new players whose business culture takes precedence over a preventative approach. The growth in the customer base is not always accompanied by a commensurate effort to develop policies and measures.
The level of professional qualifications of employees and their training in ML/TF[77] .	The need for training in this area of ML/TF has grown significantly amongst EMI, mainly due to the sector's digital growth. Although the sector has seen improvements in this area, shortcomings persist when compared with other financial sectors.
Level of internal monitoring by institutions of staff compliance.	There are legal obligations in this regard and there is increasing scrutiny within the sector regarding employees' actions, as employees may enjoy a significant degree of freedom of action which has a very significant impact on the risks of operations linked to ML/TF.
Level of compliance with obligations regarding preventive measures, particularly CDD/KYC[78] .	The very nature of the business of providing funds for trading makes it difficult to obtain adequate information about the customer, which affects the verification of the source of the funds made available. The number of customers and transactions, and the variety of methods used to conceal the identity of those topping up accounts, the funds being deposited, and the withdrawals and payments detected during investigations and supervisory checks (forgeries, identity theft, impersonation, intermediaries, etc.), all contribute to the existing ML/TF risk. This risk is heightened when an intermediary with an omnibus account is involved in the transaction, rather than a breakdown of payment accounts by beneficial ownership. Of the inspections carried out, one conducted in 2023 identified shortcomings in the identification, the purpose of the business relationship and the monitoring of transactions.
Level of identification and reporting of suspicious transaction reports	The sector is highly diverse, with EMI institutions lacking a culture of compliance coexisting alongside others that report appropriately. Between 2020 and 2025, more than 2,000 reports based on indications were submitted. The average rating for the significance of reports based on indications for the period 2022–2025 was 5.17. This category, introduced in 2021, allows the relative importance of reports to be assessed based on their link to factors such as the connection to serious crimes, the emergence of new risk typologies, the detection of criminal structures or networks and/or the involvement of large sums of money.

Conclusion on residual risk in the sector: Substantial in ML and TF

302. The EMI sector faces very high inherent risks that are common to the entire sector. These risks are even greater in cases involving electronic money issued in other countries, where controls over the holder's identity and transaction thresholds do not meet the requirements imposed at national level. However, as indicated, the specific regulatory amendments adopted to strengthen the ML/CFT regime in these institutions, the closer engagement with the sector by the regulatory and supervisory authorities, and a substantial increase in the implementation of internal policies and procedures by EMI institutions, including improvements

[77] This inherent vulnerability factor is rated as substantial/high.
[78] This inherent vulnerability factor is rated as substantial/high.

in tip-off-based reporting, have led to a substantial improvement in the sector's risk profile, which has shifted from high to significant for both ML and TF.

303. Key factors, such as the effective implementation of due diligence measures, customer identification in digital environments, intermediation via omnibus accounts or third parties, as well as the sector's heterogeneity and uneven compliance culture, present high or substantial levels of risk that limit the mitigating effectiveness of these controls. Furthermore, the sector's rapid expansion, the fragmentation of operators and resource constraints within certain entities create difficulties in continuous monitoring and the detection of suspicious patterns. Consequently, the final assessment is not based merely on the existence of formal controls, but on the extent to which they are actually implemented and their effective mitigating capacity. It is therefore concluded that, despite regulatory and supervisory progress, the residual risk is considered **substantial** for both ML and TF, in accordance with an approach based on the materiality and interdependence of risks.

Sector: Currency exchange 2026

Activity and context

304. Persons who carry out currency exchange activities on a professional basis are regulated entities under Article 2.1(i) of Law 10/2010, of 28 April.

305. The professional activity of exchanging foreign currency in establishments open to the public is subject to an authorisation regime expressly regulated by the Banco de España, and authorised entities are listed in the Register of Currency Exchange Establishments. Under these regulations, there are two types of establishments:

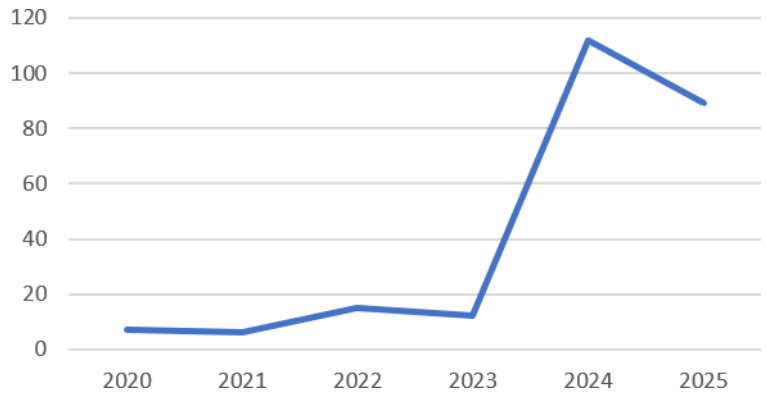
- Establishments authorised solely to purchase foreign currency and traveller's cheques in exchange for payment in euros. The regulations distinguish between entities for which this is their main activity and those for which it is a secondary activity (such as travel agencies and hotels).
- Establishments authorised, in addition, to sell foreign banknotes and traveller's cheques in exchange for their equivalent value in euros or foreign currency.

306. As at 8 March 2026, the Banco de España's Register of Foreign Currency Exchange Operators lists 17 entities authorised to buy and sell foreign currency as their principal activity. Over the years, there has been a consolidation into a small number of operators, through the acquisition of smaller operators by larger ones, and through mergers. The total assets of this sector in 2024 stood at 100 million euros, and total net turnover amounted to 120 million euros. Banco de España is responsible for the authorisation, registration and prudential supervision of foreign exchange entities.

Threats

307. The currency exchange sector presents a high level of risk in relation to ML and TF, stemming mainly from its high exposure to cash, the difficulty in verifying the origin of funds, the limited traceability of transactions, and the transactional and occasional nature of a large proportion of its clientele. These threats have been repeatedly identified by supranational and European assessments, in particular by the European Union's SNRA and by FATF/MONEYVAL reports, which rank currency exchange activities among the most vulnerable within the non-bank financial system.

308. Suspicious activity reports submitted by currency exchange establishments show low and stable levels between 2020 and 2023, with figures ranging from 6 to 15 reports per year. However, a very significant increase was observed in 2024, reaching 112 reports, followed by a slight reduction in 2025 to 89 reports, which demonstrates a notable improvement in the detection and reporting of suspicious transactions by the sector in recent years.



Source: SEPBLAC

Money Laundering through cash conversion

309. The main threat posed by the sector lies in the rapid conversion of cash of potentially illicit origin into other currencies, which makes it possible to: i) introduce cash into the financial system, ii) fragment funds through repeated small-value transactions, iii) facilitate the subsequent international movement of capital, and iv) operate without the need for complex structures or advanced technical knowledge. These characteristics make currency exchange a particularly attractive tool for the placement stage of Money Laundering, and in certain cases also for layering and integration. This threat is a recurring theme in national and international investigations.

Terrorist Financing through the use of cash and foreign currency

310. European analyses highlight that certain terrorist threats, particularly those of a jihadist nature, tend to use cash during their fundraising phases. Subsequently, it becomes necessary to convert these funds into internationally circulating currencies to facilitate: i) cross-border travel, ii) logistical support, and iii) transfers to third parties in other countries. In this context, currency exchange bureaux constitute a key mechanism for conversion, particularly where insufficient checks are carried out on the identity of the parties involved and the purpose of the transaction.

311. Furthermore, the following factor is worth noting, as it can be exploited by terrorist threats as a whole:

Factors that are frequently exploited by threats	
Splitting of transactions and concerted actions	The **STRs** received in the sector are concentrated, from in a significant manner, in: i) **operations of splitting** below control thresholds, (ii) actions carried out by **individuals or concerted groups**, and iii) repeated exchange transactions at different establishments or at close succession. This pattern makes it more difficult to detect the illicit origin of the funds and requires operators to of recurring behaviour, particularly in outlets with high transaction volumes.

Geographical and concentration in high-risk areas	The sector's risk is heightened in certain environments, in particular: • tourist areas with high visitor numbers, • areas with a significant presence of at-risk groups, • locations close to international transport hubs. The location of establishments and the profile of their clientele have a significant influence on the level of threat, resulting in diverse risk scenarios within the sector itself.
Risk of infiltration or indirect control by criminal networks	FATF/MONEYVAL reports document cases in which currency exchange service providers have been infiltrated or controlled, either directly or indirectly, by criminal organisations, particularly in the case of or have weak governance structures.

Risk factors relating to inherent vulnerability

312. The following sets out the factors relating to inherent vulnerability analysed to determine the inherent risk in the currency exchange sector.

Characteristics of the sector	
Size of the sector and volume of turnover	The high turnover in the sector makes it an attractive venue for concealing ML and TF operations.
Level of complexity of the sector's structure	Although the core activity is straightforward and uniform (the buying and selling of foreign currency), the sector comprises a diverse range of operators, ranging from small independent outlets to organisations with multiple branches and a presence in various locations, particularly in tourist areas.
Level of integration with other regulated sectors	The currency exchange sector has a moderate level of integration with other regulated sectors, as, although it operates largely independently, it maintains limited links with financial institutions and payment service providers.
Level of the entity's location, including the geographical scope of the sector's operations	The location of certain establishments in high-risk areas and locations – either due to the significant presence of high-risk groups or the nature of the clientele's main commercial activity – can have a significant impact on the risk rating of the organisation's various premises.
Nature of the products and services provided by the sector	
Level derived from the complexity of the products, due to their impact on anonymity or the limited information available on customers.	The widespread use of cash in foreign exchange transactions entails an extremely high risk of these services being used for ML and TF. The gradual digitisation of payment methods, the growth of multi-currency payment solutions and the decline in the physical use of cash are helping to reduce the sector's vulnerability by enabling greater traceability and better analysis of transactions.

The extent to which specific products and services offered are linked to intelligence reports and/or national ML or TF investigations	Reports received on the basis of indications focus on transactions involving the splitting of amounts carried out by individuals or concerted groups of individuals in insignificant amounts.
Nature of the customer	
Level derived from the nature of the business relationship with customers, based on the duration (ongoing, transactional or occasional) and frequency of the transactions	Businesses with a high number of customers, generally with occasional relationships, and a high volume of transactions face greater difficulty in fully implementing ML/TF prevention measures and present more risk factors, which requires greater oversight and investment in human and material resources.
Level derived from the customer's status	The very nature of the currency exchange business makes it difficult to obtain adequate information about the customer and their profile. The large number of customers and transactions in the sector contributes to the existing ML/TF risk.
Level derived from the customer's occupation or type of business	The diversity of customers makes it difficult to define vulnerability in a uniform manner, as profiles with an apparent low risk coexist with others whose economic activity and intensive use of cash increase the likelihood of transactions linked to ML.
Geographical scope of the sector's activities	
Level derived from specific jurisdictions/countries of interest frequently associated with the sector.	Given Spain's profile as a tourist destination and the high influx of foreign customers from a wide variety of backgrounds, whose relationship with the institution is not long-term. The high turnover of non-resident customers and the frequent use of cash amplify the inherent risk associated with certain jurisdictions. However, international tourism provides a significant legitimate economic justification for a large part of the demand for currency exchange.
Level derived from the nature of the interactions or transactions that involve countries identified by the FATF.	The high number of foreign customers in Spain means there is a wide variety of sources of funds, which can be used to conceal ML and TF operations, particularly in cash transactions.
Level arising from the nature of interactions or transactions involving countries subject to international financial sanctions.	The PF SRA included as a threat the management of overseas accounts by currency exchange bureaux (in the name of front companies carrying out sales on behalf of sanctioned entities) or Iranian professionals.
Nature of distribution channels	

A measure derived from the complexity of the channels, based on their impact on anonymity or on the limited information on customers.	The widespread use of cash in currency exchange transactions implies an increased vulnerability to the use of these services for ML/TF operations.
Level derived from the use of new technologies or payment methods.	The growing availability of electronic payment methods and applications that enable multi-currency payments helps to reduce risk due to the gradual decline in physical currency exchange transactions, which in turn enables businesses to better analyse and monitor transactions establishments.

Conclusion on the sector's inherent risk: High for both ML and TF

313. The currency exchange sector carries a high level of inherent risk due to the very nature of the activity. On the one hand, ML risk is high because of its close link to the movement of cash and the resulting difficulties in identifying its source, tracing it, its anonymity, ease of transport, etc., which make these transactions particularly attractive for such purposes. Exchanging illicit cash for another currency requires no specific planning, technical knowledge or experience for ML purposes. Furthermore, the typical TF schemes employed by jihadist threats often rely on cash due to the numerous advantages it offers. Subsequently, it is necessary to carry out a currency exchange transaction to convert the funds – obtained in local currencies through various collection systems – into internationally usable currencies.

Risk factors relating to the effective implementation (or lack thereof) of controls

314. Analysing residual risk requires an assessment of how existing controls are implemented within the sector and to what extent those controls are effective. The following section presents an analysis of the factors used to determine the residual risk in the currency exchange sector.

Risk factors relating to the effective implementation (or lack thereof) of controls	
Level of regulation of the sector	The sector is subject to comprehensive and detailed regulation, covering both prudential matters and the prevention of ML and TF.
Level of potential presence of unauthorised entities.	Entities are subject to authorisation and registration by the Banco de España. Controls are in place to prevent unauthorised entities or individuals from operating in the sector; however, unauthorised currency exchange practices have been detected in certain geographical areas.
Level of potential direct or indirect control over the entity or its management by ML networks[79]	The regulations already require control measures in this regard. However, in the case of small-scale currency exchange businesses, the potential for management or control of management – even if indirect – with the aim of carrying out ML and TF activities, poses a risk that must be taken into account.

Level of regulation of ML/TF prevention measures	Entities in the sector are regulated entities in relation to the prevention of ML and TF and are also subject to enhanced customer due diligence obligations.
Level of supervision	The sector is subject to supervision by the Banco de España, and inspections have been carried out in relation to the prevention of ML and TF. Between 2020 and 2025, seven inspections of the sector.
Level of sanctions imposed on entities in the sector.	During the period analysed, six breaches against the sector, all of which were serious.
Level of professionalism of the organisation's directors and senior managers of the organisation.	Awareness and commitment amongst organisations in the sector and their administrators and managers have increased substantially in recent years. However, this must be regarded as uneven across the various organisations operating in the sector.
Level of awareness and understanding of their obligations regarding the prevention of ML and TF[80].	There are legal obligations regarding the existence and dissemination of manuals setting out internal policies and procedures. Inspections by supervisory bodies have found that the dissemination of, and employees' level of understanding of, AML/CFT matters varies greatly depending on the type and size of the institution.
Level of the institution's commitment to ML/TF policies and measures.	Awareness and commitment amongst organisations in the sector, as well as amongst their administrators and senior managers, have increased substantially in recent years. However, this varies considerably amongst the different organisations operating in the sector. Consequently, in cases where organisations do not apply anti-money laundering (AML) and counter-terrorist financing (CFT) measures very rigorously, they become highly vulnerable to being used in ML and TF operations. The sector's total turnover, when compared with the number of tourists visiting our country each year (around 90 million), reduces the risk that the foreign currency exchanged in our country.
Level of professional qualifications of employees and their training in ML/TF prevention.	Generally speaking, and particularly in recent years, the professional qualifications of employees in the sector regarding prevention have improved significantly. However, the scale of the commercial network and the large number of employees who require specific qualifications due to having responsibilities in the area of prevention are areas for improvement that affect the level of risk of the sector being used for ML/TF purposes.
Level of internal monitoring by organisations of employee compliance[81].	Although there are legal obligations in this regard and there is growing scrutiny within the sector regarding employees' conduct, the level of monitoring of staff in some organisations leaves much room for improvement, as they are afforded a significant degree of freedom of action, which has a significant impact on risks.
Level of compliance with preventive measures obligations,	Entities in the sector are regulated entities in relation to ML/TF and, in addition, have enhanced CDD obligations.

[79] This variable was rated as medium-substantial
[80] This variable was rated as medium-substantial
[81] This variable was rated as medium-substantial

In particular CDD/KYC	
Level of identification and reporting of suspicious transaction reports	In Spain, there appears to be no problem with participation in ML networks. The implementation of anti-ML measures, as evidenced by the reports received on the basis of indications, and the low number of individuals linked to major organised crime groups or terrorist financing networks, reduce the risk. In 2024, a very significant increase was observed, reaching 112 reports, followed by a slight reduction in 2025 to 89 reports, which demonstrates a notable improvement in the detection and reporting of suspicious transactions by the sector in recent years. The average rating for the significance of reports based on indications for the period 2022–2025 was 4.58. This category, introduced in 2021, allows the relative importance of reports to be assessed based on their link to factors such as the connection to serious crimes, the emergence of new types of risk, the detection of criminal structures or networks and/or the involvement of large sums of money.

Conclusion on the sector's residual risk: Substantial for ML and TF

315. Regulatory requirements for licensing and registration, the monitoring of their activities by the Banco de España, growing technological development, compliance with a strengthened customer due diligence regime, and the sector's institutions' high level of awareness of their ML/TF prevention obligations and their supervision by SEPBLAC mean that the level of residual risk is gradually decreasing, although it is still considered **substantial** for both ML and TF.

Sector: Postal Money Orders 2026

Activity and context

316. Postal service providers involved in money transfer activities are regulated entities under Article 2.1(j) of Law 10/2010 of 28 April.

317. A postal money order is a service that allows payment orders to be sent to individuals or companies on behalf of another person using the postal network. In accordance with current regulations, this service constitutes a financial service of general economic interest and must be provided, directly or indirectly, by the operator designated by the State to provide the universal postal service.

318. In Spain, the only postal operator authorised to perform this function is the state-owned company Correos y Telégrafos, S.A. (CORREOS), which provides this service in accordance with the provisions of Law 43/2010 of 30 December on the universal postal service, as amended by Law 6/2025 of 28 July, as well as the Postal Services Regulations, approved by Royal Decree 437/2024. This service can be used both within Spain and internationally, and payments can be made in cash or by cheque. However, payments to current accounts are only permitted within Spain, with a limit of 2,500 euros on the amounts sent.

319. Unlike banks or payment institutions, which also process transfers, the provision of the postal money order service by CORREOS does not confer on the latter the status of a financial institution for the purposes of Law 10/2010. However, it is included amongst the obliged entities and must therefore comply with all the obligations relating to the prevention of ML and TF established by that Law and its Regulations in relation to that service.

320. In addition, CORREOS provides a service relating to the sale of prepaid cards (Mastercard) in various forms, in which, notwithstanding its involvement in certain aspects of the process such as registration or top-ups—which may be carried out online or through its network of branches (approximately 2,400)— the applicable due diligence measures and controls are ultimately the responsibility of the issuing entities, with CORREOS applying due diligence measures on their behalf. The figures presented by CORREOS demonstrate the residual nature of the use of this service. As regards international payments, in 2025 these amounted to 4,298 transactions totalling nearly 1.6 million euros. International money order receipts totalled 16,815 transactions amounting to over 2.6 million euros.

321. As for domestic operations, payments in 2025 totalled 251,579 transactions with a total value of 42.5 million euros. Domestic money order receipts totalled 376,842 transactions with a total volume of funds of almost 106 million euros. Furthermore, according to confidential information, Correos' turnover amounted to 1,986 million euros in the 2024 financial year, a figure that encompasses all its postal, parcel and courier services, including postal money orders, which specifically constitute an area of activity subject to anti-money laundering legislation. Both services are designed to facilitate basic financial transactions for the entire population, including areas with limited access to banking services.

Threats

322. The postal money order sector presents a range of moderate threats in relation to ML and TF, stemming primarily from its intensive use of cash, occasional transactions without a bank account, and its focus on underbanked groups, including certain segments of the migrant population.

323. Postal money orders have occasionally featured in investigations relating to: illicit remittances, certain organised crime schemes, and irregular cash flows. The small number of reports based on suspicious activity recorded in recent years reflects both the declining use of the service and the existence of residual threats that require ongoing monitoring.

324. The threat of TF associated with postal money orders is considered to be contained, given that: the service is provided in person and is not anonymous; the sender and recipient are identified; and geographical restrictions have been implemented, such as the suspension of transfers to countries in the Middle East from March 2026. However, residual use in fragmented micro-financing schemes – typical of certain types of TF – cannot be completely ruled out.

325. Furthermore, it is worth highlighting the following factors that could be exploited by threats in the postal money order sector, in line with the activities analysed in this report:

Factors that are frequently exploited by threats	
Use of money orders as a channel for depositing cash	The sector's greatest exposure lies in the use of money orders as a mechanism for placing cash, given that this allows: the transfer of funds without the need for a prior banking relationship; the carrying out of one-off, non-recurring transactions; the use of cash as the primary means of payment; or the absence of an associated account in certain schemes. These characteristics mean that the risk lies primarily in the placement stage of money laundering, although the amount limits (€2,500) and the in-person nature of the service restrict its use to smaller-scale schemes.
Splitting of transactions and repeated transfers	The sector presents an exposure factor associated with the splitting of transfers, consisting of: multiple low- or medium-value money orders, all made by the same payer or by various pre-arranged senders, all destined for the same person or geographical area. This pattern can be used to make it more difficult to detect the actual volume of funds transferred, although its effectiveness is limited by the relatively high cost of the service compared with other remittance systems.
Cross-border transactions to high-risk jurisdictions	The service's international operations – particularly in relation to transfers directed at: countries of origin of migrant communities residing in Spain, jurisdictions with lower levels of banking penetration, and countries with varying degrees of maturity in their AML/CFT systems – represent a risk exposure for the postal money transfer sector. Although the aggregate volume sent to high-risk jurisdictions identified by the FATF is low, the dispersion of individual transfers may allow for the occasional use of the service for ML purposes, particularly in the absence of banking alternatives at the destination.

Use of the service by occasional and under-banked customers	The typical customer base of the postal money transfer sector consists mainly of: individuals, occasional users, and groups with limited access to or familiarity with banking or digital services. This profile limits ongoing customer knowledge and makes it difficult to build risk profiles based on historical behaviour, thereby increasing vulnerability to one-off uses for illicit purposes.

Risk factors due to inherent vulnerability

326. The following sets out the factors relating to inherent vulnerability analysed to determine the inherent risk in the postal money transfer sector:

Sector characteristics	
Size of the sector and volume of business	A single regulated entity (CORREOS) but an extensive national and international operational network. Turnover in 2024 stood at 1,986 million euros.
Level of complexity of the sector's structure	A centralised public body; the complexity stems from the extensive territorial and operational network.
Level of integration with other regulated sectors	Operates as the sole provider of this type of service.
Location of the organisation, including the geographical scope of the sector's operations	With the exception of branches in areas considered to be at risk of TF, such as Ceuta, Melilla or certain neighbourhoods in Catalonia – where there is a more significant presence of groups from countries linked to jihadist terrorism – the scope of operations covers areas with limited access to banking services.
Nature of the products and services provided by the sector	
Level determined by the complexity of the products, due to their impact on anonymity or the limited information available on customers.	Cash transactions not recorded in an account, albeit involving low to medium amounts. With regard to similar international payments, remittances totalled 12,207 million euros in 2025; consequently, international money transfers represent a negligible percentage, amounting to approximately 1.6 million euros in 2025.
A level at which specific products and services offered are linked to intelligence-based communications and/or national ML or TF	They feature in ML/TF investigations, illicit remittances and organised criminal networks.
Nature of the customer	
Level derived from the nature of the business relationship with customers, based on duration (ongoing, transactional or occasional)	Typically an occasional customer; non-recurring transactions.

and frequency of transactions	
Level derived from the customer's status	Presence of individual customers with limited access to banking services and/or unfamiliar with digital banking, and in sparsely populated areas. The high number of migrants in Spain results in a diverse range of payers and beneficiaries, which makes it possible to disguise ML transactions amongst the remittances sent by these migrants to their countries of origin. However, there is a downward trend in the use of the product: whilst transactions processed in 2020 totalled more than 325,000, by 2025 this figure will barely exceed 16,000. As for payments from Spain, the trend is the same: from more than 13,000 in 2020, the figure has fallen to just over 4,000.
Level derived from employment status or type of client's business	Wide variety of user profiles. Heavy usage by the migrant population.
Geographical scope of the sector's activities	
Level derived from specific jurisdictions/countries of interest frequently related to the sector.	The postal money order service is geographically exposed, as it handles cross-border transfers, particularly to the countries of origin of migrant communities residing in Spain. These jurisdictions may include emerging economies or countries with lower levels of banking penetration and varying levels of maturity in their ML prevention systems, which increases the potential risk of misuse of the service.
Level derived from the nature of interactions or transactions involving countries identified by the FATF.	Postal money orders are more expensive than remittances channelled through payment service providers, particularly for small amounts. This higher cost reduces their commercial appeal, but does not eliminate their exposure to ML risks, as they continue to be used by underbanked customers who send funds to these high-risk countries.
Level derived from the nature of interactions or transactions involving countries subject to financial.	There is no evidence of direct transfers to countries subject to international financial sanctions. Furthermore, the service is more expensive than other financial remittance services, which makes its use for transfers via intermediary jurisdictions with the aim of circumventing controls more complex. Currently, since 30 March, the provision of this service to countries in the Middle East has been suspended.
Nature of the distribution channels	
Level derived from the complexity of the channels due to their impact on anonymity or the limited information available on customers.	The money order service involves a high level of cash transactions, without the need for an account, and is highly susceptible to anonymity and the splitting of payments. The financial service is provided exclusively in person. Correos has an extensive network of branches for processing postal money orders.
Level derived from the use of new technologies or payment methods.	Money orders must be made in cash, in person and at the offices of the operator authorised to do so.

Conclusion on the sector's inherent risk: medium for ML and TF

327. The postal money order service presents a **medium** level of inherent ML/TF risk, due mainly to its intensive use of cash, the possibility of splitting transactions and the presence of occasional customers, combined with cross-border operations and potential use by the underbanked and migrant populations. However, the cost of the financial service and the fact that it is provided in person mean that the risk associated with the service is not as high as in the case of remittance transfers.

Risk factors relating to the effective implementation (or lack thereof) of controls

328. To analyse residual risk, it is necessary to assess the implementation of existing controls within the sector and the extent to which these controls are effective. The following section presents an analysis of the factors used to determine the residual risk in the postal money order sector.

Risk factors relating to the effective implementation (or lack thereof) of controls	
Level of regulation in the sector	Specific regulations governing the postal service, subject to Law 10/2010 of 28 April, on AML/CFT.
Extent to which unauthorised entities may be operating operate.	Only CORREOS is authorised to handle postal money orders.
Level of potential direct or indirect control over the organisation or its management by money laundering networks	CORREOS has a centralised organisational structure, formal internal controls and is subject to public supervision and specific regulations, which significantly reduces the possibility of direct or indirect control by Money Laundering networks. The management of the postal order service is highly standardised, with defined processes, segregation of duties and little scope for individual discretion.
Level of regulation of ML/TF prevention measures	Regulated entity under Law 10/2010 of 28 April and Royal Decree 304/2014.
Level of supervision	Supervision by SEPBLAC regarding compliance with the obligations of AML/CFT and SEPI in general.
Level of sanctions imposed on entities in the sector.	Given the nature of the sector, there is a low incidence of in the past.
Level of professionalism of the organisation's directors and senior managers.	Although CORREOS is not subject to a specific financial 'commercial and professional good standing' regime, the organisation's senior executives are subject to suitability and good standing checks in accordance with public sector regulations, alongside controls relating to transparency, conflicts of interest and institutional supervision. This framework significantly reduces the risk arising from a lack of professionalism or integrity amongst senior management.
Level of awareness and understanding of its ML/TF prevention obligations.	The postal money order service is provided through an operator (CORREOS) with an extensive network of branches, staffed by customer service personnel who are not specialised in financial services, whose level of knowledge and practical understanding of prevention obligations may be vary. There are legal obligations regarding the existence and dissemination of manuals setting out internal policies and procedures.

The organisation's level of commitment to the ML/TF policies and measures.	CORREOS is subject to the obligation to have its ML/TF prevention system reviewed annually by an external expert, in accordance with Article 28 of Royal Decree 304/2014.
Level of professional qualification of employees and their training in ML/TF prevention.	Increasing training. In recent years, there has been a significant improvement in the professional qualifications of staff in the area of AML/CFT.
Level of internal monitoring by organisations of employees' compliance employees.	The level of monitoring of employees (excluding agents) by the organisation is adequate.
Level of compliance with obligations regarding preventive measures, particularly CDD/KYC	As money transfer operations are occasional and non-relational, there are limitations on obtaining detailed information about the sender, and they are exposed to schemes designed to conceal the sender's identity. However, the strict application of CDD/KYC measures to all transactions, without thresholds, ensures a high level of compliance. Furthermore, the high percentage of the population in Spain with a bank account (98 %) and the relatively high cost of the service act as a deterrent to its use for money laundering purposes, reducing its appeal for illicit schemes. Figures on the volume of money orders in Spain show that their use is marginal.
Level of identification and reporting of suspicious transaction reports	The number of reports per year reflects the use of the service, falling from 4 in 2021 to 3 in 2024 and 1 in 2025. The average rating for the relevance of reports by indicator for the period 2022–2025 was 5.3. This category, introduced in 2021, allows the relative importance of reports to be assessed based on their link to factors such as the connection to serious crimes, the emergence of new types of risk, the detection of criminal structures or networks and/or the involvement of large sums of money.

Conclusion on the sector's residual risk: low for ML and TF

329. The provision of the service by a single public operator, specific regulations, and the requirement to establish procedures relating to AML/CFT all contribute to a substantial reduction in the sector's risk profile. Furthermore, the high proportion of the population with access to banking services, the proliferation of financial services offering low-cost, digital international transfers, and the provision of this service by a single operator all help to mitigate the initial risk identified.

Sector: Financial Credit Institutions (CIs) and Lenders other than credit institutions, CIs and credit intermediaries 2026

Activity and context

330. Financial Credit Institutions (FCIs) and lenders other than credit institutions, CIs and credit intermediaries are obliged entities under Article 2.1(k) of Law 10/2010 of 28 April.

331. Under Spanish law, the professional granting of credit is not a reserved activity; in other words, it may constitute a professional activity validly carried out by any natural or legal person without the need for prior authorisation or a licence. Consequently, although it is most commonly carried out by credit institutions, there are individuals and entities which, without being classified as such, engage on a professional basis in one or more of the following credit transactions: granting loans, consumer credit, mortgage credit, financing of commercial transactions, granting guarantees, leasing (financial leasing with an option to purchase), reverse mortgages, factoring (the assignment of a portfolio of loans) and ancillary activities to ensure the administration and financing of the loans assigned to them.

(i) Financial Credit Institutions (FCIs).

332. Outside the scope of credit institutions, lenders that meet the legally prescribed requirements may obtain a licence to operate as Financial Credit Institutions (FCIs). These are institutions which, subject to administrative authorisation, may also carry out the credit activities included in their authorised programme of activities. The authorisation process for FCIs is subject to the same *'fit* and proper' checks and shareholder suitability requirements as credit institutions. In particular, it requires SEPBLAC to issue a preliminary report on the adequacy of the ML and TF bodies and procedures that the applicant intends to implement should authorisation be granted.

333. Similarly, the regulations impose very strict requirements for the conduct of business: incorporation as a public limited company with registered shares, a minimum capital of 5 million euros, the suitability of holders of significant shareholdings, commercial and professional integrity, statutory restrictions on its corporate purpose to the activities specific to an FCI unless authorised as a hybrid institution, internal control procedures, etc.

334. Following their registration in the Commercial Register, FCIs must be entered in the Banco de España's Special Register of FCIs; these entries are published in the Official State Gazette (BOE). Once incorporated, they come under the prudential supervision of the Banco de España and are subject to a regime similar to that of banks, particularly with regard to solvency, conduct and accounting, but also in relation to regulations on significant shareholdings, suitability and incompatibility, the registration of senior officers, corporate governance and remuneration policy.

335. As at December 2025, according to SEPBLAC data, the FCI sector comprised 22 FCIs and 9 hybrid FCIs – that is, those authorised to provide payment services (FCI-EP) – meaning that, in addition to special authorisations from Banco de España and SEPBLAC, they are also subject to the regulations applicable to such institutions. The data available for the 22 FCIs show a significant aggregate

of activity, with a total balance sheet of 53,395 million euros and gross lending to customers amounting to 53,430 million euros. The FCIs also report own funds of 5,884 million euros, a net interest income of 1,838 million euros and a net profit of 338 million euros.

336. Virtually all FCIs are registered as members of the National Association of Credit Institutions (ASNEF). This organisation acts as a liaison between financial institutions specialising in consumer finance and public authorities, as well as other professional associations and users of their financial products. It also provides guidance and organises events on security in the conduct of its activities (personal data, cybersecurity, prevention of ML and TF, amongst others).

(ii) Lenders other than credit institutions, financial credit institutions and credit intermediaries.

337. As it is not subject to a licence requirement, the activity of granting loans may also be carried out by lenders other than credit institutions or credit finance companies. These are natural or legal persons who grant direct financing to third parties within the national territory. Unlike other lenders (for example, in the field of consumer credit), those operating in the provision of mortgage credit are subject to entry requirements and a supervisory regime set out in Directive 2014/17/EU, which Law 5/2019 of 15 March, which regulates mortgage credit agreements, transposes into Spanish law, and which aims to ensure, at European level, a higher standard of accountability on the part of these entities in their dealings with borrowers.

338. Under this framework, in order to operate, they must be registered in a public register of the relevant Autonomous Community, in the case of professionals operating exclusively with borrowers domiciled within the territory of a single Autonomous Community, provided that their head office is located there, or in the register maintained by the Banco de España in all other cases. In the latter case, there are currently 981 entities registered. In both cases, they must appoint a representative to SEPBLAC. There are no registration requirements for other professional lenders.

Threats

339. The lending services sector, comprising both Credit Institutions (FCIs) and other non-bank lenders, presents a range of significant and distinct threats relating to Money Laundering (ML) and Terrorist Financing (TF), arising from the nature of credit products, their increasing digitalisation, the heterogeneity of the sector and the existence of operators outside a uniform prudential framework.

340. These threats are consistent with those identified in Chapter 4, particularly in relation to economic crimes and tax fraud, the use of credit as a mechanism for integrating illicit funds, shell companies, low-value, high-turnover products, and

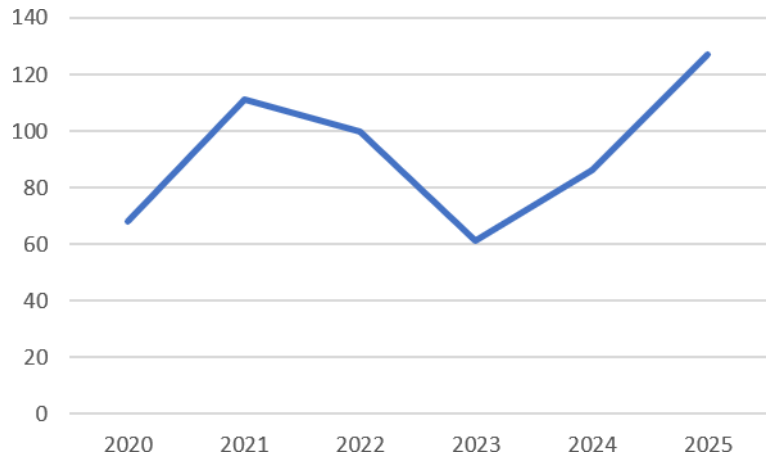
with a risk profile that varies between FCIs and non-FCI lenders.

Terrorist Financing

341. The threat of Terrorist Financing is lower than that posed by other direct money transfer services, but it is not non-existent. It manifests itself particularly in: small-value, fast-disbursement loans. Consequently, credit is used as an indirect source of financing, and there is a lack of consistent oversight of non-FCI lenders. Exposure to this threat is more significant in unsupervised or lightly regulated segments.

342. This has been detected by the LEAs both abroad (in connection with the attack on the Jewish supermarket in Paris) and in Spain (Barcelona-Cambrils), where the financing was initiated through quick loans.

343. The trend in reports based on indications is shown in the following chart. The main predicate offence for which indications have been found is money laundering in general, followed by activities related to tax fraud. Operations linked to PEP, on the one hand, and drug trafficking, on the other, have also been identified.



Source: SEPBLAC

344. Furthermore, the following factor is worth noting, as it may be exploited by the threats as a whole:

Factors that are frequently exploited by threats	
The use of credit as a means of channelling illicit funds	The sector's main focus is on the use of loans as a mechanism for integrating and legitimising capital of illicit origin, through: (i) the application for loans by natural or legal persons with illicit funds, ii) the early or cancellation of the loan using funds of criminal sources, and iii) the use of the loan to justify increases in net worth. This use places the risk primarily in the stratification and integration phases of the ML, and is particularly relevant in consumer products, microcredit and quick loans.

Special-purpose corporate structures and economic fraud	The use of shell companies or newly established companies can facilitate financing without any real economic activity, divert the funds obtained to purposes other than those declared, or subsequently lead to situations of insolvency or bankruptcy. These patterns have been detected particularly in credit transactions linked to shell companies, commercial loans and secured financing, constituting a recurring threat associated with organised economic crime.
Low-value, high-turnover and fast-disbursement products	Microcredits, instant consumer credit and deferred payment models introduce a specific risk factor associated with: i) a high volume of low-value transactions, ii) rapid approval and disbursement, iii) less in-depth customer analysis, and/or iv) difficulty in detecting aggregate patterns. This environment facilitates 'smurfing' techniques and reduces the effective traceability of financial flows.
Digitalisation, remote channels and accelerated verification	The expansion of credit granting via digital channels increases exposure to threats due to: remote identification, insufficient or falsified documentation, incomplete profiles or synthetic identities, and automated decision-making with limited real-time controls. This level of exposure is particularly relevant in business models focused on speed and scalability.
Cross-border exposure and cash flows	Although the business is predominantly domestic, there is a degree of exposure to threats due to: customers with financial links in third countries, cross-border cash movements, and schemes such as 'cash *couriers'* identified by the FATF. These factors increase the complexity of verifying the source of funds, particularly in loan repayment transactions.

Risk factors relating to inherent vulnerability

345. The following sets out the factors relating to inherent vulnerability analysed to determine the inherent risk in the FCI sector and among lenders other than credit institutions, FCIs and credit intermediaries.

Sector characteristics	
Size of the sector and turnover	The segment comprises a large number of players: formally registered FCIs and an unknown number of non-bank lenders and digital platforms not subject to mandatory registration. According to ASNEF (Dec. 2025), demand for credit reached historic highs in the final quarter of 2025 across all sub-segments (consumer, microfinance, automotive, platforms *"Buy Now,Pay Later*) (BNPL). This growth was driven by the moderation of the inflation and expectations of interest rate cuts helped to drive a recovery in consumption and consumer credit.

	Furthermore, digitalisation and the expansion of new operators facilitated easier access to finance, whilst the improvement in the risk profile and the reduction in non-performing loans encouraged banks to increase their lending activity. This significant increase in business volume raises the risk of misuse for ML and TF.
Level of complexity of the sector's structure	The ecosystem comprises FCIs integrated into banking groups, credit fintech firms, BNPL platforms, private lenders and EMI providers offering complementary services. Fifty % of FCIs' lending is carried out by subsidiaries of credit institutions, and 86 % of pension fund assets are channelled through affiliated entities. This heterogeneity creates multiple layers of ownership and structures that are difficult to supervise.
Level of integration with other regulated sectors	FCIs and lenders are integrated with credit institutions, payment institutions and fund managers, which entails sharing risks – including the channels used by criminals within the financial system – and increases the scope of exposure, as any failure in one entity can spread to another, potentially leading, for example, to operational and/or reputational contagion.
Level of the institution's location, including the geographical scope of the sector's operations	The sector operates throughout the country, supplemented by occasional cross-border operations.
Nature of the products and services provided by the sector	
Level derived from the complexity of the products, based on their impact on anonymity or limited customer information.	The risk stems mainly from the granting of credit through digital and standardised processes, which may involve less direct interaction with the customer and a high degree of reliance on automated information sources. Although the use of cash is limited and operations are highly traceable, the speed with which credit is granted and commercial pressure may reduce the depth of customer knowledge and hinder the early detection of misuse of the credit product. The use of cash to repay loans, including early repayments, would indicate the presence of risk. Payments from abroad or repayments made by third parties should trigger alerts.
Level at which specific products and services offered are linked in Communications as indication and/or national ML or TF investigations	FCIs and non-bank lenders are appearing with increasing frequency in analyses of suspicious transactions linked to consumer products, commercial defaults and informal financing. However, their incidence is lower than that of other products such as bank transfers and deposits. There were 127 reports based on indications in 2025 (FCIs, mortgage and non-mortgage loans), representing a marginal percentage of the total number of reports. There were no indirect reports from other sectors with regard to those identified
Nature of the client	
Level derived from the nature of the business relationship with customers	The existence of loans of a very diverse nature and the existence of different lending institutions with varying levels of control affect the existing ML/TF risk. Long-term loans and

depending on the duration (continuous, transactional or occasional) and the frequency of transactions	intensive transactional relationships in microcredit and BNPL make it difficult to maintain adequate and continuous monitoring. High-turnover cycles require exhaustive monitoring.
Level derived from the customer's status	The high volume of transactions and the presence of communities of foreign residents and legal entities incorporated in third countries may mean that certain credit transactions are vulnerable to being used to conceal ML/TF operations, taking advantage of the greater difficulties faced by institutions and individuals in the sector when it comes to implementing ML/TF prevention measures, identifying the source of funds being repaid, or determining the true beneficial owner of the transaction.
Level derived from the client's occupation or type of business	Sectors with high levels of debt (manufacturing, consumer goods, automotive, retail) have a higher concentration of debtors according to ASNEF. Certain economic activities present a inherent opacity.
Geographical scope of the sector's activities	
Level derived from specific jurisdictions or countries of interest that are frequently associated with the sector.	Entities in the sector operate mainly within Spanish territory.
A level derived from the nature of the interactions or transactions involving countries identified by the FATF.	Exposure to risk is thought to be linked to credit applications made by nationals of high-risk jurisdictions. Microcredit-related products present the greatest risks in relation to this factor.
A level derived from the nature of the interactions or transactions involving countries subject to international financial sanctions.	Given the product's characteristics and the lack of evidence, the risk is considered to be low.
Nature of the distribution channels	
Level derived from the complexity of the channels due to their impact on anonymity or the limited information available on customers.	Increasing use of digital channels in the credit granting process. Risks associated with remote identification procedures.
Level derived from the use of new technologies or payment methods.	There is no evidence of the use of crypto-assets in this sector. However, there may be operations involving Fintech intermediaries in the processing.

Conclusion on the sector's inherent risk: medium/substantial in ML and TF

346. With regard to the ML, for FCIs it is considered **medium/substantial** due to the diversity and complexity of credit products, the potential for misuse during the integration/stratification phases, and the presence of customers with diverse economic profiles and risk levels. Repayments made in cash, which may be made in advance, constitute a risk factor in the sector.

347. For non-FCI lenders, the risk is **substantial**, due to the heterogeneity of the sector and the absence, in many cases, of registration requirements, supervision or uniform due diligence standards. This segment includes digital micro-lenders, BNPL platforms, private lenders and online operators with very rapid onboarding processes and minimal verification, which increases the risk of operational anonymity and facilitates techniques such as *smurfing*, the simulation of economic activity or the use of loans as a mechanism for placing or integrating illicit funds. Products characterised by high turnover and low unit values, combined with fast-operating digital models, substantially increase the sector's inherent exposure.

348. With regard to TF, the FCIs face a **medium/substantial** inherent risk, arising from the fact that credit products may be used to obtain funds that are subsequently diverted to illicit activities. There is evidence of such indications in investigations carried out by the LEAs (see section 12 on threats).

349. For non-FCI lenders, the risk is **medium/substantial**, as the speed of the lending processes, the lack of standardised controls, the fact that some models operate 100 % digitally, and the low level of documentation required increase the likelihood that these products will be used to obtain funds which are subsequently transferred (either directly or via third parties) to terrorist organisations.

Risk factors relating to the effective implementation (or lack thereof) of controls

350. Analysing residual risk requires an assessment of how existing controls are implemented within the sector and to what extent those controls are effective. The following section presents an analysis of the factors used to determine the residual risk in the loan services sector provided by FCIs and lenders other than credit institutions, FCIs and credit intermediaries.

Risk factors relating to the effective (or lack of) implementation of controls	
Level of regulation in the sector	The regulatory framework covers FCIs, intermediaries and lenders providing mortgage and consumer credit (Law 10/2010, Law 5/2019, Law 2/2009). However, many digital lenders and BNPL platforms operate without mandatory registration. A significant regulatory gap remains.
Level of potential presence of unauthorised entities to operate.	The presence of informal lenders and unregistered platforms that may be used by ML/TF networks has been identified.
Level of potential direct or indirect control over the entity or its management by the ML networks[82].	The uneven situation in the sector means that whilst the regulation of FCIs imposes entry requirements and operating conditions, as well as suitability criteria for applicants and their directors and managers, including commercial and professional integrity, the institutions and professionals who do not meet these criteria are also not subject to these checks on access to the profession.

Level of regulation of ML/TF prevention measures[83]	Entities in the lending sector, whether or not they are FCIs, are regulated entities in relation to ML/TF and are also subject to specific guidelines.
Level of supervision	Two inspections were carried out in 2021 by an external expert and one in 2024 covering a general scope, the main finding of which was the use of cash to repay loans without sufficient control or monitoring. Furthermore, the activities of authorised cardholders were not reported. In these organisations, the method of loan repayment is key; any use of funds where traceability is not guaranteed would increase the risk and the due diligence measures to be applied (cryptocurrency, international transfers, cash, etc.).
Level of sanctions imposed on institutions in the sector.	During the period analysed, no administrative sanctions were imposed, but two FCIs were issued with requests to remedy the following deficiencies: CDD obligations, document retention, reporting obligations, the establishment of internal control bodies and/or procedures, training, improvements to the External Expert's report, improvements to human and technical resources, and the appointment of a representative to SEPBLAC. In total, there were 11 areas for improvement across the two institutions.
Level of the professionalism of managers and senior managers of the organisation.	FCIs possess a high level of technical expertise. In 'Fintech' and informal lenders, there are gaps in this knowledge.
Level of awareness and understanding of their obligations regarding ML and TF.	There are legal obligations in this regard, and the FCI sector association (ASNEF) is actively engaged in raising awareness and providing information on this matter. However, the level of awareness within the sector varies, particularly amongst lenders that are not FCIs and do not have an association to carry out these awareness-raising and information-sharing functions.
Level of the organisation's commitment to policies and measures for AML/TF.	A greater level of commitment is observed amongst FCIs. However, other lenders have a lower level of preventive awareness. In line with the above risk, the work carried out by ASNEF in raising preventative awareness within the sector is noteworthy.
Level of professional qualifications of employees and their training in prevention of ML and TF.	Qualifications have improved significantly, but cannot be considered fully satisfactory, and the scale of commercial networks means that training remains an area for improvement.
Level of internal monitoring by organisations of staff compliance.	Formal control procedures are in place, but inspections have revealed that they are not always adequate.

[82] This variable was rated as medium-substantial
[83] This variable was rated as medium-low.

Level of compliance with obligations regarding preventive measures, in particular CDD/KYC	The regulatory framework is robust and institutions generally apply formal identification, verification of beneficial owners, periodic updating and risk-based segmentation. However, there remain areas for improvement relating to the extent of commercial networks, the complexity of the customer base, the updating of old files and the need to strengthen staff training and internal monitoring. An inspection carried out in 2024 at an FCI confirmed structural shortcomings in KYC and ongoing monitoring (7.4 % of customers had expired documentation). 100 % of the sample lacked comprehensive and systematic monitoring, with a failure to update customer knowledge and a failure to verify the economic activity of authorised parties. Furthermore, the institution confused the source of funds with financial capacity; it classified only 90 customers as high risk despite having thousands of customers making significant cash payments. In addition, only 64 customers were subject to enhanced due diligence despite clear risk indicators, and for 98 % of the sample, the source of funds had not been verified in advance payments.
Level of identification and reporting of suspicious transaction reports	NRA statistics show a sustained increase in reports from financial institutions, a breakdown by type of predicate offence, and a growing involvement of non-financial entities. The system for reporting on the basis of indications is operational and functional, although it is not uniform across sub-sectors. Differences in detection capacity are observed, linked to the type of activity and operational volume. The role of financial institutions and mortgage lenders in reporting suspicious transactions is particularly noteworthy. The average rating for the significance of reports based on indications for the period 2022–2025 was 6.4. This category, introduced in 2021, allows the relative importance of reports to be assessed based on their link to factors such as the connection to serious crimes, the emergence of new types of risk, the detection of criminal structures or networks, and/or the existence of.

Conclusion on the sector's residual risk: medium for FCIs in ML and medium-substantial for non-FCI lenders and FCIs in TF

351. With regard to ML, for FCIs, the stringent regime governing access to and the conduct of the business, their financial links with banks, and the gradual improvement in their preventive framework mean that the residual ML risk is assessed as **medium**. However, for lenders that are not FCIs, structural threats persist (unauthorised entities, regulatory gaps in *Fintech* and BNPL) which, combined with the high complexity of technological channels and reduced oversight of service provision, result in a greater risk that such services may be used for ML by criminal networks or linked to the repayment of loans with illicit funds; consequently, the residual risk for these lenders is considered to be **medium/substantial**.

352. With regard to TF, the risk is considered to be **medium/substantial** due to the weight given to the threat identified in the investigations referred to in paragraph 12 of this factsheet. As for entities that carry out credit transactions without being classified as FCIs, the low traceability

in some transactions, the lack of controls regarding the purpose of the transaction and the beneficial owner create direct channels for TF, and small-value loans that are quickly disbursed expose these entities to a higher risk of TF, which is classified as **medium/substantial**.

Sector: Credit intermediaries 2026

Activity and context

353. Persons professionally engaged in credit intermediation are regulated under Article 2.1.k) of Law 10/2010, of 28 April.

354. Credit intermediation activities are carried out by natural or legal persons whose role is not to grant finance directly, but to act as intermediaries between the borrower and the entity granting the credit. Credit intermediaries are defined as professionals who, without being lenders themselves, offer credit agreements, advise on them or enter into them in the name and on behalf of a lender, always acting in a professional capacity.

355. This activity can be particularly useful for consumers, as it enables them to access the various financing options available on the market in a more efficient, comparable and transparent manner. Brokerage may take place in the fields of both consumer credit and mortgage lending, with each having its own legal framework governing its practice. Mortgage brokering (for residential properties) is a reserved activity and is regulated by Law 5/2019, of 15 March, on mortgage contracts, which sets out the requirements for entry into the sector, the conduct of business and supervision, and requires intermediaries to be compulsorily registered with the Banco de España's Register — which currently lists 963 registered intermediaries — or with the relevant regional register where their activity is limited to the territory of a single autonomous community.

356. Where the borrower is a consumer, and in respect of matters not directly covered by Law 5/2019, of 15 March, Law 2/2009, of 31 March, which regulates the contracting of mortgage loans or credits with consumers and intermediation services for the conclusion of loan or credit contracts, applies on a supplementary basis. Furthermore, in accordance with Royal Decree 106/2011, of 28 January, the following entities must be registered in the State Register of Mortgage Lending or Financial Intermediation Companies:

    - Non-banking firms that grant loans or mortgages to consumers.
    - Companies that act as intermediaries in the conclusion of loan or mortgage credit agreements (including those that broker, advise on or manage loan or mortgage credit transactions between consumers and lenders).
    - Companies operating in Spain but registered outside the country, provided they carry out these activities in Spain
    - Companies located in autonomous communities that have not established their own regional register (provisional registration).

357. Consumer credit intermediation is not a reserved activity and does not require registration in any specific register; it is governed by general consumer protection regulations and by obligations regarding transparency and pre-contractual information. Intermediaries may carry out their activities in association with a single lender or with several. Where advice is provided, this may be independent, which requires a greater scope of products analysed and stricter controls on potential conflicts of interest.

They may also operate in other EU Member States under the passporting regime, through a branch, a subsidiary or under the freedom to provide services.

Threats

358. The credit intermediary sector (ICC) presents a set of moderate threats in relation to ML and TF, stemming primarily from its intermediary position in the financing chain, its transactional nature, and the structural heterogeneity of the sector, which comprises a large number of operators of varying sizes and levels of organisational maturity. These threats correspond to the types identified in Chapter 4, particularly in relation to tax offences, the instrumental use of financing to give the appearance of legality to illicit funds, transactions involving complex legal entities, and indirect involvement in money laundering schemes in the stages prior to the granting of credit, although they are mitigated by the final involvement of financial institutions subject to high AML/CFT standards.

359. Historical intelligence reports from the sector show that **tax offences** are among the main predicate offences detected, alongside generic types of ML. This threat materialises when: the credit applied for does not correspond to the actual economic activity; there are significant inconsistencies in declared income; or a recurring use of credit to regularise undeclared cash flows is detected. Intermediation may facilitate the structuring of these transactions, particularly in non-mortgage segments, where the involvement of a notary does not act as an additional mitigating factor.

360. With regard to the threat of TF in the ICC sector, it is considered **very low**, as: there is no use of cash, direct payments are not processed, the activity is not geared towards international fund transfers, and transactions are executed and tracked by financial institutions. No significant patterns have been identified that structurally link credit intermediation with TF.

361. Furthermore, other factors that may be exploited by threats within the money remittance sector include:

Factors of exposure to threats	
Use of credit intermediation to justify illicit financial flows	A key factor that exposes the system to this threat is the use of credit intermediation as a mechanism to justify or channel funds of illicit origin, especially when: financing is requested with a declared financial capacity that is inconsistent; legal entities with complex corporate structures are involved; or intermediaries are used to give the transaction the appearance of technical neutrality. In these cases, credit intermediation can be used to provide an apparently legitimate financial narrative for transactions that conceal Money Laundering, particularly during the concealment or integration phase, even if the intermediary does not directly manage the funds.
Transactional relationships and lack of ongoing engagement	The sector faces a risk arising from the prevalence of occasional and transactional relationships, which: limits the gradual build-up of knowledge about the customer, reduces the ability to detect recurring patterns and concentrates the risk in one-off, higher-volume transactions. This profile increases vulnerability to sporadic use of the service for ML purposes, particularly where there are no ongoing relationships with lenders or repeat customers.

Involvement of legal entities and complex corporate structures	The sector is more exposed when the customer is a legal entity, particularly in the area of non-mortgage lending, and where the following factors are present: complex or multi-tiered corporate structures, newly established companies and intermediary vehicles with little actual activity. In such cases, intermediation can facilitate the channelling of funds into opaque structures, making it more difficult to identify the source of the funds and the beneficial owner, although this risk is mitigated by the controls put in place by the final lender.
Potential exploitation by money-laundering networks	In theory, as intermediation operates partly outside the traditional financial sector, it could prove attractive to money-laundering networks seeking to: recruit professionals as technical facilitators, indirectly influence the structuring of transactions, and exploit the diversity and fragmentation of the sector. However, intermediaries do not assume financial risk, do not manage funds and are dependent on the final approval of the loan by entities subject to AML/CFT controls.
Limited exposure to cross-border risks	The sector has a low level of international exposure, given that: most of its activity takes place in the domestic market; involvement by non-resident customers is sporadic; financial flows are ultimately channelled through national or European institutions; and transactions with jurisdictions of ML/TF concern are limited and are subject to enhanced scrutiny by lenders.

Risk factors relating to inherent vulnerability

362. The following sets out the factors relating to inherent vulnerability analysed to determine the inherent risk of the ICC sector.

Characteristics of the sector	
Size of the sector and turnover.	A fragmented sector with numerous operators. Turnover in 2024 totalled 6,436 million euros, of which 6,313 million was generated by organisations with a turnover of 2 million euros or more.
Level of complexity of the sector's structure.	A sector comprising operators specialising in brokering securing finance; and, in the property sector, chain-like structures involving intermediaries, lenders and financial institutions.

Level of integration with other regulated sectors.	ICCs interact regularly with banks and credit institutions, primarily to facilitate financing transactions.
Location of the organisation, including the geographical scope of the sector's.	Credit intermediaries operate throughout the country, with a significant proportion of operators active across multiple autonomous communities, as per their entry in the Banco de España's register. This geographical spread increases the volume and diversity of transactions, thereby increasing the complexity of control and supervision.

Nature of the products and services provided by the sector	
Level arising from the complexity of the products, due to their impact on anonymity or the limited information available on customers.	The product granted is registered in the customer's name, involving mediation between the borrower and the lender, whereby the customer is identified for the purpose of granting the credit. The final execution takes place at financial institutions subject to AML/CFT preventive measures under Law 10/2010, of 28 April.
The level at which the specific products and services offered are linked to intelligence reports and/or national ML or TF investigations.	Historically, there have been few tip-off communications in this sector. ML offences are linked to drug trafficking and PEP, and there has been an increase in communications relating to tax offences.
Nature of the customer	
Level derived from the nature of the business relationship with customers, based on the duration (ongoing, transactional or occasional) and frequency of transactions.	Transactional/occasional relationships with ICCs predominate. Ongoing relationships occur when there are recurring agreements or portfolios with entities.
Level derived from the customer's status.	Mortgage loan customers are usually individuals, occasionally foreign nationals. The risk is higher when the customer is a PEP or, primarily in the case of non-property loans, when legal entities with complex corporate structures are involved. In the case of foreign individuals, the transaction is usually carried out with the advice of solicitors.
Level derived from the client's occupation or type of business.	The activities declared by customers vary widely. The highest-risk customers are those with high liquidity, non-activities that are inconsistent with the credit applied for or when complex corporate structures are involved complex corporate structures.
Geographical scope of the sector's activities	
A level derived from specific jurisdictions/countries of interest that are frequently associated with the sector.	Limited international exposure, with isolated cases involving non-residents or funds linked to countries with weak controls. There is no evidence of operations involving countries posing a ML/TF risk.

Level derived from the nature of the interactions or transactions that involve countries identified by the FATF.	Possible economic relationships with third countries of interest, mitigated by the lender. No evidence of transactions involving countries listed by the FATF. Domestic activity in Spain involving national and regional operators.

Level derived from the nature of the interactions or transactions involving countries subject to financial.	Limited international exposure, with isolated cases involving non-residents or funds linked to countries with weak controls. There is no evidence of transactions involving countries subject to international financial sanctions.
Nature of the distribution channels	
Level derived from the complexity of the channels, given their impact on anonymity or the limited information available on customers.	Currently, online operations via credit intermediation platforms have increased. However, it should be borne in mind that the ultimate lender is, in most cases, a credit institution.
Level derived from the use of new technologies or payment methods.	No new technologies are used. Commission payments to credit intermediaries are usually made via the banking system. The loan is disbursed by the bank or FCI.

Conclusion on the sector's inherent risk: medium for ML and TF

363. The inherent risk of the ICC sector in relation to ML/TF is assessed as **medium**, mainly due to the sector's fragmented structure and the highly transactional nature of its activity, which is based largely on occasional relationships and the intermediation of financing transactions. These characteristics increase exposure to the misuse of the product for channelling or justifying financial flows. However, ICCs also have characteristics of their own, such as the registered nature of the products they broker, the final execution of transactions by financial institutions subject to high AML/CFT standards, limited international exposure, and the absence of distribution channels or technologies that increase anonymity; taken together, these factors justify the overall assessment of inherent risk as medium.

Risk factors relating to the effective implementation (or lack thereof) of controls

364. An analysis of residual risk requires an assessment of the implementation of existing controls within the sector and the extent to which those controls are effective. The following section presents an analysis of the factors used to determine the residual risk in the 'other services' sector provided by the ICC sector.

Risk factors relating to the effective implementation (or lack thereof) of controls	
Level of regulation in the sector.	Since 2019, ICCs have been subject to a specific state regulatory framework which has significantly strengthened the control and
	administrative supervision of the sector. Law 5/2019, of 15 March, and its implementing regulations have introduced standardised entry requirements, compulsory registration with the Banco de España and stricter requirements in matters relating to transparency, professional qualifications and internal organisation, thereby increasing the traceability of the activity.

Extent to which unauthorised entities may be operating	Whilst there may be instances of unauthorised practice in areas not covered by Law 5/2019, of 15 March, in the specific case of mortgage lending, the regulations require intermediaries to be registered with the Banco de España, which significantly restricts the operations of unauthorised entities and facilitates their detection.
Level of potential direct or indirect control of the entity or its management by money-laundering networks.	The activities of credit intermediaries fall partly outside the traditional financial sector, which may make them attractive for use by Money Laundering networks, particularly in relation to advisory services, the structuring of transactions or the channelling of funds. The absence of direct financial risk-taking and the fact that they do not manage funds reduce exposure; however, their involvement in the early stages of a transaction and the diversity of operators in the sector allow for potential indirect influence over management, which justifies a moderate.
Level of regulation of ML/TF prevention measures.	ICCs are regulated entities in relation to AML/TF under Law 10/2010, of 28 April.
Level of supervision.	SEPBLAC in relation to AML/CFT and the Banco de España/Autonomous Communities (Law 5/2019 of 15 March) with targeted actions, but no on-site inspections have been conducted in the sector.
Level of sanctions imposed on entities in the sector.	No sanctions were imposed on the sector during the period under review.
Level of professionalism of the organisation's directors and senior managers of the institution.	Credit intermediaries are subject to commercial and professional integrity requirements for registration with the Banco de España, which provides significant prior oversight of those run the business.
Level of awareness and understanding of their ML/TF obligations.	AML/CFT obligations are understood and staff receive regular training, although there is room for improvement in consistency across branches and agents.
The organisation's level of commitment to AML/CFT policies and measures	The level of commitment is not consistent across the sector, particularly amongst smaller operators, intermediary networks or business models with a high degree of commercial outsourcing.
Level of professional qualifications of staff and their training in ML/CFT prevention.	Varying levels; training required by Law 5/2019, of 15 March. Room for improvement in consistency across branches/agents.
Level of by the	Reliance on commercial networks, external agents or decentralized structures may make it difficult to continuously monitor

entities' monitoring of staff compliance.	the individual conduct of employees and intermediaries, particularly during stages such as customer onboarding, document verification or the detection of risk indicators. Furthermore, smaller organisations may face constraints in terms of resources, automation or internal control functions, thereby reducing the capacity for effective monitoring and periodic review of compliance.
Level of compliance with preventive measures, particularly AML/CFT and KYC.	The large number of customers in the sector, the existence of loans of a very diverse nature and the presence of different lending institutions with varying levels of control all contribute to the existing ML/TF risk. However, this can be indirectly mitigated by the execution of the loan by financial institutions and the notary's involvement in the case of mortgage loans.
Level of identification and reporting of suspicious transaction reports.	The sector has historically shown low volumes of reports based on indicators, although since 2023 the trend has been stable and in line with national risk threats such as tax offences. The average rating for the significance of reports based on indications for the period 2022–2025 was 5.68. This category, introduced in 2021, allows the relative importance of reports to be assessed based on their link to factors such as their connection to serious crimes, the emergence of new types of risk, the detection of criminal structures or networks, and/or the existence of large sums of money.

Conclusion on the sector's residual risk: low/medium for ML and low for TF

365. The residual ML risk in the ICC sector is **low/medium**: the existence of a specific regulatory framework since 2019, compulsory registration with the Banco de España, the requirements for good repute and professionalism, their status as obliged entities in relation to AML/CFT, as well as the final execution of transactions by financial institutions subject to high standards of control and, in the case of mortgages, the involvement of a notary, limit effective exposure to ML. Furthermore, the nature of the reports based on indications, in line with national threats, reinforces this assessment.

366. With regard to TF, the sector's activity takes place primarily within the domestic sphere, with limited international exposure and few links to jurisdictions or risk categories associated with Terrorist Financing. Furthermore, the high level of regulation to which the sector is subject and the limited evidence of criminal activity detected mean that the sector's risk is classified as **low.**

Sector: Property sector 2026

Activity and context

367. Property developers and those who professionally carry out agency, commission or brokerage activities in the sale or purchase of immovable property or in the letting of immovable property involving a transaction with a total annual rent of 120,000 euros or more, or a monthly rent of 10,000 euros or more, are obliged entities under Article 2.1.(l) of Law 10/2010, of 28 April.

368. Article 2.1.l) of Law 10/2010, of 28 April, lists property developers and those who professionally carry out agency, commission or brokerage activities in the sale and purchase of immovable property as regulated entities.

369. The activity of property development consists of the purchase and sale of land and buildings for the purposes of development, subdivision, construction and/or refurbishment, either directly or through third parties, with a view to their subsequent sale. A property agent is a professional who acts as an intermediary in a property transaction and who normally charges a commission (a percentage of the sale price). This role is regulated by Decree No. 3248/69, of 4 December 1969, which approves the Regulations of the Official Associations of Property Agents.

370. Both property development and agency, commission or brokerage activities relating to the sale and purchase of immovable property are unrestricted and may be carried out by any natural or legal person without any administrative requirements. In the case of estate agents, Article 3 of Law 10/2003, of 20 May, on Urgent Measures for Liberalisation in the Property and Transport Sectors distinguishes, on the one hand, between the activities carried out by estate agents in accordance with the professional qualification requirements set out in their own specific regulations, and, on the other hand, the activities of other natural and legal persons who are not required to hold any qualification or to be members of any official professional body.

371. There is no compulsory administrative register in Spain for property developers or intermediaries in the sale and purchase of immovable property. However, some autonomous communities have established a compulsory register of estate agents, such as Catalonia and the Valencian Community, or Andalusia (due to come into force in January 2026), whilst others have voluntary registers, such as Madrid, the Balearic Islands, the Canary Islands and Navarre, to protect buyers; and those with a limited scope, such as the Basque Country, which relates to accredited collaborating agents (a public rental brokerage programme promoted by the Basque Government).

372. According to data from the INE, in 2025 there were 111,425 entities with CNAE codes 411 (‘property development’) and 683 (‘property activities on behalf of third parties in Spain’), representing 91 % of those registered under these CNAE codes in 2020. Approximately 45 % of these entities are engaged in property development, with the remainder carrying out property activities on behalf of third parties.

373. In a detailed analysis of the sector, the number of entities carrying out actual economic activity linked to this category is much lower, given that only 8.4 % of the aforementioned economic agents (111,425, or 9,432 entities) report having more than two employees, and therefore have a minimal internal structure; this sub-segment comprises a group that has remained stable over time (4.3 % growth) since 2020.

These figures are similar to the number of regulated entities registered with SEPBLAC, estimated at 9,277 in 2025. The sector has an aggregate turnover of approximately 27,113 million euros, according to published data (SEPBLAC's 2024 Annual Report), which reflects the sector's relative importance in terms of economic activity compared with other sectors comprising non-financial regulated entities.

Threats

374. The property sector is one of the sectors traditionally most frequently exploited by criminal organisations for ML, given its capacity to absorb large volumes of funds, its role as a safe-haven asset, the lack of transparency resulting from the use of shell companies, and the ease with which illicit capital can be channelled through property purchases, renovations or rentals. These characteristics are fully in line with the main threats identified by the EU's Supranational Risk Analysis, which ranks the property sector as one of those most exposed to ML and, to a lesser extent, to TF, as there is no evidence of the sector being used for terrorist financing. Furthermore, recent trends detected by national FIUs, the LEAs, the AEAT and SEPBLAC show consistent use of the sector for channelling, concealing and integrating illicit funds through high-value property transactions, particularly in coastal areas and major urban centres.

Organised crime

375. The use of the property market by organised crime remains the main threat, given the possibility of channelling large sums into the formal economy, acquiring assets with appreciation potential and low risk, splitting payments via frontmen and shell companies, simulating renovations, or overvaluing or undervaluing prices. The patterns identified are consistent with practices described for other high-risk sectors, such as alternative payment mechanisms (*Hawala*), the use of complex corporate structures, bank mules and offsetting transactions. Networks originating in Latin America, Italy, the Netherlands, the Maghreb, Eastern Europe and Asia are responsible for much of this intensive use of property assets to consolidate illicit profits.

Drug trafficking

376. Drug trafficking generates massive volumes of illicit funds and uses the property sector as one of its main channels for laundering these funds, utilising properties for storage logistics or *indoor* cultivation. Both in specific areas such as the Campo de Gibraltar and in wider regions such as the Levante or the islands, local clans and members of international organisations are observed buying and renting properties for their own use or as a store of value.

Economic and financial crimes

377. Economic crimes pose a growing threat, particularly in the form of large-scale online fraud, Ponzi schemes, VAT fraud schemes and corporate fraud. Organisations committing these crimes resort to purchasing property to justify sudden increases in assets, to convert illicit profits into stable assets, and to carry out successive sales to generate the appearance of legitimate income.

The property sector is also linked to crypto-asset investment fraud, where some of the defrauded funds end up being used to acquire property either directly or through shell companies.

Corruption and offences committed abroad

378. Property investment is a common mechanism in cases of political and financial corruption, embezzlement, bribery, influence peddling and the misappropriation of public funds. Public officials or PEPs, whether national or foreign, turn to the Spanish property market — particularly luxury second homes — to conceal illicit income, split ownership through shell companies and register properties in the names of family members or frontmen.

Terrorist Financing

379. Although the property sector is not the primary channel for Terrorist Financing, the greatest threat arises from the use of properties for logistics and collaboration with terrorist organisations. The risk increases when buyers from jurisdictions where organisations linked to TF are present are involved.

380. In addition, the following factor, which may be exploited by these threats as a whole, is worth highlighting:

Factors that are frequently exploited by these threats	
International illicit flows and the use of complex corporate structures.	A key cross-cutting factor contributing to exposure to this threat is the use of *trusts*, foundations, *offshore* companies, and multi-tiered structures registered in multiple jurisdictions, particularly: the UAE, Türkiye, the Netherlands, the United Kingdom, China, Russia, former Soviet republics, and Latin American countries

<u>Risk factors based on inherent vulnerability</u>

381. The following sets out the factors relating to inherent vulnerability analysed to determine the inherent risk in the property sector.

Characteristics of the sector	
Level of sector size and business volume.	A large number of regulated entities of varying sizes and levels of complexity. In 2024, the revenue of the 10 largest real estate developers totalled 6,049 million euros, accounting for 25.74% of the total. The revenue of the 10 largest intermediaries totalled 811 million euros, accounting for 8.72% of the total.

Level of complexity in the sector's structure.	A multitude of interconnected companies involved in both marketing and brokerage activities.
Level of integration with other regulated sectors.	Relationships with financial and non-financial sectors (notaries and registrars) for the financing, formalisation and execution of transactions.
Location of the organisation, including the geographical scope of the sector's operations.	Distribution across the whole country. There is a concentration in particularly sensitive areas such as major cities and, in particular, coastal areas, including the islands. In 2025, notable increases in property sales were recorded in Castile and León (13.6 %), the Basque Country (12.0 %), Extremadura (9.9 %) and Aragon (9.1 %), whilst declines were seen in the Canary Islands and the Community of Madrid (-4.7 % in both cases).
Nature of the products and services provided by the sector	
Level derived from the complexity of the products, due to their impact on anonymity or the limited information on available to customers.	High-value assets that maintain or increase their value steadily, regarded as safe-haven assets and therefore highly attractive for ML and TF in all their phases. There are some difficulties in identifying the beneficial owner of property (legal entities that form part of complex structures).
The level at which specific products and services offered are linked in communications by indication and/or national ML or TF investigations	Despite the small number of reports, it is common for the sector's products and services to be directly affected in domestic and international operations against ML and TF (safe-haven assets). During the period analysed, 445 reports based on suspicion were made by the sector, representing an increase of more than 50 % in 2025 compared with the previous year. The sector appears to be indirectly linked to 5,638 reports based on indications submitted by other regulated entities (credit institutions, notaries and registrars are the sectors that lead the way in reporting these transactions).
Nature of the customer	
Level derived from the nature of the business relationship with customers, based on the duration (ongoing, transactional or occasional) and frequency of transactions	Most customers can be classified as occasional; however, the customer base of wholesale firms includes retail firms with which the business relationship is ongoing and consistent.
Level derived from the client's status	All types of clients, with a rise in non-national clients focused on high-value purchases. Given Spain's characteristics, there is significant property investment by foreigners. According to data from the General Council of Notaries, transactions carried out by foreigners totalled 71,155 in the first half of 2025 and accounted for 19.3% of all property sales. The nationality of the main buyers was 8.1% UK nationals United Kingdom, 7.9 % Moroccans and 6.7 % Germans.
Level derived from the occupation or type of the client's business	Variation in the types of activities carried out by different types of client.
Geographical scope of the sector's activities	

Level derived from specific jurisdictions/countries of interest, frequently associated with the sector.	Domestic operations. In terms of clientele, over 80 % are domestic and almost 20 % are foreign. In this type of transaction, there is a growing use of NPO or complex commercial structures involving entities registered in different jurisdictions. In the case of purchases made through complex corporate structures, UK nationals feature prominently, as trust-like arrangements are permitted under UK law. With regard to TF, it is important to note the proportion of Moroccan nationals who have invested in residential property.
Level derived from the nature of the interactions or transactions involving countries identified by the FATF.	Despite being highly diversified and having a predominantly domestic client base, this type of transaction involves dealings with certain jurisdictions listed by the FATF, such as Iran, as noted in the Sectoral Risk Analysis on Proliferation Financing, although there is no evidence of illicit funds being channelled for this purpose.
Level derived from the nature of the interactions or transactions involving countries subject to financial sanctions.	The FP's SRA highlights the purchase of property by Iranians as a threat. However, there is no evidence of links to the FP. On the other hand, the purchase of property by Russians on the Costa del Sol must be taken into account.
Nature of the distribution channels	
Level derived from the complexity of the channels due to their impact on anonymity or the limited information available on clients.	In general, transactions are conducted in person. Property transactions are usually carried out using banking products such as cheques or bank transfers, which help to identify the customer. However, there have been reports of property purchases made in exchange for cash, particularly involving foreign investors.
Level derived from the use of new technologies or payment methods.	Most payments are made by bank transfer, although it is increasingly common to use payment channels that favour anonymity, such as cash or bank cheques, or for transactions to be settled in instalments or via transfers ordered by companies or individuals other than the purchaser. All of this makes it difficult to trace the origin of the funds.

Conclusion on the sector's inherent risk: High for ML and medium for TF

382. The property sector presents significant inherent risks common to all regulated entities. These risks are higher in the cases of property development and estate agency. It is worth noting the absence of a centralised register and the high degree of heterogeneity amongst regulated entities, which makes it difficult to obtain an overall view of the sector's activity.

383. The severity of the threat in the property sector is considered high due to the diversity of predicate offences associated with the sector, including organised crime, drug trafficking, economic and financial crimes, and corruption. This exploitation is not occasional, but structural and ongoing, as evidenced by the patterns detected by the authorities, where criminal organisations use property sales, lettings or refurbishments to channel, conceal and launder illicit funds.

Furthermore, the specific methods identified (such as the use of front companies, frontmen, the overvaluation or undervaluation of properties, and successive purchase and sale transactions) highlight the sector's capacity to facilitate these processes.

384. Consequently, and given that the vulnerability factors have been assessed as substantial, the combination of both variables and the sector's inclusion in strategic reports identifying its use by criminal organisations linked to major VAT fraud schemes leads to the conclusion that there is a **high** inherent risk in ML.

385. In the case of TF, no evidence has been found linking the sector to the financing of terrorist organisations. Real estate transactions involve a high degree of traceability, formalisation and lengthy timeframes, which reduces their appeal for channelling funds intended for TF. The real estate sector is linked to TF in relation to the purchase of properties for individuals and/or entities associated with the organisation, which would constitute the offence of aiding and abetting terrorism, but not of Terrorist Financing. Consequently, the risk of TF is **medium.**

Risk factors relating to the effective implementation (or lack thereof) of controls

386. Analysing residual risk requires an assessment of how existing controls are implemented within the sector and to what extent those controls are effective. The following section presents an analysis of the factors used to determine the residual risk of the property sector.

Risk factors relating to the effective implementation (or lack thereof) of controls	
Level of regulation in the sector	There is specific legislation which highlights the absence in Spain of a compulsory administrative register of property developers or estate agents involved in the sale and purchase of property to protect buyers (although such registers do exist in some autonomous communities AA).
Level of potential presence of unauthorised entities.[84]	Both property development and agency, commission or brokerage activities in the sale and purchase of property are unrestricted and may be carried out by any natural or legal person without any administrative requirements; therefore, no authorisation is required to operate. There are no limits on the holding of significant or majority shareholdings. However, the involvement of notaries and registrars in corporate acts and property transactions, together with the obligations regarding the identification of beneficial ownership and corporate transparency set out in company law and Money Laundering regulations, act as mitigating mechanisms by increasing the traceability of the persons who control or manage companies in the .
Level of potential direct or indirect control over the entity or its management by money-laundering networks	Given that the activity is unregulated, it may give rise to the incorporation of companies with the sole aim of laundering funds derived from illicit activities. This level of exposure is mitigated by the involvement of notaries, registrars and credit institutions in real estate transactions.

[84] This variable is classified as Not Applicable

Level of regulation of ML/TF prevention measures	They are obliged entities under Law 10/2010 of 28 April, which sets out the relevant obligations regarding the prevention of ML and TF.
Level of supervision	Between 2020 and 2025, 16 inspections were carried out in the sector. However, given the high number of regulated entities, the global risk must be classified as substantial.
Level of sanctions imposed on entities in the sector.	The sanctions imposed as a result of inspections carried out from an AML/CFT perspective have been insignificant. During the period under review, two sanctioning proceedings were initiated, resulting in four breaches – three serious and one very serious – against entities in the sector. In addition, there is a requirement to rectify prevention procedures.
Level of the professionalism of managers and senior managers of the organisation.	Numerous companies and small businesses with a generally low level of awareness and knowledge regarding AML/CFT. Larger organisations have lower exposure to this risk.
Level of awareness and understanding of their obligations regarding ML/TF prevention.	The existence of numerous regulated entities of varying sizes and complexity, with little or no awareness of AML/CFT, means that this sector must be subject to supervision and monitoring.
The organisation's level of commitment to AML/CFT prevention.	The sector shows significant differences in terms of knowledge and implementation of prevention measures. A serious breach of AML/CFT policies and procedures has been identified.
Level of professional qualifications of employees and regarding their training in ML and counter-terrorist financing.	The sector shows significant differences in terms of professional qualifications in the area of AML/CFT. A serious sanction has been imposed regarding staff training in AML/CFT matters. The remedial requirement issued to another entity in the sector included the need to implement an annual AML/CFT training plan.
Level of internal monitoring by of the entities of employee compliance.	There are significant differences in employee compliance across the various entities in the sector. The very serious penalty was imposed for non-compliance with Article 24 of Law 10/2010, of 28 April.
Level of compliance with obligations regarding preventive measures, in particular with regard to CDD/KYC	Given the wide range and diversity of regulated entities, it is not possible to assess the overall level of compliance. However, based on supervisory experience, this factor could be classified as presenting a medium level of vulnerability.
Level of identification and reporting of suspicious transaction reports	During the period analysed, the sector submitted 445 reports based on indications, representing an increase of more than 50 % in 2025 compared with the previous year. The average rating for the significance of reports based on suspicious indicators for the period 2022–2025 was 5.67. This category, introduced in 2021, enables the relative importance of reports to be assessed based on their link to factors such as the connection to serious crimes, the emergence of new risk patterns, the detection of criminal structures or networks and/or the involvement of large sums of money.

Conclusion on residual risk in the sector: Substantial for ML and low for TF

387. ML's residual risk in the Spanish property sector is classified as **substantial**, taking into account existing mitigation measures. Whilst the sector is subject to Law 10/2010 of 28 April and has significant mitigating factors — such as the mandatory involvement of notaries, registrars and credit institutions, as well as an average level of compliance with due diligence requirements — structural weaknesses persist that prevent a further reduction in risk. The absence of a mandatory administrative register at national level, the high degree of fragmentation within the sector, the low average level of professionalism and awareness regarding AML/CFT, together with recurring shortcomings in policies, training and internal monitoring, maintain a significant exposure to risk.

388. The residual TF risk is assessed as low, given the weighting given to the absence of evidence in both the reports submitted on the basis of indications, the investigations and the inspections carried out in the sector.

Sector: Auditors, external accountants and tax advisers 2026

Activity and context

389. Auditors, external accountants and tax advisers are regulated entities under Article 2.1.m) of Law 10/2010, of 28 April.

390. In Spain, professional activities relating to auditing, accountancy and tax consultancy operate under different regulatory regimes and levels of regulation. Each professional role involves distinct functions and is subject to specific requirements, particularly in the case of auditors, whose work is strictly regulated by Law 22/2015, of 20 July, on Auditing and the technical standards approved by the Institute of Accounting and Auditing (ICAC).

Auditing

391. An audit — whether mandatory[85] or voluntary — involves reviewing and verifying annual accounts and other financial statements in accordance with the relevant financial reporting framework, with the aim of issuing an independent report that is valid vis-à-vis third parties. This activity may only be carried out by auditors registered with the Official Register of Auditors (ROAC). To practise as an auditor in Spain, it is mandatory to: i) be registered with the ROAC, ii) pass the official professional aptitude examination, iii) obtain authorisation from the ICAC, iv) demonstrate good character and the absence of a criminal record for intentional offences, and v) provide financial security.

392. As regards the sector's structure, although a high degree of concentration persists, medium-sized firms have experienced significant growth; in 2024, they achieved a turnover of 1,230 million euros, according to publicly available sector data. Official figures show a consolidated sector:

    - More than 19,000 professionals were working with auditors in 2023 – the first time this figure has been exceeded.
    - The ICAC maintains up-to-date registers of individual auditors and firms, with comprehensive information on their geographical distribution.
    - More than 72,000 audit reports were issued in 2024.
    - National turnover from professional services (audit, tax, legal and consultancy) reached 4,984 million in 2024 (+11.7 %).
    - Medium-sized audit firms generated a turnover of 1,230 million in 2024 (+12.8 %).
    - Revenue strictly attributable to audit in 2023 stood at almost 900 million, representing growth of 8 %.

393. Activity in the sector remains highly concentrated, with the *Big Four* and several medium-sized firms accounting for the lion's share of the market, whilst individual auditors (natural persons) account for only a small proportion.

[85] According to Article 263 of the Companies Law (LSC), a company must have its accounts audited if, for two consecutive financial years, it exceeds at least two of these three thresholds: Total assets > €2,850,000; Turnover > €5,700,000; Average workforce > 50 employees

External accountants and tax advisers

394. This sector is very broad and fragmented: professional directories list tens of thousands of active consultancy firms in Spain, offering a wide range of services that are largely digitalised. Unlike auditors, the qualifications of chartered accountants and tax advisers are not regulated by a specific Law but depend on professional bodies and voluntary registers such as the Register of Chartered Accountants (REC). There are also private accreditations from bodies such as the Spanish Association of Accounting and Business Administration.

395. Advisers are facing an increasingly digitalised regulatory environment. The reforms planned for 2026 include the mandatory implementation of systems such as VERIFACTU, the widespread adoption of B2B e-invoicing and the automation of tax processes. This is a highly fragmented sector:

    - The total number of professional practices (CNAE 69: legal, accounting and consultancy activities) fell from 159,083 in 2021 to 147,903 in 2023, representing a reduction of 7 %.
    - In CNAE 692 (accounting, auditing and consultancy), the number fell from 67,339 firms in 2021 to 63,084 in 2023, a decrease of 6.32 %.
    - 80.6 % of firms have fewer than 10 employees.
    - 44.6% of firms have an annual turnover of between €150,000 and €500,000.
    - 15.1 % have a turnover of between €500,000 and €1,000,000.
    - Only 8.1 % exceed one million euros.

396. This micro-firm structure is a critical factor in terms of ML/TF risks, as small firms' limited capacity to invest in internal controls significantly increases the risk of misuse.

<u>Threats</u>

397. The sector comprising statutory auditors, external accountants and tax advisers faces a range of specific threats arising both from the technical nature of their services and from the heterogeneity of the profession, particularly in the area of tax consultancy. Although statutory auditors are subject to a strict and highly professionalised regulatory framework, the tax advisory and external accountancy sub-sector — which is fragmented in structure and subject to limited entry regulations — constitutes a significant risk vector given its operational proximity to corporate structures, tax planning, accounting management and assistance with cross-border transactions.

398. These characteristics align with multiple threats identified in Chapter 4: economic crimes, tax fraud, organised economic crime and corruption.

Economic crime, corporate fraud and technical advice on opaque structures

399. Chapter 4 identifies economic and tax offences as one of the main threats to the Spanish system, with particular emphasis on tax fraud, VAT schemes, corporate offences, document forgery, accounting fraud and the manipulation of financial statements.

External tax advisers and accountants may become intentional or unintentional facilitators of: i) the creation or maintenance of shell companies, ii) the preparation of fictitious accounts, iii) the design of aggressive tax planning schemes that conceal beneficial ownership or distort income, iv) the submission of manipulated tax returns, and v) the establishment of cross-border structures designed to obscure ownership. The possibility of receiving assignments linked to complex corporate structures or clients engaged in non-transparent economic activity increases exposure to the risks of Money Laundering and tax fraud, particularly in the sub-sector comprising small or less professional firms.

Organised economic crime and the use of professionals as facilitators

400. Chapter 4 notes that certain criminal organisations use intermediaries to lend an appearance of legitimacy to their economic activities, set up shell companies, or design illicit financing channels. The tax consultancy sub-sector — due to its fragmentation, low level of regulation and limited effective supervision — is particularly vulnerable to: i) the recruitment of professionals to design opaque structures, ii) the use of small firms to conceal illicit flows, iii) technical support in false invoicing schemes, iv) the manipulation of accounts aimed at concealing the origin of funds. The level of exposure is greater where criminal networks misuse professional structures, particularly in the tax sphere, due to the fragmentation of the sector and the absence of professional entry requirements.

Tax fraud and aggressive international tax planning

401. Section 4 details that threats linked to tax fraud, money laundering through trade, VAT schemes, customs manipulation, offshore shell companies and fictitious relocations are on the rise. Tax advisers and accountants may be involved in: i) cross-border schemes designed to conceal assets, ii) the misuse of tax treaties, iii) dual-residence structures, iv) the creation of holding companies in high-risk jurisdictions, v) the design or maintenance of offshore companies, vi) transactions with sanctioned countries or those on the FATF list. This threat is concentrated primarily in tax consultancy, where the work involves strategic decisions with a direct impact on international taxation and high-risk corporate structures.

Corruption, embezzlement offences and professional support for illicit wealth structures

402. The NRA is analysing a number of recent cases of political and financial corruption, involving: companies controlled by the PEP, inflated invoicing schemes, front companies set up to receive commissions, and technical advice to conceal unjustified increases in assets. Tax advisers, external accountants and, in some cases, auditors may be used to: structure assets derived from corruption; manipulate supporting documentation; prepare returns or reports that conceal illicit enrichment; and reorganise business groups to conceal illicit profits. The sector recognises that the potential for a threat can be heightened when dealing with associates of PEP clients and the use of complex structures that may conceal beneficial ownership.

403. Furthermore, it is worth highlighting the following factors that may be exploited by threats within the registration sector, in line with the activities analysed in this report:

Factors that are frequently exploited by threats	
Cross-border risk and transactions involving high-risk jurisdictions	The NRA states that interaction with high-risk jurisdictions—particularly sanctioned countries, those included on FATF lists, or those with weak regulatory environments—constitutes a key threat vector in multiple types of ML/TF. In this sector, exposure to the threat may increase due to: i) advising companies with international operations, ii) structures with multiple corporate layers, iii) the use of foreign vehicles, and iv) international tax advisory services without sufficient documentary traceability. The risk is significant for advisors who work with offshore structures or flows connecting to high-risk third countries.
Accounting Manipulation and the Risk of Fraudulent Use of Financial Reports or Documentation	Section 4 identifies accounting manipulation as a recurring element of: economic crimes, corporate fraud, criminal insolvency, misappropriation of corporate assets, and crimes of disloyal administration. External accountants and certain advisors may be used for: accounting reconstructions for unlawful purposes, balance sheet manipulations, simulation of business activity, and/or concealment of losses or profits. Auditors, despite being highly regulated, may also face pressure or attempts to influence the outcome of their reports, although the regulatory and institutional framework significantly mitigates this threat.

Risk factors relating to inherent vulnerability

404. The following sets out the factors relating to inherent vulnerability analysed to determine the inherent risk in the registrars' sector.

Sector characteristics	
Size of the sector and turnover	A sector with a substantial overall size, but with insufficient information to ascertain its true scope, as it includes consultancy firms that may carry out other activities not subject to Law 10/2010, of 28 April.
Level of complexity of the sector's structure	The audit sector is highly concentrated, and its structure is well known. However, the tax consultancy sector is highly fragmented and presents risks that its professional structures may be exploited by criminal organisations.
Level of integration with other regulated sectors	Frequent dealings with notaries, solicitors and credit institutions in transactions that could be used for Money Laundering.
The entity's geographical location, including the geographical scope of	To a lesser extent in the audit sector and to a greater extent in the field of tax consultancy due to geographical dispersion at national level, particularly in the field of tax consultancy. There is a higher risk in areas with higher per capita income and a larger informal economy for tax consultancy.

the operations of the sector[86]	
Nature of the products and services provided by the sector	
Level arising from the complexity of the products, due to their impact on anonymity or the limited information available on clients.	Relevant in the field of tax consultancy due to the potential use of complex corporate structures, resulting in the concealment of the beneficial owner and/or the true origin of the funds.
The extent to which specific products and services offered are linked to communications under suspicion and/or national national ML or TF	Between 2020 and 2025, a total of 107 reports based on suspicious activity were made, with an annual average of 13 reports over the last four years. These figures are low. During the same period, there were 17 reports based on suspicious activity made by other sectors (lawyers, credit institutions, payment institutions, notaries and registrars) involving transactions with this sector.
Nature of the customer	
Level derived from the nature of the business relationship with customers, based on the duration (ongoing, transactional or occasional) and frequency of the transactions	Stable business relationships that enable professionals to gain a thorough understanding of the customer, with occasional transactions being uncommon.
Level derived from the client's status	Potential risk in tax advisory work arising from the design or use of complex and potentially opaque structures that make it difficult to determine beneficial ownership and the true source of funds. The presence in our country of clients—whether individuals or legal entities—originating from or resident abroad increases the possibility of concealing activities linked to offences of this nature by utilising the services in these sectors.
Level derived from the the client's occupation or type of business	A diverse range of risks that is highly dependent on the client's profile and the type of service provided by each regulated entity; higher risk in tax advisory services than in auditing.
Geographical scope of the sector's activities	
Level derived from specific jurisdictions/countries of interest, frequently related to the sector.	Risk highly dependent on the origin of clients and the type of matters handled by each regulated entity; a determining factor in the case of tax advisers regarding the design and use of complex structures and for clients from certain jurisdictions (e.g. Gibraltar)
Level derived from the nature of the interactions or transactions that	Higher risk profile in cross-border transactions and those involving different jurisdictions.

[86] This factor is rated as medium/substantial.

involve countries identified by the FATF.	
Level derived from the nature of the interactions or transactions involving countries subject to international financial sanctions.	There is no evidence of transactions linked to international financial sanctions.
Nature of the distribution channels	
Level derived from the complexity of the channels, given their impact on anonymity or on the limited information available about customers.	Risk mitigated by the existence of face-to-face business relationships, though sometimes with an increased risk due to the use of intermediaries or authorised representatives.
Level derived from the use of new technologies or payment methods.	In principle, the risk is moderate. The banking channel is used as a traditional method of payment. Given the widespread use of cash in Spain, the possibility of cash payments on occasional instances.

Conclusion on the sector's inherent risk: Medium/substantial for ML and low for TF

405. The heterogeneity of the tax advisory sector in terms of parties involved (obligated entities) and transactions, combined with the lack of a mandatory register in Spain and the growing influx of clients from high-risk jurisdictions, makes it very difficult to assess a priori the adequacy of compliance with prevention obligations, which contributes to the inherent risk being classified as substantial. In the case of auditors, the risk is mitigated by the high concentration of transactions within the sector's four largest firms, resulting in a medium risk. In the case of TF, the risk is considered low, given the specific characteristics of the sector and its low appeal to TF.

Risk factors relating to the effective implementation (or lack thereof) of controls

406. Analysing residual risk requires an assessment of the implementation of existing controls within the sector and the extent to which these controls are effective. The following section presents an analysis of the factors used to determine the residual risk in the audit sector.

Risk factors relating to the effective implementation (or lack thereof) of controls	
Level of regulation in the sector	Auditing is a highly regulated profession, requiring prior registration with the ROAC and adherence to specific professional standards. In contrast, for tax advisors and other professionals, there are no regulatory requirements for entering or practicing the profession. In recent years, there have been significant updates to the International Standards on Auditing adapted for Spain (NIA ES). The ICAC resolutions of 2025 and 2026 have strengthened the audit report, communication, and independence, and will be fully applicable to engagements contracted beginning in 2026.

Level of potential existence of entities not authorised to operate.[87]	In the conduct of an audit, this risk is remote, as a report issued under such circumstances has no legal validity and the possibility of checking registration with the ROAC is publicly available. In the case of tax advisers, this this does not apply as no such requirements exist; therefore, the risk is substantial.
Level of potential direct or indirect control of the entity or its management by money-laundering networks	Medium-low in the case of audit firms and higher in the case of the tax consultancy sector, due to the risk of professionals being co-opted by organised crime networks.
Level regulation of measures to prevent ML/TF	The sector is regulated by Law 10/2010, of 28 April.
Level of supervision	The sector is subject to supervision by SEPBLAC. There is a requirement for structured annual reporting, as is the case with other sectors, such as the legal profession, to gain a greater understanding of the operations and information of the main tax advisory firms. Between 2020 and 2025, 12 inspections were carried out in the sector.
Level of sanctions imposed on entities in the sector.	Recent experience with inspections is limited and has not resulted in any sanctions.
Level of professionalism among the organisation's directors and senior management.	The high degree of fragmentation resulting from the very structure of the tax consultancy sector. There is greater exposure in the case of larger professional firms originating from the legal sector.
Level of awareness and understanding of their obligations regarding AML/TF.	Greater amongst audit firms and more varied amongst tax advisory professionals, given the high degree of fragmentation within the sector.
The organisation's level of commitment to ML/TF policies and measures.	Larger audit and tax consultancy firms demonstrate a higher level of commitment, as they have a control structure geared towards risk management. In the case of smaller regulated entities, the implementation of these policies depends on the judgement of the professionals directly involved in the matters being handled, without additional internal supervision.
Level of professional qualifications of staff and their training in ML/TF	In both subsectors, training levels are higher among larger regulated entities.
Level of internal monitoring by organisations of employees' compliance.	A more developed control structure is found in the case of larger regulated entities. It is less developed in smaller ones and may even be non-existent.
Level of compliance with obligations regarding preventive measures, particularly DDC/KYC	A more developed control structure is found among larger regulated entities. It is less developed among smaller ones and may even be non-existent.
Level of identification and reporting of suspicious transactions[88]	There is a low volume of reported suspicious transactions. Over the last four years, the average has been 13 reports per year, with a total of 106 reports from the sector based on indications of suspicious activity. This low level of reporting may indicate a possible failure to detect suspicious transactions, which implies a shortfall in training and internal controls. This may prevent the sector's actual exposure from being adequately reflected, thereby allowing illicit structures to go unnoticed. This phenomenon is particularly relevant in the tax consultancy sub-sector, where the

[87] This variable was classified as Not Applicable

[88] This variable was rated as 'substantial-high'

	dispersion and the small size of many firms limit their operational capacity for prevention. The average rating for the significance of tip-off reports for the period 2022–2025 was 6.564. This category, introduced in 2021, makes it possible to assess the relative importance of reports based on their link to factors such as their connection to serious crimes, the emergence of new types of risk, the detection of criminal structures or networks, and/or the involvement of large sums of money.

Conclusion on the sector's residual risk: Medium/substantial for ML and low for TF

407. The high concentration of business among the major players in the audit sector (the Big 4) and the high level of regulation in this sector mean that the residual risk is **medium**. However, in the case of tax consultancy, these same factors result in business being spread across small, regulated entities (with a variety of operations and controls) and a lack of specific regulation, which requires a higher, **substantial**, residual risk rating. In the case of TF, the residual risk remains **low**; there are no factors indicating that the risk rating needs to be raised.

Sector: Notaries 2026

Activity and context

408. Notaries are regulated entities under Article 2.1(n) of Law 10/2010, of 28 April.

409. A notary is a public official of the State who is appointed to the post through a competitive examination and whose role is to provide citizens with the legal certainty established by the Constitution in the field of extrajudicial legal transactions. They are legal professionals practising in a competitive market, although their fees are standardised across the profession. Law 10/2010, of 28 April, establishes that notaries are obliged entities.

410. In the exercise of their preventive duties in the field of ML/TF, pursuant to Article 27 of Law 10/2010 of 28 April, Article 44 of the Regulation stipulates that notaries must be incorporated into the Centralised Prevention Body (OCP). As of 31 December 2025, there were approximately 2,697 practising notaries in Spain, organised into 17 notarial associations and spread throughout the country. The OCP was established in December 2005 as a direct result of the publication of Order EHA/2963/2005. The General Council of Notaries maintains the Single Computerised Notarial Register, in which all notarial acts are recorded. The General Council of Notaries' OCP has access to this register. Notaries have access to an extensive database on beneficial ownership, to which the AEAT was granted access in 2021 through the signing of an agreement to strengthen the fight against tax fraud[89].

411. Furthermore, Royal Decree 609/2023 of 11 July established the Central Register of Real Property Ownership and approved the regulations governing its operation. This Register incorporates, amongst other sources, the information contained in notarial databases. In accordance with the provisions of Law 11/2023 of 8 May on the digitisation of notarial and registration procedures, notaries may provide certain notarial services remotely, primarily of a commercial nature. These include corporate acts, commercial deeds, various types of powers of attorney, letters of payment, cancellation of guarantees, certificates of legitimacy, wills drawn up during an epidemic and, in some cases, settlements and legal acts and transactions, amongst others. These procedures are carried out via the notarial electronic portal, using videoconferencing and advanced electronic signatures. In 2025, 9,198,741 notarial acts were carried out.

Threats

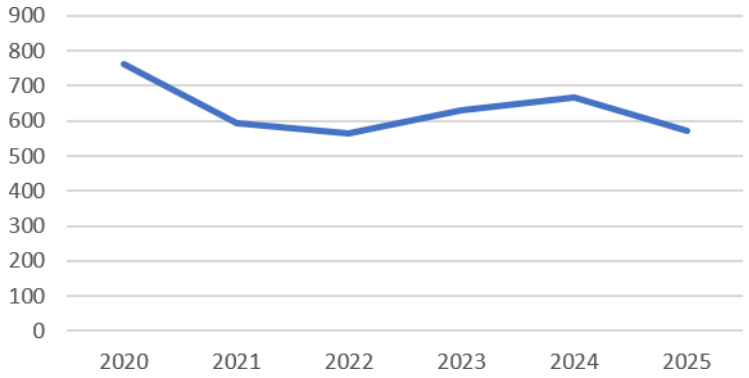
412. The notarial profession constitutes a structural element of the Spanish system of preventive legal certainty and plays a central role in the formalisation of transactions with a significant financial impact, such as property transfers, the incorporation and transfer of companies, capital increases, the acknowledgement and cancellation of debts, as well as numerous legal transactions of economic significance. The size of the profession, its widespread territorial coverage, the high

[89] The OCP also has cooperation agreements with:
- The Executive Service of the COPBLAC.
- The State Security Forces and judicial authorities (Policía Nacional, Guardia Civil, Mossos d'Esquadra, Courts and Public Prosecutors' Offices).
- The National Securities Market Commission (CNMV),
- the European Anti-Fraud Office (OLAF),
- The autonomous communities with powers in the field of Money Laundering prevention, inspection and administrative control.
- And other international bodies and forums dealing with Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT), through established mechanisms for institutional cooperation.

volume of deeds and the intense interaction with other regulated sectors place the notarial profession in an environment of significant risk, particularly in the areas of property, companies and cross-border flows, which is fully consistent with the threats identified at national level in Chapter 4.

413. Although the sector's regulatory framework and the existence of the OCP constitute a notable strength against most risks, transactions formalised before a notary remain susceptible to being exploited by criminal networks, organisations linked to economic crime, opaque corporate structures or groups involved in corruption and tax fraud.

414. As regards trends in reports based on indications, the situation has remained stable since 2021. The indicators detected are in line with the threats identified in Chapter 4; thus, although the generic category of money laundering has the highest incidence, tax fraud, participation in criminal organisations, drug trafficking and fraud are the indicators most frequently identified.



Source: SEPBLAC

415. The threats described below reflect the most significant levels of exposure.

Organised crime: legitimisation of transactions and formalisation of corporate structures

416. Chapter 4 states that organised crime uses property, companies, loans and capital increases as mechanisms for placing, layering and laundering illicit funds. Notaries play a key role in this process as they are responsible for drawing up public deeds for: i) property sales at anomalous or inflated prices,
ii) successive transfers to create the appearance of legitimacy, iii) the incorporation of companies and capital increases without any real economic justification, iv) non-monetary contributions that are difficult to value, and v) structures involving multiple parties or special-purpose vehicles from third countries. These transactions may be used to launder proceeds from drug trafficking, fraud networks, human trafficking or illicit economic activities, with the notary acting as a key point for detecting irregularities in beneficial ownership and in the economic coherence of the transaction.

Economic and tax offences and the use of shell companies

417. Section 4 highlights a significant increase in VAT fraud, corporate offences, document forgery, embezzlement, international fraud rings and criminal insolvency schemes.

In the notarial sphere, these threats may manifest themselves as: i) the creation of short-lived companies used for false invoicing, ii) transfers of shareholdings between related companies, iii) acknowledgements of debt concealing sham loans, iv) fictitious or disproportionate contributions to capital increases, v) corporate restructurings that are difficult to justify on economic grounds, such as property sales by legal entities with complex structures or deferred payments in high-value property transactions. The threat intensifies when transactions form part of complex corporate chains or involve funds whose origin is not duly substantiated.

Corruption, PEP and concealment of assets

418. Chapter 4 identifies political and financial corruption as a significant risk factor, including embezzlement, bribery, influence peddling and unjustified enrichment. In the notarial sphere, these threats converge with: i) transactions in which PEPs are involved, either directly or through representatives; ii) the acquisition of high-value properties; iii) the incorporation of shell companies; iv) transfers of assets between family members or frontmen; and v) notarial protocols used to justify structures that conceal illicit increases in wealth. The level of exposure to the threat increases when the parties involved use corporate vehicles in third countries or opaque financial structures.

419. Furthermore, it is worth highlighting the following factors that may be exploited by threats to the notarial sector in line with the activities analysed in this report:

Factors that are frequently exploited by threats	
Real estate as the main risk vector	In the notarial sphere, the threat centres on transactions such as: sales between related companies, acquisitions by non-residents from high-risk jurisdictions, payments made partly in cash or prices inconsistent with market value, the use of representatives with broad powers of attorney and chains of authorisation; formalisation via a public deed does not eliminate the threat, as criminal organisations seek precisely to legitimise the legal transaction through the notarial process.
Cross-border transactions and ties to high-risk jurisdictions	The NRA emphasises that interaction with jurisdictions on the FATF list, sanctioned territories and countries with low corporate transparency increases the vulnerability of any economic sector. In the notarial context, these threats manifest themselves in: transactions involving entities or individuals from various countries, complex beneficial ownership with multiple layers, or funds originating from or destined for high-risk third countries.
Foreign companies acting as buyers, sellers or financiers.	A lack of transparency regarding beneficial ownership — particularly prior to the establishment of the Central Register of Beneficial Ownership — poses a key threat to the detection of illicit schemes.
Instrumental use of the notarial deed	A notary may be exposed to attempts to use a notarial deed to: lend an appearance of legality to sham transactions; document legal acts that conceal undeclared loans; amend articles of association or partnership agreements to conceal ultimate beneficial owners; or grant powers of attorney that allow operate on behalf of third parties without transparency, or to register

	of dubious origin. These practices form part of methods identified in judicial and police investigations cited in the NRA.
Notarial Digitization and Associated Emerging Risks	Although the digitization of notarial services is aimed at strengthening legal certainty (electronic office, BDTR, videoconferencing, advanced electronic signature), the threats identified in Chapter 4 related to the fraudulent use of technology, remote identification, the submission of foreign or forged documentation, and identity theft can also affect the sector. Commercial and corporate transactions that can be authorized remotely may be particularly vulnerable to: attempts at impersonation during videoconferences, documentation whose authenticity cannot be verified at the source, or parties residing in high-risk countries without a physical presence in Spain.

Risk factors due to inherent vulnerability

420. Set out below are the factors relating to inherent vulnerability that were analysed to determine the inherent risk in the notarial sector.

Characteristics of the sector	
Size of the sector and turnover	A large and highly widespread group (around 2,697 notaries) and a high volume of notarial acts with financial content (4,660,482 acts, accounting for almost 51 % of the total), which increases potential exposure. According to confidential data, the sector comprising notaries and registrars has a turnover of around 3,000 million euros, although the underlying value of the transactions they handle is much higher.
Level of complexity of the sector's structure	Notaries perform public functions under a uniform legal framework, with a common scale of fees, a standardised public statute and a centralised professional organisation through the Notarial Associations and the General Council of Notaries.
Level of integration with other regulated sectors	Systemic interaction with the Land Registry and Companies Register, the property sector, law firms and financial institutions (playing a very significant role in the formalisation of transactions).
Location of the organisation, including the geographical scope of the sector's operations[90]	Nationwide coverage (including small towns). Geographical dispersion and the concentration of a higher number of property transactions, international transactions and/or corporate transactions in specific areas represent factors of greater risk for some notaries compared with others. Higher risk profile in property transactions and other legal acts of a financial nature, and links to other jurisdictions due to foreign parties or cash flows originating in third countries.
Nature of the products and services provided by the sector	
Level derived from the complexity of the products, due to their	Risks in corporate structures, contributions that are difficult to value (capital increases), anomalous prices or links between parties that make it difficult to verify the purpose and beneficial ownership.

[90] This factor is rated as medium/substantial.

impact on anonymity or on the reduced information on customers.	Objective scope with a higher risk profile in relation to certain legal transactions, relating to the transfer of company shares, transactions relating to the property sector, share capital increases and the recognition of debt.
The extent to which specific products and services offered are linked in advertising and/or national ML or TF	In tip-off reports, a concentration of risk has been detected in relation to property and companies (incorporation and transfer), alongside equity and debt financing transactions, and notarial deeds.
Nature of the customer	
Level derived from the nature of the business relationship with customers, based on the duration (ongoing, transactional or occasional) and frequency of the transactions	Occasional business with a lower frequency than ongoing relationships, particularly in the case of individuals. In the case of legal entities, the relationship may be more long-term.
Level derived from the client's status	A diverse client base, but with a predominance of natural persons. Of the total transactions, almost 37.6% involve natural persons. Greater vulnerability arises from the use of complex corporate structures and from potential exposure through the provision of advice to PEPs, either directly or indirectly. Non-residents and links to higher-risk/offshore jurisdictions increase the need for verification of beneficial ownership and the source/purpose of funds. Ownership chains where the beneficial owner is unclear increase uncertainty regarding control and beneficiaries.
Level derived from the client's (party involved) occupation or type of business	Vulnerability increases when the party involved operates in cash-intensive sectors or the informal economy, or where there are cross-border operations or foreign trade with higher-risk or offshore jurisdictions, or the presence of PEPs, particularly when the parties involved are part of complex corporate structures. Vulnerability decreases when the parties belong to listed business groups or to financial/insurance institutions regulated due to their greater transparency and supervision. In summary, vulnerability in relation to this factor is heterogeneous and varies depending on the notary's office (e.g. by location, volume and mix of transactions).
Geographical scope of the sector's activities	
A level derived from specific jurisdictions/countries of interest frequently associated with the sector.	Exposure varies depending on the notary's office. With regard to the involvement of foreign legal entities in corporate transactions, 70 % of these jurisdictions are in the EU, 12 % are in the United Kingdom and 5 % are in the United States. The remainder are in third countries.

Level derived from the nature of the interactions or transactions which involve countries identified by the FATF.	Greater exposure in cross-border structures/transactions, or those involving multiple intermediaries in different jurisdictions, which result in greater opacity regarding the beneficial owner and make it more difficult to trace the funds. 0.85 % of all corporate transactions carried out by foreign entities whose country of origin has been identified by the FATF as having strategic deficiencies in AML/CFT.

Level derived from the nature of the interactions or transactions involving countries subject to international financial sanctions.	0.02% of the corporate operations of foreign entities are linked to entities in jurisdictions subject to financial sanctions.
Nature of distribution channels	
Level derived from the complexity of the channels due to their impact on anonymity or the limited information available on customers.	The in-person notarial channel mitigates anonymity. The level of exposure increases when representatives and chains of powers of attorney are involved, or when foreign documentation or parts of the transaction take place outside the notarial circuit (e.g. private documents or transfers abroad).
Level derived from the use of new technologies or payment methods.	The digitisation of the notarial profession focuses on control tools (the Single Index, BDTR) rather than on opaque payment channels; relative exposure is lower compared with other sectors.

Conclusion on the sector's inherent risk: Substantial in ML and Medium in TF

421. The notarial sector faces significant inherent risks that are common across the entire sector. These risks are high when clients with indirect real operations (parent companies, subsidiaries or special purpose vehicles) are involved in the deed, and/or in higher-risk jurisdictions, and/or when funds originate from or are destined for those countries. The ML/TF risk is higher in certain types of transactions: transfers of shares in limited liability companies; sales of real estate; company capital increases; and loans/acknowledgements of debt.

Risk factors relating to the effective implementation (or lack thereof) of controls

422. To analyse residual risk, it is necessary to assess the implementation of existing controls within the sector and the extent to which these controls are effective. The following section presents an analysis of the factors used to determine the residual risk in the notarial sector.

Risk factors relating to the effective implementation (or lack thereof) of controls	
Level of regulation in the sector	The sector is highly regulated (civil servants, access via competitive examination) with a professional body structure and reporting to the Ministry of Justice. Furthermore, notaries are regulated under Law 10/2010, of 28 April, for transactions of financial significance.

Likelihood of unauthorised entities unauthorised to operate.	The public status of the profession and the system of entry structurally reduce the risk of unauthorised practice within the national territory.

Level of potential direct or indirect control over the entity or its management by money-laundering networks	The endogenous risk is considered low due to the nature of the role and its institutional oversight; the risk of exogenous abuse exists (attempts to use the deed for legitimisation).
Level of regulation of anti-money laundering and counter-terrorist financing (ML/TF) measures	Law 10/2010 of 28 April provides for the OCP. The OCP of the General Council of Notaries standardises criteria and functions and provides the sector with specialised AML/CFT procedures. The creation of the OCP is intended to intensify and strengthen collaboration between registered professionals and the judicial, police and administrative authorities, enabling a higher level of specialisation in these tasks within the group of obliged entities.
Level of supervision	SEPBLAC is the supervisory authority and the OCP acts as a centralised support and monitoring mechanism (Single Register, analysis, channelling of CI/CPI), which increases the sector's coverage and analytical capacity compared with other groups. Eight inspections were carried out during the period under review (2020–2025).
Level of sanctions imposed on entities in the sector.	No sanctioning measures have been taken. However, 6 requests for corrective action have been issued, requiring improvements to 15 preventive procedures.
Level of professionalism of the organisation's directors and senior managers of the organisation.	Access via competitive examination, legal training and collegial governance ensure a high level of professionalism across the sector as a whole, resulting in a low risk.
Level of awareness and understanding of their obligations regarding ML and TF.	Mandatory registration with the OCP and the use of standardised tools and guidelines foster a higher level of practical understanding of obligations within this group, in relative terms, compared other professional sectors.
The organisation's level of commitment to policies and measures for ML/TF policies and measures.	The centralised model (OCP), together with the Single Computerised Index and the Beneficial Ownership Database, reflects an institutionalised commitment to AML/CFT (standardisation of practices and coordinated reporting).
Level of professional qualifications of staff and their training in ML/TF prevention.	Notaries possess a high level of legal qualification (gained through competitive examination) and receive specialised support from the OCP of the General Council of Notaries (uniform criteria, analysis and channelling of indicators), which raises the level of expertise in AML/CFT matters.
Level of internal monitoring by organisations of employees' compliance.	The centralisation of information and specialised analysis within the OCP enable cross-cutting monitoring, exceeding the capacity of an individual notary's office.

Level of compliance with obligations regarding preventive measures, in particular CDD/KYC	In-person formal identification, access to the Beneficial Ownership Database and the channelling of indicators facilitate robust compliance; the challenge persists in complex structures and when dealing with jurisdictions posing a higher risk, where it is required to carry out enhanced verification of TR and origin/purpose.
Level of identification and communication of suspicious transaction reports	Notaries have an advanced ML/TF detection system following the establishment of the Centralised Body for Prevention within the General Council of Notaries, which utilises highly sophisticated tools, such as the Single Computerised Notarial Index, which cross-references information on millions of notarised transactions throughout the country, which are duly analysed by the OCP's specialist team, or the Beneficial Ownership Database, which enables notaries, authorities and regulated entities to verify the accuracy of declarations made by the ultimate beneficial owners of legal entities carrying out transactions subject to a public deed. The average rating for the significance of reports based on evidence for the period 2022–2025 was 5.81. This category, introduced in 2021, enables the relative importance of reports to be assessed on the basis of their link to factors such as their connection to serious crimes, the emergence of new types of risk, the detection of criminal structures or networks and/or the involvement of large sums of money.

Conclusion on the sector's residual risk: Medium and low/medium for TF.

423. Despite the level of inherent risks, particularly in relation to property transactions, the incorporation and transfer of companies, capital increases, and the recognition or cancellation of debt, the effectiveness of the controls implemented through the OCP means that the residual risk is reduced to **medium** for the ML and **low/medium** for TF.

Sector: Land, commercial and movable property registrars 2026

Activity and context

424. Registrars are obliged entities under Article 2.1(n) of Law 10/2010, of 28 April.

425. Land, commercial and chattel registrars are civil servants of the State who are appointed to their posts following a competitive examination, and whose role is to maintain the land, commercial and chattel registers in Spain. Registrars shall, under their own responsibility, assess the legality of all types of documents on the basis of which registration is sought. For documents to be entered in the relevant registers, the registrar must give a favourable assessment.

426. Under the law, only documents formalised by a notarial deed, or a judicial or administrative decision may be entered in the registers; consequently, any registration procedure requires the prior involvement of a notary, a judge or an administrative authority, subject to the exceptions laid down by law. Under the law, documents formalised by a notarial deed, or a judicial or administrative decision are eligible for registration; consequently, any registration procedure requires the prior involvement of a notary, a judge or an administrative authority, subject to the exceptions laid down by law. However, certain registers also accept private documents (albeit rarely), particularly in areas such as movable property or certain entries in the Commercial Register. In such cases, the registrar must identify the parties involved and verify compliance with the applicable legal requirements. Furthermore, the registrar maintains control over aspects such as methods of payment, the validity of the transaction and compliance with tax obligations.

427. In Spain, there are around 1,140 registrars in 2025 (2024, updated figure). Registrars do not operate on a competitive basis but are assigned on the basis of territorial jurisdiction; consequently, citizens do not have a free choice of registry, which guarantees the independence of registrars in the performance of their duties. This unique arrangement means that registrars are not subject to market forces.

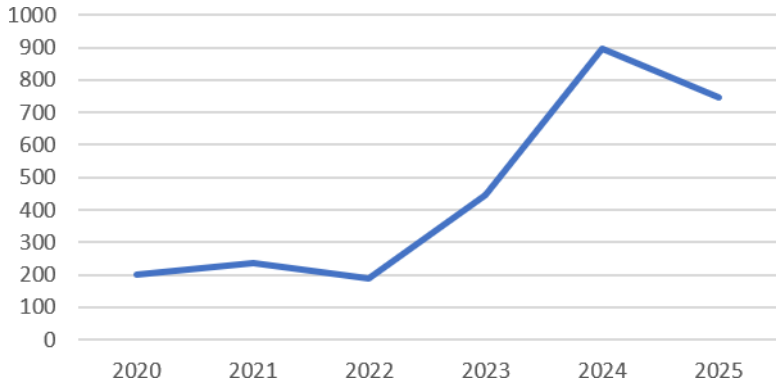
428. In carrying out their preventive duties in the field of ML/TF, as also mentioned in the analysis of notaries, Law 10/2010 of 28 April provides for the possibility of establishing centralised prevention bodies within the professional bodies. Registrars have a centralised prevention body, the Anti-Money Laundering Registry Centre (CRAB), established in 2015, and membership of this body is compulsory.

Threats

429. The registrars' sector faces a range of ML and TF threats which, whilst relatively limited compared with other non-financial sectors, are significant in certain types of transactions due to the high economic and legal value of the deeds entered in the registers and their role in the integration and legitimisation phase of money laundering.

430. These threats are in line with those identified in Chapter 4, particularly in relation to economic crimes, the use of complex corporate structures, the concealment of beneficial ownership, corruption and cross-border operations involving high-risk jurisdictions, although they are clearly mitigated by the public, regulated and non-competitive nature of the registry function.

431. With regard to trends in tip-off reports, the following chart shows the rise in the number of reports submitted, driven by increased registration activity and the introduction of detection tools by the CRAB. The main type of operation reported relates to generic money laundering cases; however, as outlined in Chapter 4, tax offences, fraud, corruption and involvement in criminal organisations are the indicators most frequently identified in these reports.



Source: SEPBLAC

Economic offences and the use of complex corporate structures

432. Chapter 4 identifies economic and corporate offences as a significant threat. In the context of the register, this threat manifests itself when the following are involved: i) shell or vehicle companies, ii) complex chains of ownership, iii) directors and nominal shareholders without effective control, iv) corporate restructurings with little economic justification. These structures can make it difficult to identify the beneficial owner and the origin or purpose of the funds, increasing the risk that the register will be used to consolidate opaque corporate structures.

Corruption and the use of the register to conceal assets

433. Chapter 4 identifies political and financial corruption as a significant threat. The land registry sector may be implicated in this threat when it is used to (i) register assets acquired with funds derived from corruption, (ii) fragment ownership amongst family members or frontmen,
iii) reorganise assets through successive transfers, iv) consolidate unjustified increases in wealth. The threat is heightened in transactions of high economic value and where PEPs or companies linked to them are involved, particularly where there is an international dimension.

Terrorist Financing

434. The threat of TF in the land registry sector is low, given that: i) the registrar does not manage funds, ii) it does not process payments, and iii) it acts following the intervention of other regulated entities.,

However, in exceptional circumstances, certain heritage listings could be used to conceal assets or facilitate logistical arrangements, although this threat is considered to be minimal.

435. Furthermore, it is worth highlighting the following factors that may be exploited by threats to the registration sector in line with the activities analysed in this report:

Factors that are frequently exploited by threats	
Use of the register as a mechanism of legitimising of assets	The main risk lies in the use of access to the register as a means of formally legitimising assets that have previously been introduced into the economic circuit through other stages of the money-laundering process. In particular: i) the registration of rights in rem over immovable property, ii) the incorporation, amendment or transfer of companies, iii) the registration of security interests and financing transactions, and iv) corporate restructuring with financial implications. In these cases, the register can be used as the final stage of integration, conferring an appearance of legality and legal stability on assets of illicit origin. This threat has been repeatedly highlighted in national and international analyses of ML/TF, particularly in sectors linked to property and commercial sectors.
Concealment of beneficial ownership and misuse of front men	The registration sector faces difficulties in identifying the ultimate beneficial owner where the following factors are present: foreign legal entities, multi-tier holding companies, fiduciaries, *trusts* or similar arrangements, and representation through authorised representatives or chains of powers of attorney. Although the Spanish registration system and the Register of Beneficial Ownership (RETIR) represent a very significant step forward, a considerable level of risk remains in particularly complex or cross-border structures, where the information provided may be incomplete or difficult to verify.
Cross-Border Exposure and High-Risk Jurisdictions	The sector is exposed to transactions involving: i) non-resident natural or legal persons, ii) funds originating from or destined for third countries, iii) jurisdictions identified by the FATF or subject to sanctions, iv) structures with a presence in multiple countries. In these scenarios, a mismatch between the jurisdiction of registration and that of the actual operations may hinder traceability comprehensive overview of the funds and increase exposure to ML/TF risk.
Representation, powers of attorney and documentation abroad	Another significant exposure factor stems from the extensive use of: legal representatives, powers of attorney granted abroad, private documentation or foreign court orders, and registered acts based on non-notarial deeds in certain registers. Although these cases are in the minority, they can hinder the full verification of the identity, legal capacity and effective control of the parties involved, thereby increasing the risk when there is insufficient supplementary information is available.

Risk factors due to inherent vulnerability

436. The following sets out the factors relating to inherent vulnerability analysed to determine the inherent risk in the registrars' sector.

Characteristics of the sector	
Size of the sector and turnover	A large and highly fragmented group (1,185 registrars) with a high volume of transactions, which increases exposure due to materiality. According to registry statistics[91] , the sector's activity continues to rise, with data for the final quarter of 2025 showing a 10 % increase in company incorporations[92], a 3.7 % increase in the registration of company wound-ups and a 5.5 % increase in capitalisation transactions, all compared with the same period in 2024. As regards property sales, year-on-year growth in 2025 compared with the final quarter of 2024 stood at approximately 4.7 %, although the underlying value of the transactions processed is much higher.
Level of complexity of the sector's structure	The sector is characterised by low complexity, comprising natural persons operating under public statute and territorial allocation. It has a centralised prevention body to which membership is compulsory.
Level of integration with other regulated sectors	The registration of legal acts in the register forms part of a chain comprising other entities subject to Law 10/2010 of 28 April, such as the property sector or the financial sector.
Location of the entity, including the geographical scope of the sector[93]	The service covers the whole country. There are regional registers, meaning that those located in areas identified as being most vulnerable at national level – particularly in property transactions – pose a greater risk.
Nature of the products and services provided by the sector	
Level derived from the complexity of the products, due to their impact on anonymity or the limited information on the clients.	The product consists of the registration of corporate, movable property and immovable property transactions. There is no anonymity, as the party involved must have been identified. However, there is a risk of concealment of beneficial ownership when the parties involved are entities with complex structures, or when funds from third countries are used for the transaction.
The extent to which specific products and services offered are linked in STRs and/or national ML or TF investigations	Capital increases, company formations, transfers of shares, as well as transfers of property and loans of international origin, including those with early repayment, feature prominently in the reports based on evidence submitted by the sector.
Type of client	
Level derived from the nature of the business relationship with customers,	The relationship with the user of the registers is occasional, as the documents submitted for registration in the registers are those which contain the registrable legal transaction, which the registrar assesses,

91 https://www.registradores.org/documents/33383/44818926/BER_61_2025-Diciembre+%282%29.pdf/2a4ce6f0-561b-955f-18f5-2119e5aa70bd?t=1766060945773

92 Construction and real estate activities together account for 26.8% of the companies established during the period, followed by trade, which accounts for 15.1%, and professional, administrative and service activities, with 14.4%. The hospitality sector accounts for 10.1% of the total
of newly incorporated companies.

93 This factor is rated as medium/substantial.

depending on the duration (continuous, transactional or occasional) and frequency of transactions	and which the competent authority (notarial, judicial or administrative) has previously identified the parties appearing before it and attested to their identity. In cases where private documents are entered in the register, the registrar applies the identification rules laid down in the prevention regulations. The service provided by registrars operates on the basis of territorial jurisdiction, meaning that citizens do not have a free choice of registry. This distinctive feature provides an additional safeguard, as registrars are not subject to market forces in the performance of their duties.
Level derived from the client's status	The types of parties involved are diverse. The level of exposure increases in the case of legal entities and complex corporate structures, and where there is direct or indirect involvement of PEPs amongst the parties or beneficiaries; non-residents and links to higher-risk or offshore jurisdictions heighten the need for verification of beneficial ownership and the origin or purpose of funds; chains of ownership where the beneficial owner is unclear increase uncertainty regarding control and beneficiaries. Exposure is mitigated when the parties are listed groups or financial/insurance institutions subject to regulation, owing to their greater transparency and oversight. As regards individuals involved in property transactions, the risk is low, as 87 % of transactions were carried out by Spanish nationals. The foreign nationals with the greatest presence in these transactions are UK nationals. Among those who may be considered higher risk are Moroccans (0.57 % of transactions), Chinese (0.39 % of transactions) and Russians (0.23 % of transactions)[94].
Level derived from the client's occupation or type of business	The level of exposure varies according to the register (Property/Commercial/Movable Assets) and its scope (location, volume and mix of registrable titles). It increases when the parties involved belong to cash-intensive sectors or the informal economy, when there are cross-border operations or foreign trade with higher-risk or offshore jurisdictions, or when they operate through complex corporate structures where the beneficial owner is not transparent; it decreases when the parties are listed groups or financial institutions and insurers, due to their greater transparency and supervision. With regard to company incorporations[95], construction and real estate activities together account for 26.8 % of the companies established during the period, followed by trade, which accounts for 15.1 %, and professional, administrative and service activities, at 14.4 %. The hospitality sector accounts for 10.1 % of all newly incorporated companies.
Geographical scope of the sector's activities	
Level derived from specific jurisdictions/countries of frequent interest	The registration process is national. However, it should be borne in mind that exposure varies depending on the Register, as there are areas with a high proportion of foreign nationals residing in Spain and where international interaction is greater, which increases the risk.

[94] Data for the last quarter of 2025. Statistical Register Bulletin.
[95] Data for the final quarter of 2025. Registry Statistics Bulletin.

related with the sector.	
Level derived from the nature of the interactions or transactions involving countries identified by the FATF.	A risk is perceived in connection with the purchase and sale of property in certain geographical areas of Spain with communities of foreign nationals from those countries. The exposure is greater in cross-border structures or transactions, or those involving multiple intermediaries in different jurisdictions, which entail greater lack of transparency regarding the beneficial owner and making it more difficult to trace the funds.
Level derived from the nature of the interactions or transactions involving countries subject to international financial sanctions.	Given the presence of Iranian and Russian nationals, corporate, commercial and property transactions have been carried out with nationals from these jurisdictions.
Nature of the distribution channels	
Level derived from the complexity of the channels due to their impact on anonymity or the limited information available on customers.	The registration channel comprises the electronic headquarters of the Association of Registrars and the actual reception desks at the relevant registers. The level of exposure increases when chains of representatives or intermediaries are involved in a transaction submitted to the register for registration. As regards the flow of funds, the transactions recorded may involve a disbursement of funds, typically channelled via bank transfers and cheques. The risk in these cases is greater when there are transactions with third parties countries.
Risk arising from the use of new technologies or payment methods.	The registry does not process payments (the risk associated with the payment method lies with the underlying business and other regulated entities); the digitisation of the system and tools such as RETIR and CRAB improve traceability and standardise criteria, thereby reducing the exposure of the registry channel.

Conclusion on the sector's inherent risk: substantial in ML and moderate in TF

437. The materiality and pervasiveness of the collective, the legitimising and enforceable effect of registration, and the concentration of exposure in property sales, corporate transactions (e.g. capital increases and organisational changes) and loans/acknowledgements of debt. The risk is exacerbated where there are complex or opaque corporate structures and cross-border links with higher-risk jurisdictions, which limit visibility in the register.

Risk factors relating to the effective implementation (or lack thereof) of controls

438. Analysing residual risk requires an assessment of how existing controls are implemented within the sector and to what extent those controls are effective. The following section presents an analysis of the factors used to determine the residual risk in the registration sector.

Risk factors relating to the effective implementation (or lack thereof) of controls	
Level of regulation in the sector	The sector is subject to extensive regulation. Registrars form a public body with access via competitive examination, a fee system, territorial demarcation and reporting to the Ministry of Justice; a robust formal framework. They are obliged to comply with AML/CFT requirements.
Level of potential presence of entities not authorized to operate[96]	The public status and territorial allocation preclude the risk of unauthorised practice or unauthorised operation.
Level of potential direct or indirect control over the entity or its management by or networks involved in money laundering	Registrars are appointed to their posts through a highly regulated and rigorous competitive examination system. Furthermore, their professional practice is restricted to the geographical area of jurisdiction of each registry.
Level Regulation of ML/TF prevention measures	Registrars are obliged parties under Law 10/2010, of 28 April. Since 2015, membership of the CRAB has been compulsory. This centralised prevention body standardises criteria and functions.
Level of supervision	The CRAB acts as a sector-specific mechanism to support and monitor registry activities. Between 2020 and 2025, three inspections were carried out, including a review of the CRAB's work.
Level of sanctions imposed on organisations in the sector.	In 2025, a follow-up review of the CRAB's activities was carried out, resulting in two recommendations regarding the standardisation of the alert software and effective cross-checking of lists.
Level of professionalism among the organization's administrators and executives.	Registrars are highly qualified in legal matters, as they gain entry to the profession through a competitive examination. They operate under a collegial governance structure, with their registration qualifications subject to accountability.
Level of awareness and understanding of their obligations regarding ML/TF prevention.	The CRAB and sectoral practice raise awareness and standardise preventive procedures within the profession. There are legal obligations in this regard, and the existence of the CRAB facilitates the delivery of training activities, although the geographical dispersion of the regulated entities makes face-to-face training difficult.
Level of the organisation's commitment to ML/TF prevention policies and measures[97].	The centralised model (CRAB) + RETIR + qualification requirements underpin an institutionalised commitment to AML/CFT. Awareness amongst registrars is steadily increasing. Clearly, geographical dispersion makes it difficult for the CRAB to deliver training, but the organisation's commitment is unwavering; on the one hand, this is evident in the CRAB's launch, even before the ministerial order establishing it came into force, and on the other, in terms of institutional collaboration in this area.
Level of professional qualifications of staff and their training in the prevention of ML and TF.	The level of awareness and training amongst registry staff has improved substantially. The CRAB provides training in accident prevention for both registrars and their staff; generational changes within the registry workforce have led to higher professional qualifications and a greater interest in accident prevention training. Furthermore, registrars' staff are notcivil servants.

[96] This variable is classified as Not Applicable
[97] This variable was rated as low-medium

Level of internal monitoring by the organisations of employee compliance.	The registration rating and centralised flows managed by CRAB enable monitoring.
Level of compliance with obligations regarding preventive measures, in particular CDD/KYC	The registration requirements — including the need for a TIN and the identification of payment methods on documents where applicable, together with the RETIR (beneficial ownership) system and the channelling of evidence via the CRAB — underpin robust compliance. The registration of third-party service providers with the Commercial Register represents a further step in managing this risk. In 2018 (and in subsequent annual updates), a Ministerial Order established the forms for the submission of commercial companies' annual accounts to the Commercial Register, mandating the declaration and updating of their beneficial ownership, which is subject to registration in RETIR. This system has a very positive impact on national systems for monitoring beneficial ownership and on the level of awareness amongst the authorities and obliged entities, in line with national and international requirements for combating ML/TF.
Level of identification and reporting of suspicious transaction reports	Between 2020 and 2025, registrars have almost tripled the number of reports based on indications, which demonstrates the sector's awareness of preventive measures and the development of tools to detect suspicious transactions. The average rating for the significance of reports based on indications for the period 2022–2025 was 6. This category, introduced in 2021, allows the relative importance of reports to be assessed based on their link to factors such as the connection to serious crimes, the emergence of new risk patterns, the detection of criminal structures or criminal networks and/or the involvement of large sums of money.

Conclusion on the sector's residual risk: medium for ML and low/medium for TF

439. The public function of the Register (publicity, legitimisation and presumption of legality) makes it an inevitable target for attempts at external abuse; however, the conditions of access and the legal framework governing the Register, the registration assessment (assessment of legality), the CRAB as a centralised prevention body, and the RETIR (actual ownership linked to the filing of accounts) together form an advanced preventive system that substantially reduces residual risk. Exposure remains, particularly in relation to property, loans and corporate operations.

440. In the case of ML, the risk is higher for ML transactions due to certain types of high-risk transactions: sales of real estate, loans/acknowledgements of debt and corporate transactions of various kinds, such as capital increases and the transfer of shares (an act which has not been recorded in the Commercial Registers since 1989, being reflected solely in the share and participation registers maintained by companies, with access restricted to shareholders). All of these are routine transactions in the course of professional practice, which is why the residual risk associated with their use is classified as **medium**.

441. For TF, the types of transactions that must be submitted for registration do not currently correspond to TF's existing risk profile; therefore, in general, the level of residual risk is considered to be **low/medium.**

Sector: Lawyers 2026

Activity and context

442. Lawyers are obliged entities under Article 2.1(ñ) of Law 10/2010, of 28 April.

443. The legal profession is subject to AML/CFT legislation only in cases where legal professionals are involved in the following activities:

- The planning, execution or provision of advice on transactions on behalf of clients relating to the sale or purchase of immovable property or commercial entities,
- The management of funds, securities or other assets,
- The opening or management of current accounts, savings accounts or securities accounts,
- Organising the contributions necessary for the creation, operation or management of companies,
- The creation, operation or management of trusts, companies or similar structures,
- When acting on behalf of clients in any financial or property transaction.

444. Furthermore, when these independent professionals carry out activities relating to the provision of corporate services, as set out in Article 2.1(o) of Law 10/2010, of 28 April, they shall also fall within the scope of that Law.

445. The Code of Ethics of the Spanish Bar, approved by the Plenary Session of the General Council of the Bar on 6 March 2019, reaffirms compliance with ML/TF obligations in the course of professional practice. It should be emphasised that, in accordance with current legislation, lawyers are not subject to AML/CFT obligations with regard to information they receive or obtain from their clients when determining the client's legal position or carrying out their duty to defend that client in or in connection with legal proceedings, including advice on the initiation of proceedings or on how to avoid them, regardless of whether they have received or obtained such information before, during or after such proceedings, all with a view to safeguarding a fundamental right such as the right to a defence, which is specifically protected under our constitutional framework.

446. There are approximately 150,000 lawyers, many of whom are members of the roughly 2,900 professional firms operating in Spain. However, the number of professionals who meet the requirements to be considered obliged entities under Article 2.1.ñ of Law 10/2010 of 28 April is much lower, as it includes only those members of the bar who carry out the activities listed above and covered by the Law. Consequently, the number of professionals, including firms, who are actively involved in advisory functions subject to AML/CFT legislation stood at around 1,250 operators, according to information from SEPBLAC (2022–2024).

447. Furthermore, according to confidential information, it is estimated that the group of professionals with a significant level of turnover or business volume – and therefore with more complex internal control processes – would be smaller, comprising fewer than 300 regulated entities, amongst which are the country's leading firms. The economic scale of this latter group, measured in terms of aggregate turnover, amounts to approximately 5,300 million euros, although this figure would include, on an aggregate basis, turnover from both regulated and non-regulated activities

Threats

448. The legal sector faces a number of significant threats in relation to ML and TF, arising from the strategic nature of the legal services provided, its involvement in transactions of high economic value, and its potential role as a technical facilitator and legitimiser of complex financial, corporate and property structures.

449. These threats correspond fully to those identified in Chapter 4, particularly in relation to economic crimes, the use of shell companies, the concealment of beneficial ownership, corruption and cross-border operations involving high-risk jurisdictions; the sector is one of the most exposed amongst independent professionals due to its capacity to design, structure and advise on complex transactions. It should be emphasised that these threats are confined exclusively to the scope of activities subject to Law 10/2010 of 28 April, with actions relating to the right to a defence being excluded, in accordance with the current legal framework.

450. It is worth noting that legal services can be used to facilitate ML at any stage of the process (placement, layering and integration), through: advice on the sale and purchase of property and company shares; the structuring of complex corporate transactions; the design of financing or asset reorganisation schemes; and the management or channelling of assets on behalf of clients. Criminal organisations and perpetrators of economic crimes need to give the appearance of legality to illicit profits, and to do so they require the advice of professionals with in-depth knowledge of the legal system, which makes the legal profession a priority target for recruitment as a facilitator.

Economic crimes and the use of complex corporate structures

451. Chapter 4 identifies economic and corporate offences as structural threats. In the legal profession, the threat arises when the services provided are aimed at: (i) the creation and management of shell companies or companies with no real business activity; (ii) the design of multi-layered ownership structures; (iii) the use of directors; or (iv) nominal partners acting as intermediaries; and corporate reorganisations without a clear economic justification. These structures may be designed to conceal the origin of funds or disguise effective control, thereby hindering the identification of the beneficial owner and the analysis of ML/TF risk.

Corruption and technical support for asset concealment

452. Chapter 4 highlights political and financial corruption as a significant threat. In this context, the legal profession may be implicated when it is used to: i) structure assets obtained through corruption; ii) fragment ownership amongst family members or frontmen; iii) justify unexplained increases in assets; or iv) design legal vehicles to channel illicit payments.

453. The threat intensifies when PEPs, high-value transactions or international elements are involved, with legal advice being a key element in providing formal cover for these operations.

454. Furthermore, there is a risk that a legal professional or a law firm may make their own bank accounts available to channel clients' funds. This practice may constitute an intermediary mechanism designed to hinder the traceability of transactions, conceal the identity of the true parties involved, or create opacity regarding the origin, movement and destination of the funds, thereby increasing the risk of asset concealment.

Terrorist Financing

455. Exposure to terrorist financing (TF) in the legal sector is considered secondary, given that lawyers do not usually manage clients' funds directly. However, in exceptional circumstances, legal advice could be used to: structure asset vehicles, conceal assets, or indirectly support logistical networks. This threat exists, although its impact is limited compared with ML.

456. Furthermore, it is worth highlighting the following factors that may be exploited by threats within the legal sector in line with the activities analysed in this report:

Factors that are frequently exploited by threats	
Exposure cross-border and jurisdictions of risk	A cross-cutting factor in this sector is its growing exposure to cross-border operations, particularly in firms specialising in commercial, tax and property law, which manifests itself in: • advising non-resident clients, • structures with subsidiaries or parent companies in third countries, • fund flows originating in or destined for high-risk jurisdictions, • the use of offshore territories. The combination of legal complexity and an international dimension increases the difficulty of verifying the origin and purpose of funds, aligning fully with the risk typologies identified in the NRA.
Concealment of beneficial ownership and the use of intermediaries	In the legal sector, a significant factor contributing to the sector's exposure is the lack of transparency in identifying the ultimate beneficial owner where the following apply: • foreign companies or multi-tier holding companies, • trusts or similar structures, • the use of complex powers of attorney, • the involvement of multiple legal entities in different jurisdictions. Despite the existence of beneficial ownership registers, these structures can make it difficult to clearly reconstruct effective control, increasing the likelihood that, whether knowingly or not, the lawyer may contribute to maintaining opaque arrangements.
Occasional assignments and transactional relationships	The sector is particularly vulnerable in cases of one-off or occasional assignments, which: limit in-depth knowledge of the client, concentrate risk in specific transactions, and reduce the ability to observe long-term patterns of behaviour. This risk may be exacerbated in complex, short-term transactions, such as major property or corporate deals, where the intensity of the work coincides with a peak in exposure to ML and TF.
Use of intermediaries,	Another significant exposure factor stems from the use of: legal representatives and chains of power of attorney, foreign corporate documentation, and

representation and foreign documentation	established outside Spain, and professional intermediaries. These elements may hinder the effective verification of identity, representation and control, increasing the risk when sufficient or verifiable information is not available.

Risk factors due to inherent vulnerability

457. The following sets out the factors relating to inherent vulnerability that were analysed to determine the inherent risk in the legal profession

Characteristics of the sector	
Size of the sector and turnover	A sector with a large number of professionals, although only a fraction are involved in AML/CFT activities (advice on the incorporation, sale and purchase, and financing from various sources of companies, and property transactions). Materiality is concentrated in large law firms with a primarily commercial/tax practice.
Level of complexity of the sector's structure	A highly fragmented structure (a large number of individual practitioners and SMEs) alongside large firms. Varied levels of maturity in AML/CFT controls.
Level of integration with other regulated sectors	Frequent interaction with notaries, registries, financial institutions and estate agents in transactions that are classic money-laundering channels (company formation, advice on complex corporate structures, property sales, etc.).
Location of the organisation, including the geographical scope of the sector's operations	It operates nationally, although the major firms have offices in other countries (Portugal, Mexico, Colombia, Belgium, the United Kingdom and the United States, etc.). Public sources indicate an increase in activity by major law firms in South America.
Nature of the products and services provided by the sector	
Level determined by the complexity of the products, due to their impact on anonymity or the limited information on the clients.	Opaacity regarding the beneficial owner in complex structures and chains of intermediaries, making it difficult to verify the origin and purpose of funds. Occasional instructions, the use of intermediaries and the use of different companies within the same group (in different jurisdictions), which limit the monitoring of the business relationship.
The extent to which specific products and services offered are linked to STRs and/or national ML or TF investigations	During the period analysed, 673 reports were made by other regulated entities involving indications of activities involving lawyers. The main reporting sector is credit institutions, followed by registrars and notaries.
Nature of the client	
Level referred from the nature of the relationship	Transactional/occasional assignments predominate, although in to a lesser extent than in long-term relationships. There are

commercial relationships with customers, depending on their duration (ongoing, transactional or occasional) and the frequency of transactions	one-off complex transactions (e.g., property and cross-border deals) that generate peaks in risk during execution.
Level derived from the client's status	The sector is exposed to the potential use of complex corporate structures and to possible exposure through the provision of advice to politically exposed persons (PEPs), either directly or indirectly. Non-residents and links to higher-risk/offshore jurisdictions, such as Gibraltar due to its geographical proximity, increase the need for verification of beneficial ownership and the source and purpose of funds. Ownership chains where the beneficial owner is not transparent increase uncertainty regarding control and beneficiaries.
Level derived from the client's occupation or type of business	The sector is diverse and varies according to the firm's profile (size and specialisation determine the composition and complexity of the client base). The level of exposure increases when the client comes from cash-intensive sectors or the informal economy, or when they engage in cross-border operations or foreign trade with higher-risk or offshore jurisdictions; and it decreases when clients belong to listed business groups or regulated financial institutions, due to their greater transparency and supervision.
Geographical scope of the sector's activities	
Level derived from specific jurisdictions/countries of interest, frequently associated with the sector.	Operations are mainly domestic, although there has been an increase in international operations, particularly with Latin America. This growth is due to factors such as: • The growth in Latin American investment in Spain (+103 % since 2010)[98] . • The rise in corporate, property and international mobility transactions handled by law firms specialising in *'Latam Desk' services*. • The expansion of Spanish law firms into Latin America and the consolidation of international networks.
Level derived from the nature of the interactions or transactions involving countries identified by the FATF.	The level of exposure is higher in cross-border structures or transactions, or those involving multiple intermediaries in different jurisdictions, which result in greater opacity regarding the beneficial owner and make it more difficult to trace the funds.
Level derived from the nature of the interactions or transactions involving countries subject to international financial sanctions.	The PF SRA identified the use of front men to carry out direct settlements with specific bank accounts through the intermediation of professionals who coordinate the collection and payment for goods without there being a direct transfer to or from Iran.
Nature of the distribution channels	

[98] https://www.investinspain.org/content/icex-invest/es/noticias-main/2025/global-latam.html

Level derived from the complexity of the channels due to their impact on anonymity or on the less information available on clients.	Most of the interaction between lawyers and their clients usually takes place through the traditional face-to-face channel, which mitigates anonymity; however, exposure increases with remote engagements, or through intermediaries and chains of authorisations that make it difficult to identify the beneficial owner.
Level derived from the use of new technologies or payment methods.	The level of exposure could be higher for lawyers who accept alternative payment methods (e.g. payment service providers, e-money or crypto-assets) rather than traditional bank transfers, due to their speed, potential for fragmentation and lack of transparency.

Conclusion on the inherent risk of the sector: substantial/high for ML and medium for TF

458. The inherent risk in ML is assessed as **substantial/high** due to the combination of a highly fragmented and heterogeneous sectoral structure with the concentration of activities of greatest significance for ML/TF in large firms specialising in commercial, tax and property matters. The complexity of the services provided, the frequent use of complex and cross-border corporate structures, the lack of transparency in identifying the beneficial owner, and the predominantly transactional or occasional nature of the engagements increase the inherent vulnerability. Added to this is the intense interaction with other sectors traditionally exposed to ML, and the operational evidence reflected in reports based on indications submitted by other regulated entities.

459. The inherent TF risk in the sector is classified as **medium**, given a lower structural exposure than that of the ML sector. Legal advice may be used as a tool in transactions involving opaque structures, intermediaries or cross-border relationships, particularly with jurisdictions identified by the FATF or subject to financial sanctions. The occasional nature of some mandates and the involvement of non-resident clients increase the difficulty of early detection, although the limited evidence of TF threats in the sector amply justifies a lower inherent risk assessment.

Risk factors arising from the effective (or ineffective) implementation of controls

460. To analyse residual risk, it is necessary to analyse the implementation of existing controls within the sector and the extent to which these controls are effective. The following section presents an analysis of the factors used to determine the residual risk in the legal profession.

Risk factors relating to the effective implementation (or lack thereof) of controls	
Level of regulation in the sector	The profession is a professional body with its own regulations. The scope of activities under Law 10/2010, of 28 April, is limited to those set out in Article 2.1(ñ).
Level of potential presence of unauthorised entities operating in the sector.	As it is a collegial body, unauthorised practice is reduced; however, the free provision of legally regulated activities in this sector does not require any specific licence or registration, which makes it difficult to identify the professionals carrying out these operations.

Level of potential direct or indirect control over the entity or its management by money-laundering networks	The interest of networks in recruiting professional facilitators to act as intermediaries in illicit transactions means there is a non-negligible endogenous risk, particularly in small organisations. The risk associated with this factor is low for large firms.
Level of regulation of AML/TF prevention measures	Entities and professionals in the sector are regulated entities in relation to ML/TF prevention when they carry out the transactions expressly specified in the law (Law 10/2010 of 28 April, Article 2.1.ñ). In addition, there are sector-specific guidelines, which may be implemented inconsistently due to differences between sectors.
Level of supervision	SEPBLAC acts as the AML/CFT supervisory authority for the sector. The scope of supervision is determined by the prioritisation of EBRs and by the sector's low track record of reporting. Given that a significant proportion of the activity is concentrated in a small number of large firms, the supervisory actions carried out on these firms provide, in relative terms, a meaningful sector-wide overview. Progressive, individualised understanding is being achieved through tools such as prevention questionnaires, which were introduced in 2024 for 50 regulated entities and expanded in 2025 to 60 firms based on the scale of their activity. As regards on-site inspections, 21 were carried out between 2020 and 2025.
Level of sanctions imposed on entities in the sector.	There has been a high frequency of inspections resulting in administrative requirements or sanctions, coinciding with the change in approach to the review of this category of regulated entities. During the period in question, SEPBLAC issued six remedial requirements to large law firms, containing 22 requests for improvement. Furthermore, three disciplinary proceedings were initiated, which resulted in findings of serious breaches.
Level of the Professionalism of administrators and senior managers of the organisation.	The level of professionalism in medium-sized and large firms is, in general, high, and across the sector as a whole there is variation linked to the size and degree of formalisation of compliance functions.
Level of awareness and understanding of their obligations regarding the prevention of ML and TF.	Regulatory knowledge exists but varies in terms of scope and degree of specialisation; there is room for improvement in the risk-based approach and the graduated application of due diligence measures, particularly those relating to beneficial ownership and business activities. Areas of confusion persist within the sector regarding the classification of activities subject to AML/CFT legislation, which may result in the uneven application of controls.
The organisation's level of commitment to ML/TF policies and measures.	Commitment increases with size: medium-sized and large firms tend to have formalised policies and defined roles and sometimes have specialised teams at group level that reinforce compliance with policies; in smaller organisations, the degree of formalisation is more variable.
Level of professional qualifications of the employees and their training in ML/TF	Training is available and more systematic in medium-sized and large firms, although there is still room for improvement in terms of both content (adapted to the operational actual of the firm and to the extent of the responsibility of the recipients), as well as the

prevention.	amount of time spent each year to training. There are no penalties or requirements regarding breaches of training policies in this sector.

Level of internal monitoring by the organisations of employee compliance.	This should be carried out by reviewing records and files to verify the effectiveness of the system; its implementation varies according to size and structure: in firms with a dedicated compliance function, monitoring is documented, whilst in smaller organisations it tends to be more basic and operational. In many small-to-medium-sized organisations, there is no formal internal audit department, which reduces the professionalism and frequency of internal checks
Level of compliance with preventive measures, particularly CDD/KYC	CDD/KYC procedures are applied, but the recurring challenge lies in cases involving above-average risk, particularly in the effective verification of the beneficial owner and the documentation of the source and purpose of funds in complex and cross-border structures, or where third parties are involved. There are no penalties for non-compliance with due diligence obligations. However, improvements to these procedures were requested in 5 out of the 6 findings identified.
Level of identification and reporting of suspicious transaction reports	A historically low figure (131 reports during the period analysed, averaging almost 22 reports per year), suggesting under-reporting. Weaknesses were identified in the recording and reporting of merely attempted transactions (requests for services that were ultimately not provided as they did not pass the customer onboarding processes). There is a need for improvement in the reporting obligations to an organisation. The average rating for the significance of reports by indicator for the period 2022–2025 was 5.6. This category, introduced in 2021, allows the relative importance of reports to be assessed based on their link to factors such as the connection to serious crimes, the emergence of new risk typologies, the detection of criminal structures or networks, and/or the involvement of large sums of money.

Conclusion on the sector's residual risk: substantial in ML and low/medium in TF

461. Starting from an inherent ML risk initially assessed as **substantial/high**, the analysis of the mitigating measures applicable to the legal profession reveals a partial reduction in the level of risk, stemming primarily from the existence of a specific regulatory framework, the gradual intensification of risk-based supervision, and the recent strengthening of inspection and sanctioning measures. However, significant structural vulnerabilities persist, linked to the heterogeneity of the sector, the endogenous risk of recruiting professionals as frontmen, recurring weaknesses in enhanced due diligence in complex and cross-border scenarios, and a historically low level of detection and reporting of suspicious transactions, which limits the overall effectiveness of the preventive system. Consequently, it is concluded that, despite the progress observed, the residual ML risk is **substantial**.

462. With regard to TF, based on an inherent risk initially assessed as medium, the set of mitigating

measures analysed is, in general terms, adequate and proportionate to the sector's actual exposure, taking into account that no evidence has been detected compared with ML, as well as the application of the common preventive framework and the supervision exercised by the competent authority. Whilst there are still areas for improvement, no deficiencies have been identified. It is therefore concluded that the residual risk of TF is at a **low/medium** level.

Sector: Provision of corporate services to third parties 2026

Activity and context

463. Providers of corporate services to third parties are obliged entities under Article 2.1.o) of Law 10/2010, of 28 April.

464. Article 2.1.o) of Law 10/2010 of 28 April includes as obliged entities those persons who, on a professional basis and in accordance with the specific regulations applicable in each case, provide the following services on behalf of third parties:

- to incorporate companies or other legal entities;
- to hold executive positions or serve as non-director secretaries on the board of directors or as external advisers to a company, as a partner in an association, or to perform similar functions in relation to other legal entities, or to arrange for another person to perform such functions;
- provide a registered office or a business, postal or administrative address, and other related services, to a company, an association or any other legal entity or person;
- to act as a trustee in a trust or similar legal arrangement, or to arrange for another person to act in such a capacity; or
- acting as a shareholder on behalf of another person, except in the case of companies listed on a regulated market within the European Union and subject to disclosure requirements in accordance with EU law or equivalent international standards ensuring adequate transparency of information on ownership or arranging for another person to perform such functions.

465. The Commercial Register does not publish official figures for those registered in the Register of Service Providers to Companies and Trusts. As of December 2024, the Register of Corporate Service Providers to Third Parties listed 5,464 natural persons and 9,888 legal entities providing this service. By category, 2,571 provide advisory services, 641 provide legal services (solicitors), and 187 provide services in both fields. Registration takes place at the regional Commercial Registers, with Barcelona and Madrid having the highest number of registered providers, followed by Valencia, Seville and Málaga.

466. As part of their obligations, they must submit an annual declaration reporting on the services provided during the previous financial year. In 2025, 1,160 corporate service providers filed returns, declaring a turnover of 12,007 million euros from services provided in 2024. Of these, 133 were listed as unregistered and accounted for 1 % of the total declared turnover.

Threats

467. The sector providing corporate services to third parties faces a number of significant ML/CFT threats, arising from its role as a corporate legal facilitator, its high degree of heterogeneity, the fragmentation of regulated entities, and frequent interaction with complex and cross-border corporate structures.

468. These characteristics are fully consistent with several of the threats identified in Chapter 4, particularly in relation to economic crime and tax fraud, the use of shell companies, opaque structures, the concealment of beneficial ownership, corruption, and international operations targeting high-risk jurisdictions. Although the number of potential professionals is high, the effective scope of SO is difficult to quantify, which introduces an additional structural threat relating to the incomplete identification of the sector and the uneven application of AML/CFT obligations.

Economic crimes and the use of shell companies

469. The provision of corporate services enables, amongst other things: i) the incorporation of companies with no real economic activity, ii) the provision of fictitious or shared registered offices, iii) the appointment of nominee directors or shareholders, iv) the establishment of complex corporate chains, v) the reorganisation of business groups for opaque purposes. These functions make the sector a critical entry point for shell structures used to commit or conceal economic crimes, particularly in small or less specialised firms where controls are less robust.

Organised crime and the recruitment of professional facilitators

470. National threats highlight that criminal organisations are increasingly turning to professional facilitators to give their operations the appearance of legality. In this sector, the threat manifests itself through: i) the use of lawyers or agents to create opaque corporate structures, ii) the recruitment of small law firms to maintain companies, iii) the provision of administrative or fiduciary services without adequate know-your-client checks, and
iv) use of third-party nominal owners to conceal effective control. There is a risk of professionals being co-opted from within, particularly in small organisations with low levels of formalised compliance.

Corruption and asset concealment

471. Corporate services may be used to: i) conceal assets derived from corruption,
ii) channelling covert payments through intermediary companies, iii) structuring shareholdings in the names of family members or frontmen, iv) reorganising assets to conceal unjustified increases in wealth. The level of exposure to this threat increases when PEPs, cross-border structures or jurisdictions with low corporate transparency are involved.

Terrorist Financing

472. The risk of terrorist financing (TF) is lower than that of money laundering (ML) due to the asset-based nature of the services, but it is not non-existent. National threat assessments warn that certain corporate structures may be used to: i) channel covert donations, ii) serve as a logistical or financial vehicle for terrorist groups, and iii) conceal flows to third countries through complex legal structures.

473. Furthermore, it is worth highlighting the following factors that may be exploited by threats within the online corporate service providers sector, in line with the activities analysed in this report:

Factors that are frequently exploited by threats	
Concealment of Beneficial Ownership and the Use of Trusts and Similar Structures	High exposure in: i) services related to *trusts*, fideicomisos, or similar legal vehicles; ii) the incorporation of foreign companies with intermediate layers; iii) chains of powers of attorney and mandates; iv) nonresident clients who use structures that are uncommon in Spain. These patterns make it difficult to identify the ultimate beneficiary and the source of the funds, significantly increasing the risk of ML/TF.
Cross-Border Exposure and High-Risk Jurisdictions	This threat can materialize through: (i) clients from countries with a tradition of trust, (ii) companies incorporated abroad but managed in Spain, (iii) multi-level structures spanning multiple jurisdictions, and (iv) the use of intermediaries in high-risk countries.
Use of Online Channels and Foreign Documentation	The exposure associated with non-face-to-face channels and foreign national documents increases the risk when: i) orders are placed remotely, ii) intermediaries are involved, iii) foreign powers of attorney are used, iv) documents that are difficult to verify are provided. These circumstances undermine the effectiveness of customer identification and foster opacity.

Risk factors due to inherent vulnerability

474. The following sets out the factors relating to inherent vulnerability analysed to determine the inherent risk in the sector.

Characteristics of the sector	
Size of the sector and turnover	This sector comprises a large number of professionals. A very small proportion of these operate in the provision of corporate services; however, the lack of official turnover figures means that, when assessing risk exposure based on the size of the sector, a cautious approach is taken and this lack of information is factored into the assessment. Furthermore, in Spain, this activity is typically carried out by both lawyers and administrative managers. These administrative managers usually carry out tax advisory work.
Level of complexity of the sector's structure	A highly fragmented structure (a large number of individual practitioners and SMEs) alongside large law firms. There is considerable variation in the maturity of AML/CFT controls. As mentioned, there are 5,464 individuals and 9,888 legal entities registered as of December 2025.
Level of integration with other regulated sectors	Frequent interaction with notaries, registries and financial institutions in transactions that may serve as traditional ML channels (company formation, advice on complex corporate structures, property sales, etc.). Furthermore, account must be taken of the data included in the sector description regarding the estimated number of regulated professionals providing these services: 2,571 of whom 641 provide legal services (as solicitors) and 187 provide services in both professions.
The entity's geographical location, including the geographical scope of the sector's operations	Based on the annual returns, it is estimated that 97 % of operations are carried out at a national level and 3 % at an international level. Furthermore, if a breakdown is required within the national territory, as mentioned, the registers with the highest number of registered service providers are Barcelona and Madrid, followed by Valencia, Seville and

	Málaga, which have the highest number of registered providers.

Nature of the products and services provided by the sector	
Level derived from the complexity of the products, due to their impact on anonymity or the limited information available on customers.	Acting as an intermediary in the incorporation of companies and the provision of corporate services to nationals of another country carries an extremely high risk that these services may be used for ML/TF operations. The lack of a physical presence and the consequent difficulty in verifying the identity of beneficial owners – particularly in the case of trusts and similar arrangements – increases the need to use alternative measures for verifying the identity of customers, which hinders potential ML/TF operations concealed under these circumstances.
The extent to which specific products and services offered are linked to tip-off reports and/or investigations[99].	It is not possible to estimate the services provided by the sector that are involved in tip-off communications.
Nature of the customer	
Level derived from the nature of the business relationship with customers, based on the duration (ongoing, transactional or occasional) and frequency of transactions	Difficulty in monitoring transactions, as these are, in many cases, one-off transactions. However, as this is an activity typically provided by solicitors, accountants and consultants, some relationships tend to be ongoing due to the provision of services ancillary to corporate services.
Level derived from the client's status	The distinct nature of corporate service provision operations, particularly those involving nationals of another country, entails a substantial risk of such operations being used for ML/TF purposes. This, combined with the difficulty in identifying the beneficial owners, increases the need to use alternative control measures to verify clients' identities; however, the application of these measures is not uniform given the fragmentation of the sector. In the annual returns submitted to the Register, 74 % of corporate service providers have declared that they conduct business solely with residents, whilst 26 % have provided services to non-resident third parties.
Level derived from the client's occupation or type of business	Vulnerability is varied and depends on the profile of the solicitor/adviser (the size and specialisation of the practice determine the composition and complexity of the client base); it increases when the client comes from cash-intensive sectors or the informal economy, when they engage in cross-border operations or foreign trade with higher-risk or offshore jurisdictions; and it decreases when clients belong to listed business groups or financial institutions subject to greater transparency and supervision.
Geographical scope of the sector's activities	
Level derived of jurisdictions/countries specific of interest	74 % of corporate services provided and declared annually are carried out for people resident in Spain; 26 % are for non-residents who have received services from service providers domestic shareholders.

[99] This variable was classified as 'substantial-high'

frequently related to the sector.	3% of operations are international in scope; the remaining 97% have been carried out in Spain.
A level resulting from the nature of the interactions or transactions involving countries identified by the FATF.	It is not possible to quantify international operations with high-risk countries. However, it should be borne in mind that, of the annual returns submitted, only 3 % relate to international operations.
Level derived from the nature of the interactions or transactions involving countries subject to financial.	Whilst it is not possible to quantify international operations, it should be borne in mind that, of the annual returns filed, only 3 % relate to international activities. Furthermore, there is no evidence of corporate services being provided in jurisdictions subject to international financial sanctions.
Nature of distribution channels	
Level derived from the complexity of the channels, given their impact on anonymity or on the limited information available about clients.	Traditionally, face-to-face channels mitigate anonymity, but the level of vulnerability increases with the recent rise in remote corporate services.
Level derived from the use of new technologies Or payment methods.	There is no evidence of the use of new technologies in this sector, nor of payments using crypto-assets.

Conclusion on the sector's inherent risk: Substantial/High for ML and low–medium for TF.

475. The inherent risk associated with ML is classified as **substantial/high** due to the sector's marked fragmentation and high degree of heterogeneity, combined with the complexity of certain corporate services. Key risk factors include the widespread use of legal structures, difficulties in correctly identifying and verifying the beneficial owner — particularly in the case of non-resident clients — and the existence of occasional transactions, which complicates the traceability and ongoing monitoring of transactions. Furthermore, risk exposure is heightened by frequent interaction with sectors that are particularly sensitive from an ML (money laundering) perspective, such as notaries, registers and financial institutions, as well as by the significant presence of foreign clients, who account for approximately 26 % of the total, thereby increasing the likelihood of potential misuse of these services.

476. With regard to TF, the inherent risk is assessed as **low/medium**, given that the provision of corporate services does not, generally speaking, constitute a channel commonly used for this type of illicit activity, and the analysis of the factors examined focuses primarily on offences typically associated with the ML.

Risk factors relating to the effective implementation (or lack thereof) of controls

477. To analyse residual risk, it is necessary to assess the implementation of existing controls within the sector and the extent to which these controls are effective. The following section presents an analysis of the factors used to determine the residual risk in the corporate services sector.

Risk factors relating to the effective implementation (or lack thereof) of controls	
Level of regulation in the sector	There is no specific regulation governing the provision of corporate services. However, as this activity is carried out by solicitors and administrative managers, the regulations governing these sectors apply to professionals engaged in the provision of corporate services.
Level of potential presence of unauthorised entities.	As a result of the transposition of Directive (EU) 2015/849 on the prevention of the use of the financial system for ML, through Royal Decree Law 11/2018 introduced the obligation for natural or legal persons providing any of the services described in Article 2.1.o) of Law 10/2010, of 28 April, to register in the Register of Service Providers to Companies and Trusts within the Commercial Register. This measure reduces unauthorised practice, although there is no data on the effectiveness of compliance.
Level of potential direct or indirect control over the entity or its management by money-laundering networks	The interest of networks in recruiting professional facilitators is not a negligible endogenous risk, particularly in small organisations and in the case of individuals who are registered as providers of these services.
Level of regulation of ML/TF prevention measures	Law 10/2010, of 28 April, and Royal Decree 304/2014 of 5 May, applicable to scope 2.1. Additionally, sector-specific guidelines with the potential for uneven implementation due to differences in size and profile of payment service providers.
Level of supervision	The sector is subject to ML/TF inspections by SEPBLAC, which cover independent professionals who may carry out corporate services, such as lawyers. Between 2020 and 2025, three inspections were carried out on these regulated entities.
Level of sanctions imposed on entities in the sector.	Of the three inspections carried out on these regulated entities, the outcome was one disciplinary proceeding and one formal notice requiring a remediation plan to address the deficiencies identified. Deficiencies were identified in internal control procedures, reporting on suspicious activity and training.
Level of the professionalism of administrators and senior management of the organisation.	The level of professionalism amongst medium-sized and large regulated entities is generally high, and across the sector as a whole there is considerable variation linked to the size and degree of formalisation of compliance functions; consequently, the need for training in AML/CFT is significant for this sector.
Level of dissemination and awareness of its	Regulatory awareness is strongly supported and promoted by professional bodies, but its implementation varies due to the size and degree of specialisation of the regulated entities; there is

obligations to prevent ML and TF.	There is room for improvement in the risk-based approach and the graduated application of due diligence measures, particularly those relating to beneficial ownership and business activity. There remain areas of confusion regarding the scope of the activities covered, which may result in the uneven application of controls.
The organisation's level of commitment to ML/TF policies and measures.	Commitment increases with size: medium-sized and large regulated entities tend to have formalised policies and defined roles, and sometimes have specialised teams at group level that reinforce compliance with policies; in structures un small firms, the degree of formalisation varies more widely.
Level of professional qualifications of employees and their training in ML/TF prevention.	Training is more systematic in medium-sized and large regulated entities, although there is still room for improvement both in terms of content (tailored to the firm's actual operations and the level of responsibility of the recipients) and the annual time devoted to training. The risk is considered substantial.
Level of internal monitoring by the entities of employee compliance.	This should be strengthened by including records and file reviews to verify the system's effectiveness; its implementation varies according to size, structure and type of operations. In small-to-medium-sized organisations, there is no formal internal audit department, which reduces the professionalism and frequency of internal audits.
Level of compliance with obligations regarding preventive measures, particularly CDD/KYC	CDD/KYC procedures are generally applied, but the recurring challenge lies in cases involving above-average risk, particularly in the effective verification of the beneficial owner and the documentation of the source and purpose of funds in complex, cross-border structures, or through intermediary third parties.
Level of identification and reporting of suspicious transaction reports [100]	Given the lack of consistency in the application of AML/CFT measures, stemming from a large number of small-scale regulated entities, differences in training and awareness, the absence of formal compliance departments, and confusion regarding the scope of activities subject to regulation. This fragmentation hinders the early detection of suspicious transactions and creates systemic gaps that can be exploited by illicit networks.

Conclusion on the sector's residual risk: Medium/substantial for ML and low for TF

478. The residual risk in relation to ML stands at a **medium/substantial** level**.** Whilst the sector has a clear AML/CFT regulatory framework, mandatory registration and supervision by SEPBLAC, the effectiveness of controls is unevenly implemented, particularly in small firms and among individual professionals. The absence of specific sectoral regulation, the risk of ML networks recruiting facilitators, and persistent difficulties in identifying the beneficial owner in complex and cross-border structures limit the overall capacity for risk mitigation. Professionalism and commitment are higher among medium-sized and large regulated entities, which partially reduces the risk; however, the average level of effective compliance, combined with a substantial risk in the detection and reporting of suspicious transactions, prevents the residual risk from being reduced to low levels.

479. The residual risk in relation to TF is assessed as **low**. Based on a low–moderate inherent risk, the mitigating factors — the predominance of domestic operations, reduced international exposure,

[100] This variable was rated as substantial–high

the absence of links to sanctioned jurisdictions and the widespread implementation of AML/CFT measures—are sufficient to classify this risk.

Sector: Gambling: casinos, lotteries, slot machines and gaming venues, in-person betting, online gambling, sports and charity pools (quinielas) 2026

Activity and context

480. Casinos, lotteries, slot machines and gaming venues, in-person betting, online gambling and sports-charity pari-mutuel betting (football pools) are obliged entities under Article 2.1(p) and (u) of Law 10/2010, of 28 April.

481. The gambling sector in Spain comprises various types of activities which are grouped according to the level of jurisdiction: in this case, state and regional.

482. All forms of gambling are subject to the provisions of the prevention regulations, although there are differing levels of requirement regarding prevention obligations due to their varying exposure to the risk of ML and TF.

483. The gambling market is a significant economic activity in Spain, involving various types of organisations, including large international groups, public bodies and private national organisations of varying sizes, which operate across both land-based and online activities. In online systems, the level of exposure to ML is high; consequently, it has recently been stipulated that operators must use centralised systems to identify and verify the identity of customers.

National scope

484. The Directorate-General for the Regulation of Gambling (DGOJ) is responsible at national level for authorisation, supervision and control, with the aim of ensuring the proper functioning of the sector and the protection of players and vulnerable groups. The applicable regulations cover the technical requirements for gambling activities and the enforcement of subjective prohibitions on participation in games. They also set out rules on the verification of identity details and the verification of information provided by participants, regulating in great detail the procedures for identity verification and the documentation provided by online players.

485. With regard to gaming licences, authorisations and registrations, the regulations stipulate that SEPBLAC must assess, prior to authorisation by the DGOJ, the mechanisms in place to prevent fraud and the systems for preventing ML and TF.

Lotteries

486. Lotteries, unlike betting, are not linked to any sporting or other event organised by third parties; their winning numbers or combinations are determined by chance. They are operated by the State Lottery and Betting Society (SELAE), the National Organisation of the Spanish Blind (ONCE) and the Red Cross.

487. In 2024, lotteries sold by the operators SELAE, ONCE and the Red Cross reached13,099 million euros in stakes, showing an upward trend since 2020, when stakes totalled 9,181 million euros, representing a total increase of 43 %. These are mainly sold in-person, although there is a growing trend towards online sales, particularly for weekly games.

488. In 2024, €10,230 million corresponded to SELAE games, a figure representing a 36 % increase from 2020, when it stood at €7,537 million: the National Lottery (regular draws, El Niño, Christmas Draw) rose from 4,589 million euros in 2020 to 6,398 million euros in 2024, and the active games managed by SELAE (Primitiva, EuroMillions, Bonoloto, Gordo de la Primitiva and Loto Turf) will generate 3,832 million euros in 2024, compared with 2,948 million euros in 2020.

489. The games marketed by ONCE have shown significant growth over the 2020–2024 period. In 2020, the total turnover from in-person and online channels reached 1,615 million euros, whilst in 2024 this figure rises to 2,829 million euros. This represents an absolute increase of 1,214 million euros and a percentage growth of 75 % compared with the initial figure. Alongside the various types of lottery tickets, which account for the bulk of its business, ONCE sells instant lotteries and certain active lotteries [(101),]drawing on a network of sales outlets across the whole of Spain (20,309 direct sellers in 2024 compared with 18,812 in 2020) and a long-standing tradition in Spain.

490. In addition, the Red Cross lottery saw 40 million euros staked in 2024, compared with 29 million in 2020, representing steady growth of 38 %.

Betting

491. The management of betting, like other state-run online games, takes place via national-level websites (.es) which must comply with strict requirements established by Spanish legislation aimed at preventing gambling operations from taking place on illegal platforms. These operators are authorised, regulated and monitored by the DGOJ, which grants them a seal of quality and security.

492. This market will generate bets worth around 10,275 million euros in 2024, compared with 7,035 million euros in 2020, across both online and in-person gaming channels. Despite strong growth in recent years (46 %), the peak was reached in 2021 (€11,065 million), followed by a significant decline in 2023. Meanwhile, wagers placed through SELAE have increased by 10 %, from 150 million in 2020 to 166 million in 2024.

493. In 2023, SELAE managed to reverse the downward trend that La Quiniela had been experiencing up until 2019. This was partly due to the introduction of Elige 8, a game inspired by the early English pari-mutuel betting systems. Sales of La Quiniela reached 162 million euros in 2023, compared with 143 million in 2019; although this figure remains 18 % lower, it has reversed the downward trend seen between 2020 and 2022.

Other nationwide online games.

[101] Eurojackpot, Triples and Mi día.

494. The online gambling sector has a lower turnover than land-based gambling but is significantly exposed to ML and TF. Specifically, online gambling accounted for 11.5 % of total real-money gambling in 2023. Recent inspections carried out by SEPBLAC have shown that, beyond the obligations inherent to responsible gambling, AML/CFT obligations are not being met and that gambling accounts are being used as de facto current accounts without any due diligence measures being applied. Cases of identity theft and the existence of 'mule' accounts were detected, as well as a lack of control over payment methods and a lack of customer knowledge and monitoring, making this sector an attractive niche for ML.

495. The online gambling market is served by 77 licensed operators, of whom 64 are licensed to offer gambling services to end consumers; the majority of these offer casino games (49) and sports betting (43). The monthly average number of active accounts in 2024 was 1,433 million, representing a 23 % increase on the previous year, whilst the monthly average number of new gambling accounts was 152,000 users, with an annual growth rate of 35 %.

496. In the online gambling sector, the total amount wagered reached 35,092 million euros in 2024, consolidating an upward trend that began in 2020, when the figure stood at 21,475 million euros. This growth represents a cumulative increase of 63 % over the period analysed.

497. The betting segment recorded €10,277 million in wagers, representing a growth rate of 46% compared with 2020. This trend is due to the increase in conventional sports betting and the market for other forms of betting, although the market for horse racing betting has declined. Bingo accounted for €92 million in wagers, representing a 24 % decline since 2020.

498. The casino segment saw growth in 2024, with €21,525 million in wagers and an 85 % increase compared with 2020. This growth is mainly due to the performance of slot machines, which, since their introduction in 2015, have led to the casino's market share steadily increasing relative to the other segments. In 2024, prize draws saw a 99 % decrease in the amount wagered compared with 2020, totalling 45,000 euros, with the decline being particularly sharp in 2021.

499. In 2024, poker saw a 13 % increase in the amounts wagered compared with 2020, totalling 3,199 million euros. A distinction is made between tournament poker, which accounts for 73.58 % of the market, and cash poker, which accounts for the remaining 26.42 %. It is also worth noting that since the launch of shared liquidity for poker with France and Portugal in January 2018, six platforms have been set up in Spain.

Regional level.

500. At regional level, the regulatory framework for gambling activities in each of the autonomous communities is based on the relevant regional law, which is implemented through various regulatory instruments. In this context, gambling—which includes casinos, bingo halls, gaming halls, betting shops, racecourses and 'B' and 'C' type machines—is regulated in accordance with the provisions of each Autonomous Community, with the supervision and control of these establishments and terminals falling outside the remit of the DGOJ.

501. The national legislation on the prevention of ML and TF, Law 10/2010, of 28 April, designates casinos as obliged entities under Article 2.1.p) and, furthermore, those responsible for the management, operation and marketing of lotteries or other games of chance, whether conducted in person or via computerised, telematic or interactive means ('online' gambling), Article 2.1.u), without distinguishing whether the gambling is organised at regional or national level. In the case of lotteries, charitable sports betting, competitions, bingo and 'Type B' amusement machines, this applies solely to prize payment transactions.

Betting and premises offering betting games.

502. Betting managed and regulated by the autonomous communities totalled some 2,485 million euros in stakes in 2024, compared with 1,272 million euros in 2020, of which 2,189 million corresponded to in-person betting and the remainder to online betting, with an upward trend since 2020, as has been the case at national level. In terms of in-person betting, in 2024 this form of gambling takes place in 16,201 specific betting outlets, gaming halls or other gambling establishments, of which 11,845 are hospitality venues and 3,846 are gaming halls, to highlight the most significant figures in the total amount.

Casino games and casinos.

503. Land-based casino games (blackjack, punto banco, roulette and poker, as well as 'C'-type gaming machines) generated a total of 2,118 million in wagers in 2024, compared with 828 million in 2020, continuing the growth trend observed. These games can only be played in casinos. In Spain, there are 49 open casino venues, 6 annexe venues and 911 'C'-type gaming machines, as well as a total of 398 casino gaming tables. In total, they attract nearly 4 million visitors annually. In addition to the casino games mentioned above, casinos also offer other types of games of chance ('B' machines), which in 2024 accounted for 62 % of the total amount wagered, amounting to 1,305 million.

Bingo games and bingo halls.

504. In 2024, there were 322 bingo halls in Spain, compared with 329 in 2020, and the amounts wagered have shown a steady increase, rising from 1,002 million euros in 2020 to 1,927 million euros in 2024, representing a total growth of 92 %. Bingo halls are recovering from the effects of the pandemic, during which their gaming turnover was halved. The improvement in their figures is due both to customers returning to the halls and to their 'transformation' through the introduction of online bingo, an expanded range of games featuring B-type machines, and improvements to their facilities. Online bingo accounted for 62 % of the amounts wagered in 2024, concentrated in Madrid and Andalusia, whilst traditional bingo accounted for the remaining 38 %, with the latter concentrated in Catalonia and the Valencian Community.

Gaming halls.

505. Gaming halls, whilst subject to stringent requirements for operating their business, may offer different gaming activities depending on the autonomous community. The number of gaming halls remained stable between 2020 and 2024, with 3,751 halls in 2024, representing a slight increase of 2 % compared with 2020.

The autonomous community with the highest number of gaming halls was Andalusia, with 921 in 2024. They are generally small in size and offer 'Type B' gaming machines, sports betting or other forms of betting, alongside other services such as a café or arcade machines. The potential impact from a ML/TF risk perspective lies in the different gaming activities carried out by each hall.

'Type B' gaming machines.

506. These machines (although they are known by a different name in some autonomous communities) can award cash prizes in exchange for a stake, using a probabilistic programme based on a cycle of games (rather than a random outcome in each individual game, as is the case with 'C'-type machines typically found in casinos). These machines may be installed in gaming halls, casinos or bingo halls, but also in pubs and restaurants. In 2024, there were 177,000 'B' type machines, with hospitality venues accounting for 84 % of these machines. They are spread across 99,000 premises, with a particularly high concentration in Andalusia, Catalonia and the Valencian Community. The prize amounts are limited (most offer a maximum prize of 500 euros), which virtually eliminates their vulnerability from a ML/TF risk perspective.

In-person betting and betting terminal machines.

507. Betting terminals are operated in person by users and are connected to a central betting system. They may be located in dedicated betting premises or in betting areas within bingo halls, casinos, gaming halls, sports centres, racecourses or hospitality establishments, as authorised by each autonomous community.

508. In 2024, there were 4,356 gaming premises with auxiliary betting machines (298 bingo halls, 1 racecourse, 3,846 amusement arcades and 210 betting shops) and 11,845 hospitality establishments.

509. In-person bets are anonymous at the time the bet is placed and take the form of bearer tickets. Player identification is deferred until the prize is paid out and is required only for prizes exceeding 2,000 euros. Some autonomous communities also require prizes exceeding 2,500, 3,000 or 3,005 euros to be reported.

510. Regional regulations do not set quantitative limits on stakes or prizes, leaving these to be determined by the operators' specific terms and conditions, except for bets placed in hospitality venues and only in the regions of Galicia, the Valencian Community and La Rioja, which limit the maximum single stake to between 20 and 50 euros.

511. Betting presents a specific risk profile from the perspective of Money Laundering prevention, insofar as, unlike pure games of chance, the outcome is not entirely random but probabilistic, based on real events and amenable to analysis and estimation through odds. This characteristic allows betting strategies to be devised that can generate economically plausible outcomes through the use of odds and combinations, thereby facilitating the ex post justification of the winnings obtained.

512. Added to this is the fact that customer identification only takes place when prizes exceeding certain thresholds are paid out, which creates a window of risk that could be exploited by splitting bets or transferring tickets.

513. The following risk factors therefore exist: probabilistic outcome, anonymity when placing a bet, transferable bearer tickets, customer identification only at the time of collection, and the absence of prize limits.

Lotteries.

514. There are also some lottery activities managed by regional governments with a low turnover. In 2024, the autonomous communities' own lotteries stood at around 56 million euros in amounts wagered through in-person and online channels. They show an irregular trend, reaching their peak in 2021 at 69 million, after which a downward trend began, culminating in the current figure of 56 million.

Online gambling.

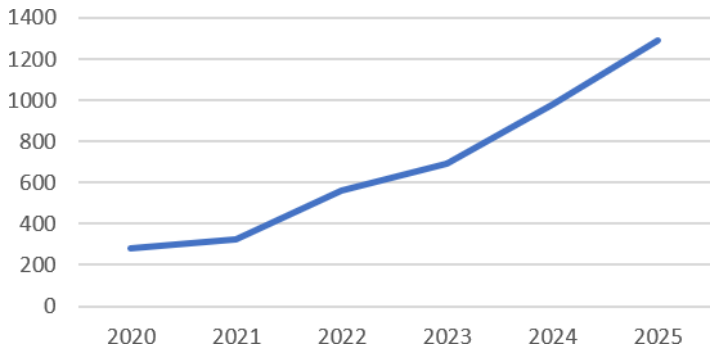
515. Regional online gambling accounts for a very small percentage of the gambling market: 298 million in stakes in 2024 compared with 228 million in 2020 (of which 99 % relates to sports betting). The Basque Country is the regional regulator with the largest share, accounting for 59 % of the stakes

Threats

516. The gambling sector in Spain encompasses a wide variety of formats — lotteries, betting, casinos, bingo, gaming halls, amusement machines and online gambling — with varying levels of exposure to ML and TF threats. This diversity, combined with the high overall economic volume, the massive participation of players, and the growing digitalisation of the activity, gives rise to a set of significant risks in certain segments of the sector.

517. These threats correspond directly to the types identified in Chapter 4, in particular ML offences and economic fraud involving the use of cash, digital channels, identity theft, 'mule' accounts, electronic payments and gambling activities. There is, however, a clear distinction between traditional land-based gambling (B-type machines, bingo, lotteries) and online betting and gambling, with the latter being the area most exposed to the relevant threats facing the sector.

518. Among the reports received from this sector, the following chart shows an exponential increase in reports, highlighting the presence of criminal activities linked to fraud and scams, in relation to the economic crime threats identified at national level.



Source: SEPBLAC

Money Laundering through gambling as a mechanism for placement and legitimisation

519. The gambling sector is a potential channel for ML, particularly during the placement and integration phases, as it allows for: i) the conversion of illicit funds into apparent gambling winnings, ii) the legitimisation of income through prizes, iii) the laundering of cash via bets or the purchase of chips, and iv) the interweaving of illicit activity amongst legitimate gambling transactions.

520. These patterns occur to varying degrees depending on the form of gambling. In traditional land-based gambling, prize limits and supervision reduce its appeal. In land-based betting, however, its probabilistic nature, the anonymity involved in placing a bet, the use of transferable bearer tickets with customer identification required at the time of collection above certain thresholds, and the absence of prize limits significantly increase the risk. The same applies to online gambling, due to its digital nature, the use of electronic payment methods and the absence of a physical presence.

Fraud, identity theft and the use of 'mule' accounts in online gambling

521. At national level, the rise in digital fraud and identity theft stands out as one of the main threats to the financial system. Recent inspections cited in the sectoral report show that online gambling is particularly vulnerable to: i) the creation of accounts using stolen identities, ii) the use of 'mule' accounts to operate on gambling platforms, and iii) the use of third parties to withdraw winnings, the use of unverified cards and payment methods, and the use of gambling accounts as disguised current accounts, without effective due diligence controls.

522. These practices make the sector an attractive niche for laundering funds of illicit origin, particularly when controls focus primarily on responsible gambling rather than AML/CFT.

Economic crimes and tax fraud linked to prizes and winnings

523. The gambling sector can be used to: i) justify undeclared capital gains, ii) conceal proceeds from economic crimes, iii) launder funds through the collection of winnings, and iv) channel income to third parties via front men.

524. Chapter 4 highlights tax fraud and economic crimes as significant threats, and the gambling sector — particularly where enhanced due diligence measures for prize payouts are not properly applied — can facilitate these types of crime.

Terrorist Financing

525. The level of exposure to the threat of TF, despite the fact that the gambling sector presents a low risk of TF, given:

- the recreational nature of the activity,
- gambling's limited suitability for terrorist logistical purposes,
- the limited strategic value of the products.

However, in the online environment, there could be isolated instances of scattered micropayments or the instrumental use of accounts, although the exposure is considered to be limited.

526. Furthermore, it is worth highlighting the following factors that may be exploited by threats in the online gambling sector in relation to the activities analysed in this report:

Factors that are frequently exploited by threats	
Intensive use of electronic payment methods and fragmentation of transactions	The threats identified in Chapter 4 highlight the use of prepaid cards, electronic payments, microtransactions, and fragmented transactions as recurring techniques for concealing the source of funds. In the gambling sector, and especially in online gambling, these threats manifest as: i) frequent deposits and withdrawals of small amounts, ii) the use of multiple payment methods by a single player, iii) splitting bets and winnings to circumvent controls, and iv) a lack of consistency between the player's profile and the volume of play. The high number of active accounts and new registrations reinforces this structural risk.
Cross-border exposure in the online gaming industry and operators providing services on a cross-border basis	In identifying national threats, the report warns of the risks associated with cross-border operations, especially when operators providing services under the freedom to provide services, technology platforms, and jurisdictions with varying prevention standards are involved. In the gambling sector, this risk is concentrated in the online channel: i) platforms accessible from different jurisdictions, ii) interaction with foreign payment providers, iii) difficulty verifying the player's true identity and location, and iv) a lack of knowledge regarding the final destination of the funds. These factors significantly increase the risk in online gambling compared to in-person gambling.

Risk factors due to inherent vulnerability

527. The following sets out the factors relating to inherent vulnerability analysed to determine the inherent risk in the gambling sector.

Characteristics of the sector	
Size of the sector and turnover	Size is relevant because of the total amounts involved in transactions. The high number of operators in segments of this sector with medium vulnerability (lottery and gambling authorities) and high risk in online gambling, with a smaller number of operators.
Level of complexity of the sector's structure	The existence of distinct segments within the sector, all of which are highly regulated.
Level of integration with other regulated sectors	It is not integrated with other regulated sectors, except for payment services with financial institutions.
Location of the organisation, including the geographical scope of the sector's operations[102]	The vulnerability is low for all operators except for online gambling, where – by its very nature, particularly in the case of operators providing services under the freedom to provide services – the vulnerability is substantial. Casinos are typically located in areas with high tourist numbers, a large volume of financial transactions and a significant presence of international customers, which increases exposure to transactions linked to Money Laundering. Furthermore, the in-person nature of the activity and the possibility of conducting transactions involving large amounts of cash facilitate greater operational anonymity and, in certain cases, make it difficult to trace the origin of the funds. All of this places the risk for casinos at a substantial level for this factor, higher than for other categories of in-person gambling. In the land-based betting and betting terminal sub-sector, the high degree of geographical dispersion of terminals and betting outlets – which are found not only in dedicated premises but also in hospitality establishments, gaming halls, bingo halls, casinos and sports centres – significantly increases the difficulty of controlling and uniformly supervising transactions; consequently, the risk is classified as substantial.
Nature of the products and services provided by the sector	
Level derived from the complexity of the products, due to their impact on anonymity or the limited information available on customers.	The vulnerability is low across all categories except for online gambling, given the nature of the transactions involved, where the vulnerability would be high. In the case of casinos, despite being brick-and-mortar establishments, they present a substantial risk due to their operational characteristics, which involve high levels of cash handling, the possibility of exchanging chips and prizes, as well as the greater volume and complexity of certain transactions. The risk, due to its impact on anonymity or the limited information available on customers, is substantial in the case of in-person betting and betting terminals. This is because bets are placed anonymously using transferable bearer tickets, with no identification of the player at the time of the transaction; such identification is deferred until the collection of winnings exceeding certain thresholds.
Level at which specific products and services offered are linked to intelligence reports and/or national ML or TF investigations	Vulnerability is low for all categories of gambling except online gambling. With regard to in-person operations at casinos, the risk rises to a substantial level due to the high use and circulation of cash and the high volume of transactions. Given the number of reports received from the sector, the level of vulnerability for online gambling is high. Indirectly, this sector is linked to 743 reports based on indications, notably those made by entities within the same sector regarding other competing entities, credit institutions and CASPS.
Nature of the customer	
Level derived from the nature of the business relationship with customers,	Depending on the business relationship or the tendency towards the possible concealment of ongoing relationships in certain types of gambling, there would be lower vulnerability in land-based gambling due to the physical proximity of the customer.

[102] The rating has been weighted across factors where there is a clear distinction between online gambling and other forms of gambling, in order to arrive at an aggregate rating for each factor.

depending on the duration (continuous, transactional or occasional) and frequency of transactions	In the case of online gambling, the commercial relationship takes place entirely remotely and on a continuous basis, allowing for a high frequency of transactions and round-the-clock operations. Online gambling encourages the opening and use of gambling accounts with intensive and recurring activity, which may make it difficult to properly identify actual patterns of customer behaviour and to detect ongoing relationships concealed behind multiple seemingly independent transactions. The risk in this case is high.
Level derived from the customer's status	The majority are individuals and nationals. There is greater vulnerability in online channels due to a possible lack of awareness and the growing risk of identity theft. In the case of casinos, the risk is heightened – despite them operating in person – as this type of establishment more frequently attracts international customers, high-net-worth individuals and transactions involving larger sums. In the case of in-person betting, the possibility of using transferable bearer tickets and splitting bets or winnings further increases the difficulties in identifying the true owner of the funds and in properly detecting higher-risk profiles, such as high-net-worth clients or individuals with public profile.
Level derived from the client's occupation or type of business	The sector is heterogeneous due to the diversity of its clientele and, consequently, there is greater exposure to vulnerability.
Geographical scope of the sector's activities	
Risk arising from specific jurisdictions or countries of interest frequently associated with the sector.	The risk arising from specific jurisdictions or countries of interest related to the sector is, generally speaking, limited in most forms of land-based gambling, given that operations take place primarily at a national level. However, in the case of casinos, the risk rises to a substantial level, due to their greater exposure to international customers and frequent interaction with people from multiple jurisdictions. Furthermore, the location of many casinos in tourist areas and their dealings with non-resident customers increase the complexity of operations. Therefore, in the case of casinos, the risk is substantial, whilst for other forms of land-based gambling it is low. In the case of online gambling, due to the cross-border nature of this sub-sector's operations, the risk is substantial.
Level derived from the nature of interactions or transactions involving countries identified by the FATF.	Operations generally take place at a national level, with the exception of online gambling. The risk associated with this factor relates to nationals of these jurisdictions who reside in Spain.
Level derived from the nature of the interactions or transactions involving countries subject to international financial sanctions.	There is no evidence of operations with these jurisdictions, nor of communications involving nationals of jurisdictions subject to financial sanctions.
Nature of the distribution channels	
Level derived from the complexity of the channels due to their impact on anonymity or the reduced	Non-face-to-face registration for online gambling. Over 3,000 reports of identity theft have been detected. The use of cash in in-person transactions has been identified.

information on customers[103].	
Level derived from the use of new technologies or payment methods.	There are online gaming platforms that accept crypto-assets as a means of payment. Evidence of this vulnerability can be seen in the 27 reports submitted by the CASPs since 2021.

Conclusion on the sector's inherent risk: Substantial for ML and medium for TF

Land-based casinos.

528. The land-based casino sector generates a significant turnover, characterised by high-value transactions and operations involving heavy use of cash. The wide variety of games (table games, slot machines, tournaments), each with different dynamics and rapid betting and payout cycles, potentially facilitates strategies for splitting or reallocating funds. On the other hand, there is a diverse customer base comprising individuals, both residents and non-residents, potentially including high-net-worth clients, with predominantly occasional engagement. These variables mean that the inherent risk of ML is **substantial** and the inherent risk of TF **is low**.

Lotteries and online lotteries

529. The main inherent vulnerability in lotteries stems from the possibility of buying and selling winning tickets, which introduces intermediaries who are not part of the initial gaming relationship and makes it possible to sever the link between the origin of the prize and the final beneficiary. This factor increases the risk of the system being used for ML purposes, particularly in relation to tax fraud. This is a sector with a strong social presence and a high volume of transactions, although the individual amounts involved are generally small, which limits its appeal for complex ML schemes. The clientele consists mainly of individuals, both nationals and foreigners, which reduces the inherent risk associated with complex profiles or corporate structures. In the online channel, the inherent risk is increased due to the lack of face-to-face interaction, although the impact is limited by the very nature of the product and the amounts wagered. Analysis of these factors indicates that the inherent ML risk for the TF is **medium** to **low**.

Charitable sports betting pools (quinielas)

530. When betting on a number of unrelated sporting events, it is difficult to manipulate results. However, combinatorial techniques allow funds to be invested with a limited expected return, introducing a medium level of inherent risk. The average economic value of bets and winnings is relatively low, which reduces the inherent appeal of the product to larger criminal organisations. The customer profile is diverse, comprising mainly individuals, both nationals and foreigners. The assessment of inherent risk is **low/medium** for ML and **low** for TF.

[103] The overall rating for this factor is substantial-high.

Bingo halls and 'B'-type gaming machines

531. These forms of gambling are characterised by small stakes, limited prizes and prolonged playing cycles, which make them unattractive for the efficient channelling of illicit funds. The clientele typically consists of regular customers with close ties to the establishment and little financial complexity. The inherent ML/TF risk is assessed as **low**.

In-person betting

532. In-person betting takes place via terminals connected to a central system and is characterised by anonymity when placing a bet, the issuance of transferable bearer tickets, customer identification only when collecting winnings above a certain threshold, and the absence of prize limits. All of this, combined with the probabilistic nature of the game itself, means that the game presents a specific risk profile from the perspective of ML prevention through the fragmentation of bets or the transfer of betting slips.

533. The assessment of the inherent risk to ML is **substantial** and **moderate** for TF.

Online gambling

534. Online gambling takes place entirely in a remote environment, which significantly increases the inherent risk of identity theft, the use of intermediary identities, and the difficulty in verifying the customer's true identity. The existence of cross-betting, fast-cycle games, high turnover of funds and multiple simultaneous products substantially increases the system's inherent vulnerability.

535. The use of multiple payment methods, including prepaid cards, multiple credit/debit cards and, in some cases, crypto-assets, increases the inherent risk arising from the lack of transparency regarding the source of funds and the ease of transfer. Cross-border operations and the ability to operate under the freedom to provide services increase the inherent risk associated with foreign jurisdictions and the fragmentation of oversight. The client base is predominantly made up of individuals, both domestic and foreign, with difficulties in distinguishing recreational behaviour from systematic ML operations, which increases the inherent exposure. The assessment of inherent risk is **high** for ML and **medium** for TF.

536. In conclusion, the gambling sector as a whole presents a **substantial** inherent risk for ML and a **medium** risk for TF. Key factors include the materiality and pervasiveness of the sector, the legitimising effect and enforceability of registration, and the concentration of exposure in property sales, corporate operations (e.g. capital increases and organisational changes) and loans/acknowledgements of debt. The risk increases where there are complex or opaque corporate structures and cross-border links with higher-risk jurisdictions, which limit visibility in the register

Risk factors relating to the effective implementation (or lack thereof) of controls

537. Analysing residual risk requires an assessment of how existing controls are implemented within the sector and to what extent those controls are effective. The following section presents an analysis of the factors used to determine the residual risk in the gambling sector.

Risk factors relating to the effective (or lack of) implementation of controls	
Level of regulation in the sector	A highly regulated sector.
Potential presence of unauthorised operators.	Entities in the sector are subject to a strict licensing regime to operate in the gambling sector. Both the competent authorities of the autonomous communities and the DGOJ carry out continuous supervision to prevent the presence of unlicensed entities. Consequently, there are high barriers to entry. Unauthorised operators (both land-based and online) are prohibited from engaging in advertising, sponsorship or promotion in any form. Unauthorised operators (both land-based and online) are prohibited from engaging in advertising, sponsorship or promotion in any form. Illegitimate funds used by these unauthorised operators cannot be legalised, either by the prize winner or by the operator, as they are obtained through an illegal activity. In terms of TF, there may be a risk of unauthorised individuals or organisations carrying out gambling or games of chance activities to raise funds for that purpose.
Level of potential direct or indirect control over the organisation or its management by money-laundering networks	A sector characterised by high barriers to entry and a lack of understanding of its control structure on the part of the relevant authorities. However, there is evidence that criminal organisations linked to drug trafficking exert control over lottery operators, which represents a gap in the established access controls. Hence the risk for this mitigation factor.
Level of regulation of AML/TF prevention measures	Entities in the sector have been regulated entities in the field of ML/TF for many years (under Law 10/2010 of 28 April) and are also provided with specific instructions and guidelines.
Level of supervision	A gradual increase in the level of supervision through inspections of both the online and land-based gambling sectors. During the period 2020–2025, six inspections were carried out in the sector, mainly in the online sector (five of them), revealing numerous shortcomings in customer identification and in verifying the source of funds. In 2026, a further five inspections are being carried out, four of which are of online casinos, focusing specifically on due diligence measures and the monitoring of means of payment.
Level of sanctions imposed on entities in the sector.	As a result of an inspection during the period under review, the inspected entity received a serious penalty. In addition, two rectification orders were issued to two entities, requiring improvements to 15 procedures within the entity's.
Level of professionalism of	Although Law 13/2011, of 27 May, on the regulation of gambling does not expressly regulate the good repute of senior managers as a As a separate requirement, this requirement has its legal basis in the

directors and senior managers of the organisation.	implementing regulations, in particular Royal Decree 1614/2011. Articles 13 (applications for general licences) and 14 (supporting documentation) set out the obligation to provide information regarding directors, senior managers and significant shareholders, enabling the competent authority to assess their suitability, which in practice incorporates elements characteristic of commercial and professional integrity. Furthermore, this requirement is set out explicitly and in operational terms in the terms and conditions of general licence calls for applications (from 2011 onwards) approved by the DGOJ, for online gambling and nationwide gambling operators (the terms and conditions do not apply to casinos and reserved games such as SELAE and ONCE).
Level of awareness and understanding of their AML/TF obligations.	There are legal obligations in this regard. Supervisory bodies have highlighted variations in the level of awareness depending on the type of gambling: very high in the case of casinos and lotteries, and lower in gaming halls. The requirements have called for improvements in AML/CFT bodies and procedures, so there is room for improvement. In this context, it is evident that, following various awareness-raising initiatives in recent years, operators' understanding of their obligations is greater than in the past.
Level of the organisation's commitment to ML/TF policies and measures.	As indicated, knowledge of preventive policies, awareness and commitment vary across the sector but are generally high. In both findings, requests for improvement were made regarding the prevention manual and the provision of technical and human resources.
Level of professional qualifications of staff and their training in ML/TF prevention.	Generally speaking, and particularly in recent years, the professional qualifications of employees in the sector regarding ML/TF prevention have improved significantly; there have been no requests for improvements to the training provided.
Level of internal monitoring by organisations of employees' compliance with employees.	Although there are legal obligations, in some forms of gambling the level of monitoring of employees' compliance is more complex and is not always adequate, which affects the risk of ML and TF activities.
Level of compliance with obligations regarding preventive measures, particularly CDD/KYC	In the two requests for procedural rectification, improvements to due diligence procedures have been requested. In the case of the online gambling sub-sector, given the shortcomings identified in the inspections carried out, the risk is high.

Level of identification and reporting of suspicious transaction reports	The number of reports based on indications, as mentioned above, has increased significantly. Despite this, the corrective action notices issued to the inspected institutions have called for improvements to special examination procedures and reporting obligations to SEPBLAC. The average rating for the relevance of reports based on evidence for the period 2022–2025 was 4.68. This category, introduced in 2021, makes it possible to assess the relative importance of reports terms of their link to factors such as their connection to serious crimes, the emergence of new types of risk, the detection of criminal structures or networks, and/or the involvement of large sums of money.

Conclusion on the sector's residual risk: Medium for ML and Low/Medium for

TF Land-based casinos

538. The combination of a stringent regulatory framework, a high level of professionalism and effective supervision significantly reduces the risk to ML. However, the risk is not entirely eliminated due to the very nature of the activity, which involves the handling of cash and the existence of high-value prizes. Consequently, the residual risk to ML is rated as **medium.** No additional significant factors have been identified that would increase exposure to the risk of Terrorist Financing, and the existing controls are considered adequate and sufficient to mitigate this risk. The residual risk for TF is rated as low.

Lotteries and online lotteries

539. This sector presents a **medium** ML risk, mitigated by the fact that it is a mass-market product with low unit values, simple operations and a customer base consisting mainly of individuals. There is extensive experience in identifying prize winners and a well-established regulatory and supervisory framework, particularly for public lotteries. However, structural risks persist arising from the buying and selling of winning tickets, which allows the origin of the prize to be separated from the ultimate beneficiary, and, in the online channel, from the lack of face-to-face interaction, although the impact is limited. Specific areas for improvement have also been identified in due diligence and the reporting of suspicious transactions. The risk of TF is considered **low** due to the small amounts involved, the traceability of prizes and the existing institutional controls.

Charitable sports betting pools (football pools)

540. The combination of limited financial incentive, the simplicity of the product and the effectiveness of preventive controls effectively mitigate the inherent risk. The residual risk rating for both ML and TF is **low**.

Bingo halls and 'B' type machines

541. The low inherent risk, combined with the simplicity of the product and the existing controls, allows the identified vulnerabilities to be adequately mitigated. The risk for ML/TF is **low**.

In-person betting

This activity is characterised by the handling of cash, anonymity and the absence of prize limits. However, the controls in place for the sector, the supervision and the lower number of tip-offs received regarding this sector mean that the residual risk for ML is rated as **medium**.

542. No indicators have been identified to suggest a medium exposure to the risk of TF, and the existing controls are considered adequate and sufficient to mitigate the residual nature of this exposure. The residual risk for TF is classified as **low**.

Online gambling

543. Although existing controls make it possible to significantly reduce the risk from very high levels, the very nature of the business model – which is digital, remote and cross-border – prevents the risk of ML from being fully mitigated. The risk is **substantial/high** for ML.

544. As regards TF, the risk is classified as **low/medium** in relation to remote and cross-border operations, despite there being no evidence of the systematic use of online gambling for the purposes of terrorist financing.

Sector: Jewellery, precious stones and metals 2026

Activity and context

545. Article 2.1.q) of Law 10/2010, of 28 April, includes, as obliged entities, persons who trade professionally in jewellery, precious stones or precious metals. According to SEPBLAC's Annual Report (2024), 1,602 entities in this sector were identified as active obliged entities.

546. This activity is carried out within a framework of free enterprise by various natural or legal persons, although there are regulations to protect customers regarding the characteristics that the items traded must meet and the information to be provided to consumers. Thus, Law 17/1985 on articles made of precious metals sets out the characteristics of precious metals for the purposes of their marketing and administrative control. In particular, Article 1 defines gold, silver and platinum as precious metals.

547. The professional trade in jewellery, gemstones and precious metals is carried out primarily by jewellers and, to a lesser extent, by auction houses. There is no compulsory register of jewellers or individuals who trade professionally in jewellery, gemstones or precious metals. Most professionals are represented by the Spanish Association of Jewellers, Silversmiths and Watchmakers (AEJPR).

548. The Spanish jewellery, silversmithing and watchmaking sector consists mainly of small and medium-sized enterprises (SMEs) engaged in artisanal and industrial manufacturing, distribution and retail trade. According to the Spanish Association of Jewellers, Silversmiths and Watchmakers, in 2024 the sector comprised approximately 8,490 small and medium-sized enterprises, including those involved in industrial or artisanal manufacturing, distribution and retail trade. Of these, approximately 1,890 companies are engaged in the production of jewellery, silverware or watches, including repairs, and of these, only around 400 companies have more than two employees.

549. This is a sector of relative economic importance, with an aggregate turnover (according to confidential information) that could reach 8,650 million euros, of which around 6,200 million euros would be concentrated among taxpayers with a turnover of 2 million euros or more, and, in particular, 59 regulated entities registered with SEPBLAC and with a turnover of 10 million euros or more, which in 2024 recorded an aggregate turnover of 4,152 million euros. Their activity is structured as follows: i) Manufacturing: items made of gold, silver, platinum and other metals; artisanal production with a significant presence of subcontracted workshops; ii) Distribution: a diversified wholesale and retail channel, dominated by chains; iii) Retail sales: 55–56 % of sales are concentrated in jewellery and costume jewellery, with a further 39–40 % in watches; and iv) Exports: Spain is a net exporter of gold and jewellery, with gold exports reaching 4,280 million euros in 2025, up 40 % on the previous year.

550. In addition to the activity of jewellers proper, there is also that carried out by 'gold-buying' shops, which operate as establishments that purchase jewellery and other items made of precious metals from private individuals for recycling, smelting or resale. Their business has grown in tandem with the rise in the price of gold and the demand for liquidity from households.

Threats

551. The professional trade in jewellery, gemstones and precious metals faces a number of significant ML/TF threats, stemming from the intrinsic nature of the goods traded — high-value, small-sized and highly liquid assets —, the frequency of occasional transactions, and the fragmented structure of the sector, with a significant presence of small operators.

552. These threats correspond to the typologies set out in Chapter 4, particularly in relation to organised crime and the use of goods as a store of value.

553. There is a significant threat associated with the trade in goods originating from robbery, theft or other property offences, particularly in the following segments: i) 'gold-buying' shops, ii) the purchase of second-hand jewellery from private individuals, and iii) establishments with inconsistent checks on the seller's identity. These practices facilitate the conversion of stolen goods into cash and their subsequent integration into commercial circuits, and this pattern has been repeatedly detected in major police operations.

554. Although the sector does not constitute a primary channel for TF, there is a residual threat linked to the use of jewellery as: i) a mechanism for transferring value, ii) a medium of exchange or store of value, and iii) indirect logistical support for organisations. The incidence is low compared with other sectors, but the threat is not non-existent.

555. Furthermore, it is worth highlighting the following factors that may be exploited by threats within the jewellery, gemstones and precious metals sector, in line with the activities analysed in this report:

Factors that are frequently exploited by threats	
The use of jewellery and precious metals as a means of investing and storing value	The sector's main vulnerability lies in the use of jewellery, precious stones and precious metals as a means of channelling and storing the value of funds of illicit origin. These goods make it possible to: convert illicit cash into high-value physical assets; preserve the value of capital over time without significant depreciation; facilitate transport, concealment and subsequent resale; and defer or avoid the direct use of cash. This method is particularly attractive to criminal networks.
Buying and selling and subsequent disposal of precious metals	The sector is exposed to ML schemes in which the acquired goods are resold, melted down or recycled to reintegrate the funds into the economic system under the guise of legitimate activity. In particular: smelting and refining activities; resale to wholesalers or secondary markets; the export of gold and jewellery; and the disposal of items acquired from private individuals. These transactions may involve stages of layering and integration, making it difficult to trace the origin of the goods and the underlying capital.
Exposure cross-border and international trade	The sector is subject to additional exposure arising from its international dimension, particularly in: the import and export of gold and jewellery, transactions with non-resident customers, dealings with producing countries or refining markets, refining markets, and high-net-worth clients from

	high-risk jurisdictions. These transactions may make it more difficult to verify the origin of the goods and funds
Use of new payment channels and methods	The growing use of remote channels and alternative payment methods introduces additional exposure, as it facilitates transactions without direct contact with the customer, payments via instruments with reduced traceability, and the fragmentation of amounts and faster transaction speeds. These dynamics, whilst not predominant, increase the sector's exposure to modern ML schemes.

Risk factors due to inherent vulnerability

556. The following sets out the factors relating to inherent vulnerability analysed to determine the inherent risk in the jewellery, gemstones and precious metals sector:

Characteristics of the sector	
Size of the sector and turnover	Numerous regulated entities of varying sizes and complexity, although with a significant degree of concentration, with the main operators accounting for around 50 % of the sector's activity.
Level of complexity of the structure of the sector	A multitude of interconnected companies, including wholesalers, retailers and companies specialising in the smelting and refining of precious metals.
Level of integration with other regulated sectors	Links with the financial system for the processing of collections and payments.
Location of the organisation, including the geographical scope of the sector's operations	Spread throughout the country. With a certain concentration in specific locations of traditional importance, such as Córdoba.
Nature of the products and services provided by the sector	
A level derived from the complexity of the products, due to its impact on anonymity or the limited information available about customers.	High-value, small-sized goods that maintain their value—if not increasing it—since no depreciation in prices is observed.
The extent to which specific products and services offered are linked to communications arising from intelligence and/or ML or TF investigations	A small number of reports. Major police operations involving some of the sector's leading companies indicate that these items are used as a means of payment between criminal organisations. During the period analysed, 407 reports based on suspicion were made. In 2025, the number of reports had fallen by 50 % compared with 2022. Indirectly, the sector appears to be linked to an estimated 718 reports based on suspicion made by other sectors. These reports have have been carried out mainly by credit institutions and payment institutions.
Nature of the customer	
Level derived from the nature of the business relationship with customers, based on the duration (ongoing,	Most customers can be classified as occasional or transactional, which limits the accumulation of customer knowledge. However, the customers of wholesale companies include retail companies with which they maintain an ongoing and consistent business relationship.

transactional, or occasional) and frequency of transactions	

Level derived from the customer's status	A diverse client base with a certain level of purchasing power. Growth in non-domestic clients and an increase in exports. Also, in remote channels and an increase in high-net-worth clients from countries in conflict, e.g. Russia, Syria, Venezuela.
Level derived from the client's occupation or type of business	Heterogeneous occupational profile of clients. Indicative evidence suggests clients with high purchasing power, although given the granularity of the sector and access to the retail public, the occupational profile is heterogeneous.
Geographical scope of the sector's activities	
Level derived from specific jurisdictions/countries of interest frequently associated with the sector.	Operations are primarily domestic. However, account must be taken of the proportion of foreign nationals residing in Spain in areas such as the Costa del Sol, Madrid and Barcelona, who have high purchasing power. From the intelligence reports, it is evident that there are also non-residents carrying out purchases in Spain.
A level derived from the nature of the interactions or transactions involving countries identified by the FATF.	Purchases by residents in jurisdictions identified by the FATF as high-risk, such as Monaco, have been identified. This evidence stems from reports of suspicious communications.
Level derived from the nature of interactions or transactions involving countries subject to international financial sanctions.	There is no evidence of residents in sanctioned jurisdictions carrying out transactions with this sector.
Nature of the distribution channels	
Level derived from the complexity of the channels due to their impact on anonymity or the limited information available on customers.	Reports received from this sector are associated with traditional banking payment methods such as debit/credit cards and bank transfers. However, in areas of the country prone to criminal activities such as drug trafficking, a high level of cash usage as a means of payment can be identified in this sector.
Level derived from the use of new technologies or payment methods.	Most payments are made via bank transfers or card payments (of unknown origin). There is growing activity in non-remote channels, but there is no use of crypto-assets

Conclusion on the inherent risk of the sector: Substantial for both ML and TF

557. The trade in jewellery, precious stones or precious metals is highly exposed to risk due to the very nature of the activity. Transactions are particularly lucrative because of the ease with which these goods can be acquired (placement phase) and their ownership subsequently transferred

(integration phase). They can also be used to settle the trafficking of illicit goods – e.g. drugs –, as they offer advantages over cash, such as ease of safekeeping, retention of value and untraceability.

Risk factors relating to the effective implementation (or lack thereof) of controls

558. To analyse residual risk, it is necessary to assess the implementation of existing controls within the sector and the extent to which these controls are effective. The following section presents an analysis of the factors used to determine the residual risk in the jewellery, gemstones and precious metals sector.

Risk factors relating to the effective implementation (or lack thereof) of controls	
Level of regulation in the sector	The specific regulations governing this sector date from the 1980s and, in certain respects, are completely out of date, particularly with regard to the monitoring of purchases of precious metals made by gold-buying shops for subsequent smelting.
Extent to which unauthorised entities unauthorised to operate	As this is an unregulated activity, no prior authorisation is required to operate. Formal restrictions on 'gold-buying' shops are largely ineffective.
Level of potential direct or indirect control over the business or its management by money-laundering networks	A freely practised activity that may lead to the incorporation of companies with the sole aim of laundering funds derived from illicit activities.
Level of regulation of AML/TF prevention measures	The sector is subject to all the obligations set out in Law 10/2010, of 28 April.
Level of supervision	Inspections have begun, starting with the main foundry, with the aim of gradually moving on to smaller facilities and increasing the number of visits. Between 2020 and 2025, five inspections were carried out in the sector.
Level of penalties imposed on entities in the sector	During the period analysed, a serious penalty was imposed on one company in the sector.
Level of professionalism of the directors and senior managers of the organisation	This depends on the size of the company; large firms in the sector present a lower risk in this regard. However, numerous companies and small businesses with a low level of knowledge AML/CFT matters.
Level of awareness and understanding of their ML/TF obligations.	Limited awareness. The culture of prevention is not sufficiently robust in the sector, meaning that controls tend to be lax when it comes to customer identification, as their profits are entirely linked to the volume of goods they manage to sell. It is a sector that has traditionally suffered from very low or no awareness of AML/CFT and has therefore been the subject of close monitoring in recent years.

The entity's level of commitment to AML/TF policies and measures.	Positive developments in recent years following supervisory measures and the increasing involvement of the jewellers' association.

Level of professional qualifications of staff and their training in ML/TF prevention.	Positive developments in recent years regarding the level of awareness of AML measures within the sector.
Level of internal monitoring by organisations of employees' compliance employees.	Significant variation across the sector due to its highly fragmented nature, which may undermine compliance levels.
Level of compliance with obligations regarding preventive measures, in particularly CDD/KYC	Disparity in compliance levels due to the existence of one-off transactions and the wide variety of regulated entities. Higher levels of compliance among large companies in the sector.
Level of identification and reporting of suspicious transaction reports	There are few reports based on indicators and the analysis is not very thorough. The occasional nature of client reporting limits the accumulation of knowledge and hinders: the identification of anomalous behaviour patterns, the early detection of money laundering through the use of multiple transactions, and the effective assessment of the origin of assets or funds for proper detection. The average rating for the relevance of reports based on indicators for the period 2022–2025 was 4.9. This category, introduced in 2021, allows the relative importance of reports to be assessed based on their link to factors such as the connection to serious crimes, the emergence of new risk typologies, the detection of criminal structures or networks and/or the involvement of large sums of money.

Conclusion on the sector's residual risk: medium for ML and low-medium for TF

559. This is a sector that has traditionally shown little or no awareness of AML/CFT, and as such has been closely monitored in recent years. Large companies, which are most susceptible to being used for ML, are now more aware of the issues. Significant efforts have been observed to implement effective preventive measures within the sector. Of particular note is the work carried out by the AEJPR to raise awareness amongst its members and to improve preventive systems, which has a positive impact on the final risk rating.

Sector: Art and antiques 2026

Activity and context

560. Article 2.1.r) of Law 10/2010, of 28 April includes, among obliged entities, persons who trade professionally in works of art or antiques. In Spain, the buying and selling of such works of art or antiques is carried out under the principle of freedom of enterprise, without prejudice to the administrative controls applicable to assets forming part of Spain's historical heritage.

561. As regards companies and professionals in the sector, there is no compulsory national register of art or antiques dealers, although some members of the sector are grouped within associations such as the Spanish Association of Art and Collectables Auction Houses (AESSAC). The study *The Spanish Art Market in 2021*, published by the Institute of Contemporary Art (IAC), noted that the gallery sector in Spain comprises around 2,400 registered businesses as of 2020, including galleries, private dealers and antique shops. Whilst these include a large number of small businesses and dealers, there is a core of around 600 art and antiques galleries operating in different sectors, which account for at least 80 % of sales in the market.

562. That study concluded that the estimated value of sales in art galleries in 2020 stood at 236 million euros, compared with 425 million euros in the previous financial year. With regard to AML/CFT, SEPBLAC is responsible for supervising compliance with AML/CFT obligations by persons who trade professionally in works of art or antiques. According to SEPBLAC's 2024 annual report, there are 82 active regulated entities, with a slight upward trend in the sector's growth (5 % growth over the 2021–2024 period). The aggregate turnover of these entities stands at around 75 million euros.

Threats

563. The professional art and antiques trade sector faces a number of significant ML and TF threats, stemming from the intrinsic nature of the goods traded — items of high economic value, easily transportable and subject to subjective valuation — as well as from the complex and opaque structure of the market, characterised by the routine use of intermediaries and a traditional culture of confidentiality.

564. These threats correspond fully to the typologies identified in Chapter 4, particularly in relation to economic crimes, the use of assets as a store of value, the concealment of the origin of funds, the circumvention of international sanctions, and the use of markets with a high degree of structural opacity.

565. With regard to TF in the art and antiques sector, the level of exposure to threats is considered secondary, and the sector does not constitute a preferred channel. However, it may exist to a residual extent in: asset concealment schemes, the use of goods as a store of value, and indirect support for wider illicit networks. The threat is limited compared with the ML but not non-existent.

566. Furthermore, it is worth highlighting the following factors that may be exploited by threats in the art and antiques sector, in line with the activities analysed in this report:

Factors that are frequently exploited by threats	
Use of art and antiques as a vehicle for investment and a store of value	The key focus of this sector lies in the use of works of art and antiques as a means of channelling and storing illicit funds, given that these assets make it possible to: transform funds of illicit origin into tangible and durable assets; retain value over time without significant depreciation; facilitate physical transport and the concealment of assets; or justify increases in wealth through subjective revaluation. This method is widely documented internationally as one of the classic forms of money laundering involving high-value physical assets.
Subjectivity in valuation and its use for stratification	The inherent subjectivity in the pricing of works of art and antiques constitutes a significant vulnerability to the threat, as it allows for: the overvaluation or undervaluation of items for the purpose of covertly transferring value, the simulation of apparent losses or profits, or the concealment of fund movements under the guise of legitimate financial results. This characteristic makes art a particularly suitable instrument for the layering phase, as it makes it difficult to detect artificial prices and transactions that are not in line with the market.
Use of intermediaries and opaque structures	The art market presents a level of structural exposure stemming from the common use of intermediaries, such as: dealers and consignees, auction houses, pre-established companies and intermediary vehicles, or professional representatives. These practices, which are accepted in the ordinary functioning of the market, can conceal the identity of the beneficial owner, make it difficult to identify the actual payer and fragment the traceability of funds, significantly increasing exposure to ML/TF.
Cross-border transactions and sanctions evasion	Spain is a major international hub for the art and antiques trade, particularly in cities such as Madrid and Barcelona, and maintains a significant cross-border flow of goods with the EU and Latin America. This creates a level of exposure to risks associated with: non-resident clients, companies established in other jurisdictions, high-net-worth buyers, or individuals on sanctions lists or linked to high-risk countries. The ease with which items can be physically moved and the use of foreign corporate structures may enable the circumvention of restrictive measures and the use of the market as a mechanism for concealing assets.
High transaction volume and private sales	The predominantly transactional and private nature of the sector's operations exposes it to risk due to: one-off high-value transactions, low repeat business with the same clients, sales at fairs, exhibitions or auctions, and the absence of ongoing business relationships. This pattern limits the development of a progressive understanding of the client and reduces the effectiveness of controls based on historical behaviour or recurring patterns.

Emerging risks from digitalisation and new instruments	The dynamics arising from the digitalisation of the market – such as online auctions and remote sales, the use of digital payment methods, the acceptance of crypto-assets in certain transactions, and the emergence of NFTs and the tokenisation of artworks – facilitate rapid, cross-border transfers of value with reduced traceability, thereby exacerbating existing risks in a structurally opaque market.

Risk factors due to inherent vulnerability

567. Set out below are the factors relating to inherent vulnerability analysed to determine the inherent risk in the art and antiques sector.

Characteristics of the sector	
Size of the sector and turnover	The market size is significant but limited, in that the aggregate turnover of the 82 identified regulated entities stands at around 75 million euros. There is a certain degree of concentration of activity amongst a relatively small number of operators.
Level of complexity of the sector's structure	The art trade involves a chain of transactions in which multiple parties are involved (suppliers, galleries, art fairs, auctions, dealers, consignees, pre-established companies), which increases opacity and makes it more difficult to trace the provenance and origin of funds. The complexity does not depend on the size of the transaction (even a small transaction may involve multiple intermediaries), which increases vulnerability.
Level of integration with other regulated sectors	The process relies heavily on other entities subject to AML/CFT regulations, such as credit institutions and payment institutions, which are used to channel receipts and payments arising from the sale and purchase, consignment and auction of works of art and valuables; or tax, accounting and legal advisers, who are involved in tax planning, asset valuation, the structuring of transactions and compliance with tax obligations.
Location of the organisation, including the geographical scope of the sector's operations	Activity is concentrated in cities with an international profile (e.g. Madrid/Barcelona, with a 42% share) and maintains significant cross-border flows (links between the EU and Latin America). As art and antiques generally consist of high-value goods that are easy to transport, vulnerability due to location and geographical scope is high, mitigated by the need for administrative procedures at and a high number of cases (permits export licences).
Nature of the products and services provided by the sector	
Level derived from the complexity of the products, due to their impact on anonymity or on the reduced amount of information available about customers.	Art and antiques dealers are involved in the sale of items of subjective value, which makes it possible for such items to be overvalued or undervalued for the purpose of concealing the origin of funds. Furthermore, such items are generally easy to transport, and there is traditionally a culture of privacy surrounding sales in this market. In addition, the art market is inherently vulnerable to the purchase of art through opaque mechanisms that hinder the

	traceability of the beneficial owner or the source of funds, such as purchasing through third parties or a pre-established company.
The extent to which specific products and services offered are linked to communications identified in national ML or TF investigations	Despite the low number of reports based on evidence (12 in total between 2020 and 2025, according to SEPBLAC), this figure reflects the sector's limited detection capacity, rather than reduced vulnerability, as the art market presents significant structural risks that are often under-reported. Indirectly, 98 reports based on indications have been made, mainly by financial institutions such as credit and payment institutions, although there are also reports from notaries and, notably, three reports in 2025 from the CASPS.
Nature of the customer	
Level derived from the nature of the business relationship with customers, based on the duration (ongoing, transactional or occasional) and frequency of transactions	The art and antiques market is dominated by one-off, private, high-value transactions, often channelled through intermediaries, which reduces the continuous traceability of customers and makes it difficult to monitor behavioural patterns (particularly at fairs and exhibitions). This transactional nature significantly reduces the ability to apply controls based on behavioural patterns, even with enhanced monitoring. However, transactions are not liquid but typically involve a protracted sales process.
Level derived from the customer's status	Spain operates as an international hub, primarily through Madrid and Barcelona. Furthermore, it maintains a significant cross-border flow of people and capital (links with the EU and Latin America), meaning that the presence of non-residents and corporate vehicles based in other jurisdictions is common. Market confidentiality, the use of structures and the possibility of evading sanctions are factors that increase vulnerability, particularly with PEPs or foreign counterparties; this, combined with the frequent use of companies in jurisdictions with low transparency and the ease of transferring artworks across borders, significantly increases exposure to the risk of sanctions evasion and misuse by PEPs and clients with substantial international high-net-worth individuals.
Level derived from the client's occupation or type of business	The inherent vulnerability based on the customer's occupation or activity is medium-high and rises to high when the purchaser or payer is a PEP or someone associated with them, an intermediary, a corporate vehicle or trust, or an operator linked to crypto or NFTs, given the combination of opacity, intermediation, subjectivity in valuation and digital transfers of value. By contrast, museums and public bodies that pay via traceable channels tend to present a low or medium risk, with the risk in such cases predominantly related to the provenance of the asset.
Geographical scope of the sector's activities	
A level derived from specific jurisdictions/countries of interest frequently associated with the sector.	As mentioned, Spain operates as an international hub. Furthermore, it has significant cross-border flows, meaning that the presence of non-residents and corporate vehicles based in other jurisdictions is common. Market confidentiality, the use of structures and the possibility of circumventing sanctions increase the risk, particularly with PEPs or foreign counterparties.
Level derived from the nature of the	Art and antiques can be used as stores of value for individuals, including those from countries identified by the FATF.

interactions or transactions that involve countries identified by the FATF.	This is particularly due to the common use of intermediary companies and the possibility of moving works across borders with limited traceability.
Level derived from the nature of interactions or transactions involving countries subject to financial.	Although there is no evidence of cross-border remittances to these sanctioned jurisdictions, a certain level of risk must be taken into account due to the presence in Spain of foreign nationals from Iran and Russia, as well as Chinese nationals who may act as intermediaries, remitting funds to their country of origin.
Nature of the distribution channels	
Level derived from the complexity of the channels due to their impact on anonymity or the limited information available on customers.	Distribution channels, which typically include intermediaries and private sales, combined with the culture of privacy that characterises the sector and the subjectivity involved in valuing items, increase opacity and inherent risk.
Level derived from the use of new technologies or payment methods.	There is growing exposure due to the use of remote transactions (virtual auctions) and digital payment methods, particularly those that facilitate anonymity (cryptocurrencies), which make it easier to transfer value across borders with limited traceability. This is particularly relevant in a sector that already suffers from structural opacity and subjectivity in the valuation of the items (NFTs, crypto-assets, tokenisation).

Conclusion on the sector's inherent risk: Substantial in ML and TF

568. Artworks and antiques are attractive to ML/TF at all stages. Transactions are particularly lucrative for ML/TF due to the ease of acquiring artworks or antiques (placement phase); to realise significant gains or losses, given the subjectivity of their valuation, which allows funds to be transferred under the guise of financial returns (concealment phase); and to subsequently transfer ownership (integration phase). This, combined with the lack of traceability and the growing use of digital payment methods, results in a **substantial** level of risk.

Risk factors relating to the effective implementation (or lack thereof) of controls

569. To analyse residual risk, it is necessary to assess the implementation of existing controls within the sector and the extent to which these controls are effective. The following section presents an analysis of the factors used to determine the residual risk in the art and antiques sector.

Risk factors relating to the effective implementation (or lack thereof) of controls	
Level of regulation in the sector[104]	The activity is governed, to a large extent, by civil, commercial and consumer legislation of general application. There is no system of prior administrative authorisation, specific sectoral licences or ongoing supervision for the ordinary buying and selling of works of art and antiques.
Extent to which unauthorised entities may be operating operate.[105]	The trade in art and antiques does not require administrative authorisation.
The extent to which money-laundering networks may exercise direct or indirect control over the entity or its management	There is a possibility that the company, as a regulated entity, forms part of the corporate structure devised by money-laundering networks; however, this does not appear to be the case for the main operators.
Level of regulation of AML/TF prevention measures	Companies and agents trading in this type of product are regulated entities under Spain's AML/CFT regulations and are supervised by SEPBLAC.
Level of supervision	No inspections of the sector were carried out between 2020 and 2025.
Level of sanctions imposed on entities in the sector.	During the period 2020–2025, penalties were imposed on companies in the sector, resulting in two serious infringements. These penalties related to to inspections carried out prior to the period covered by this analysis, but the administrative proceedings were concluded during the period in question.
Level of professionalism among the organisation's directors and senior managers.	Those involved in trading in this type of item have financial incentives to prevent Money Laundering, in addition to their legal obligation. In this regard, it is a sector in which the reputational risk faced by galleries plays a key role; furthermore, galleries have a vested interest in verifying transactions to prevent non-payment. In conclusion, there are financial and reputational incentives that align with the objectives of AML/CFT regulations; however, it is to be expected that the resources available to regulated entities in the sector will lead to inconsistencies in the compliance with their AML/CFT obligations.
Level of awareness and understanding of their AML/TF obligations.	Intermediaries in the art and antiques market are generally professional dealers with a high degree of specialisation, although there are significant differences in their understanding of AML/TF obligations given the diverse nature of the sector.
The organisation's level of commitment to policies and measures for AML/TF policies and measures.	On the one hand, it is worth noting the existence of financial and reputational incentives; on the other, there are significant differences amongst the various players within the sector.
Level of professional qualifications of staff and their	There are significant differences within the sector, with higher levels of qualifications and training found among the larger regulated entities in the sector, as

[104] This factor is rated as 'Medium-substantial'
[105] This factor is rated as 'Not applicable'

training in ML/TF prevention.	to provide more resources. One of the sanctions imposed concerned staff training.
Level of internal monitoring by organisations of employees' compliance employees.	Financial incentives within the sector that are aligned with the objectives of AML/CFT regulations help to increase the level of monitoring within the sector, although there are significant differences between regulated entities, leading to inconsistencies in compliance of their AML/CFT obligations.
Level of compliance with obligations regarding preventive measures, in particularly CDD/KYC	Variability amongst the different regulated entities within the sector, with particular focus on legal entities and repeat customers (generally high-value). Pawnbrokers have incentives to know their customers in order to maintain their reputation and avoid default
Level of identification and reporting of suspicious transaction reports	Despite the low number of reports based on evidence (7 in total in 2022–2024 according to SEPBLAC), this figure reflects the sector's ability to detect issues in a highly fragmented market with significant structural risks. The average rating for the significance of suspicious activity reports during the 2022–2025 period was 4. This category, introduced in 2021, enables the relative importance of reports to be assessed based on their link to factors such as the connection to serious crimes, the emergence of new types of risk, the detection of criminal structures or networks and/or the involvement of large sums of money.

Conclusion on the sector's residual risk: Medium for ML and TF

570. A sector with characteristics that make it suitable for use in ML and TF operations, but to a limited extent, given its size and the self-interest of major operators due to the significant impact in terms of reputational and legal risks, which leads to the existence of controls that limit the sector's higher risk.

Sector: Tangible assets 2026

Activity and context

571. Article 2.1.s) of Law 10/2010, of 28 April, designates as obliged entities those persons who professionally carry out the activities referred to in Article 1 of Law 43/2007, of 13 December, on the protection of consumers in the contracting of goods with an offer of a refund.

572. The activity in this sector involves investment in tangible assets, such as stamps, works of art, antiques, jewellery, trees, natural forests and animals, as well as any other assets that can be traded with an offer of a refund of the purchase price and, in most cases, with a promise of capital appreciation.

573. In Spain, there are currently companies that sell tangible goods whilst offering customers the possibility of recovering the price paid and, in many cases, with the prospect of a return on investment. However, these companies do not constitute a specific legal category recognised by Spanish law, and their activities fall within a particularly sensitive legal framework, since, depending on how the transaction is structured and advertised, it may come close to raising savings for investment purposes, thereby being subject to significant regulatory and supervisory restrictions.

574. Consumers of these goods are deemed to be natural or legal persons who, as end users, acquire, use or enjoy movable or immovable property, products, services, activities or functions, regardless of whether those who produce, facilitate, supply or dispatch them are public or private, individual or collective in nature.

575. Suppliers are defined as business owners or professionals established in Spain or with a permanent establishment there, as well as those established in another country, provided the consumer is domiciled in Spain. Natural or legal persons who professionally provide investment services in tangible assets do so under the principle of freedom of enterprise and are not subject to any authorisation or registration requirements. However, given the nature of their activity, they are subject to specific consumer protection rules.

576. With regard to the ML, the situation facing this type of entity is similar to that of investment companies, although the fact that they are not supervised by a market authority increases the risk. At present, there are no regulated entities operating in this sector.

Threats

577. The tangible goods sector offering price refunds presents a range of potential threats in terms of ML and, to a lesser extent, TF, arising from the hybrid nature of its operations, which can straddle the line between retail trade and the raising of savings for investment purposes, without being subject to the supervision typical of financial markets.

578. These threats have been consistently identified in Chapter 4, particularly in relation to fraud schemes, bogus investments, the use of physical assets as a means of investment and a store of value, and the exploitation of sectors with weak or non-existent sector-specific supervision. With regard to the threat of TF to which the tangible assets sector is exposed, this is considered to be very low, given that: it does not structurally manage third-party funds, it does not channel international transfers, and its operations are predominantly domestic and retail-based. However, the possibility of occasional use within broader schemes cannot be completely ruled out, although there are currently no such regulated entities in Spain.

579. Factors that may be exploited by threats in the tangible goods sector, in line with the activities analysed in this report, include the following:

Factors that are frequently exploited by threats	
Use of tangible goods as a mechanism for placement and store of value	In theory, the sector's main exposure factor lies in the use of tangible assets (stamps, works of art, antiques, animals, trees, forests or other physical assets) as: a means of converting illicit cash or funds into apparently legitimate assets; a store of value outside the traditional financial system; and a means of justifying subsequent increases in wealth. These patterns are well known in the context of the ML, particularly where assets are concerned that are difficult to value objectively and have limited immediate liquidity, although their actual realisation depends on the scale and continuity of the activity.
Fraudulent investment schemes and associated money laundering	One factor contributing to exposure to this threat is linked to the sale of goods with an offer of a refund and explicit or implicit promises of appreciation in value, which may facilitate: fund-raising schemes under the guise of legitimate commercial activity, large-scale investment fraud, and the reuse of proceeds of crime to give the appearance of legitimate income. The historical cases of Forum Filatélico and Afinsa demonstrated the potential of these structures to channel large volumes of funds, although their impact has been significantly reduced by a loss of investor confidence and the sector's current limited presence in Spain.
One-off transactional relationships and limited knowledge of the customer	Most transactions in this sector take place through occasional, low-value relationships, which makes it difficult to: maintain ongoing knowledge of the customer, identify behavioural patterns, and detect unusual or fragmented transactions at an early stage. This circumstance increases the sector's theoretical vulnerability to sporadic use for ML purposes, even if the aggregate impact is limited.
Use of remote channels and digital payment methods	The growing use of distance selling and electronic payments, although still limited, poses an additional threat linked to: reduced face-to-face contact, greater reliance on technological intermediaries, and greater difficulty in verifying the source of funds in one-off transactions.

	This factor is consistent with the cross-cutting typologies identified in Chapter 4 for sectors involving small amounts but with limited specific supervision.

Risk factors relating to inherent vulnerability

580. The following sets out the factors relating to inherent vulnerability analysed to determine the inherent risk in the tangible goods sector:

Sector characteristics	
Size of the sector and turnover	There are currently no regulated entities.
Level of complexity of the sector's structure	There are currently no regulated entities, but past experience shows that the structure is simple: individual traders or small businesses engaged in trading with price-refund schemes. It is not a sector in which sophisticated corporate networks or complex corporate structures.
Level of integration with other regulated sectors	There are currently no regulated entities that would allow this risk factor to be assessed.
Location of the entity, including the geographical scope of the sector's operations	There are no regulated entities in Spain; therefore, there is no risk associated with this factor.
Nature of the products and services provided by the sector	
A level derived from the complexity of the products, due to their impact on anonymity or the limited information available on customers.	There are currently no regulated entities, but past experience shows that the products offered are straightforward and aimed at retail customers, with no features that facilitate anonymity or complex structures. However, operations may involve a certain lack of information on customers when one-off or low-value transactions are carried out, moderately increasing vulnerability.
Level at which specific products and services offered are linked to intelligence-led communications and/or national ML or TF	As there are no obliged entities, there are no reports based on suspicion.
Nature of the customer	
Level derived from the nature of the business relationship with customers, based on duration (ongoing, transactional or occasional)	There are currently no obliged entities, but past experience shows that relationships tend to be one-off or occasional, which limits knowledge of the customer and makes it difficult to detect anomalous patterns. The low frequency of interaction reduces the capacity for continuous monitoring, moderately increasing vulnerability.

and frequency of transactions	
Level derived from the customer's status	There are currently no obliged entities, but past experience shows that the client base consists mainly of retail clients, natural persons and those with a low-risk profile. There are very few transactions involving legal entities or clients with significant wealth or PEP profiles, which reduces the risk, although it does not eliminate it entirely given the possibility of occasional transactions with more sensitive profiles.
Level derived from the client's occupation or type of business	There are currently no obliged entities, but past experience shows that the sector mainly attracts private clients with no professional activities linked to high-risk categories. No significant concentrations of high-risk sectors or occupational patterns that increase exposure to ML have been observed.
Geographical scope of the sector's activities	
Level derived from specific jurisdictions/countries of interest frequently associated with the sector.	There are no regulated entities in Spain; therefore, there is no risk associated with this factor.
Level derived from the nature of interactions or transactions involving countries identified by the FATF.	There are no regulated entities in Spain, so there is no risk associated with this factor.
Level derived from the nature of interactions or transactions involving countries subject to international financial sanctions.	There are no regulated entities in Spain, so there is no risk associated with this factor.
Nature of the distribution channels	
Level derived from the complexity of the channels due to their impact on anonymity or reduced customer information.	There are currently no regulated entities, but past experience shows that the products are simple and consumer-oriented, with no structures that facilitate anonymity. However, as these are one-off transactions with low traceability, there may be less customer information in certain cases, which moderately increases vulnerability.
Level derived from the use of new technologies or payment methods.	There are currently no regulated entities, but past experience shows that the sector operates mainly using traditional methods.

Conclusion on the sector's inherent risk: Low for ML/TF.

581. With regard to money laundering, the situation facing this type of entity is similar to that of investment firms. The characteristics of the sector present vulnerabilities to ML and TF which could, in theory, pose an inherent medium-level risk; however, there are currently no regulated entities operating in this sector, as the risk can be assessed as low.

Risk factors relating to the effective implementation (or lack thereof) of controls

582. To analyse residual risk, it is necessary to assess the implementation of existing controls within the sector and the extent to which these controls are effective. The following section presents an analysis of the factors used to determine the residual risk in the tangible assets sector.

Risk factors relating to the effective implementation (or lack thereof) of controls	
Level of regulation in the sector	There are currently no regulated entities, but previous experience shows that the sector is formally included as a regulated sector but lacks a detailed and specific regulatory framework. Activity within the sector may generally be varied, which could make it difficult to apply the obligations consistently.
Extent to which unauthorised entities may be operating.	There are currently no regulated entities, but past experience shows that the activity may be carried out by individuals or small businesses without clear registration or prior detection mechanisms. The absence of official registers increases the risk of informal operators without AML/CFT controls. This may also be affected by the provision of services by companies from other EU countries under the freedom to provide services.
Level of potential direct or indirect control of the entity or its management by money laundering networks	There are currently no regulated entities, but past experience shows that this is not a sector typically used by criminal networks to acquire control, given its low profit margins.
Level of regulation of AML/TF prevention measures	The obligations are fully in force, although there are currently no regulated entities registered.
Level of supervision	In the absence of regulated entities, it is not possible to assess the level of supervision.
Level of sanctions against entities in the sector.	In the absence of regulated entities, it is not possible to assess this factor.
Level of professionalism of the directors and senior managers of the organisation.	No persons subject to the regulations have been identified; therefore, there is no evidence on which to assess the level of professionalism of the directors and senior management.
Level of awareness and understanding of its ML/TF obligations.	No regulated entities have been identified; therefore, there is no evidence on which to assess the level of awareness and understanding of AML/CFT obligations.

Level of the organisation's commitment to ML/TF policies and measures.	No regulated entities have been identified; consequently, there is no evidence on which to assess the organisation's level of commitment to AML/CFT policies and measures.
Employees' level of professional qualifications and their training in ML and TF.	No regulated entities have been identified; therefore, there is no evidence on which to assess staff training.
Level of internal monitoring by organisations of employees' compliance employees.	No regulated entities have been identified; therefore, there is no evidence to assess the level of internal monitoring by the organisations.
Level of compliance with obligations regarding preventive measures, in particular CDD/KYC	No regulated entities have been identified; therefore, there is no evidence to assess the degree of compliance with obligations regarding preventive measures.
Level of identification and reporting of suspicious transactions suspicious transactions	As no regulated entities have been identified, it is not possible to assess the level of reporting and communication.

Conclusion on the sector's residual risk: low for ML and TF

583. In conclusion, the characteristics of the sector could present vulnerabilities in relation to ML and TF; however, there are currently no regulated entities operating in this sector, and the residual risk is therefore also assessed as low.

Sector: Cash-in-transit 2026

Activity and context

584. Article 2.1.t) of Law 10/2010, of 28 April, defines as obliged entities those persons engaged in the professional deposit, safekeeping or transport of funds or means of payment. In Spain, these activities are carried out by private security companies, which, according to Law 5/2014, of 4 April, on Private Security, are private natural or legal persons authorised or subject to the self-declaration regime to provide these services. Article 5.1 of Law 5/2014, of 4 April, sets out the activities of private security, including, amongst others, the deposit, safekeeping, counting and sorting of coins and banknotes, securities, jewellery, precious metals, antiques, works of art or other objects which, due to their economic, historical or cultural value and the expectations they generate, may require special surveillance and protection, as well as their transport and distribution.

585. In order to provide private security services, private security companies must obtain administrative authorisation. Article 9 of Law 5/2014, of 4 April, stipulates that no private security service may be provided unless it has been previously contracted and, where applicable, authorised. Contracts for the provision of the various private security services must, in all cases, be drawn up in writing and notified to the Ministry of Home Affairs or, where applicable, to the competent regional authority, prior to the commencement of such services.

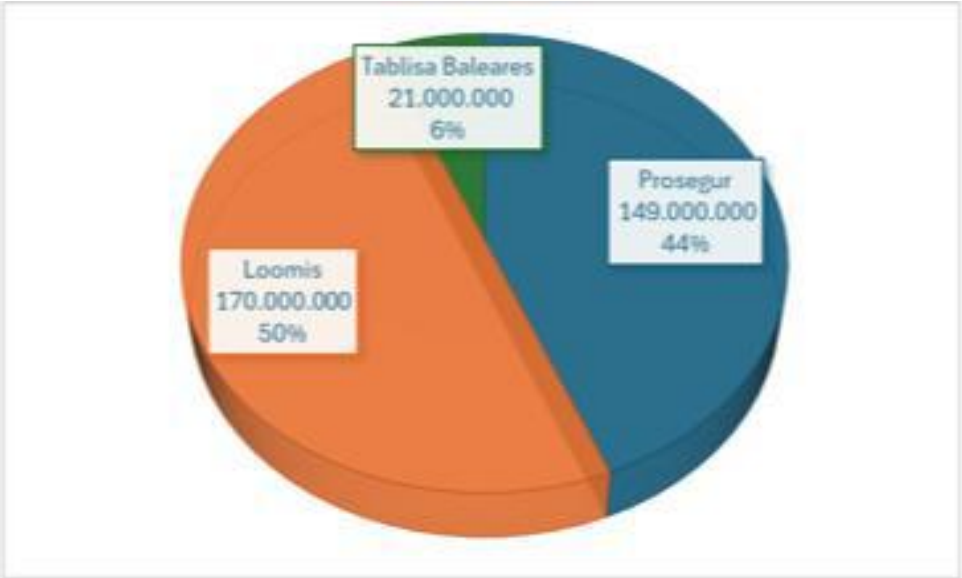
586. Private security companies shall be automatically entered in the Ministry of Home Affairs' National Register of Private Security, once the relevant authorisations have been granted, where they are not required to be entered in the registers of the autonomous communities (in cases where they have their registered office in an autonomous community and their scope of operations is limited to that territory). The National Register will contain not only information relating to the private security companies that are registered with it, but also information relating to private security companies registered in the registers of the autonomous communities with jurisdiction in this area. According to data from the Directorate-General of Policía Nacional on the list of registered companies, updated as at 3 September 2025, three companies were registered to carry out the transport and storage of funds.

587. All three companies are authorised to operate nationwide in the cash-in-transit sector; however, in the case of cash storage, Trablisa carries out this activity at regional level. According to information included in SEPBLAC's 2023 Annual Report, the sector's turnover amounted to approximately 321 million euros, which highlights the sector's overall scale and degree of concentration. According to figures provided by the security sector's trade association, the sector's turnover has been as follows:

	2020	2021	2022	2023	2024
Fund of funds (millions of €)	261	273	301	321	340
Total sector turnover (millions of €)	4,214	4,431	4,622	4,919	5,334

588. In the 2024 financial year, the turnover of the three cash-in-transit companies totalled approximately 340 million euros, which highlights the overall scale and degree of concentration within the sector.

Turnover of cash-in-transit companies



Threats

589. The professional cash-in-transit sector faces a range of ML and TF threats arising primarily from the handling of large volumes of cash, its central role in the operations of cash-intensive sectors, and its function as critical logistical infrastructure within the payments system.

590. However, these threats are significantly constrained and mitigated by the high concentration within the sector, the high level of administrative regulation, intensive supervision by the competent authorities and the stability of the operators – factors which substantially reduce the likelihood of the sector being used directly as a primary channel for ML/TF, in line with the threats outlined in Chapters 4 and 5.

591. The threat of TF in the sector is considered to be very limited, given that: operations are essentially domestic; clients are well-known companies and institutions; there are prior administrative and contractual controls in place; and the service is not provided on an occasional or informal basis. No significant patterns have been identified in which professional cash-in-transit services have been used to any significant extent for TF in Spain.

592. Furthermore, other factors that may be exploited by threats within the cash-in-transit sector include:

Factors that may be exploited by threats	
Handling and movement of large volumes of cash	The sector's most significant exposure stems from the transport, safekeeping and counting of large quantities of cash, originating mainly from: financial institutions, retailers and businesses with high cash generation, retail distribution networks, and economic activities involving a high volume of cash payments. The high unit volume of funds transported means that any potential misappropriation or abuse would have a significant impact. This type of risk is mainly confined to the ML's placement phase, although the sector itself does not determine the ultimate origin of the funds.
Indirect use of the sector by high-risk economic activities	The sector may be indirectly exposed to ML threats when it provides services to customers whose activities structurally generate large volumes of cash, such as certain sub-sectors of retail, leisure or the hospitality industry. In such cases, cash-in-transit operations may: facilitate the systematic channelling of cash into the financial system; form part of money-laundering schemes involving the splitting or bundling of cash; or make it difficult to identify the illicit source of funds where customer due diligence is insufficient. This exposure depends largely on the risk profile of the clientele rather than on the intrinsic nature of the cash-in-transit companies' operations.
Use of cash-in-transit services as logistical support for money-laundering schemes	In theory, the sector could be used as a logistical support for ML schemes requiring the physical transfer of funds between different locations. However, the level of exposure would be mitigated by: the requirement for prior contracts to be formalised and reported to the authorities; the internal traceability of shipments; strict custody protocols; and regular collaboration with SEPBLAC and AEAT. Consequently, the deliberate use of the sector as a direct channel for ML is unattractive compared with other, more opaque means.

Risk factors due to inherent vulnerability

593. The following section sets out the factors relating to inherent vulnerability analysed to determine the inherent risk of the cash-in-transit sector.

Characteristics of the sector	
Size of the sector and turnover	Low intrinsic turnover and a small number of operators but involving high transaction amounts.
Level of complexity of the sector's structure	Very small number of operators (3 companies were recorded as having registration for the transport and storage of funds).
Level of integration with other regulated sectors	High degree of interrelation with the payments system. There is a functional dependence on the controls applied by its customers, as: it does not participate in the generation of funds, does not decide on the legality of the underlying activity, nor does it have a direct relationship with end customers. If customers' preventive controls prove insufficient, the transport of funds may become a passive link within a broader ML scheme, although without the autonomous capacity to detect illicit origins.
Level of the entity's location, including the geographical scope of the sector's operations	Operations carried out throughout the country.
Nature of the products and services provided by the sector	
A level derived from the complexity of the products, due to its impact on anonymity or on the reduced amount of information available about customers.	High-volume cash-in-transit operations related to the activities of client companies that generate large volumes of cash.
Level at which specific products and services offered are linked to intelligence reports and/or national ML or TF investigations	The number of reports has always been low and has decreased in recent years: 2023: 26; 2024: 15; and 2025: 11. There are no reports from other regulated entities linked to the activity of this sector. The reports received regarding its operations have been submitted by the sector itself.
Nature of the customer	
Level derived from the nature of the business relationship with customers, based on the duration (ongoing, transactional or occasional) and frequency of the transactions	These are normally relationships that develop over an extended period of time, rather than being merely occasional.
Level derived from the customer's status	Clients usually comprise companies with a proven track record, such as financial institutions, large *retail* chains and high-street *retailers*, major jewellery brands or petrol stations, alongside other smaller enterprises.

Level derived from the client's sector or type of business	Companies that structurally operate with high levels of cash.
Geographical scope of the sector's activities	
Level derived from specific jurisdictions/countries of interest frequently associated with the sector.	Interaction with national institutions and companies. Greater risk in areas such as the Campo de Gibraltar, where the use of cash is identified as one of the greatest vulnerabilities in the area.
Level derived from the nature of interactions or transactions involving countries identified by the FATF.	Interaction with institutions and companies at national level.
Level derived from the nature of interactions or transactions involving countries subject to financial.	Interaction with national institutions and companies.
Nature of the distribution channels	
Level determined by the complexity of the channels, given their impact on anonymity or on the limited information available about customers.	Face-to-face collection and transfer of funds arising from commercial transactions settled in cash.
Level derived from the use of new technologies or payment methods.	Traditional underlying payment methods, which do not entail a level of exposure to new technologies, payments or crypto-assets.

Conclusion on the sector's inherent risk: medium for ML and low for TF

594. The volume of funds under management and cash handling indicates, in theory, the existence of substantial inherent risk. However, in Spain, the activity is confined to the domestic market, there are only three operators, the client base consists mainly of businesses, and the long-standing relationships significantly reduce the inherent risk, which has ultimately been assessed as **medium** in relation to ML and **low** for TF.

Risk factors arising from the effective (or ineffective) implementation of controls

595. To analyse residual risk, it is necessary to analyse the implementation of existing controls within the sector and the extent to which these controls are effective. The following section presents

an analysis of the factors used to determine the residual risk in the 'other services' sector, specifically the cash-in-transit sector

Risk factors relating to the effective implementation (or lack thereof) of controls	
Level of regulation in the sector	Highly regulated entities subject to high control standards.
Extent to which unauthorised entities may be operating.	They must hold administrative authorisation and be entered in an administrative register managed by the Ministry of Home Affairs. To obtain authorisation, it is necessary to comply with strict regulatory requirements and to have significant material and human resources, which makes it difficult to enter the sector[106].
Level of potential direct or indirect control over the entity or its management by money-laundering networks	Owing to the high degree of administrative oversight. The regulations require very strict administrative controls over companies and their operations, which makes it difficult for criminal networks to infiltrate these entities in any way.
Level of regulation of ML/TF prevention measures	Entities in the sector are regulated entities in relation to ML/TF under Law 10/2010, of 28 April.
Level of supervision	SEPBLAC carried out two inspections of the sector in 2019. Details of all transactions involving the deposit or withdrawal of banknotes at banks, cash machines and shops belonging to major retail chains.
Level of sanctions imposed on entities in the sector.	No formal requests or disciplinary proceedings have been brought against entities in the sector since 2019. SEPBLAC receives more than 7 million detailed transaction records annually, which are analysed to produce strategic reports; as such, the oversight is considered effective. Furthermore, they are supervised by the Ministry of Home Affairs and Banco de España in relation to auxiliary deposits
Level of professionalism of the organisation's directors and senior managers of the institution.	High level of awareness, with senior managers who, in some cases, have previous experience in security matters.
Level of awareness and understanding of their obligations regarding preventing ML and TF.	There are legal obligations in this regard, and companies in the sector and their employees have demonstrated a high level of awareness of and compliance with their obligations regarding the prevention of ML and TF.
Level of the organisation's commitment to policies and measures for prevention of ML/TF.	High level of commitment to compliance with AML/CFT obligations.

[106] Requirements, which include: (a) being legally incorporated and registered in the commercial register or the relevant public register, and having as their sole purpose all or some of the activities referred to in Article 5.1 of Law 5/2014;
b) be a national of an EU/EEA Member State; c) have adequate human, training, financial, material and technical resources; d) have in place the security measures laid down by regulation; e) take out a civil liability insurance policy or provide other financial guarantees of a sufficient amount; f) provide a surety or performance bond; and g) not have been convicted by a final judgement of certain offences

Level of professional qualification of employees and their training in ML/TF prevention.	High level of training. In one case, the group offers AML/CFT outsourcing services to third parties.
Level of internal monitoring by the entities of employees' compliance with employees.	High, due to the inherent risks of the business.
Level of compliance with obligations regarding preventive measures, particularly CDD/KYC	No shortcomings have been identified in compliance with due diligence obligations.
Level of identification and reporting of suspicious transaction reports	During the period analysed, the sector has made a number of reports based on indications that is commensurate with the number of companies comprising the sector. The average rating for the significance of suspicious transaction reports for the period 2022–2025 was 4.45. This category, introduced in 2021, allows the relative importance of reports to be assessed based on their link to factors such as the connection to serious crimes, the emergence of new risk profiles, the detection of criminal structures or networks, and/or the involvement of large sums of money.

Conclusion on the sector's residual risk: low for ML and TF

596. The residual risk for the sector is considered **low** for both ML and TF. It is regarded as a well-established sector, with the same three operators having been in place for some time, supervised by the authorities, with adequate controls and an improvement in the quality of reports based on indications.

Sector: Professional trade in other high-value goods 2026

Activity and context

597. Article 2.1.w) of Law 10/2010, of 28 April, includes, as obliged entities, persons who trade professionally in goods, in accordance with the terms set out in Article 38.

598. Without prejudice to the restrictions on cash payments laid down in Article 7.1 of Law 7/2012[107], natural or legal persons who trade in goods on a professional basis shall be subject to the obligations set out in Articles 3, 17, 18, 19, 21, 24 and 25 in respect of transactions in which receipts or payments are made by non-resident natural persons using the means of payment referred to in Article 34.2 of this Law and for an amount exceeding 10,000 euros, whether carried out in a single transaction or in several transactions between which there appears to be some kind of connection. This category would include, provided they are not already covered by a specific category, (high-end) vehicles, boats, aircraft, luxury watches, collectables or other goods easily convertible into cash, provided that a professional trader is involved and the other party is a non-resident individual.

599. The sector of professional trade in high-value goods comprises small and medium-sized enterprises and includes manufacturing, distribution and retail. In addition to these companies and brands, there are foreign companies and brands targeting customers with high purchasing power, established in the country through franchises or subsidiaries. Compared with other countries, these types of companies are small, with an annual average turnover from luxury goods sales lower than in other countries; however, in recent years there has been exponential growth with a marked geographical component, meaning that activity is concentrated in major cities and coastal areas, including the islands. There are no registration data or official figures on transactions.

Threats

600. The sector involving the professional trade in other high-value goods (which includes, amongst others, the professional sale and purchase of high-end vehicles, boats, aircraft, luxury watches, collectables and other goods easily convertible into cash) presents a low level of exposure to ML and TF risks compared with other non-financial sectors.

601. This profile can be explained by a combination of structural mitigating factors, notably the prohibition and strict restrictions on cash payments, the obligation to use bank-based payment methods, controls on cross-border capital movements, and the sector's almost complete integration into the regulated financial system. However, given the nature of the goods traded (assets of high economic value and which are potentially transferable), there are threats that must be considered from a preventive perspective, in line with the typologies set out in Chapter 4.

[107] Law 7/2012, amending tax and budgetary legislation and adapting financial regulations to step up measures to prevent and combat fraud.

602. In intelligence reports and requests for information from authorities dealing with organised crime, there is evidence of a growing use of second-hand vehicles and luxury watches as a form of currency in their transactions.

603. Furthermore, the following factors may be exploited by threats within the professional trade sector for other high-value goods, in line with the activities analysed in this report:

Factors that are frequently exploited by threats	
Use of high-value goods as a store of value	Chapter 4 identifies the acquisition of high-value goods as a classic form of value storage, used to preserve wealth outside traditional financial instruments. In this sector, the threat manifests itself through the acquisition of luxury goods as an alternative to holding bank balances, the preservation of value in tangible assets as opposed to other forms of investment, or the eventual resale of the goods to obtain liquidity under the guise of legitimate activity.
Occasional transactions with non-resident individuals	One of the significant exposure factors relates to occasional transactions with non-resident individuals, particularly in areas with high tourist traffic, coastal areas and islands. In such cases, the following may be observed: i) limited knowledge of the customer due to the non-recurring nature of the relationship, ii) difficulty in determining the economic origin of funds in isolated transactions, or iii) use of the acquired asset outside Spain following the transaction.
Occasional use of legal entities as a vehicle for acquisition	Although not common practice, the use of legal entities as purchasers or intermediaries introduces a risk factor associated with: reduced immediate visibility of beneficial ownership; simple corporate structures set up for asset management purposes; and one-off transactions that are difficult to compare with previous patterns. The impact is limited, given the small proportion of this type of client in the sector and the general absence of complex corporate structures in this area.
Channels non- face-to-face channels and increasing digitalisation	The growing use of non-face-to-face channels, digital marketing platforms and online payments introduces a risk factor related to: reduced face-to-face interaction with the customer, one-off transactions with no prior history, and the need to strengthen identification processes when the relationship is established remotely. This is consistent with trends in economic crime, although its impact is mitigated by the simplicity of the products and the predominance of controlled bank payments.

Risk factors due to inherent vulnerability

604. The following section sets out the factors relating to inherent vulnerability analysed to determine the inherent risk in the sector of professional trade in other high-value goods.

Characteristics of the sector	
Size of the sector and turnover	The sector is small, with economic activity centred on a few transactions that may involve large sums. There are no registered obliged entities as such, but the following sectors may carry out such transactions: art galleries and fairs, jewellers, luxury car dealerships, boat sales, and dealers in antiques and precious metals. The low transaction volume reduces exposure to the ML.
Level of complexity of the sector's structure	The typical structure is usually straightforward: individual traders or small businesses engaged in marketing, although there may also be groups of companies operating internationally through franchises. It is not a sector in which sophisticated corporate networks or complex corporate structures are common.
Level of integration with other regulated sectors	There are restrictions on cash payments, and interaction with the financial sector is very high, which reduces exposure to the channelling of illicit funds.
Level of the entity's localisation, including the geographical scope of the sector's operations	Operations are usually local and concentrated in specific geographical areas but may extend to multiple locations through the growing use of remote channels, which would moderately increase vulnerability by making traceability and consistent monitoring more difficult.
Nature of the products and services provided by the sector	
Level derived from the complexity of the products, due to their impact on anonymity or the limited information available on customers.	The products offered are straightforward and aimed at retail customers, with no features that facilitate anonymity or complex structures. However, operations may involve a certain lack of information on customers when one-off transactions are carried out or when dealing with legal entities.
The extent to which specific products and services offered are linked to intelligence-led communications and/or investigations domestic ML or TF	Second-hand vehicles and luxury watches are increasingly being used by criminal organisations as alternative means of payment to cash.
Nature of the customer	
Level derived from the nature of the business relationship with customers, based on duration (ongoing, transactional or occasional)	Relationships are usually one-off or occasional, which limits knowledge of the customer and makes it difficult to detect anomalous patterns. Conversely, in the case of repeat customers or corporate clients, continuous monitoring is necessary, and the vulnerability increases moderately.

and frequency of transactions	
Level derived from the customer's status	The client base consists mainly of retail clients, individuals with a low-risk profile. Transactions involving legal entities, high-risk clients or PEPs are generally infrequent, although the risk associated with such transactions increases.
Level derived from the client's occupation or type of business	The sector mainly attracts private individuals whose professional activities are not linked to high-risk sectors. There are no significant concentrations of high-risk sectors or occupational patterns that increase exposure to money laundering.
Geographical scope of the sector's activities	
A level derived from specific jurisdictions/countries of interest that are frequently associated with the sector.	There are no countries typically associated with the sector, which reduces exposure to cross-border risks; however, the presence of communities of nationals from various countries in different geographical areas of Spain, particularly coastal areas and islands, means that the risk is higher in those areas
Level derived from the nature of interactions or transactions involving countries identified by the FATF.	The business model does not require transactions with countries identified as high-risk in terms of ML/TF (the goods are located in Spain), which significantly limits vulnerability.
Level derived from the nature of interactions or transactions involving countries subject to international financial sanctions.	The sector does not routinely conduct business with customers or suppliers located in countries subject to sanctions or designated by the FATF. The domestic nature of the business reduces or virtually eliminates the likelihood of exposure to high-risk jurisdictions.
Nature of the distribution channels	
Level derived from the complexity of the channels due to their impact on anonymity or the limited information available on customers.	Business relationships are predominantly face-to-face, with little or no digital interaction.
Level derived from the use of new technologies or payment methods.	Although the sector operates mainly using traditional methods, the growing use of remote interactions, online payments and digital platforms introduces additional risks.

Conclusion on the sector's inherent risk: Medium for ML and low for TF

605. With regard to ML, the sector presents a medium risk due to the sale of high-value goods that are easily transferable and used as cash substitutes. Occasional customer relationships predominate, limiting customer knowledge and making it difficult to detect anomalous patterns. The existence of high-value one-off transactions increases vulnerability. The risk is particularly concentrated in products such as second-hand vehicles and luxury watches.

606. With regard to TF, operations are predominantly domestic and there is no systematic exposure to high-risk jurisdictions or sanctioned countries. The goods traded and the customer profile do not fit the usual TF patterns, which typically involve small amounts and rapid flows; consequently, the risk is considered low.

Risk factors relating to the effective implementation (or lack thereof) of controls

607. An analysis of residual risk requires an assessment of how existing controls are implemented within the sector and to what extent those controls are effective. The following section presents an analysis of the factors used to determine the residual risk in the sector for the professional trade in other high-value goods.

Risk factors relating to the effective implementation (or lack thereof) of controls	
Level of regulation in the sector	The sector lacks a detailed and specific regulatory framework. The activities carried out are diverse, which may hinder the consistent application of prevention obligations. However, the existence of strict controls on cash payments means that the risks are very low. In this regard, the sector is regulated by Article 7 of Law 7/2012, of 29 October, amending tax and budgetary legislation and adapting financial regulations to step up measures to prevent and combat fraud (subsequently amended by Article 18 of Law 11/2021 of 9 July on measures to prevent and combat tax fraud), which sets out the following restrictions on cash payments: • Transactions in which any of the parties involved acts in their capacity as a business owner or professional, and where the amount is equal to or greater than 1,000 euros (or the equivalent in foreign currency). • The above amount is 10,000 euros (or the equivalent in foreign currency) where the payer is a natural person who can prove that they are not resident for tax purposes in Spain and is not acting in a business or professional capacity.
Level of potential presence of entities not authorised to operate.	The activity may be carried out by individuals or companies without the need for prior administrative authorisation. The absence of official registers increases the risk of informal operators operating without AML/CFT controls.
Level of potential direct or indirect control of the entity or its management by money laundering networks	There is a possibility that legal entities engaged in this type of trade form part of the corporate structure devised by ML networks.
Level of regulation of ML and TF measures	They are regulated entities under Law 10/2010, of 28 April, with specific obligations set out in Article 38 of that Law.

Level of supervision	No thematic inspections have been carried out in relation to this activity. However, account must be taken of the points made regarding the size of this sector and the inspections carried out on other obliged entities that may carry out this activity as well as those engaged in art and antiques or jewellers.
Level of sanctions imposed on entities in the sector	The level of sanctions in this sector has historically been zero. However, sanctions are imposed on regulated entities[108] authorised to carry out this activity.
Level of professionalism among directors and senior managers of the organisation	Although there is no direct evidence regarding the carrying out of this activity, a similar level of risk is applied as for jewellers and art galleries, as they are regulated entities that may engage in this activity.
Level of awareness and understanding of their AML/TF	Although there is no direct evidence regarding the carrying out of this activity, a similar risk level is applied as for jewellers and art galleries, as they are regulated entities that may engage in this activity.
Level of the organisation's commitment to AML/CFT policies	Although there is no direct evidence regarding the carrying out of this activity, a similar level of risk is applied as for jewellers and art galleries, as they are regulated entities that may engage in this activity.
Level of professional qualification of employees and their training in ML/TF prevention	Although there is no direct evidence regarding the carrying out of this activity, a similar risk level is applied as for jewellers and art galleries, as they are regulated entities that may engage in this activity.
Level of internal monitoring by organisations of compliance by employees	Although there is no direct evidence regarding the carrying out of this activity, a similar level of risk is applied as for jewellers and art galleries, as they are regulated entities that may engage in this activity.
Level of compliance with obligations regarding preventive measures, in particular with regard to CDD/KYC	Although there is no direct evidence regarding the carrying out of this activity, a similar risk level is applied as for jewellers and art galleries, as they are regulated entities that may engage in this activity.
Level of identification and reporting of suspicious transactions suspicious transactions	Although there is no direct evidence regarding the carrying out of this activity, a similar level of risk is applied as for jewellers and art galleries, as they are regulated entities that may engage in this activity.

Conclusion on the residual risk for the sector: Low for ML and TF

608. The risk is classified as **low** because, despite the assessment of mitigating factors, the strict regulation governing cash payments and the lack of evidence in Spain of its use for ML and TF justify this classification.

[108] See the sector profile for art, antiques and jewellers.

Sector: Emission rights 2026

Activity and context

609. Section 2.5 of Law 10/2010, of 28 April, provides that the provisions governing the greenhouse gas emissions trading scheme set out in Law 1/2005, of 9 March, which regulates the greenhouse gas emissions trading scheme, subject to any exceptions laid down by regulation, the reporting and internal control obligations set out in Chapters III and IV of this Law.

610. In Spain, the service is provided solely by the Spanish Office for Climate Change (with the support of the private entity *Iberclear*, with which a service contract has been signed), in its capacity as National Administrator of the Spanish section of the Union Registry. Therefore, although it cannot be considered a regulated entity as such, it is subject to the reporting obligations set out in Chapter III[109].

611. The National Emissions Right Registry (RENADE) is the official database in which the issuance, ownership, transfer and cancellation of emissions rights arising from the obligations established under the Kyoto Protocol, the Paris Agreement and Directive 2003/87/EC (EU ETS) are recorded. In the case of sectors regulated under the EU Central Emissions Trading Registry (hereinafter 'EU ETS'), accounts are managed through the Union Registry, which forms part of the Consolidated System of European Union Registries (CSEUR). Although this is a common system for all Member States, each account is administered by its respective National Administrator.

612. There are currently around 2,000 users of the Register, acting as authorised representatives of the more than 1,200 accounts held. As of 1 January 2026, the Register had a total of 949 holders corresponding to industrial facilities, representing an average annual decrease of 18 holders. Meanwhile, the number of aircraft operators stands at 89, with an average annual increase of 9. In the case of shipping companies, there are 697 account holders; however, no data is available on trends in this sector, as it has only very recently been incorporated into the EU ETS.

613. As for fuel suppliers to the road transport and residential sectors (ETS2), no account holders were recorded as of the date indicated, as account opening is expected to begin in the course of 2026, with no official estimate of the number of operators yet available. Finally, the group of voluntary participants — such as *traders*, *brokers* and market intermediaries — totals 90 account holders, with an average annual growth rate of 5.

614. In the case of sectors covered by the EU ETS, the verified emissions figures as of 1 October 2025, corresponding to the 2024 financial year, are used, as these are considered a good indicator of the volume of trading, insofar as they reflect the number of emission rights that must be purchased on the market and surrendered to meet regulatory obligations. For voluntary participants (*traders*, *brokers* and market intermediaries), the balance is recorded

[109] The National Emissions Right Registry (RENADE) is the official database in which the issuance, ownership, transfer and cancellation of emissions rights arising from the obligations established under the Kyoto Protocol, the Paris Agreement and Directive 2003/87/EC (EU ETS) are recorded. In the case of sectors regulated under the EU Central Emissions Trading Registry (hereinafter 'EU ETS'), accounts are managed through the Union Registry, which forms part of the Consolidated System of European Union Registries (CSEUR). Although this is a common system for all Member States, each account is administered by its respective National Administrator.

total volume of emission rights held in accounts within the Spanish section of the Union Registry as of 31 December 2025.

615. From a quantitative perspective, operators of industrial installations account for the largest volume of trading, with approximately 77 million emission rights. They are followed by voluntary participants, with an aggregate total of 50 million rights, which highlights their significance in the market's operations. Air operators account for a volume of 9 million rights, whilst shipping companies account for 5 million. In the case of fuel suppliers to the road transport and residential sectors (ETS2), quantitative information is not yet available. Overall, the total volume of rights associated with the various sectors analysed amounts to 141 million.

Threats

616. The greenhouse gas emissions trading sector (EU ETS / EU Emissions Trading Scheme) presents a limited set of threats in terms of ML and TF, arising mainly from the financial and intangible nature of the rights, the existence of cross-border markets, and the economic scale associated with certain trading operations. However, these threats are clearly mitigated by the highly centralised European regulatory framework, public oversight of the system, the mandatory identification of all participants, and the historical experience gained from addressing vulnerabilities identified in the early stages of the scheme, in full alignment with the threats outlined in Chapters 4 and 5.

617. The most significant threat historically identified in the sector was the use of emission rights in VAT carousel fraud schemes, a variant of Money Laundering based on: the VAT exemption on intra-Community acquisitions, the rapid resale of rights in different Member States, and the misappropriation of the VAT charged. This type of fraud was detected mainly between 2008 and 2010 – including, in Spain, Operation Blue Sky – and also affected other Member States such as France, Germany and the United Kingdom. It should be noted that, during the period analysed, no current evidence of this type of operation has been detected, following the regulatory reforms introduced at European and national level.

618. With regard to the threat of TF in this sector, it is very low, given that: it is not a channel for collecting or directly transferring funds; transactions are settled via traditional bank transfers; account holders are fully identified; and there is constant supervision by national and European authorities. No significant patterns or national investigations have been identified that link emissions trading to TF.

619. Furthermore, there are factors that could be exploited by threats in the emissions trading sector:

Factors that could be exploited by threats	
Potential use of emissions trading for ML	From a theoretical perspective, the buying and selling of emission rights could be used as a ML mechanism by enabling: the acquisition of an intangible asset with funds of illicit origin; the carrying out of multiple successive trades; and the subsequent sale of the rights to obtain income that appears to be lawful. This type of vulnerability stems from the intangible nature of the asset, the

	speed of electronic transactions and the existence of a structured transnational market – elements that have historically been utilised in other financial markets for money-laundering schemes.
Cross-border transactions and non-resident participants	The sector is exposed to the associated risk arising from transactions with non-resident participants, particularly in the following segments: air carriers, shipping companies that have recently joined the EU ETS, and voluntary participants (traders, brokers, and market intermediaries). However, the level of exposure is mitigated by the requirement to open accounts in the EU Registry, the full identification of account holders and representatives, and the uniform application of European due diligence standards. The volume of accounts linked to higher-risk jurisdictions is very low (0.5%), which limits the potential impact.
Trading accounts and volunteer participants	There is a certain level of exposure to risk associated with trading accounts and voluntary participants, which is limited in scope and concentrated in the specific segment of trading accounts and voluntary market participants, given that: they are not subject to direct environmental regulatory obligations, they operate with greater flexibility in the trading of rights, and they can accumulate significant balances of rights. Even so, these participants are subject to strict admission policies, enhanced identification requirements (LEI, beneficial ownership, background checks), and ongoing transaction monitoring, which significantly reduces the possibility of misuse of the system.

Risk factors relating to inherent vulnerability

620. The following section sets out the factors relating to inherent vulnerability that were analysed to determine the inherent risk in the emissions trading sector.

Characteristics of the sector	
Size of the sector and volume of turnover	The sector accounts for 15 % of the European market in Spain. The number of account holders is relatively low, with the greatest risk lying in a specific segment relating to trading accounts.
Level of complexity of the sector's structure	Well-known key operators, with a higher degree of complexity in the case of shipping companies and legal entities holding trading accounts. The sector's structure is clearly defined: clearly identified competent authorities, which act as market makers (injecting rights into the market). Operators in the EU ETS, who must hold an account in the Registry and acquire emission rights in order to make a surrender. Voluntary market participants: the structure is similar to that of any other financial market (MiFID requirements).
Level of integration with other regulated sectors	A specific market for transactions that are based on regulatory requirements.

Level of the entity's location, including the geographical scope of the sector's operations	The regulated entity is the Spanish Office for Climate Change, which is based in Madrid. With regard to operations, in the case of the aviation and maritime sectors, accounts held by third-country nationals are managed, some of whom appear on the FATF lists. However, the volume of corporate accounts in these countries is very low (0.5 %), and the customer onboarding policy mitigates the risk of fraud in these cases.
Nature of the products and services provided by the sector	
Level derived from the complexity of the products, due to their impact on anonymity or the limited information available on customers.	Emissions rights are traded via accounts held in the Registry. Account management in the Registry is an administrative service that facilitates access to the EU ETS market and compliance with obligations under the scheme. All account holders must comply with strict due diligence standards, as set out in European regulations.
The extent to which specific products and services offered are linked to communications by implication and/or national investigations national ML or TF	Since the launch of the EU ETS in 2005, fewer than five indications have been reported to SEPBLAC. No national investigations are known to have taken place.
Nature of the customer	
Level determined by the nature of the business relationship with customers, based on its duration (ongoing, transactional or occasional) and the frequency of transactions	The relationship is ongoing, particularly with sectors subject to the EU Anti-Money Laundering Directive.
Level derived from the customer's status	Currently, all account holders are legal entities. Throughout the EU RCDE, activity by natural persons has been marginal. As of 1 January 2026, 41 % of account holders are foreign nationals, mostly from the maritime sector.
Level derived from the client's occupation or type of business	Account holders carry out activities subject to sector-specific and/or financial regulation; they must therefore hold the relevant licences and are subject to supervision. The risk centres on the structure that account holders who are natural persons.
Geographical scope of the sector's activities	
Level derived from specific jurisdictions/countries of interest frequently associated with the sector.	Most entities are Spanish or European, although operations involving high-risk jurisdictions have been identified.
Level derived from the nature of the interactions or	Of all accounts, less than 1% belong to companies based in countries included on the FATF lists.

transactions that involve countries identified by the FATF.	
Level derived from the nature of the interactions or transactions involving countries subject to international financial sanctions.	Of all accounts, less than 1% belong to businesses located in countries included on the EU sanctions lists.
Nature of distribution channels	
A measure derived from the complexity of the channels, based on their impact on anonymity or on the reduced amount of information available about customers.	When buying or selling on the market, the transaction is settled in cash, usually by bank transfer
A level derived from the use of new technologies or payment methods.	The channel used is bank transfers. No crypto-assets are used.

Conclusion on the sector's inherent risk: medium for ML and TF

621. Taking into account the factors analysed and the specific characteristics of this sector, in particular the limited scope of this universe (a single company), the inherent risk is considered **medium**.

Risk factors relating to the effective implementation (or lack thereof) of controls

622. An analysis of residual risk requires an assessment of how existing controls are implemented within the sector and to what extent those controls are effective. The following section presents an analysis of the factors used to determine the residual risk in the emissions trading sector.

Risk factors relating to the effective implementation (or lack thereof) of controls	
Level of regulation in the sector	High level of regulation for the majority of operators (account holders account holders).
Extent to which unauthorised entities may be operating.	Regulated entities are subject to specific rules: as regards market participants, it is not possible to open an account for regulated sectors unless they hold the relevant operating licence. In the case of voluntary entities (traders or brokers), they are not required to provide details of their MiFID authorisation, but they must provide their LEI code.
Level of potential direct or indirect control over the entity or its management by money laundering networks	There is no record of any specific account profiles affected by this risk. However, amongst the various due diligence requirements, identification of the beneficial owner of the company holding the account in the Register. This rule applies to account types categorised as posing the highest risk (trade accounts).

Level of regulation of ML and TF measures	The sector is regulated under Law 10/2010 of 28 April and must comply with the obligations set out in Chapter III.
Level of supervision	*Iberclear* is the operator of the Central Register, and its control framework is subject to supervision by the CNMV and the Banco de España. With regard to market participants, controls are applied in the form of client admission policies, periodic audits, and daily/weekly monitoring of transactions. These controls are implemented by the National Administrators of the Member States, and in addition, the European Commission also maintains coordination with the relevant European authorities (Europol, ESMA, etc.).
Level of sanctions imposed on entities in the sector.	No sanctions have been imposed for non-compliance with obligations relating to the prevention of ML/TF.
Level of professionalism of the organisation's directors and senior management.	The staff of the Spanish Office for Climate Change and Iberclear are highly qualified in the emissions trading market and financial markets. As a condition for the formalisation of the contract, Iberclear must sign a declaration confirming the absence of any conflict of interest. The opening of an account or the appointment of its representatives may be refused, and representatives' access to the account may be suspended, in cases where the company's representatives or its directors are subject to investigation or have, within the last five years, been found guilty of fraud in relation to emission rights, ML, TF or other serious offences for which the account could be used as an instrument.
Level of dissemination and awareness of its obligations regarding the prevention of ML and TF.	The Procedures Manual for the prevention of ML and TF is distributed to the relevant individuals by the regulated entity.
The organisation's level of commitment to ML/TF policies and measures.	As a regulated entity, the OACC has procedures in place to fulfil its ML/TF prevention obligations. The Manual of Procedures for the Prevention of ML and TF stipulates that the representative before SEPBLAC is the Deputy Director-General for Carbon Markets at the OECC, and identifies the authorised persons acting under his direction and responsibility. The public nature of this regulated entity helps to mitigate existing risks.
Level of professional qualifications of staff and their training in preventing ML/TF.	Staff in the sector take part in regular workshops organised by the EU Registry Administrators Group, during which specific issues relating to fraud within the EU ETS are analysed.
Level of internal monitoring by organisations of employees' compliance employees.	Transactions carried out by staff in the Registry must be conducted in accordance with the dual validation principle (one person proposes, and another approves). All transactions are recorded, identifying the individuals who carried them out.
Level of compliance of obligations regarding	The customer admission policy sets out strict measures, governed by European regulations.

preventative measures, in particular CDD/KYC	All account holders must comply with strictly regulated due diligence standards. This involves information requirements (identification of representatives and legal entities, criminal records, beneficial ownership, etc.). The documentation requirements for opening accounts involve a rigorous due diligence process: notarised and, where applicable, legalised copies of identity documents, proof of permanent residence, criminal records, notarised powers of representation, proof of group structure, LEI code identification, etc.
Level of identification and reporting of suspicious transactions reports.	Since the introduction of the EU Anti-Money Laundering Directive in 2005, the OECC has reported fewer than five instances of suspicious activity to SEPBLAC. Of these, there is no evidence, or it has been ruled out, that they could constitute money laundering or terrorist financing.

Conclusion on residual risk in the sector: Low for ML and TF

623. Taking into account the inherent characteristics, as well as the level of controls in place, the residual risk for both ML and TF is **low**.

Sector: Crypto-asset Service Providers 2026

Activity and context

624. Article 2.1.z) of Law 10/2010, of 28 April, designates providers of services involving the exchange of virtual currency for fiat currency and the custody of electronic wallets as obliged entities.

625. Under the transitional period provided for in MiCA, which ends in July 2026, crypto-asset service providers (hereinafter 'CASPs') have been able to continue operating provided they were already effectively providing these services in accordance with current regulations. By the end of 2025, only one CASPS held a MiCA licence granted by the CNMV[110], alongside four Spanish banks authorised to operate in crypto-assets under the notification regime[111].

626. At the start of 2026, there were 104 entities listed in the Banco de España's register of virtual currency exchange service providers. This register is no longer accepting new registrations and remains in force solely for information purposes during the transitional period. This number is expected to fall sharply (to below 30 entities) following the end of the transitional period, partly because not all registered entities have submitted a formal application for authorisation to the CNMV.

627. Since the MiCA Regulation came into force, the CNMV has been the competent authority for authorising CASPS's applying for a MiCA licence from Spain. Furthermore, this register will also include all CASPS's that, having obtained a MiCA licence in another EU Member State, have declared their intention to provide services in Spain. There are currently four distinct groups: a) Approximately 12 % of all CASPS registered with the Banco de España fall into the category of large crypto-asset *exchanges*, due to higher trading volumes, the number of clients and operations in a greater number of countries; b) Around 8 CASPS are engaged in managing crypto-asset ATMs, most of which are installed in shopping centres and third-party retail outlets; c) 4 are Spanish banking institutions; and d) The remainder are small or medium-sized CASPS.

628. Many of them provided evidence in response to the Structured Request for Information (hereinafter R.I.E.).[112] that they had never actually carried out any business in Spain (26), whilst others offered a wide variety of services (some of which were unregulated): custody, consultancy, asset tokenisation, intermediation, the issuance of *NFTs* and other tokens (sports tokens, etc.), as well as three individuals who ceased trading following the end of the transitional period due to the requirements of the MiCA Regulation.

629. As regards the volume of CASPS operations, the data on payments received from clients—compiled via the R.I.E.s requested by SEPBLAC from the CASPS—amounted to a minimum total volume of around 20,000 million euros. Meanwhile, a study carried out by Chainalysis indicates that the total volume of crypto-assets received by Spanish investors between May 2024 and May 2025 amounted to around 68,800 million euros (80,000 million

[110] Bitcoinforme, S.L.

[111] BBVA, Cecabank, Openbank and Renta4

[112] The R.I.E. (Structured Information Request) is a questionnaire sent annually to organisations in various sectors.

dollars)[113]. In any case, it is estimated that the volume of actual trading would fall within a range of 20,000 and 68,800 million euros.

Threats

630. The crypto-asset sector, comprising CASPS, presents a high level of threats in relation to ML, TF and financial crime, stemming from the technological nature of the products, their distinctly cross-border nature, the intensive use of remote channels, and the continued presence of actors that are not fully regulated and which operate with customers resident in Spain.

631. These threats are consistent with the EU's SNRA, the FATF's conclusions and the National Strategy against Organised Crime and TF and are exacerbated by the use of CASPS located in high-risk jurisdictions or those with compliance standards lower than European ones.

Money Laundering via crypto-assets

632. Reports based on intelligence and investigations carried out by the LEAs indicate a growing use of crypto-assets as a tool for channelling illicit funds, replicating patterns already known from the traditional financial system, notably:

- The unauthorised opening of accounts at CASPS using multiple identities, the repeated use of IP addresses, or access from high-risk locations.
- The use of AI tools in combination with fraudulently obtained identity documents, mainly from the *Dark Web* to open accounts with CASPS for the purposes of ML, TF and/or financial crime.
- The use of intermediaries (mules), often with limited technological knowledge or in a situation of economic vulnerability, particularly in schemes linked to drug trafficking or fraud.
- Carrying out scams and fraud (fake investment schemes, romance *scams*, *phishing*), which generate intense and unstructured transaction activity between *wallets* and P2P platforms without a coherent economic justification.
- A preference for *stablecoins* as a vehicle for moving illicit funds, given their high liquidity and lower volatility.

Use of crypto ATMs to deposit cash

633. The use of crypto ATMs to introduce cash of illicit origin into the crypto ecosystem has been identified, through:

- systematic splitting of transactions below certain thresholds,
- limited customer identity verification for low-value transactions,
- rapid conversion between fiat currency and crypto-assets.
- The inspections carried out have revealed significant shortcomings in this channel, which increase the risk of ML/TF compared with other service delivery models.

[113] It should be noted that this latter figure is significantly higher, as it includes more CASPS than Chainalysis would have detected as being actively operating in Spain; in other words, it does not only include those officially registered with the Banco de España.

Furthermore, a chained operation has been observed that integrates the phases of placement, layering and integration, through the combined use of crypto ATMs for depositing cash, anonymisation platforms (notably the RAILWAY platform) that hinder the traceability of funds, and DeFi applications that allow the origin of funds to be justified and facilitate their reintegration into the formal financial system.

Terrorist Financing

634. According to the FATF's findings, there is a growing trend towards the use of crypto-assets in relation to TF and PF, particularly for:

- the collection and cross-border transfer of funds intended for terrorist organisations, exploiting the speed and pseudonymity of the system,
- circumvention of international sanctions relating to weapons proliferation, through the use of foreign platforms, mixers, DeFi services and CASPS with limited international cooperation.

635. The factors most frequently exploited by threats in the CASPS environment are as follows:

Factors most frequently exploited by threats	
Operational and high-risk jurisdictions	A cross-cutting factor across the sector is the high exposure to high-risk jurisdictions, both due to the location of the most significant CASPS platforms by volume and due to frequent interaction with: • foreign *exchanges* not authorised in the EU, • platforms that are subject to sanctions or linked to countries subject to international sanctions, • offshore structures that make it difficult to trace the origin and destination of funds. *Reverse solicitation* is seen as a recurring channel for unauthorised practice, allowing unauthorised CASPS to operate with residents without effective oversight.
Product complexity, anonymity and DeFi	Exposure is heightened in those CASPS that permit: i) interactions with self-hosted addresses or with third-party CASPS outside the EU, ii) the use of crypto-assets that facilitate anonymity, and iii) participation in the decentralised finance (DeFi) ecosystem, where user identification may be non-existent and traceability limited. Whilst European regulations introduce additional obligations, their effective implementation still presents operational challenges. It is important to note that purely peer-to-peer (P2P) transactions between private individuals, carried out without the involvement of a professional crypto-asset service provider, are not directly subject to the MiCA authorisation regime and obligations, and are therefore not subject to obligations regarding the identification of the parties involved.
Nature of the client and embedded embedded	Although resident individuals predominate, exposure increases in the case of: i) legal entities with complex structures, and ii) 'embedded structure' models, in which foreign CASPS entities without a European licence

	use the infrastructure and authorisation of a local payment service provider to provide services to third parties, thereby significantly increasing the risk.
Remote channels	The sector operates almost exclusively through remote onboarding processes, supported by technological verification tools which, in some cases, do not fully comply with national regulations and, in others, can be circumvented by combinations of AI tools, whether or not these are used in conjunction with fraudulently obtained identity documents.
Weaknesses in due diligence	Inspections have identified significant shortcomings in the implementation of CDD/KYC measures, particularly during the *onboarding* phase, as well as deficiencies in the identification and reporting of suspicious transactions

Risk factors due to inherent vulnerability

636. The following sets out the factors relating to inherent vulnerability analysed to determine the inherent risk of CASPS:

Sector characteristics	
Size of the sector and turnover	Although turnover figures and transaction volumes have increased over the past year, they remain fairly modest compared with those of the traditional financial sector. Given the decentralised and opaque nature of the sector, we are unaware of a significant proportion of the flows channelled by many of the unofficial actors operating within it.
Level of complexity of the sector's structure	The prevailing trend amongst CASPS companies is not to officially consolidate as a group, although subsidiaries of parent companies based abroad have been identified. It should also be noted that it is difficult to verify their actual activity in Spain, as their annual accounts (where these have been filed in Spain) are not always reliable. There are cases in which part of the Spanish subsidiary's actual activity is channelled through the accounts of its parent company abroad. In other cases, no information is available regarding the activity of the foreign company operating in Spain (both those arising from *reverse solicitation* [114] and those foreign companies that incorrectly declare that they do not carry out any activity in Spain).
Level of integration with other regulated sectors	Following the entry into force of the MiCA Regulation, there has been an influx into the sector of other regulated financial institutions, primarily banks (both domestic and foreign), although an emerging interest has also been detected on the part of agencies and securities firms. Furthermore, the use of payment platforms owned by payment institutions, *neobanks*, credit institutions or electronic money institutions to convert fiat currency

[114] *Reverse solicitation* is the only legal means by which a foreign CASPS—which is neither registered nor authorised in the EU—may provide crypto-asset services to a European client without a MiCA licence, provided that it is the client themselves who exclusively and spontaneously initiates the business relationship without any solicitation, advertising, marketing, prior contact or influence on the part of the CASPS.

	into crypto (and vice versa) means that these sectors are exposed to the risk associated with the level of integration between online gambling operators and other regulated sectors. Finally, sports betting is also affected by the online gambling sector, as the permissiveness regarding the use of cryptocurrencies as a means of payment on online gambling platforms introduces new risks and financial dynamics.
Location of the entity, including the geographical scope of the sector's operations	Of the CASPS entities with the most significant activities in terms of channelled turnover (specifically 13 *exchanges*), only one is incorporated in Spain; the majority are of Asian origin and, to a lesser extent, North American, with a few European ones. Some of these CASPS entities rely on structures previously established in their countries of origin, with a culture of regulatory compliance that differs substantially from European standards.
Nature of the products and services provided by the sector	
Level derived from the complexity of the products, due to their impact on anonymity or the reduced amount of information available on clients.	The greatest exposure to risk is borne by those CASPS that allow their clients to interact with external parties, both in receiving and sending crypto-asset transactions to and from self-hosted addresses, or those hosted by third-party CASPS, whilst their actual knowledge of the counterparties in such transactions is very limited. Regulation (EU) 2023/1113 requires CASPS to put in place certain controls to request information from their customers; however, these controls are left to the discretion of the reporting entity without any means of verification. Furthermore, many of these CASPS still currently list certain crypto-assets that facilitate anonymity[115]on their platforms, despite the publication of the ban on trading in them within the EU, with effect from 1 July 2027. Finally, it is worth noting the growing use of the decentralised finance (DeFi) ecosystem within the crypto sector, an area in which users can interact with *wallets* and *smart contracts* without needing to identify themselves and whose use, although still limited, is being actively promoted by various players in the sector.
The extent to which specific products and services are linked to tip-off reports and/or national ML or TF investigations	Reports based on evidence of ML and TF in which crypto-assets are used as a tool to channel funds continue to show a fairly marked upward trend. A significant number of the reports received indicate that criminals continue to prefer the use of *stablecoins* to move their funds. In this regard, it is worth noting that the *stablecoin* with the highest market capitalisation globally, accounting for 60 % (USDT), cannot be offered, marketed, admitted to trading or made available for ordinary purchase by European CASPS entities such as if it were a MiCA-compliant *stablecoin*.
Nature of the customer	
Level derived from the nature of the business relationship with customers, based on duration (ongoing, transactional or	Although ongoing business relationships with customers are the norm in the sector, the supervisory authority has found that certain CASPS fail to verify the identity of their customers under the pretext of an alleged occasional relationship, which does not apply in such cases. Specifically, this concerns those CASPS that operate crypto ATMs and which, as a general rule, do not verify the identity of customers making deposits in

[115] Monero, ZCash or DASH

occasional) and the frequency of	in cash below the threshold of 1,000 euros. In some cases, customers are only asked for a telephone number, with instances of splitting transactions having been detected, along with a clear risk of ML and TF.
Level derived from the customer's status (natural person v. legal entity, national v. foreign national, high-net-worth customers, PEPs, amongst others)	The predominant profile amongst registered CASPS clients is that of individual clients, the majority of whom are Spanish nationals and/or residents, and who present an acceptable level of risk. On the other hand, amongst the corporate clients also present, the risk rises significantly, given the profile of many of them. For example: embedded structures are observed, that is, foreign CASPS third parties (without a licence to operate in Europe) which act as clients by leveraging the structure and licence already obtained by a local CASPS, from which they provide services to their respective clients.
Level derived from the client's occupation or type of business	In line with the client status indicated above, although there is generally a higher proportion of individuals in low-risk occupations, among corporate clients there is a high number of business relationships likely to be regulated as obliged entities: not only as CASPS but also as foreign EP and EMI, which operate in European territory without the relevant licence.
Geographical scope of the sector's activities	
A level derived from specific countries of interest that are frequently associated with the sector.	It is common to find high-risk jurisdictions associated with the sector, partly due to the origin of many of the software programmers and developers, who are highly regarded within the sector. Furthermore, it is common to find companies in the sector based in Gibraltar or the Seychelles, both of which are included on the list of jurisdictions that do not share tax information with Spain. Less common, but still occurring, are cases in which some of the main organisers behind the launch of new tokens showing signs of fraud end up seeking refuge in Middle Eastern jurisdictions that present themselves as *supposed* technology hubs
A level derived from the nature of the interactions or transactions involving countries identified by the FATF.	With regard to transactional dealings with designated countries, the risk is significantly higher, given that a substantial proportion of the business relationships underpinning these transactions involve opaque activities and, in some cases, show signs of criminal behaviour.
Level derived from the nature of the interactions or transactions involving countries subject to financial sanctions international	In the operations of global CASPS platforms, it is common to encounter interactions with known sanctioned *exchanges* (e.g. Nobitex, based in Iran, and the well-known Garantex – now renamed Grinex – based in Russia, both of which are subject to sanctions).
Nature of the distribution channels	
Level derived from the complexity of the channels due to their impact on anonymity or the	The vast majority of CASPS operators in this sector use remote *onboarding* processes. There is a certain prevalence in the use of specific identity verification tools, with many of these being marketed by companies based in countries outside the EU, and in any event failing to adapt their

minimal information on customers.	systems to our current regulations (specifically Law 10/2010 and its associated Regulations). Furthermore, the very nature of crypto-assets—which, through the use of techniques such as *mixers*, *coinjoin*, DEXs or private crypto-assets—reinforces anonymity and obscures the identity of customers. Added to this are the speed and cross-border nature of transfers, as well as self-custody without intermediaries, which hinders the traceability of funds and increases the risk of Money Laundering and illicit terrorist financing.
Level arising from the use of new technologies or payment methods.	The long-standing relationship between CASPS organisations and financial institutions (banks, EP, EMI, etc.) – whereby the latter provide the financial services required to process their customers' payments in fiat currency – has given rise to hybrid structures designed to channel all types of funds and adapt to more restrictive regulatory environments.

Conclusion on the sector's inherent risk: High for ML and TF

637. The inherent risk of the crypto-asset sector being used for ML/TF purposes is considered high, primarily due to the nature of the products and services offered and the marked cross-border component of its operations.

638. In terms of typology, the sector is highly diverse: (i) a core group of 13 large *exchanges* in terms of trading volume, customer base and multinational presence; (ii) 8 crypto-ATM operators with a widespread presence in shops and shopping centres across the country; (iii) four Spanish banks; and (iv) a majority of small and medium-sized crypto-asset service providers (CASPS) engaged in a variety of activities (custody, consultancy, tokenisation, intermediation, issuance of NFTs and other tokens). This fragmentation, combined with the lack of standardised group-level consolidation and the difficulty in verifying their actual activity in Spain, increases the inherent vulnerability arising from organisational complexity and a lack of transparency.

639. From a threat perspective, tip-off-based investigations involving crypto-assets continue to rise, with the most common predicate offences being: fraud, tax offences, participation in a criminal organisation, illicit drug trafficking, as well as a substantial increase in TF offences, amongst others. Despite effective international cooperation, prosecutions and convictions are progressing at a moderate pace compared with the massive proliferation of crimes involving the use of crypto-assets.

640. In terms of products and services, the risk is heightened in those payment service providers (PSPs) that allow transfers to and from self-hosted addresses or those hosted by PSPs established outside the EU, where their knowledge of the counterparties is much more limited, despite the obligations set out in Regulation (EU) 2023/1113, the effective compliance with which remains to be verified. It should be added that some CASPS continue to list crypto-assets that facilitate anonymity (Monero, Zcash, Dash), despite the announcement of their future ban in the EU from 1 July 2027.

641. As regards the nature of clients, it should be noted that, although individuals predominate, there are also legal entities with significantly higher risk profiles, including embedded structures (foreign CASPS without a MiCA licence that 'rely' on the licence obtained by a local CASPS to provide services).

642. By distribution channel, virtually all *onboarding* processes are carried out remotely, using verification tools that are often not in line with current legislation (Law 10/2010, of 28 April, and its associated Regulations).

A specific area of concern within the sector in Spain is crypto-ATMs, where the failure to verify identities for cash transactions involving amounts under €1,000 has revealed serious vulnerabilities in terms of ML/TF risks.

Risk factors relating to the effective implementation (or lack thereof) of controls

643. To analyse residual risk, it is necessary to assess the implementation of existing controls within the sector and the extent to which these controls are effective. The following section presents an analysis of the factors used to determine the residual risk of CASPS.

Risk factors relating to the effective implementation (or lack thereof) of controls	
Level of regulation in the sector	With the entry into force of the MiCA Regulation and the Fund Transfers Regulation, much of the sector is now subject to regulation in key areas such as the services that may be provided by authorised providers, as well as the obligation to carry out due diligence on the origin and destination of certain transactions. However, there is still a long way to go in terms of regulation to achieve more effective oversight of the sector (through the European RTS).
Extent to which unauthorised entities may be operating.	Unauthorised practice remains a constant issue within the sector, with unauthorised CASPS operators in Spain unduly relying on what is known as *'reverse solicitation*'. The controls currently in place are not yet sufficiently effective.
Level of potential control, whether direct or indirect, exercised by money laundering networks over the entity or its management	Corporate control systems and beneficial ownership verification procedures—in particular, the verification procedures supported by the Central Registry of Beneficial Ownership (RCTIR) and established by the competent authority and other collaborating agencies—mitigate this risk. The regulations applicable to crypto-asset service providers, contained in the MiCA Regulation, establish strict authorization and supervision requirements by the National Securities Market Commission, including an assessment of the integrity, knowledge, skills, and experience of the entity's directors and executives (Articles 59, 62, and 63), as well as an assessment of shareholders with significant holdings and of direct or indirect control structures, in order to prevent them from hindering effective supervision or facilitating the infiltration of money laundering or terrorist financing networks.
Level of regulation for AML/TF measures	The regulation of ML/TF measures for these types of entities—with respect to the provision of services involving the exchange of cryptoassets for fiat currencies and the custody of cryptoassets—is consistent with that of other equivalent sectors. However, under Law 10/2010, of 28 April on the prevention of ML and TF, not all categories of PSCA identified by the FATF are currently regulated as regulated entities. In particular, activities involving the exchange of one or more cryptoassets, the transfer of cryptoassets, and the participation in and provision of services

	related to the offering or sale of crypto-assets by an issuer are not expressly included.
Level of supervision	The number of CASPS entities included in SEPBLAC's inspection plan continued to rise throughout 2025. Three general-scope inspections were launched, along with three thematic inspections focusing on compliance with the *Travel Rule*, and a further two focusing on the authorisation process. Furthermore, in 2025, a Structured Information Request was drawn up and sent to all CASPS entities, which will serve to improve understanding of the sector's entities and their risks. Overall, serious deficiencies were found in identification procedures, due to inadequate remote identification models, a lack of information on the purpose of transactions, and severe breaches in the monitoring of business relationships resulting from a lack of knowledge regarding the counterparties to transactions, which leads to ineffective risk management and the need for special examinations and communications based on indications of non-compliance.
Level of sanctions imposed on entities in the sector.	Although many of the inspections resulted in a recommendation to initiate disciplinary proceedings, the number of CASPS organisations currently subject to sanctions remains relatively low, and the low level of the fines provides little deterrent. During the period analysed, one CASPS organisation was sanctioned for seven serious infringements.
Level of professionalism among the organisation's directors and senior managers.	Given the still limited maturity of the CASPS sector, it is particularly difficult to identify directors and senior managers with proven experience in this field. The shortage of professionals with specific experience in crypto-assets has meant that, in many cases, senior management positions are filled by entrepreneurs and technology-background professionals who, whilst bringing solid technical knowledge, lack managerial or leadership experience in regulated financial sectors – a factor that has become evident during the inspections carried out.
Level of awareness and understanding of their AML/TF obligations.	As recruitment of staff in CASPS is fairly limited, it is common to find that administrators and senior managers are fully focused on core business areas and therefore end up hiring anti-money laundering experts, who are usually responsible for communicating these obligations.
The organisation's level of commitment to AML/CFT policies and measures.	In a sector as volatile and dynamic as that of crypto-assets, many CASPS prioritise growth to ensure their survival, even at the expense of neglecting their regulatory compliance obligations.
Level of professional qualifications of staff and their training in ML/TF prevention.	In line with the above, business areas are the priority, with training limited to the minimum necessary to meet the supervisor's requirements.
Level of internal monitoring by the	It is observed that, generally speaking, the organisations have adequate mechanisms for monitoring and supervising regulatory compliance by their employees.

entities regarding employees' compliance with	These mechanisms include periodic checks, formalised internal policies and established internal audits.
Level of compliance with obligations regarding preventive measures, particularly CDD/KYC	The inspections carried out have identified serious shortcomings in the application of customer due diligence measures, primarily during the *onboarding* process.
Level of identification and reporting of suspicious transaction reports (STRs)	The inspections have also revealed shortcomings in identifying and making reports based on evidence. The average rating for the significance of reports based on indications for the period 2022–2025 was 5.5. This category, introduced in 2021, allows the relative importance of reports to be assessed based on their link to factors such as their connection to serious crimes, the emergence of new types of risk, the detection of criminal structures or criminal networks and/or the involvement of large sums of money.

Conclusion on the sector's residual risk: High for ML and TF

644. Following the impact of the MiCA Regulation coming into force, combined with the reduction in the effective number of CASPS institutions and the stringent supervisory measures adopted over the last two years, the sector's residual risk has been partially mitigated, although it generally remains classified as **high**.

645. Whilst pockets of high risk persist — stemming mainly from cross-border operations, exposure to high-risk jurisdictions and a compliance culture that still leaves room for improvement — the fact is that the introduction of effective regulation and supervision of the sector has set in motion a process of gradually weeding out bad actors, a process that should become more firmly established in the medium to long term.

646. However, the residual risk must be assessed on a case-by-case basis depending on the profile:

a) For regulated CASPS's (MiCA licence) and, pending the consolidation of the sector following the end of the transitional period, the residual risk can be considered **moderate**, subject to the quality of their controls (effective implementation of the Travel Rule, for example);
b) For crypto-ATMs, the residual risk remains **substantial** due to the intensive use of cash and the high total number of crypto-ATMs in Spain;
c) Unregulated CASPS's operating with Spanish residents (through the aforementioned *reverse solicitation*) pose a **high** residual risk, given the clear lack of control over their activities, as well as the lack of cooperation with the supervisory authorities in their countries of origin.

Sector: Crowdfunding Platform Activities 2026

Activity and context

647. Crowdfunding Platforms (CPs) connect project promoters seeking funds through the issue of securities and shares or by applying for loans with investors or fund providers seeking a return on their investment. Crowdfunding is an alternative form of financing for start-ups and small and medium-sized enterprises (SMEs), which typically relies on small investments. It represents an increasingly significant form of intermediation in which a crowdfunding service provider, without assuming any risk of its own, operates a crowdfunding platform open to the public with the aim of connecting investors with companies seeking funding. In other words, crowdfunding platforms have a financial component through which the investor expects to receive a monetary return on their financial contribution.

648. CPs must be distinguished from other forms of financing also grouped under the term 'crowdfunding', as the latter are carried out via online platforms, but in which the funders are not investors seeking a financial return, but rather contributors who provide funds through other systems without financial interest, such as donations, product purchases, interest-free loans, or others. These 'crowdfunding' systems, known as micro-patronage schemes, are generally distinct from the investment and credit systems of CPs.

649. On loan-based CPs, also known as 'crowdlending' platforms, individuals can apply for a loan to achieve a specific aim. The platform operators assess the applicant and their request, establishing risk levels and an interest rate to be paid on the amount granted should the target be met. Once approved, the request is advertised on the platform to raise funds from lenders. Investment-based crowdfunding platforms, also known as *'equity* crowdfunding', allow business projects in need of funding to be presented via the platform, with shares in the business project being offered to potential investors through the platform. These include projects for the purchase of homes or commercial premises.

650. From June 2027, Regulation (EU) 2024/1624 requires CP entities to be designated as obliged entities in each country, regardless of the project's economic interest. CPs require prior authorisation to carry out their activities and must meet a series of requirements: they must be incorporated as a limited company with an indefinite duration, have paid-up share capital, be domiciled in the EU, have an exclusive corporate purpose, and be authorised and registered with the CNMV; this registration will be public and take place after entry in the Commercial Register. With regard to sector figures, as of March 2026 there were 27 CPs registered with the CNMV in Spain and 43 European CPs providing services in Spain. According to Universo Crowdfunding, the market for this type of financing (including donations) has grown from 17 million euros in 2013 to 522 million in 2024, increasing thirtyfold in eleven years.

Threats

651. The CPs sector presents a range of significant threats in relation to ML and, to a lesser extent, TF, arising from its financial nature, its digital and cross-border character, and the intermediation of investments and loans without the platform assuming any risk itself. These threats are consistent with those identified in Chapters 4 and 5 and in the EU's SNRA, particularly in relation to the instrumental use of investments to give the appearance of legitimacy to illicit funds, opaque corporate structures, the channelling of funds to fictitious projects, and cross-border operations with limited traceability, although there is greater exposure to ML than to TF due to the economic logic of investment and lending operations; this is because, in the case of TF, operations are aimed at generating financial returns, require relatively structured disbursements, and do not constitute a channel for repeated micro-transfers. Nevertheless, certain crowdfunding models or small-value contributions could be used to a limited extent for TF, which justifies their classification as a moderate threat.

652. Factors have been identified that could be exploited by threats in the CPs sector:

Factors that can be exploited by threats	
Use of CPs as a mechanism for laundering illicit funds	The sector's main exposure to the threat lies in the use of platforms as a channel for money laundering, through: the investment of funds of illicit origin in real or fictitious projects; the granting of loans that generate apparently legitimate returns; and participation in financing structures that enable financial flows to be justified. This use places the sector's exposure to the threat primarily in the concealment and integration stages of money laundering, by providing a legitimate financial narrative for funds of illicit origin.
Fictitious or instrumental projects promoted by criminal organisations	CP entities may be used to present financing projects promoted by criminal networks, whether: as a mechanism for intra-organisational self-financing, to raise funds from third parties through seemingly legitimate investments, or to launder illicit funds by mixing them with legitimate contributions. This risk is heightened where there is a lack of transparency regarding the promoter, complex corporate structures or insufficient verification of the final destination of the funds.
Complexities in identifying the beneficial owner and the source of funds	Another structural threat to the sector stems from a potential lack of transparency regarding the beneficial owners of the parties involved, both investors and promoters, particularly when: special purpose vehicles are used, non-resident investors are involved, or the funds originate from multiple jurisdictions. The fragmentation of contributions and the dispersion of participants make it difficult to carry out an aggregate analysis of the economic origin of the funds.
Cross-border operations and exposure to high-risk jurisdictions	CPs schemes are inherently cross-border in nature, as they allow for the participation of investors and developers located in different countries. This characteristic introduces risks linked to: jurisdictions with varying AML/CFT standards, countries identified by the FATF or subject to sanctions, and transnational financial flows that are difficult to track. This risk is exacerbated by the use of open digital platforms and the provision of services under the freedom to provide services within the EU.

Occasional relationship and absence of an ongoing connection	The relationship between the CPs and its users is usually sporadic and limited to specific projects, which: reduces the gradual understanding of the client, makes it difficult to identify behavioural patterns, and concentrates risk on individual financing transactions. There is nothing to prevent the same developer or investor from participating in multiple projects, thereby increasing aggregate risk if there is no consolidated view of their activity.
Use of new technologies and payment methods	The sector is adopting digital technologies that may increase exposure to the threat, particularly where the following are permitted: the use of electronic money, intermediation via external payment service providers, or, in as yet limited scenarios, the use of crypto-assets. These factors may adversely affect the traceability of the origin of funds, especially prior to the full implementation of the AML Regulation.

Risk factors based on inherent vulnerability

653. The following sets out the factors relating to inherent vulnerability analysed to determine the inherent risk of the CPs sector.

Characteristics of the sector	
Size of the sector and turnover	Funding is growing but remains small in absolute terms. The sector's size in Spain is modest.
Level of complexity of the sector's structure	Due to the presence of multiple players (developers, investors, platforms and payment providers), fragmented financial flows and a high volume of low-value transactions. Added to this is the of digital channels.
Level of integration with other regulated sectors	Payments are processed through financial institutions and payment service providers; this increases operational dependence and the need for effective coordination amongst obliged entities to ensure the consistency and effectiveness of preventive measures. Payment service providers (PSPs) authorised by the CNMV generally operate exclusively with fiat currency, using bank transfers or payment service providers. However, although there is no evidence to suggest otherwise, it is possible that there are foreign CPs operating with CASPS.
Level of the entity's location, including the geographical scope of the sector's operations	CPs are cross-border in nature, which makes their supervision difficult. Furthermore, clients or promoters may be located anywhere in the world, including high-risk countries.
Nature of the products and services provided by the sector	
Level derived from the complexity of the products, due to their impact on anonymity or reduced	The existence of structured products, digital intermediation and transactions involving multiple parties makes it difficult, in certain cases, to correctly identify the investor, understand the origin of the funds and ensure the full traceability of the transactions.

information on the clients.	It may be the case that funds are raised for a project for which remain in the investor's account until the project is formally approved.
The extent to which specific products and services offered are linked in communications through references and/or national ML or TF	There is evidence of foreign CPs organisations, which have been reported for fraud, that have made offers regarding the possibility of investing in the cultivation of cannabis plants.
Nature of the customer	
Level derived from the nature of the business relationship with customers, based on the duration (ongoing, transactional or occasional) and frequency of transactions	Typically, the business relationship is occasional, limited to the financing of a single project. However, there is nothing to prevent the same project promoter from submitting several projects to a platform.
Level derived from the of the client	Any type of client may initially participate in this type of funding, and contributions of varying amounts may be made
Level based on the client's occupation or type of business	Developers may operate in a wide variety of economic sectors, including innovative, emerging or newly established activities with little operational track record. Investors follow a similar pattern, with a wide range of profiles: employees, the self-employed, entrepreneurs, investment companies, etc.
Geographical scope of the sector's activities	
A level derived from specific jurisdictions/countries of interest, often linked to the sector.	CPs are cross-border in nature, which makes them difficult to supervise. Furthermore, clients or promoters may be located anywhere in the world. There is no data on the jurisdictions with which transactions occur most frequently.
Level derived from the nature of interactions or transactions involving countries identified by the FATF.	The lack of information on the beneficial owner and the origin of the funds allows international transactions to be carried out to or from countries at risk of ML/TF or by persons from those countries, which gives rise to a risk of possible links to ML/TF activities.
Level derived from the nature of the interactions or transactions involving countries subject to international financial sanctions.	The lack of information on the owner and origin of the funds enables international transactions to be carried out to or from countries at risk of ML/TF or by persons from those countries, which gives rise to a risk of possible links to ML/TF activities.
Nature of the distribution channels	
Level derived from the complexity of the channels due to their impact	The intensive use of online channels reduces direct interaction with customers, which may hinder proper identification, verification and understanding of the user's actual profile.

who remain anonymous or for whom limited information available on customers.	
A level arising from the use of new technologies or payment methods.	FPFs authorised by the CNMV generally operate exclusively with fiat currency, using bank transfers or payment service providers. However, although there is no evidence, it is possible that there are foreign CPs that operate with CASPS.

Conclusion on the sector's inherent risk: high for ML and TF

654. As highlighted by the EU's SNRA, the use of participatory financing platforms for crowdfunding and crowdlending activities may be considered high-risk activities in terms of both ML and TF. However, due to their financial nature, participatory financing platforms carry a higher risk of being used for ML purposes than for TF operations, given the very nature of the lending and investment activities they facilitate. It is therefore a sector with a high inherent risk of being used for ML and TF operations for the following reasons: (i) it is possible to use illicit funds to give them the appearance of investments or loans directed at third-party recipients who, in turn, may also present fictitious projects; and (ii) CPs may be used by criminal organisations, either through projects submitted by criminal organisations for funding via investment funds or loans of illicit origin from the organisation itself, or simply through the financing of projects submitted by third parties that may be funded with illicit funds.

Risk factors relating to the effective implementation (or lack thereof) of controls

655. An analysis of residual risk requires an assessment of how existing controls are implemented within the sector and to what extent those controls are effective. The following section presents an analysis of the factors used to determine the residual risk in the CPs sector.

Risk factors relating to the effective implementation (or lack thereof) of controls	
Level of regulation in the sector	Since 2015, the CPs sector has been subject to detailed regulation. Since 10 November 2023, the Regulation on European Crowdfunding Service Providers (ECSP) has harmonised the regulatory approach to investment and business lending crowdfunding platforms across the European Union. It requires all payments to be made through an authorised payment service provider (PSP) and introduces other safeguards to mitigate these risks, such as due diligence by platforms regarding project promoters and authorisation procedures.
Extent to which unauthorised entities may be operating.	System of prior authorisation and supervision by the CNMV, in accordance with Regulation (EU) 2020/1503 of the European Parliament and of the Council and its transposition into national law through Law 5/2015 of 27 April, on the promotion of business financing, as amended by Law 18/2022 of 28 September. This regulatory framework significantly reduces the presence of unauthorised operators.

	However, there are limited cases ('non-harmonised' CPs) that fall outside the scope of Regulation (EU) 2020/1503 and are governed by national legislation (Law 5/2015 of 27 April). In these specific cases, an authorisation as a harmonised PSFP may not be required, provided that the legal conditions are strictly met.
Level of potential direct or indirect control over the entity or its management by money-laundering networks	One of the risks facing the sector is precisely the intrinsic risk posed by these entities, as their creation and/or control by criminal organisations enables illicit funds to be raised through legitimate loans or investments for the purposes of ML and TF, circumventing the relevant administrative controls and concealing the ownership and origin of the funds. Whilst the requirements set out in the sectoral regulations act as a to mitigate this risk.
Level of regulation of AML/TF prevention measures	Entities in the sector are not currently regulated entities for the purposes of ML/TF prevention. However, they will become so from July 2027.
Level of supervision	The sector is not subject to ML and TF inspections.
Level of sanctions imposed on entities in the sector.	As the sector is not subject to inspection, there are consequently no penalty.
Level of professionalism among the organisation's directors and senior managers.	Awareness and commitment amongst the directors and senior managers of these organisations are currently low, as they are not subject to ML and TF obligations. Furthermore, one of the factors that may make this sector attractive is precisely this lack of oversight in this area.
Level of awareness and understanding of their obligations regarding ML/TF.	The fact that they are not designated as regulated entities for the prevention of ML and TF means that awareness amongst organisations in the sector is currently low.
The organisation's level of commitment to policies and measures for the prevention of ML/TF.	Commitment amongst organisations in the sector is currently low, as they are not subject to ML/TF obligations
Level of professional qualifications of staff and their training in ML/TF.	There is no legal obligation to promote employees' knowledge of ML/TF within organisations.
Level of internal monitoring by organisations of employees' compliance.	There are no legal obligations in this regard.
Level of compliance with obligations regarding preventive measures, in particular CDD/KYC	There are no legal obligations in this regard.
Level of identification and reporting of suspicious transactions reports	There are no legal obligations in this regard.

Conclusion on the sector's residual risk: substantial for ML and moderate for TF

656. With regard to ML risk, when assessing the current risk posed by CPs – whether for crowdfunding, crowdlending or equity crowdfunding – in relation to their use for ML activities, the following must be taken into account: (i) the current regulation is confined to the prudential sphere (definition of CPs, conditions for their establishment, registration and operating regime); (ii) they are not subject to any obligations regarding the prevention of ML and TF, nor are they subject to supervision in this regard; and (iii) there are inherent risks that the services provided by CPs may be used for unlawful purposes. These circumstances are offset by the fact that the number of entities, the volume of funds raised, and the activities carried out by these entities are currently of very little significance, although they are growing. For all these reasons, it is considered that, at present, the residual risk of them being used for ML activities is **substantial**.

657. With regard to TF, given that the very nature of CPs operations relates to financial activities involving loans and investments that require an outlay in order to subsequently generate a return, the risks associated with TF are considered to be lower than those of ML. Crowdfunding systems linked to participatory financing procedures would be more susceptible to TF activities involving small sums. Consequently, there is a risk of use for TF purposes that should be regarded as **moderate**.

658. It is therefore considered that regulation of the sector—both in terms of the conduct of business and the prevention of ML and TF—is of great importance. In this regard, it should be emphasised that there is a lack of regulation concerning the prevention of ML and TF in this sector at a global level, meaning that entities may operate with the same degree of lack of control and supervision as in other countries. In other words, the lack of regulation and supervision in this area is a global vulnerability that can be exploited by criminal organisations. In Spain, although there was a draft bill proposing to include CPs as regulated entities, it was not passed. However, with the implementation of the AML Regulation from June 2027, CPs will become regulated entities.

Sector: Multiple IBANs 2026

Activity and context

659. There are currently nine institutions, and the Banco de España is the authority responsible for their authorisation/registration and the relevant requirements. The types of institutions providing the service and their characteristics are credit institutions.

660. The sector is characterised by a high degree of operational concentration, given that 97 main accounts account for the entirety of reported transactions, for which 2.7 million multiple IBANs have been issued. This issuance is concentrated almost entirely in 18 main accounts, belonging mainly to large non-financial corporations, together with some regulated entities (two securities firms, a branch of a foreign credit institution and two payment service providers). Of these 18 accounts, 3 hold almost half of the multiple IBANs issued.

Threats

661. The sector associated with the issuance and use of multiple IBANs presents a set of specific threats in relation to money laundering (ML) and terrorist financing (TF), arising primarily from the nature of the product, its distribution structure, and the potential disconnect between the issuing institution, the formal holder of the main account and the end user of the multiple IBAN.

662. These threats are not linked to large-scale operations that differ from those of the traditional banking system, but rather to specific usage scenarios in which there is a loss of visibility, particularly when third-party regulated entities or jurisdictions other than that of the issuing institution are involved.

Terrorist financing

663. Although the sector is not the main channel for TF, a risk is recognised, linked to:

- rapid transfers of moderate amounts,
- the use of non-face-to-face accounts,
- spreading funds across multiple IBANs,
- links to foreign entities or conflict zones.

664. These patterns are consistent with current models of low-value, highly fragmented TF, although their prevalence is lower than that observed in other sectors.

665. Factors have been identified that may be exploited by threats in the multiple IBAN sector:

Factors that may be exploited by threats	
Lack of visibility regarding the end user of the multiple IBAN	The sector's greatest exposure to threat is the issuing institution's potential lack of knowledge regarding the end user of multiple IBANs, when: • the multiple IBAN is assigned by a third party other than issuing bank,

	• the holder of the main account is not the same as the end user, • there are no effective information-sharing agreements in place. This situation may prevent the issuing institution from properly applying due diligence measures in relation to the end user, making it difficult to identify the beneficial owner of the funds and creating a potential risk of functional anonymity, despite the fact that it is formally a banking product.
No distinction between multiple IBANs and third parties	Multiple IBANs are, to third parties, indistinguishable from a traditional IBAN, which constitutes a significant exposure risk, as: • it makes it difficult for other financial institutions to identify that this is a virtual number, • it may lead to the mistaken belief that a separate bank account exists, • it may facilitate the use of the multiple IBAN as a means of dispersing or fragmenting cash flows. This feature, whilst providing operational efficiency, introduces a structural threat in terms of the traceability and transparency of the origin and destination of funds.
High operational concentration and structural complexity	The extraordinary concentration of multiple IBANs in a very small number of main accounts poses an additional threat, as it amplifies the potential impact of any operational shortcomings. In particular: • a limited number of accounts hold millions of multiple IBANs, • a single account may hold several hundred thousand IBANs, • The scale makes it difficult for the issuing entity to carry out detailed monitoring. This concentration increases the risk of operational opacity and reduces the ability to detect anomalous patterns at an early stage when there are no specific control mechanisms tailored to the product.
Use of multiple IBANs by other regulated entities without specific agreements	Where multiple IBANs are issued in connection with accounts held by another regulated entity (for example, securities firms or payment service providers), and there are no formal agreements in place to ensure the transmission of information on end customers, this could lead to: fragmentation of know-your-customer (KYC) procedures, overlapping or gaps in preventive responsibilities, and the issuing institution's inability to adequately assess ML/TF risk. This scenario is identified as one of the situations presenting the greatest theoretical exposure to the threat within the sector.
Geographical misalignment	There is a significant exposure risk associated with the possibility of issuing multiple Spanish IBANs linked to main accounts held abroad, which may result in: a lack of knowledge regarding the effective jurisdiction from which the customer operates, and difficulties in the consistent application of due diligence measures, and

	challenges in cross-border cooperation and the exchange of information. This territorial misalignment introduces additional exposure, particularly when jurisdictions with different AML/CFT frameworks are involved.
Potential misuse for activities requiring authorisation	In the absence of specific regulation of the product, there is a residual risk that multiple IBANs may be used, directly or indirectly, to facilitate regulated activities without the necessary authorisation, where: • the issuing institution is unaware of the end use of the IBAN, • the holder of the main account provides financial services to third parties, • there is no visibility regarding the actual economic activity being carried out. Although this scenario is not considered to be widespread, it constitutes a threat that must be addressed from a preventative perspective. These threats are consistent with the typologies identified in the ANR2026, as well as with European analyses of innovative payment services, which highlight the risk of fragmentation of payment flows, dilution of accountability and exploitative use by illicit networks.
Use of multiple IBANs as bridge accounts for Money Laundering	The main threat to the sector is the use of multiple IBANs as intermediary accounts to: • receiving funds of illicit origin from bank accounts, payment platforms or digital wallets, • splitting amounts into multiple low- or medium-value transfers, • redirect funds to other accounts, fintech platforms, crypto-assets or indirect withdrawals, • make it difficult to fully reconstruct the financial trail. This use as a layering mechanism makes multiple IBANs an attractive tool for criminal networks seeking speed, flexibility and low operating costs, particularly when multiple jurisdictions are involved.
Fraud, scams and the use of digital 'mule accounts'	Multiple IBANs feature repeatedly in fraud schemes, in particular: • investment fraud, • online scams and commercial fraud, • phishing and *business email compromise* schemes, • fundraising through the deception of individual victims. In these scenarios, multiple IBANs are used as temporary receiving accounts, often opened in the names of front men, newly established companies or vulnerable individuals, before the funds are rapidly transferred to other channels. The digital nature of these operations and the ability to operate without in-person interaction exacerbate this threat.

Misuse in cross-border transactions	The sector is highly exposed to cross-border operations, given that many providers operate under the freedom to provide services, clients may be non-residents, and funds may move between multiple countries within very short timeframes. This is particularly evident when multiple IBANs are used to channel funds between jurisdictions with differing AML/CFT standards, increasing the risk of regulatory arbitrage and hindering effective cooperation between authorities
Dilution of customer and beneficial owner due diligence	In certain business models – particularly embedded IBANs, nested accounts or BaaS (Banking as a Service) solutions – there are factors that expose the system to risk because they allow for: incomplete identification of the end customer; excessive reliance on third parties for KYC; difficulty in identifying the beneficial owner of the funds; and a lack of visibility regarding the actual use of the account. This dilution may facilitate the use of multiple IBANs by front companies, shell companies or customers with little actual economic activity.
Intensive use of microtransactions and splitting of payments	Another significant factor contributing to exposure to this threat is the systematic use of microtransactions, characterised by: multiple small-value deposits and payments; splitting transactions to avoid automated detection; high turnover of balances without significant accumulation; and apparent simulated commercial activity. This pattern, which is common in modern ML fraud and schemes, makes it difficult to identify suspicious transactions when sufficiently sophisticated monitoring systems are in place.
Integration with other high-risk sectors	Multiple IBANs are increasingly integrated with fintech platforms, payment service providers, marketplaces and digital platforms, crypto-assets and exchanges, or money transfer services. This interconnection creates an additional factor of exposure to the threat, as it facilitates rapid movements between sectors with different levels of control and maturity in AML/CFT, thereby increasing the complexity of comprehensive risk monitoring.

Risk factors by inherent vulnerability

666. The following section sets out the factors relating to inherent vulnerability analysed to determine the inherent risk of the multiple IBAN sector.

Characteristics of the sector	
Size of the sector and turnover	The sector is currently concentrated amongst nine credit institutions, including major banks as well as branches of foreign institutions. Turnover is currently low. However, several SSOOs have consulted SEPBLAC on how to implement this operation, and we believe this is a type of product that is expanding and will grow significantly in the near future.
Level of complexity of the sector's structure	Although only 97 main accounts with associated multiple IBANs have been reported, the total number of multiple IBANs issued and declared stands at 2,779,765; this implies an average of 28,657.4 Multiple IBANs per main IBAN. However, the issuance of these multiple IBANs is concentrated in 18 accounts, which account for

	2,765,723 multiple IBANs, accounting for 99.5 % of the total. It should be noted that six accounts have more than 200,000 multiple IBANs per account, with three of them having 817,871; 500,000 and 300,000 multiple IBANs respectively.
Level of integration with other regulated sectors	There is potential for the use of multiple IBANs by regulated entities that are not authorised to take deposits. Among the holders of the 18 main accounts are two securities firms, a branch of a foreign credit institution and two payment service providers. As already mentioned, the possible discrepancy between the formal holder of the main IBAN and the end user may create a lack of transparency regarding the applicable responsibilities and controls. However, based on the information reported, in no case does the ultimate user differ from the main account holder, which suggests that, even if the account holder were a regulated entity, multiple IBANs would be used primarily for the reconciliation of receipts and payments. Their use by regulated entities as a channel for deposits appears to be minimal, given that the majority of corporate clients in the sector are large non-financial corporations.
Level of the institution's location, including the geographical scope of the sector's operations	Possibility of a discrepancy between the jurisdiction of the institution issuing the multiple IBAN and that of the associated main account
The nature of the products and services provided by the sector	
Level derived from the complexity of the products, given their impact on anonymity or on the reduced information available about customers.	Lack of visibility regarding the end user of the multiple IBAN, as well as the jurisdiction of the main account to which it is linked, if this is not in Spain
The extent to which specific products and services offered are linked to communications in connection with intelligence and/or investigations national ML or TF	Not available
Nature of the customer	
Level derived from the nature of the business relationship with customers, based on duration (ongoing, transactional or occasional) and frequency of transactions	When the account holder is a large company, business relationships between the company and the organisation tend to be long-term, which helps the organisation to get to know the company better.
Level derived from the customer's status of the client	As they are mostly used by large companies, the information available on them is extensive.

Level derived from the client's occupation or type of business	Except in cases where multiple IBANs are issued for an account held by another regulated entity, the occupation of the clients does not represent a risk factor, insofar as they are large non-financial companies
Geographical scope of the sector's activities	
Level derived from specific jurisdictions/countries of interest frequently associated with the sector.	It is possible to issue multiple Spanish IBANs for main accounts located in foreign jurisdictions. There is a territorial mismatch which makes identification difficult, particularly when the Spanish institution is unaware of the ultimate jurisdiction of the party operating through its customer; this is compounded by the fact that the jurisdiction of the main account may not be located in Spain, thereby increasing the level of exposure in cross-border scenarios.
Level derived from the nature of interactions or transactions involving countries identified by the FATF.	Not available
Level derived from the nature of interactions or transactions involving countries subject to international financial sanctions.	Not available
Nature of the distribution channels	
Level derived from the complexity of the channels due to their impact on anonymity or on the limited information available about customers.	In the case of multiple IBANs issued to an account held by another obliged entity that allocates them to its customers, the absence of agreements enabling the issuing institution to identify the end user substantially increases the risk.
Level derived from the use of new technologies or payment methods.	Not available

Conclusion on the sector's inherent risk: substantial in ML and TF

667. The analysis of the sector's inherent risk associated with the issuance and use of multiple IBANs reveals a significant level of exposure, stemming both from the product's intrinsic characteristics and from the operational and geographical structure within which it operates. The sector is of considerable size, concentrated amongst nine credit institutions — including major national banks as well as branches of foreign institutions — which creates a broad and diversified operational environment.

668. The analysis shows that the inherent risk in the sector is high; however, given the current low volume, we can classify it as **substantial**, driven primarily by the product's lack of structural transparency, potential opacity regarding the end user, the extraordinary concentration of multiple

IBANs in a small number of accounts, and the complexity arising from its geographical scope. Whilst certain factors linked to the customer profile and the duration of the business relationship help to mitigate exposure, these elements do not fully offset the vulnerabilities arising from the design, distribution and operation of multiple IBANs.

Risk factors relating to the effective implementation (or lack thereof) of controls

669. Analysing residual risk requires an assessment of how existing controls are implemented within the sector and to what extent these controls are effective. The following section presents an analysis of the factors used to determine the residual risk in the multiple IBAN sector.

Risk factors relating to the effective implementation (or lack thereof) of controls	
Level of regulation in the sector	The product is marketed in a regulated sector, although there are no specific measures relating to the marketing of these products.
Potential presence of entities not authorised to operate.	In the absence of controls on the IBAN holder, an IBAN with multiple associated IBANs could be marketed to someone carrying out regulated activities without authorisation. In scenarios where the issuing institution lacks visibility over the end customer of the main IBAN —particularly where third-party regulated entities are involved without the necessary information-sharing agreements— there is a possibility that multiple IBANs may be associated with activities requiring authorisation but which do not hold such authorisation. This lack of effective control over the end user increases vulnerability to misuse of the product.
Level of potential direct or indirect control over the institution or its management by money-laundering networks	This is not a product that allows for control over the institution.
Level of regulation of preventive measures against ML/TF	The product is marketed in a regulated sector, although there are no specific measures relating to the marketing of these products.
Level of supervision	Specific reporting obligations regarding the products have been introduced, and inspections have begun at institutions with the highest number of multiple IBANs. Furthermore, the introduction of specific reporting obligations relating to the use of multiple IBANs provides an additional mechanism for control and visibility on the part of the competent authorities.
Level of sanctions imposed on entities in the sector.	The regulations do not provide for penalties for failing to report the use of multiple IBANs.
Level of professionalism of the organisation's administrators and senior management.	Most institutions marketing the product are well-regarded and operate within the traditional banking sector.

Level of awareness and understanding of their ML and TF obligations.	Existence of supervisory dialogue to ensure institutions are aware of the risks associated with the product.
The institution's level of commitment to anti-money laundering and counter-terrorist financing policies and measures ML/TF.	The types of institutions providing the service and their characteristics are credit institutions. The sector's commitment, as analysed in its sector profile, is high.
Level of professional qualifications of staff and their training in ML/TF.	Institutional integrity and internal governance are reinforced by the fact that most of the organisations that market multiple IBANs belong to the traditional banking sector and have directors and senior managers with high levels of professionalism.
Level of internal monitoring by institutions of compliance by employees.	The types of institutions providing the service and their characteristics are credit institutions. The same assessment given to this factor in the sector-specific fact sheet is included.
Level of compliance with obligations regarding preventive measures, in particular CDD/KYC.	The types of institutions providing the service and their characteristics are credit institutions. The same assessment given to this factor in the sector-specific fact sheet is included.
Level of identification and reporting of suspicious transaction reports	The credit institutions sector is by far the one that has consistently submitted the highest number of suspicious activity reports to SEBPLAC. For example, of the total of 21,667 suspicious activity reports received by SEBPLAC in 2025, more than 55 % were from credit institutions (12,105 reports). The sector's assessment of the quality of communications has been positive over the period analysed, given the sector's high level of prevention awareness. In 2025, the sector's average rating stood at 9.49, representing an increase of more than 1 point compared with 2025.

Conclusion on the sector's residual risk: medium for ML and TF

670. An analysis of the risk factors associated with the implementation of controls in the sector reveals a predominantly **medium** level of residual risk, influenced by the existence of a sufficiently robust general regulatory framework which, however, does not incorporate specific due diligence measures tailored to the particular characteristics of the multiple IBAN product. This mismatch between sector-specific regulation and product-specific risks constitutes one of the main sources of vulnerability in this category. Although this area is regulated under the general anti-money laundering (AML) and counter-terrorist financing (TF) framework, there are no specific provisions governing the marketing of multiple IBANs, creating an operational gap that may limit the effectiveness of controls. This same assessment applies to the specific regulation of AML/TF prevention measures, where, once again, the absence of detailed requirements for this product prevents an adequate level of risk mitigation from being guaranteed.

671. Overall, although the sector demonstrates institutional strengths and a sound general regulatory environment, the absence of specific measures tailored to the product and limited visibility regarding certain operational aspects introduce a significant structural vulnerability.

8. CONCLUSIONS

672. The analysis highlights that **ML threats** in Spain are persistent, increasingly complex and constantly evolving, centring on organised crime, drug trafficking and economic crimes such as fraud and VAT schemes, whilst also noting the sharp rise in investigations into corruption offences. These activities generate large volumes of illicit funds and are becoming increasingly professionalised, with models such as 'crime-as-a-service' and the interconnection between different types of crime being particularly notable. Furthermore, these threats have become globalised and increasingly technologically sophisticated, with intensive use of crypto-assets, artificial intelligence and informal money transfer systems, which increases their opacity and makes them harder to detect, particularly in the context of transnational operations and complex corporate structures.

673. **TF threats** in Spain are characterised by the predominance of jihadist terrorism (particularly Daesh) and a growing use of the digital environment for recruitment, radicalisation and financing. These operations typically involve small amounts of money, combining traditional methods such as cash or *hawala* with modern tools such as *crowdfunding*, crypto-assets or fundraising through video games. Furthermore, there is a clear link to organised crime and the use of seemingly legitimate structures, which, together with its international and technological dimensions, constitutes a constant and difficult-to-detect threat.

674. **Vulnerabilities** stem from a combination of structural, geographical, technological and social factors that facilitate the concealment and movement of illicit funds. Notable factors include the widespread use of cash and the informal economy, growing exposure to digital environments and crypto-assets characterised by a high degree of opacity, and the existence of sectors and activities with a greater capacity to channel funds in complex ways (such as the financial, property and professional services sectors). Added to this are risks associated with globalisation, links to high-risk jurisdictions and the geostrategic position of certain areas, as well as demographic dynamics that can be exploited by criminal networks. Taken together, these vulnerabilities create an environment conducive to illicit activity, making it more difficult to monitor, trace and effectively control financial flows.

675. The **analysis of inherent risk** shows that it is predominantly concentrated within the financial system, specifically in credit institutions, electronic money, payment services, currency exchange and crypto-assets. Similarly, crowdfunding platforms, the property sector, high-value assets, online gambling and land-based betting (other than lotteries and bets organised by SELAE), and corporate and legal services are sectors with high levels of risk in Spain. These sectors present high or substantial levels of risk, due to factors such as the size of the sector, the volume of customers, international operations, the speed of transactions, and the possibility of failing to identify beneficial ownership, particularly in the case of operations with complex structures that allow for operational traceability. Conversely, other sectors show medium or low levels of risk, generally associated with a lower volume of transactions or greater structural control.

676. The adjustment factors show that the **level of residual risk** in the various sectors depends to a large extent on the effectiveness of the preventive, regulatory and supervisory controls in place. In general, the most heavily regulated sectors, such as banking, exhibit relatively low levels of

regulatory and compliance risk, whilst other areas with a higher degree of digitalisation or lower supervisory maturity (such as crypto-assets, certain payment services or non-financial sectors) exhibit greater weaknesses in control, supervision and regulatory compliance. Furthermore, factors such as the possible presence of unauthorised operators, the extent to which institutions are committed to prevention policies, staff training and the ability to identify and report suspicious transactions have a significant influence on risk. In short, these moderating factors indicate that risk increases when there are shortcomings in the effective application of controls, reduced supervision or limitations in training and compliance culture.

677. The residual risk analysis shows that, despite the existence of preventive measures, certain sectors remain highly or significantly exposed to ML and, to a lesser extent, to TF, due to their own operational characteristics. In particular, within the financial sector, electronic money institutions, money transfer services and crypto-assets stand out, alongside non-financial sectors such as property, the legal profession, online gambling and land-based betting (other than lotteries and bets organised by SELAE). Although in some cases, such as credit institutions, the risk is mitigated by more robust controls, overall a significant level of exposure persists, mainly due to the varying application of mitigating factors across the sector.

678. Sectors with low residual risk include mutual guarantee societies, postal money orders, tangible assets, cash-in-transit services, the professional trade in other high-value goods, and emission rights – either due to the high level of regulation to which the sector is subject, the sector's small size and/or limited activity, or the extensive implementation of preventive measures.

679. Based on this sectoral risk analysis, the mitigating measures designed to address these risks are integrated in a coordinated manner into the National Strategy to Combat Money Laundering, as well as into the forthcoming update of the 2020 National Strategic Plan against Terrorist Financing (PENCFIT), in line with the National Counter-Terrorism Strategy (ENCOT), updated in 2023. This establishes a comprehensive framework for action that enables the strengthening of prevention, detection and investigation in the areas of greatest risk exposure.

ANNEX 1. Bibliography

a) The National Risk Analysis for Spain published in 2020.
b) The Addendum to the 2024 Sectoral Risk Analysis.
c) The 2023 Sectoral Risk Analysis of Crypto-assets and Crypto-asset Service Providers.
d) The 2022 National Security Strategy, coordinated by the Department of National Security and issued by the Prime Minister's Office.
e) The National Strategy against Organised Crime and Serious Crime and the National Strategy against Terrorism, coordinated by the Centre for Intelligence against Terrorism and Organised Crime (CITCO).
f) The various existing sectoral risk analyses, which were assessed by the FATF in 2014, and the follow-up reports from 2017 and 2019.
g) Annual Report of the Confiscated Assets Fund 2024.
h) The Supra-national Risk Analysis prepared by the European Union (hereinafter the EU SNRA).
i) The annual reports of public institutions involved in the fight against ML and TF.
j) The Annual Reports of the National Security Council, submitted annually to the Joint Congress-Senate Committee.
k) Statistics published in these areas, including those relating to prevention, supervision, police investigations and judicial proceedings.
l) Consultations carried out with the various competent authorities in each area of activity and documents drawn up by them, some of which are classified.
m) Contributions from representatives of regulated entities and the private sector.

ANNEX 2. Collaborating public institutions and private-sector entities

The public institutions involved in the preparation of the NRA are:

- State Tax Administration Agency (AEAT).
- Banco de España.
- National Intelligence Centre.
- Centre for Intelligence against Terrorism and Organised Crime (CITCO).
- General Commissariat of the Judicial Police of the National Police.
- General Directorate of Information of the National Police.
- General Directorate of Information of the COS of the Mossos d'Esquadra.
- General Directorate of Criminal Investigation of the Mossos d'Esquadra
- National Securities Market Commission (CNMV).
- General Council of the Judiciary.
- Government Delegation for the National Drugs Plan.
- Department of National Security.
- Directorate-General for the Regulation of Gambling.
- Directorate-General for Foreign Policy and Security.
- Directorate-General for the Policía Nacional (Government of Catalonia)
- Directorate-General for Legal Security and Public Trust.
- Directorate-General for Insurance and Pension Funds.
- Prosecutor General's Office.
- Special Anti-Drugs Prosecutor's Office.
- Public Prosecutor's Office of the Audiencia Nacional.
- Special Public Prosecutor's Office for Combating Corruption and Organised Crime.
- Guardia Civil Information Directorate (JI).
- Office for Asset Management and Recovery.
- Spanish Office for Climate Change.
- Navarre Regional Police.
- Economic Crimes Section of the Central Criminal Investigation and Police Nacional Section of the Ertzaintza
- Secretariat of State for Security.
- General Secretariat for the Treasury and International Finance.
- Executive Service for the Prevention of Money Laundering (SEPBLAC).
- Criminal Intelligence Unit of the Judicial Police of the Guardia Civil (UTPJ).

The private-sector organisations involved in drawing up the NRA are:

- Aliseda Servicios de Gestión Inmobiliaria, S.L.U.
- Spanish Banking Association
- Spanish Association of Payment Institutions (AENPA)
- Spanish Fintech Association (AEFI)
- National Association of Credit Institutions (ASNEF)
- Madrid Association of Property Developers
- BCC-Cajamar Group
- Banco Bilbao Vizcaya Argentaria (BBVA)
- Banco Santander

- Binance Spain S.L.
- Caixabank
- Cecabank
- Spanish Confederation of Savings Banks (CECA)
- Spanish Association of Registrars
- General Council of the Spanish Bar
- General Council of Notaries
- Deutsche Bank
- Inverco Association of Collective Investment Institutions and Pension Funds
- Prosegur Cash Services Spain S.L.U
- National Union of Credit Cooperatives (UNACC)

APPENDIX 3. List of tables, charts and graphs

Tables

Table 1. Reports of suspected offences, investigations, judgements and convictions relating to organised crime Table 2. Reports of suspected offences, investigations, judgements and convictions relating to drug trafficking Table 3. Quantities of drugs seized

Chart 4. Amounts of cash seized in euros

Table 5. Number of assets seized and values of assets sold at auction Table 6.

Identification of groups involved in drug trafficking

Table 7. Reports based on evidence and investigations relating to fraud offences Table 8.

Reports based on evidence and investigations relating to tax fraud Table 9. Reports

based on evidence and investigations relating to corruption offences

Table 10. Number of formal or informal requests for international cooperation by category of offence. Estimated volume of funds involved (ORA CITCO).

Table 11. International cooperation under the O.R.A. by predicate offence. Requests received.

Table 12. International cooperation under the O.R.A. by predicate offence. Requests processed.

Table 13. International cooperation within the framework of ORGA.

Table 14. Trends in Money Laundering cases (2021–2025) handled by ORGA

Table 15. Reports based on evidence, investigations, arrests, judgements and convictions for TF offences

Table 16. Declarations and amounts declared (euros) for the period 2020–2025 at customs.

Table 17. Percentages of declarations and amounts from customs in the Gibraltar Area in relation to the total declared at Spanish customs.

Table 18. Crypto-asset returns to the AEAT Table 19.

CASPS returns to the AEAT

Tables

TABLE 1. Methods used by criminal organisations to channel funds TABLE 2. Types of

organised crime groups

TABLE 3. Types of criminal groups

TABLE 4. Methods used to channel funds derived from drug trafficking

TABLE 5. Methods used to channel funds derived from fraud TABLE 6. Types of organisations linked to fraud offences TABLE 7. Types of jurisdictions linked to fraud offences
TABLE 8. Methods used to channel illicit funds from corruption
TABLE 9. Types of assets used to channel funds derived from corruption
TABLE 10. Methods used to channel illicit funds derived from international crimes into Spain
TABLE 11. Methods used to channel illicit funds linked to TF

Charts

Chart 1. Counter-terrorism activity carried out by the LEAs in 2025

ANNEX 4. Acronyms

AEAT. Agencia Estatal de Administración Tributaria (State Tax Administration Agency).

AEB. Asociación de Banca Española (Spanish Banking Association).

AEF. Asociación Española de Fundaciones (Spanish Association of Foundations).

AECID. Agencia Española de Cooperación Internacional para el Desarrollo (Spanish Agency for International Development Cooperation).

AEJPR. Asociación Española de Joyeros, Plateros y Relojeros (Spanish Association of Jewellers, Silversmiths and Watchmakers).

AENPA. Asociación Española de Entidades de Pago (Spanish Association of Payment Institutions).

ASNEF. Asociación Nacional de Establecimientos Financieros de Crédito (National Association of Credit Institutions).

AML/CFT. Anti-Money Laundering and Countering the Financing of Terrorism.

BdE. Banco de España (Bank of Spain).

BD. Database

BNPL. Buy Now, Pay Later

CASP. Crypto-asset Service Providers.

CECA. Confederación Española de Cajas de Ahorros (Spanish Confederation of Savings Banks).

CECT. Comité Especializado contra la lucha del Terrorismo (Specialised Committee for the Fight against Terrorism).

CECII. Closed-End Collective Investment Institutions.

CENDOJ. Centro de Documentación Judicial (Judicial Documentation Center).

CGI. Comisaría General de Información. Policía Nacional (General Information Directorate. National Police).

CGPJ. Consejo General del Poder Judicial (General Council of the Judiciary).

CITCO. Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (Centre for Intelligence against Terrorism and Organised Crime).

CI. Credit Institutions.

CII. Collective Investment Institutions.

CNI. Centro Nacional de Inteligencia (National Intelligence Centre).

CNMV. Comisión Nacional del Mercado de Valores (National Securities Market Commission).

CP. Crowdfunding Platforms.

CRAB. Centro Registral Antiblanqueo (Anti-Money Laundering Registry Centre).

DGOJ. Dirección General de Ordenación del Juego (Directorate-General for the Regulation of Gambling).

DGSFP. Dirección General de Seguros y Fondos de Pensiones (Directorate-General for Insurance and Pension Funds).

EBA. European Banking Authority.

ECB. European Central Bank.

EDD. Enhanced Due Diligence

EMI. Electronic Money Institutions.

ENCOyDG. Estrategia Nacional contra el Crimen Organizado y Delincuencia Grave (National Strategy against Organised Crime and Serious Crime).

ENCOT. Estrategia Nacional Contra el Terrorismo (National Strategy Against Terrorism).

FAF. Financial Advisory Firms.

FCI. Financial Credit Institutions.

FGE. Fiscalía General del Estado (State Prosecutor General's Office).

FIU. Financial Intelligence Unit.

FTF. Fichero de Titularidades Financieras (Financial Ownership Register).

FATF. Financial Action Task Force.

GOIF. Grupo Operativo de Inteligencia Financiera (Financial Intelligence Task Force).

GRUSEFIT. Working Group III for the Monitoring of the National Strategic Plan to Combat Terrorist Financing.

ICAC. Instituto de Contabilidad y Auditoría de Cuentas (Institute of Accounting and Auditing).

INE Instituto Nacional de Estadística (National Statistics Institute)

ISF. Investment Services Firm.

JI. Jefatura de Información de la Guardia Civil (Information Directorate).

LEA Law Enforcement Agencies

LPS. Libertad de establecimiento y libre prestación de servicios (Freedom to provide services).

ML. Money laundering.

MGS. Mutual Guarantee Societies.

NRA. National Risk Assessment.

NGDOs. Non-Governmental Development Organisations.

NPOs. Non-Profit Organisations.

OCP. Órgano Centralizado de Prevención (Centralised Prevention Body).

ONCE. Organización Nacional de Ciegos Españoles (National Organisation of the Blind of Spain)

PF. Proliferation Financing.

PI. Payment Institutions.

PELCEIL – Strategic Plan to Combat the Illicit Enrichment of Criminal Organisations and Offenders.

PENCFIT. National Strategic Plan to Combat Terrorist Financing.

PENCRAV. National Strategic Plan to Prevent and Combat Violent Radicalisation.

PEP-PRP. Politically Exposed Persons.

RCTIR. Registro Central de Titularidades Reales (Central Register of Beneficial Ownership).

SAREB. Sociedad de Gestión de Activos Procedentes de la Reestructuración Bancaria (Asset Management Company for Assets Arising from Bank Restructuring).

SELAE Sociedad Estatal de Loterías y Apuestas del Estado (State Lottery and Betting Society)

SEPBLAC. Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (Executive Service for the Prevention of Money Laundering).

SEPI Sociedad Estatal de Participaciones Industriales (State-Owned Industrial Holdings Corporation)

SGEIC. Sociedades Gestoras de Entidades de Inversión de tipo Cerrado (Closed-End Investment Entity Management Company).

SGIIC. Sociedades Gestoras de Instituciones de Inversión Colectiva (Collective Investment Institutions Management Companies).

SICAV. Sociedades de Inversión Colectiva en Activos Variables (Undertakings for Collective Investment in Transferable Securities).

SNCE. Sistema Nacional de Compensación Electrónica (National Electronic Clearing System).

SNRA. (EU) Supra-National Risk Assessment.

SOCIMI. Sociedades Cotizadas de Inversión en el Mercado Inmobiliario (Listed Real Estate Investment Companies).

STR. Suspicious Transaction Report

SVA. Servicio de Vigilancia Aduanera (Customs Surveillance Service).

TF. Terrorist financing.

UCO. Unidad Central Operativa de la Guardia Civil (Central Operational Unit of the Civil Guard).

UDEF. Unidad Central de Delincuencia Económica y Fiscal. Policía Nacional (Central Unit for Economic and Fiscal Crime. National Police).

UNACC. Unión Nacional de Cooperativas de Crédito (National Union of Credit Cooperatives).

UNESPA. Unión Española de Entidades Aseguradoras y Reaseguradoras (Spanish Union of Insurance and Reinsurance Companies).

UNODC. United Nations Office on Drugs and Crime.

UNSCR. United Nations Security Council Resolutions.

UTPJ. Unidad Técnica de la Policía Judicial de la Guardia Civil (Criminal Intelligence Unit of the Guardia Civil).

VCF. Venture Capital Funds.