

NATIONAL RISK ASSESSMENT

ON MONEY LAUNDERING AND TERRORIST FINANCING - 2020

(PUBLIC VERSION)

CONTENTS

(I) INTRODUCTION TO THE NATIONAL RISK ASSESSMENT. 4
Presentation 4
Objectives 5
(II) METHODOLOGY. 6
Participating institutions 6
Identification of threats and vulnerabilities 7
(III) REGULATORY AND INSTITUTIONAL FRAMEWORK. 9
Regulatory framework: FATF, European Union and national regulations 9
Preventive framework: national coordination 9
National AML/CFT supervisory framework 11
Investigation and prosecution framework 12
(IV) MONEY LAUNDERING THREATS 14
Organised Crime 14
Drug trafficking 17
Economic crimes 18
Money laundering by third parties and for offences committed abroad. 19
(V) THREATS OF TERRORIST FINANCING. 20
Jihadist terrorism 20
ETA terrorism… 23
Other terrorist groups 24
(VI) VULNERABILITIES IN MONEY LAUNDERING AND TERRORIST FINANCING 25
Stemming from the population 25
Derived from geographical factors 27
Derived from the nature of the entity or activity carried out. 28
Issues arising from payment methods, the use of cash and the informal economy. 29
Arising from technological innovations in financial transactions 31
(VII) SECTOR-SPECIFIC RISKS: THE FINANCIAL SECTOR. 34
a) Financial services provided by credit institutions 36
Private banking operations 39
Corporate banking operations 40
Bank deposits 41
Institutional investment operations. 41
International fund transfers 42
Granting of loans 43
Cross-border correspondent banking 43
b) Loan services. Credit institutions and other persons and entities 44

c) Insurance and pension funds 47
d) Investment services, collective investment undertakings and management companies 50
e) Mutual guarantee societies. 53
f) Money transfers by payment institutions 54
g) Other services provided by payment institutions 57
h) Electronic money transactions. 59
i) Currency exchange activities 61
j) Crowdfunding platform activities. 62
(VIII) SECTOR-SPECIFIC RISKS: USE OF CASH AND VIRTUAL CURRENCIES. 65
a) Use of cash, cash flows and cash-intensive businesses 65
b) Activities involving virtual currencies or assets 68
(IX) SECTOR-SPECIFIC RISKS: NON-FINANCIAL ACTIVITIES AND PROFESSIONS. 72
a) Postal services 73
b) Credit intermediation activities 74
c) Real estate transactions. 75
d) Auditors, external accountants and tax advisers 79
e) Activities carried out by notaries 81
f) Activities carried out by land, commercial and movable property registrars 84
g) Certain specific activities carried out by solicitors and other professions 86
h) Provision of corporate services to third parties 89
i) Gaming sector. 92
j) Professional trade in jewellery, precious stones and metals 98
k) Buying and selling of art and antiques 101
l) Professional trade in other high-value goods. 103
m) Investment in tangible assets 105
n) Cash-in-transit services provided by private security firms 106
(X) RISKS BY TYPE OF COMPANY AND LEGAL INSTRUMENT: TRUSTS 108
a) Commercial Companies 110
b) Trusts and similar fiduciary structures 116
(XI) CHARITABLE ORGANISATIONS (OSFL). 122
a) Associations and public benefit associations 122
b) Foundations 123
c) “Third sector”: Non-Governmental Development Organisations (NGDOs). 125
d) Religious organisations 126
(XII) CONCLUSIONS 134
Abbreviations used 135
List of key regulatory provisions 137

(I) INTRODUCTION TO THE NATIONAL RISK ASSESSMENT.

Presentation of the National Risk Assessment.

The fight against money laundering and terrorist financing (hereinafter ML/TF) presents a constant challenge for institutions and authorities at both national and international level. The constant evolution of money laundering and terrorist financing techniques, which rely on exploiting vulnerabilities in national systems, requires continuous updating of the analyses and controls that enable authorities and regulated entities to identify changes in modus operandi, new patterns, ways in which technological advances are exploited, and developments in the types of jurisdictions that pose a risk in these areas.

As a result of these analyses, the authorities must adopt mitigating measures, update the regulatory framework, strengthen the resources deployed, and improve internal coordination and international cooperation, in both preventive and enforcement contexts.

Whilst it is true that the fight against money laundering and terrorist financing must be global, when establishing priorities for action and the corresponding mitigating measures at national level, each country must take into account its particular characteristics, which determine its exposure to the specific ML/TF risks that most significantly affect it.

The Financial Action Task Force (FATF), an intergovernmental body that adopts international standards applicable to money laundering, terrorist financing and proliferation, assigns a fundamental role to national risk assessments in the fight against both crimes, stating in its Recommendation 1 that countries have a duty to identify, assess and understand the ML/TF risks to which they are exposed and to coordinate actions at national level to address them.

In the same vein, Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (4th Directive) stipulates in Article 7 that Member States must:

- Make a summary of the national risk assessments available to the public.
- Make the results of their risk assessments available to the European Commission, supervisory authorities and other Member States.
- Prepare their national risk assessment taking into account the European Commission's Report on the Supranational Risk Assessment on Money Laundering and Terrorist Financing (SNRA[1]) affecting the market and relating to cross-border activity, published on 26 June 2017, the second version of which was published in July 2019.

To this end, this National Risk Assessment, approved by the Commission for the Prevention of Money Laundering and Monetary Offences (Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias) (hereinafter, COPBLAC), has taken into account the content and format of the European Union's Supranational Risk Assessment on Money Laundering and Terrorist Financing (SNRA), insofar as it facilitates the detection, understanding, management and mitigation of money laundering and terrorist financing risks in Europe and in Spain.

[1]https://eur-lex.europa.eu/resource.html?uri=cellar:d4d7d30e-5a5a-11e7-954d-01aa75ed71a1.0001.02/DOC_1&format=PDF.

Objectives of the National Risk Assessment.

In Spain, various analyses or risk assessments relating to ML/TF have been in place for some years, although these analyses are sector-specific or relate to specific activities or regional risks. This document aims to review and update the various existing risk assessments, with the participation of authorities and institutions involved in the fight against money laundering and terrorist financing, and, furthermore, to consolidate the conclusions of this study into a single document that can be disseminated[2].

Specifically, the National Risk Assessment aims to:

- Define the national framework for combating and preventing money laundering and terrorist financing in Spain (ML/TF) and its scope of action within the European and international context.
- To consolidate into a single document the analyses and conclusions of various existing documents on risks and threats in these areas, taking into account the framework of the National Security System.
- Review the threats to which Spain is exposed and their significance in determining the ML/TF risk.
- To identify the general vulnerabilities of the system and detail their evolution across different sectors.
- Identify the inherent risks associated with each sector or type of activity based on an analysis of their intrinsic characteristics, threats and vulnerabilities[3].
- Identify and assess residual risks once the measures adopted in the regulatory, preventive, supervisory and financial intelligence spheres have been implemented.
- Identify those sectors which, due to their exposure to risk, are considered priorities for the development of mitigation measures.
- Determine courses of action for mitigating the identified risks[4].

[2] The National Risk Assessment is confidential and restricted. This document is a summary version intended for public use.
[3] The public version of the National Risk Assessment does not include the risk sheets containing the individualised analysis of each activity and the risk assessments for each of the indicators.
[4] The public version of the National Risk Assessment does not include risk mitigation measures.

(II) METHODOLOGY OF THE NATIONAL RISK ASSESSMENT.

In preparing this document, in accordance with the FATF Guidance on the identification and assessment of money laundering and terrorist financing risks, and with Directive (EU) 2015/849, various national and international sources of information have been taken into account and consultations have been held with the competent public authorities in each area and with representatives of the private sector. Specifically, this document is based on:

a) The 2017 National Security Strategy, coordinated by the Department of National Security and issued by the Office of the Prime Minister.
b) 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, Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO).
c) The various existing sectoral risk analyses that were assessed by the FATF in 2014, as well as those that have subsequently been drawn up or updated.
d) The Supra-National Risk Assessment prepared by the European Union (hereinafter the EU SNRA).
e) The annual reports of public institutions involved in the fight against money laundering and terrorist financing.
f) The Annual Reports of the National Security Council, submitted annually to the Joint Congress-Senate Committee.
g) Statistics published in these areas, including those relating to prevention, supervision, police investigations and judicial proceedings.
h) Consultations carried out with the various competent authorities in each area of activity and documents produced by them, some of which are classified.
i) Contributions from representatives of regulated entities and the private sector.

Participating institutions.

The public bodies involved in compiling the NRA are:

- Spanish Tax Agency, Agencia Estatal de Administración Tributaria (AEAT)
- Bank of Spain, Banco de España
- National Intelligence Centre, Centro Nacional de Inteligencia (CNI)
- Centre for Intelligence against Terrorism and Organised Crime, Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO)
- General Commission of the Judicial Police of the National Police
- General Directorate of Information of the National Police
- National Securities Market Commission, Comisión Nacional del Mercado de Valores (CNMV)
- General Council of the Judiciary, Consejo General del Poder Judicial (CGPJ)
- Government Delegation for the National Plan on Drugs
- Department of National Security
- Directorate-General for Gaming Regulation
- Directorate-General for Foreign Policy and Security
- Directorate-General for Legal Security and Public Trust
- Directorate-General for Insurance and Pension Funds, Dirección General de Seguros y Fondos de Pensiones (DGSFP).
- Office of the Prosecutor General (Fiscalía General del Estado).
- Special Anti-Drug Prosecutor's Office.

- Prosecutor's Office of the Audiencia Nacional
- Special Prosecutor's Office for Corruption and Organised Crime
- Guardia Civil Intelligence Directorate (JI)
- Asset Management and Recovery Office
- Secretariat of State for Security
- General Secretariat of the Treasury and International Finance
- Executive Service for the Prevention of Money Laundering (Sepblac)
- Sub-Directorate General for the Supervision of Foundations
- Criminal Intelligence Unit of the Guardia Civil (UTPJ)

Identification of risks, threats and vulnerabilities.

The identification of money laundering and terrorist financing risks must combine an identification of (i) the threats existing in Spain, (ii) of the vulnerabilities in the system and the country's context that allow these threats to carry out their activities, and (iii) of 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 money laundering or terrorist financing activities by taking advantage of existing vulnerabilities.

According to the FATF, 'threats' are those individuals, groups of individuals or their activities that pose a potential danger due to their capacity to cause harm to the State, society, the economy or other fundamental elements of a country's life.

Given that threats have criminal and destabilising aims, their analysis in the context of AML/CFT must primarily take a law enforcement approach, through their assessment by the authorities responsible for investigating and prosecuting criminal activities, such as the police authorities (Guardia Civil, Policía Nacional), CITCO, CNI, the State Public Prosecutor's Office, judges and courts, or the AEAT in matters relating to customs and taxation.

For their part, **'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.

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

- Geographical factors.
- Demographic.
- Technological.
- As a result of the activities carried out, their regulation, and its prudential supervision and supervision regarding AML/CFT.
- Derived from the type of legal entity: size, business model, national/international presence, exposure to higher-risk customers, etc.
- Derived from means of payment, use of cash and the informal economy.

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

Each chapter therefore analyses the risks associated with specific activities, sectors and types of institutions, taking into account the identified threats, characteristics, context, turnover, main vulnerabilities and risk exposure of each. To this end, consideration will be given to their vulnerabilities arising from **endogenous and exogenous** risk factors, as well as their inherent risks and residual risks:

a) 'Endogenous' risks are those intrinsic risk factors arising from the nature and characteristics of the sector, which may allow 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.

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

<table>
<tr><th colspan="2">Risk factors</th></tr>
<tr><th>Endogenous</th><th>Exogenous</th></tr>
<tr><td>Establishment or control of an Entity for ML/TF purposes.</td><td rowspan="2">Associated with the misuse of services/channels/products by the clients/stakeholders in operations with AML/CFT.</td></tr>
<tr><td>Recruitment of dishonest employees.</td></tr>
</table>

The result is an assessment of the various types of risk affecting each sector of activity, taking into account the type of natural or legal persons operating in that sector, the products they market, the services they provide, the characteristics of their customers, and the countries in which they operate. In addition to the specific nature of their operations and services, factors such as information gathered from supervisory experience, knowledge of the activity through routine and ad hoc communications, and external expert reports, amongst other sources, are assessed.

Specifically, for each sector, type of institution or activity, the **inherent risk** of them being used for ML/TF purposes due to their vulnerabilities and specific characteristics is determined. This inherent risk is adjusted in line with the mitigating measures adopted at national level for that sector, taking into account factors such as its prudential regulation, level of supervision, criminal prosecution, the sector's understanding of risks, the extent to which AML/CFT prevention measures are implemented, and the quality of its internal control procedures.

These mitigation measures are what enable the **residual risk** of sectors, entities and activities being used for purposes related to money laundering and terrorist financing to be determined.

In accordance with the risk level classification established by the European Commission in the EU **Supranational Risk Assessment on Money Laundering and Terrorist Financing** (EU SNRA), the risk levels in this analysis may be classified as:

- Low
- Moderate
- Significant
- High

(III) REGULATORY AND INSTITUTIONAL FRAMEWORK.

Regulatory framework: FATF, European Union and national regulations.

The Financial Action Task Force (FATF) is the global supervisory body for money laundering and terrorist financing. It is the intergovernmental body that sets international standards and ensures the effective implementation of legal, regulatory and operational measures to combat money laundering and terrorist financing. The FATF Recommendations, updated on several occasions, have been the direct inspiration for the EU Directives and the main reason for amendments to national legislation.

Consequently, Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May on the prevention of the use of the financial system for the purposes of money laundering and terrorist financing incorporates the new provisions adopted by the FATF in 2012, establishing a general framework that must not only be transposed but also supplemented by the Member States.

This Directive was amended by Directive (EU) 2018/843 of 30 May, which strengthens the regulatory and institutional framework of preventive measures to be implemented and developed in Member States.

Spain's commitment to combating money laundering and terrorist financing has led to the successive adoption of various regulatory initiatives. In this regard, Law 10/2010 of 28 April on the prevention of money laundering and terrorist financing was amended in 2013 and 2018.

In addition, Royal Decree 304/2014 of 5 May, approving the Regulations of Law 10/2010 of 28 April, completes the risk-based approach of AML/CFT legislation in Spain, incorporating the main updates to the international standards adopted by the FATF in 2013.

Alongside these two pieces of legislation, which form the legal framework for AML/CFT prevention at national level, the main repressive regulation is set out in the Criminal Code, which underwent successive amendments in 2015 and 2019, both regarding the criminalisation of money laundering and that of terrorism and its financing.

In development or directly linked to the above regulations, there is a wide range of provisions applicable to AML/CFT matters, covering both preventive and repressive aspects, with varying legal standing, which are listed in the section entitled "List of main regulatory provisions".

Preventive framework: national coordination.

The COPBLAC is the body responsible for promoting, developing and coordinating national policies on the prevention of ML/TF and is involved in the imposition of sanctions for non-compliance with the ML/TF prevention obligations established in Law 10/2010. It comprises 26 members from the main national institutions involved in the fight against ML/TF.

CHAIR OF THE COPBLAC

State Secretary for the Economy and Business Support.

- MEMBERS
- Director-General of the Treasury and Financial Policy.
- Chief Public Prosecutor of the Audiencia Nacional
- Chief Prosecutor of the Anti-Drugs Prosecutor's Office.
- Chief Prosecutor of the Public Prosecutor's Office for Corruption and Organised Crime.
- Member of the CGPJ.
- Secretary General of the Banco de España.
- Director of Supervision at the Banco de España.
- Director-General of the Legal Service of the Comisión Nacional del Mercado de Valores.
- Director-General of Insurance and Pension Funds.
- Director-General of Trade and Investment.
- Director-General of Legal Security and Public Trust.
- Director-General of Foreign Policy and Multilateral, Global and Security Affairs.
- Director of the Spanish Data Protection Agency.
- Chief of Staff to the Secretary of State for Security.
- Commissioner General of the Judicial Police of the Policía Nacional.
- Chief of the Judicial Police of the Guardia Civil.
- Director of Intelligence at the Centro Nacional de Inteligencia (CNI).
- Director-General of Customs and Excise at the AEAT.
- Director of the Department of Financial and Tax Inspection at the AEAT.
- Director of the Basque Autonomous Police (Ertzaintza).
- Director of the Navarre Regional Police.
- Director-General of the Police of the Government of Catalonia – Mossos d'Esquadra.
- Director of the Commission's Executive Service (SEPBLAC).

SECRETARIAT OF THE COPBLAC

Deputy Director-General for Inspection and Control of Capital Movements. Directorate-General for the Treasury and Financial Policy.

The COPBLAC meets at least twice a year and acts in plenary session or through its subordinate committees: the Standing Committee and the Financial Intelligence Committee.



The Standing Committee is primarily responsible for coordinating supervisory activities. It receives and analyses inspection reports prepared by supervisors, which detail the level of compliance with AML/CFT regulations by regulated entities. It is responsible for initiating disciplinary proceedings for breaches in this area and issuing improvement notices to regulated entities.

The Financial Intelligence Committee is responsible for the more operational aspects and for analysing risks, trends and vulnerabilities. It is supported by a technical body, the Grupo Operativo de Inteligencia Financiera (GOIF), and by a working group specialising in risks and measures relating to cash movements and means of payment (Cash Group).

The COPBLAC and its subordinate committees are supported by the COPBLAC and the Commission's Executive Service, Sepblac.

The COPBLAC falls under the Sub-Directorate General for Inspection and Control of Capital Movements of the Directorate General of the Treasury and Financial Policy, which, amongst other functions, is responsible for investigating disciplinary proceedings for breaches of obligations relating to the prevention of ML/TF and formulating proposals for resolutions, as well as proposing, drafting and following up on improvement requirements communicated to regulated entities.

The Commission's Executive Service, Sepblac, is the **Financial Intelligence Unit** in Spain and the national supervisory authority for the prevention of ML/TF. It is responsible, amongst other functions, for receiving reports submitted by regulated entities, analysing the information received, assisting the judicial authorities, supervising regulated entities and issuing the reports required by law.

National AML/CFT supervisory framework.

At national level, Sepblac is responsible for supervising compliance with AML/CFT obligations by regulated entities. In the case of financial institutions, the prudential supervisors of financial institutions—**Banco de España, Comisión Nacional del Mercado de Valores (CNMV) and the Dirección General de Seguros y Fondos de Pensiones (DGSFP)**—also carry out supervisory and inspection functions in the area of AML/CFT, taking into account the cooperation agreements signed.

Supervisory action on AML/CFT prevention is carried out using a risk-based approach. Indeed, SEPBLAC's dual role as a financial intelligence unit and as a supervisory authority creates synergies between these two functions, with the body serving in both capacities as a key source of information used in assessing risks at national, sectoral and institutional levels.

The supervisory bodies examine the risks, policies, internal controls and procedures relating to AML/CFT within institutions. In the case of financial institutions, the guidelines approved by the European Authorities on risk-based supervision and the risk factors to be taken into account by obliged entities when applying due diligence measures are taken into consideration.

SEPBLAC, as the general supervisor, carries out risk assessments specific to each sector and each individual institution, and this information is used as the basis for preparing the Annual Inspection Plan. Risk assessments are updated at least once a year or as determined by financial intelligence information, in the event of a change of ownership, an increase in shareholding or any other relevant information.

Prudential supervisors also carry out risk-based AML/CFT supervision, whereby supervisory plans and resources are allocated to institutions according to their risk profile and supervisory priority.

Alongside this national framework, there is a European institutional framework for the supervision of financial institutions, amended through the so-called CRD-V package[5], aimed at reducing risks in the European financial system and improving cooperation between competent authorities in the prevention of ML/TF. In particular, it incorporates measures to promote cooperation and the exchange of information between prudential supervisors, competent authorities for AML/CFT and financial intelligence units (FIUs). Furthermore, in the supervisory review and evaluation process (known as the SREP), AML/CFT matters must be considered by supervisory bodies in their risk analyses of financial institutions, and the European Banking Authority (EBA) and the national competent authorities responsible for AML/CFT must be notified when weaknesses in this area are identified in the governance model, business activities or business model of institutions in the sector. Furthermore, within the framework of the EU Action Plan on AML/CFT, discussions are currently underway regarding the possible creation of a supervisor with centralised powers at EU level, coordinated with national AML/CFT supervisors.

Investigation and prosecution framework.

Spain has a comprehensive institutional framework for investigation and prosecution comprising: (i) the law enforcement agencies, which have the status of judicial police, and (ii) the prosecutors and judges entrusted with the responsibility of ensuring that ML/TF offences and their predicate offences are properly investigated.

The two main police forces, the Policía Nacional and the Guardia Civil, are responsible for combating all offences, including money laundering and terrorist financing, under the direction of the Secretary of State for Security (Ministry of Home Affairs). The Customs Surveillance Service, which reports to the Agencia Estatal de Administración Tributaria (AEAT), is also responsible for investigating and prosecuting tax offences, smuggling and associated money laundering, and forms part of the judicial police. Furthermore, Catalonia, the Basque Country and Navarre have their own police forces, which operate under the direction of the authorities of the respective Autonomous Communities.

All units and investigation teams within the judicial police are authorised to conduct parallel financial investigations in connection with their criminal investigations, under the supervision of the judicial authorities and the Public Prosecutor. They may also refer cases to other authorities for further investigation, where deemed necessary, regardless of where the predicate offence was committed. Investigations by law enforcement agencies are coordinated by **CITCO**, and are supported by coordination mechanisms, such as cooperation and information-sharing agreements and joint working groups or teams, to facilitate investigations into priority matters.

The police units specialising in investigating specific predicate offences and related offences of money laundering and terrorist financing are as follows:

a. **Policía Nacional:** the Central Unit for Economic and Fiscal Crime (**UDEF**), which is responsible for investigating and prosecuting criminal activities, both nationally and internationally, relating to economic and fiscal crime, as well as for operational coordination and technical support to the respective regional units; the Central Unit for Drugs and Organised Crime; **UDYCO**, which is responsible for investigating and prosecuting criminal activities, both nationally and internationally, related to drug trafficking and organised crime, as well as for operational coordination and technical support to the respective regional units; and the General Information Directorate (**CGI**), responsible for investigating offences related to terrorism and its financing, as well as their national and international coordination, and for gathering information on these matters for intelligence purposes.

[5] Capital Requirements Directive and Regulation.

b. **Guardia Civil:** the Intelligence Directorate (**JI**) combats terrorism and its financing in the various provinces of the country through Command Intelligence Groups (GIC), and nationwide through the Intelligence Service, which has an Economic Investigation Section that carries out complex investigations and advises the GICs on these matters. The Judicial Police Directorate, which combats money laundering, has the Criminal Intelligence Unit (**UTPJ**), which includes a unit responsible for financial intelligence within its remit, and there are regional judicial police units in the various provinces. At central level, the Central Operational Unit (**UCO**) has a specialist investigation team and handles the most complex money laundering investigations.

c. **Agencia Estatal de Administración Tributaria (AEAT)**: the Customs Surveillance Service (**SVA**), which operates as a Deputy Directorate within the Department of Customs and Excise, is tasked with the prosecution and investigation of certain crimes and offences relating to tax fraud, smuggling and money laundering, acting in this capacity as a judicial police force. The Department of Customs and Excise is the customs authority in Spain and is solely responsible for controls relating to foreign trade, including those concerning movements of means of payment, relying for this purpose on officials from the Customs Surveillance Service and on the support of the Guardia Civil in the exercise of its functions as the State's fiscal guardian and in the prevention and suppression of smuggling. The Asset Investigation Unit of the Sub-Directorate General for Operations, which reports to the Deputy Directorate for Customs Surveillance, is responsible, amongst other tasks, for coordinating the activities of the Customs Surveillance Service in relation to money laundering, including cash control operations.

Meanwhile, within the **State Public Prosecutor's Office,** the prosecution units specialising in investigating specific predicate offences and related offences of money laundering and terrorist financing are:

- **Special Anti-Drug Prosecution Service**: for drug trafficking offences and money laundering related to this offence.
- **Special Prosecutor's Office against Corruption and Organised Crime:** for offences related to corruption (bribery, abuse of office, embezzlement, etc.), organised crime and money laundering related to these offences (excluding drug trafficking or terrorism offences).
- **Prosecutor's Office of the Audiencia Nacional**: for offences of terrorism and the financing of terrorism.

In the judicial sphere, cases involving money laundering offences may be tried, depending on the circumstances and the seriousness of the offences, by the **Provincial Courts, the Audiencia Nacional** and, in exceptional cases, by the **High Courts of Justice** of the Autonomous Communities.

For its part, the Audiencia Nacional has exclusive jurisdiction to hear cases involving the financing of terrorism and money laundering related to it.

(IV) MAIN THREATS OF MONEY LAUNDERING[6].

When identifying ***threats*** within the context of the fight against money laundering and terrorist financing, the definition provided by the FATF, as cited above, should be followed; this defines a threat as *"those individuals, groups of individuals or their activities that pose a potential danger due to their capacity to cause harm to the state, society, the economy or other fundamental aspects of a country's life".*

In the specific case of money laundering, criminal organisations and their activities constitute the threats that exploit the system's vulnerabilities to give the appearance of legality to the illicit financial gains obtained from these criminal activities.

The identification of the main threats posed by money laundering activities is carried out through various analyses and contributions from those public institutions responsible for prosecuting such organisations and activities.

In Spain, as reflected both in the Annual ML/TF Statistical Report published by the COPBLAC with financial intelligence information from SEPBLAC and the LEAs, and in the Ministry of Home Affairs' Crime Statistics System, the main threats in the area of money laundering stem from:

(i) Organised crime.
(ii) Drug trafficking.
(iii) Economic and financial crimes, mainly related to fraud and corruption.

To these offences must be added the threats related to money laundering activities linked to crimes committed in Spain and other countries.

Organised crime.

The National Security Strategy and the National Strategy against Organised Crime and Serious Crime[7] (ENCOyG) identify organised crime as one of the main threats to Spain's internal security, as reflected in the statistical data published annually by CITCO and in the crime figures set out in the reports of the Ministry of Home Affairs. It is a transnational, flexible and opaque phenomenon with an enormous capacity for destabilisation, which can affect social, economic or political structures and values.

The ENCOyDG, as a key strategy to combat this threat, and the "National Strategic Plan Against Illicit Enrichment – PENCEIL" (pending final approval) are coordinated by CITCO with the participation of all law enforcement agencies and are intended to review and update the previous Strategy, as changes in certain criminal, technological, social and international aspects necessitate its updating to provide a renewed strategic vision.

[6] Sources: Ministry of Home Affairs' Crime Statistics System; Annual Reports of the Fiscalía General del Estado; Annual Reports of CITCO; Annual Reports of SEPBLAC; Annual Statistical Report on Money Laundering and Terrorist Financing (ML/TF) of the COPBLAC.

[7] National Security Strategy 2017 and National Strategy against Organised Crime and Serious Crime 2019–2023, approved by resolutions of the National Security Council, the highest body for state policy on national security.

The threat posed by global organised crime is increasingly intertwined with other major threats and risks (including terrorism, proliferation and cybercrime, amongst others), and has become one of the most insidious yet high-impact risks to our societies, the economy and well-being, and, ultimately, to the political and economic institutions and principles upon which our way of life and progress are founded.

According to the National Strategy, CITCO Reports and the information provided by all police forces, organised crime operating in Spain has a marked international dimension and exhibits a profile characterised by criminal specialisation centred on money laundering as a cross-cutting activity. Certain types of crime are common within these organisations, such as drug trafficking, property offences and activities related to corruption, fraud, control of routes and networks for illegal immigration and human trafficking, cybercrime, and document forgery linked to organised crime offences.

From a social and economic perspective, organised crime encompasses a wide range of activities, sometimes under the guise of legitimate businesses, whose ultimate aim is to obtain huge financial gains and which often resort to violence both to carry out their criminal activities and to reaffirm or define their sphere of influence or field of action vis-à-vis other criminal groups or networks, or vis-à-vis the State itself.

It is a dynamic, innovative and flexible phenomenon, resistant to the actions of state instruments and international institutions, with a strategy of maximising its profits and minimising its risks in the face of action by the authorities. Specialised groups operate in supranational territorial spheres, separating the locations where actions are carried out from those chosen for the operations to introduce the goods and funds obtained.

Due to its nature as a global threat, amplified by new technologies and cyber-networks, which causes serious harm to society, the economy, and national and international security, organised crime represents one of the most serious threats to the security of states and their citizens, and a powerful factor in the destabilisation of the political and economic foundations of society and the international community.

Every year, there are numerous police operations targeting organised crime groups. Specifically, on average more than 200 groups are completely or partially dismantled each year, and according to CITCO data, 82% of the groups detected were dismantled in 2018. For this reason, it is considered that organised crime groups will continue to pose the main threat from criminal activity in Spain in the future.

The main types of organised crime groups in Spain are as follows:

1) Groups linked to **drug trafficking networks.** The most significant are:

   a) Groups involved in drug trafficking from Latin America that operate in Spain in cooperation with local networks facilitating the introduction and distribution of drugs. In these cases, there is a direct link between the predicate offence and money laundering activities. These groups operating in Spain introduce drugs into Europe mainly via pre-established routes through our country. The funds they generate are channelled into the financial system via networks of individuals and entities, including companies involved in the trade of goods and services, which allows them to justify their transfers and income through various means (alleged commercial transactions, cash receipts, human couriers or remittances, amongst other methods).

   b) Groups linked to drug trafficking from the Maghreb, which, as in the previous case, operate in Spain in cooperation with local networks that facilitate the smuggling and distribution of drugs. Spain is by far the country with the highest volume of cannabis trafficking in the EU, as analysed in the following section. Due to its geographical proximity, these organised groups use Spain, above all, as a transit point to other European destinations, in coordination with local criminal groups, which has created a serious security situation affecting

particularly the Campo de Gibraltar area. This illegal trafficking generates huge amounts of cash, with frequent cash-in-transit operations, human couriers and operations to deposit funds into the financial system under the guise of supposed commercial transactions.

2) Groups linked to **tax fraud associated with commercial activities**, primarily through companies involved in the production and wholesale distribution of goods manufactured abroad and their sale through the retail network throughout the country. These groups, mainly of Chinese and East Asian origin, manage to generate huge sums of money in breach of tax regulations, which they send abroad (either in cash, making significant use of money couriers, or via transfers disguised as commercial transactions) or invest in Spain, mainly through the purchase of commercial premises. These money-laundering activities, stemming from tax offences, also sometimes involve other predicate offences such as sexual offences, violations of workers' rights, illegal drug trafficking or illegal gambling, amongst others.

3) Groups specialising in **property offences**, burglaries of business premises and homes, illicit vehicle trafficking, and other violent crimes against banks and establishments holding high-value goods such as jewellery and art. These are generally groups of foreign origin, mainly from Eastern Europe and Western Asia, in some cases itinerant, who do not always have a stable residence in Spain. Due to the very nature of the crimes committed and the measures in place within the economic system itself, it is difficult for the proceeds to be integrated into the Spanish financial system; consequently, they are frequently transferred to other territories, sometimes outside the European Union, where they are deposited in financial institutions, offered for sale, etc.

4) Groups specialising in the **fraudulent use of payment methods,** particularly credit and debit cards. The weaknesses in the system and the number of fraud cases have led issuing institutions to develop complex systems to ensure the security of users, who are exposed to theft and the illegal copying of data. The groups committing these crimes operate across all EU countries, distinguishing between the territories of the cardholders' residence, where the data is captured, and where the fraudulent use takes place. The expansion of the range of establishments where transactions can be carried out online to purchase goods and services, place bets or participate in games of chance, etc., has introduced a factor that greatly facilitates the laundering of funds derived from these crimes.

5) Groups specialising in **large-scale cyber fraud**. For several years now, organisations specialising in the fight against crime have been warning of a highly specialised criminal network involved in large-scale fraud, mainly originating in West Africa, through the sending of *the* original *'Nigerian* letters', in which messages (postcards, telephone calls, emails, etc.) are sent to potential victims in order to obtain funds. Links between these groups and other crimes (including those involving sexual exploitation) have also been established. Financial transactions involving funds sent by victims are rapidly transferred via various systems, including the use of payment service providers and bank accounts opened under false identities or for fraudulent purposes.

6) Groups that **carry out criminal activities in their own countries but bring illicit funds into Spain**. This is a form of crime which, in Spain, generally does not involve specific criminal acts, but rather money laundering operations through the purchase of luxury goods and property. Notable is the presence of groups from other European countries where they commit crimes related to corruption, extortion and illicit trafficking, who seek to establish Spain as the location for investment or the purchase of residences for some of their leaders and members, sometimes through complex money laundering schemes. These groups integrate their illicit profits through complex corporate and commercial operations, utilising commercial companies registered in various jurisdictions, some of them in EU countries, with initial banking transactions occurring in countries across all continents, including, in some cases, EU countries.

7) Groups linked to **political or financial corruption schemes**, both national and international. Generally speaking, these groups engage in activities with implications across several countries, such that the country in which the criminal act through which the corruption (misappropriation of funds, bribery, fraud, etc.) or the corresponding financial crime is committed differs from the country of residence of the perpetrators, and also differs from the country in which the funds are received or the assets—primarily real estate—are acquired.

The **Spanish groups** involved in such activities carry out their criminal acts in our country, generally linked to urban development and public services projects, and use foreign countries to maintain accounts and deposits and to register the commercial companies under whose ownership these accounts are held.

For their part, **foreign groups** linked to these corruption offences choose Spain as one of the countries to which to channel funds, through complex international transfer schemes involving two or more countries, and the subsequent use of those funds to purchase assets, generally luxury real estate in tourist areas, but also in the more affluent neighbourhoods of major cities.

Drug trafficking[8].

Spain remains a major transit point on **intercontinental drug trafficking routes**, as demonstrated by seizures made by Spanish LEAs and specialist reports (Europol, UNODC, CITCO). Data on drugs seized in 2018 show very high figures: over 500 tonnes, exceeding the 411 tonnes seized in 2017 and the 373 tonnes in 2016.

The figures for **seizures** of cannabis resin (hashish), mainly in the Mediterranean and originating from Africa (436 tonnes in 2018), account for approximately 70% of seizures across the European Union. Seizures of other types of cannabis are also very high. The implementation of the Special Security Plan for the Campo de Gibraltar and the increased pressure on the so-called 'Strait Route' have led to a rise in the quantities seized.

Seizures of cocaine originating from Latin American countries have once again been very high over the last two years, standing at around 50 tonnes per year. This drug is smuggled via maritime trafficking (both in containers and on other types of vessels). Indicators suggest that its current availability is at a very high level.

However, seizure figures are not as significant for other drugs such as heroin, traditionally smuggled from the Middle East via the so-called "Balkan route", or for synthetic drugs, which in many cases originate in Europe.

In 2018, 21,664 **arrests** were made for drug trafficking offences (an upward trend that began in 2017, in contrast to the downward trend of previous years). Fifty-three per cent of these arrests were for cannabis trafficking, followed by cocaine trafficking (29%), opiates (7%) and amphetamine-type drugs (7%).

According to the National Drug Plan Office, the **consumption data** regularly provided by the Spanish Observatory on Drugs and Drug Addiction show a downward trend for both legal and illegal drugs. However, the high level of cannabis use in Spain remains a particular cause for concern.

[8] Sources: Annual statistics on drugs in Spain 2018; "Annual Report of the National Plan against Drugs"; Reports and Statistics from the Spanish Observatory on Drugs and Addictions (OEDA); "EU Serious and Organised Crime Threat Assessment 2017"; Report on the situation of organised crime in Spain (CITCO, 2018); and Report on Drugs 2019.

The total number of **cases** handled by the Special Anti-Drug Prosecutor's Office relating to drug trafficking in 2018 was 17,348[9], a figure similar to that of recent years, although in percentage terms this represents a 18% decrease since 2014. Alongside Madrid and Barcelona, the figures for the provinces of Cádiz and Las Palmas stand out, as these areas are more exposed to drug trafficking due to their geographical location. As for the origin of those convicted of drug trafficking by the Audiencia Nacional in 2018, the data show that more than half of those convicted (53%) are of foreign origin, a percentage similar to that of 2017 (55%).

With regard to the links between drug trafficking activities and **organised crime groups**, CITCO has identified that in 2018 the largest number of groups involved in drug trafficking were primarily engaged in trafficking hashish (26%), cocaine (24%) and cannabis (11%), whilst the involvement of organised crime groups in the trafficking of other types of drugs is lower: heroin (5%) and synthetic drugs (4%).[10]

A description of the activities of criminal groups linked to drug trafficking offences can be found in the previous section on organised crime groups and their types, primarily with regard to those groups originating from Latin America and the Maghreb in collaboration with local criminal networks specialising in drug trafficking.

Economic and financial crimes: fraud, tax offences, and cases linked to corruption.

There is a significant variety of criminal conduct related to corruption and fraud. The Special Prosecutor's Office against Corruption and Organised Crime highlights that the criminal offences for which charges are most frequently brought within its remit are administrative malfeasance, fraud against the State, embezzlement of public funds, influence peddling, bribery and offences against the Treasury. In each of these cases, a number of individuals are prosecuted, and the proceedings also cover various criminal activities related to these offences:

- **Social Security fraud**: there are various ways of committing Social Security fraud, which may involve failing to pay the contributions due for employees, or claiming benefits or public assistance on false pretences. This type of fraudulent activity has a detrimental impact on unfair competition; the black economy; corruption; workers' rights; and the development of conduct associated with human trafficking for labour exploitation, amongst other matters.

- **Influence peddling**, **embezzlement, perversion of justice and bribery (proper and improper)**: these are offences linked to corrupt activities that are often related to decisions by public authorities to award certain private entities the right to carry out public activities through contracts, concessions, licences, etc., in many cases relating to public services or public works and planning permissions. These decisions may involve the issuing of false invoices, financial or material benefits for the awarding authority, or concessions to entities indirectly controlled by the awarding authority itself, thereby enabling the automatic legitimisation of the profits obtained from the criminal activity.

- **Tax fraud**: alongside traditional tax offences involving non-payment of taxes to the Treasury (income, wealth, corporation), figures remain high regarding the commission of criminal activities related to VAT fraud, either by avoiding payment or through the fraudulent claiming of VAT refunds by national authorities following a chain of transactions (so-called 'carousel' schemes). In recent years, the AEAT has allocated a considerable number of resources to prosecuting such conduct through the courts, and these resources are increasing every year.

[9] Source: Public Prosecutor's Office Annual Report 2019. The number of proceedings initiated is not included, as the complexity of the cases does not reflect the judicial proceedings involved.

[10] Source: Report on the situation of organised crime in Spain. CITCO 2018.

- **Customs fraud:** the most significant criminal activity involves the importation of goods by undervaluing both the quantities of products traded, and the values declared to Customs, thereby defrauding the EU Treasury of import duties (tariffs). Such fraud is particularly prevalent in products imported from Asia. Criminal groups use various schemes to avoid paying taxes and generate significant profits by selling these products (genuine or counterfeit) at prices lower than their market equivalents, which creates situations of unfair competition. The scale and number of operations carried out by the AEAT in recent years have highlighted the existence of major money-laundering operations and schemes within these activities. Other significant frauds relate to the origin or tariff classification of goods, as well as the abuse of certain schemes such as non-customs warehousing and *scheme 42* (obtaining VAT exemption when imported goods are dispatched to another EU Member State).

- **Corporate offences:** these involve diverse types of conduct carried out by company directors or executives who, to achieve certain personal ends, engage in market activities to the detriment of the company itself, its shareholders or third parties. In many cases, these are linked to offences of corporate document forgery.

- **Fraud in public subsidies**: involving the improper obtaining of public funds by falsifying the conditions required for their award, concealing circumstances that would have prevented their award, or failing to comply with the conditions or purposes for which the subsidy was granted.

Money laundering by third parties and for offences committed abroad.

Investigations and legal proceedings relating to money laundering offences have demonstrated the existence of organised crime groups dedicated to laundering in Spain funds derived from criminal activities committed in other countries, without the predicate offence having any connection whatsoever with our country.

Cases of money laundering have also been identified involving the purchase of property and luxury goods within Spain by criminal organisations operating abroad, as well as money laundering activities carried out by professionals acting on behalf of these organisations or their intermediaries. The activities of these groups have already been described in the analysis of both national and international organised crime groups.

Consequently, complex networks of companies set up for the purpose of money laundering have been identified and dismantled. The channelling into Spain of proceeds from crimes committed abroad, often through professionals, is subject to special monitoring by the Spanish authorities, both when it is carried out as a primary activity and when it occurs in connection with another offence.

(V) MAIN THREATS OF TERRORIST FINANCING.[11]

In accordance with the FATF's definition of 'threat' outlined in previous sections, and based on the analyses and contributions of the various national public institutions responsible for combating terrorist organisations and activities, the main threats in Spain regarding terrorist financing activities stem from the evolution of **jihadist terrorism**, which has completely transformed the terrorist threat landscape in which we operate. Whilst traditional terrorist organisations, of a local nature and linked to territorial segregationist ideologies (ETA) or of a revolutionary Marxist nature (GRAPO), are in the process of disappearing, international jihadist terrorism has established itself as a global threat.

Thus, according to the strategic reports of the Ministry of Home Affairs and the latest Annual Reports of the Public Prosecutor's Office of the Audiencia Nacional there has been a sharp increase since 2015 in the number of preliminary investigations linked to jihadist terrorism. Thus, whilst in 2014 preliminary investigations into this type of terrorism accounted for 106 of the 312 preliminary investigations opened – that is, less than 40% – since then, investigations related to jihadist terrorism have accounted for between 50% and 60% of the total. This serves to confirm that, in contrast to the virtual disappearance of secessionist or political terrorism, "international jihadist terrorism has established itself as a global problem of particularly serious and alarming proportions, currently constituting the greatest threat to the freedom and security of our democracies".

The total figures for those arrested and prosecuted in recent years for activities linked to terrorism confirm this: according to data from the Ministry of Home Affairs, between 2015 and 2019, 179 police operations related to jihadism were carried out (an annual average of 36 operations, compared to 13 in 2014), with a total of 318 detainees (an annual average of 63, compared to 36 in 2014). Meanwhile, according to data from the Public Prosecutor's Office of the Audiencia Nacional in 2016 there were 25 people prosecuted for jihadist terrorism, and all were convicted; in 2017, 34 people were prosecuted and 27 were convicted, and in 2018 the figures rose to a total of 73 convicted of jihadism.

As for the figures for those arrested for ETA terrorism, the situation is very different from that of a few years ago, and arrests and convictions for links to the terrorist group are mainly due to activities committed in previous years.

Jihadist terrorism.

Jihadist terrorism has taken on ever-greater dimensions, projecting its radical ideology and actions on a global scale, and terrorist attacks on European soil have increased exponentially since the public emergence of the Islamic State terrorist organisation and the proclamation of the Universal Caliphate in June 2014. In the current scenario, the main protagonist of this threat is Daesh, which, due to its operational capacity, resources, media presence and rapid expansion, has become the benchmark for jihadist terrorism.

However, these groups are characterised by their rapid adaptability and their ability to adjust to the changes and strategies employed against them. Indiscriminate attacks in crowded places, on public transport or against critical infrastructure represent a current trend in jihadist terrorism, which operates through cells as well as individually, with the aim of causing the greatest number of casualties and a strong propaganda impact.

[11] Sources: "National Security Strategy 2017", "Annual Report of the General State Prosecutor's Office. National High Court Prosecutor's Office", "Counterterrorism against ETA and international terrorism" – 12th Parliament. Ministry of Home Affairs.

Spain is a target of the jihadist threat, and the counter-terrorism operations carried out confirm the persistence of that threat. The dismantled cells constituted highly organised structures that fully embraced the ideology of Daesh, following its slogans and directives through a powerful communication and media dissemination campaign on social media and websites. The activities carried out by members of the dismantled jihadist terrorist structures in Spain have mainly involved recruitment, indoctrination and the dispatch of activists to conflict zones. Similarly, arrests have been made for involvement in terrorist networks, logistical support, acts glorifying terrorism and serious threats for terrorist purposes. Individual terrorist activity is prosecuted. The internet and social media are investigated, analysed and prosecuted when used as a virtual terrorist space or as a communication tool.

Therefore, the main elements and activities related to jihadist threats that must be addressed are:

- Currently, the main threat stems from **terrorists or autonomous cells** capable of carrying out attacks—seizing opportunities and using means that are unsophisticated yet highly lethal—against targets repeatedly highlighted in jihadist propaganda or previously attacked in the West (large gatherings of people, tourist sites, military and police personnel, or places of worship of various religious denominations). However, organised attacks by structured cells linked to Daesh cannot be ruled out.

- **Terrorist fighters returning** from theatres such as Syria and Iraq, having gained knowledge and experience in the handling of weapons, contacts, and knowledge of routes and facilitators, act as both ideological and operational catalysts. The process of sending fighters to conflict zones is carried out through national and international networks, which has led to residents of Spain travelling to Syria and Iraq, with funding activities for their travel and stay in those areas having been detected.

- Radicalisation, **recruitment and indoctrination** for terrorist purposes are also among the threats that have come to the fore in recent years. This is not only due to the ideologies underpinning them, but also because they constitute the preliminary stage before individuals involved in these processes ultimately join terrorist groups and organisations.

- **Technological development** has also broadened access to resources available to terrorist groups, increasing their capacity for **financing, recruitment, training, propaganda and glorification**. Against a backdrop of widespread use of social media, the risks of the dissemination of terrorist propaganda and forms of radicalisation and violent extremism are growing. The internet has been the most effective tool for jihadist propaganda and recruitment. The idea of 'global jihad' has taken shape for thousands of sympathisers or followers through messages that distort reality, with an epic glorification of jihadist fighters. Videos convey messages expressing the need to embrace violence to combat injustice and the West's lack of understanding.

- Spain, due to its **geographical location** within the European continent, is more vulnerable to certain terrorist groups. Its proximity to the Maghreb, coupled with the intense terrorist and counter-terrorist activity in the countries comprising that region, makes it a focal point for jihadist terrorism, which can exploit the high volume of people travelling to infiltrate terrorist elements into Spain and the rest of Europe.

Spain is committed to the fight against terrorism with a response based on a comprehensive model that draws on its experience and coordinates action with its allies, in international initiatives and particularly with the EU. The various actors involved in counterterrorism are drawing on past experience and maintaining constant preparedness in the present. Global terrorism, such as jihadist terrorism, requires a high degree of international cooperation, yet at the same time exhibits local characteristics that make it a form of domestic terrorism; this necessitates coordinated work between the CNI, Sepblac and LEAs (CITCO, Policía Nacional, Guardia Civil, Mossos d'Esquadra and Ertzaintza).

Spain has developed, as a result of democratic consensus, a comprehensive regulatory framework containing effective investigative tools, as well as a new definition of activities considered to be terrorist, encompassing those preliminary spaces of ideological transformation without which violent action would not exist.

Work over recent years has been ongoing on all these fronts: analysing the jihadist phenomenon from new angles and using new methodologies; studying new criminal offences and adapting them to the jihadist reality; analysing criminal intelligence to contextualise the phenomenon of Daesh terrorism; addressing the issues surrounding minors and returnees from conflict zones; and studying the ideological reorientation of those who have been recruited and indoctrinated.

The financing of jihadist terrorism.

Spain, given its experience in the fight against terrorism, is fully aware of the need to cut off sources of funding and to identify and mitigate vulnerabilities in the system through which funds, whether of lawful or unlawful origin, are channelled for terrorist purposes or to support such purposes in any form.

In the case of jihadist terrorism, the financing and economic needs of terrorist groups have evolved substantially since the attacks of 11 September 2001, when there were significant movements of funds through the international financial system. Currently, the recent attacks in Europe, most of which have been poorly planned and of limited complexity, have required little financial backing for their execution.

Thus, unlike previous systems of terrorist financing, jihadist groups tend to operate through small cells that are essentially self-financing, obtaining their funds in Spain or neighbouring countries from both legal and illegal sources to finance their terrorist activities, without needing the support of the terrorist group's parent organisation. Generally, these cells obtain and use small sums of money for their operations and activities, following a 'micro-financing' system.

In most cases, transfers of funds for terrorist financing, mainly to or from neighbouring countries, attempt to bypass the formal financial system, particularly banks, and involve the movement of small sums of money to make detection by alerts or controls more difficult.

The difficulty in accessing the banking system, measures adopted in the international financial sphere and terrorist groups' reliance on cash have led these organisations to use alternative money transfer systems and the **'hawala'** system**.** Hawala is an informal clearing system that allows funds to be made available in different parts of the world. This system allows operations to be financed without physically moving funds or using the financial system, making these transactions undetectable by official financial control systems. Some hawala networks have complex bureaucratic structures and offices in different cities, as well as security systems to prevent detection by the authorities.

Fund transfers, originally intended for humanitarian purposes, have also been detected; these are directed to conflict zones and may end up in the hands of terrorist groups operating under the guise of various entities or camouflaged projects.

With regard to the financing of travel by displaced terrorist fighters to join international groups, primarily Daesh, various methods and types of fundraising have been detected, both legal and illegal, carried out either by the terrorists themselves, their associates or supporting organisations.

The use of **international remittances** has also been detected as a means for the families of those who have travelled from Europe to Syria and Iraq to send funds to them periodically; these transfers are made in small amounts and often via predetermined and highly precise methods, involving the use of third countries and intermediaries, which makes them difficult to detect.

ETA terrorism.[12]

ETA has maintained the 'cessation of its armed activity' announced in October 2011 and, consequently, has not carried out any attacks. Its dissolution as an organisation was announced in spring 2018. Law enforcement agencies have also confirmed that the terrorist group's traditional funding systems, particularly through extortion via the collection of the so-called "revolutionary tax", have ceased.

However, there are dissident factions opposed to the strategy implemented following the declaration of the 'cessation of activities' who have increasingly made public statements criticising that strategy, seeking to gain greater support amongst the Basque nationalist movement through campaigns or events in support of and in solidarity with the prisoners. Some individuals linked to these factions have been involved in violent and sabotage-related acts confined to the Basque Country and Navarre, and their evolution and activities must be subject to appropriate monitoring and surveillance.

The State's firmness in its counter-terrorism action following the declared cessation of activities, both in its police and judicial aspects, and the resolute and ongoing international collaboration and support, particularly from France, as well as significant public mobilisation, have been factors that have encouraged dissent.

With regard to their **financing systems**, it should be noted that following the cessation of terrorist activity, the activities that had traditionally been the terrorist group's sources of income have also come to an end.

Other terrorist groups.

In recent years, the terrorist organisation PCE(r)-GRAPO has remained in a weakened state, committing no terrorist acts and limiting its activities to proselytising and recruitment within anarchist and radical left-wing circles. Despite this situation, it has never publicly renounced armed struggle or its revolutionary principles, which are incompatible with current legislation.

Meanwhile, some terrorism-related activity linked to Catalan independence movements has recently been detected and is being monitored by the relevant authorities.

With regard to violent activity carried out by individuals or groups of anarchist ideology, this has shown a marked downward trend over the last five years, both in qualitative and quantitative terms.

Police action in response to the resurgence of violent activity during the early years of this decade has clearly influenced the current situation, in which recorded violent acts are limited to attacks and acts of sabotage against the traditional targets declared by the group, as well as to provoking disturbances and clashes with police units during certain rallies and demonstrations.

[12] Annual Report of the Fiscalía General del Estado, Chapter 4.5 on the Audiencia Nacional

National Counter-Terrorism Strategy.

The 2019 National Strategy Against Terrorism (ENCOT) was approved by the National Security Council to replace the previous Comprehensive Strategy against International Terrorism and Radicalisation of 2012 and is aligned with the 2017 National Security Strategy. This Strategy, coordinated by CITCO, has been drawn up in collaboration with all the institutions and authorities with competence in this area.

The ENCOT is, in turn, being implemented through various sectoral strategic plans against terrorism-related activities, such as the **National Strategic Plan against the Financing of Terrorism** (PENCFIT)[13] or the Strategic Plan against Violent Radicalisation (PENCRAV).

Furthermore, in the preventive sphere, the COPBLAC, at the proposal of the Standing Committee on the Prevention of Money Laundering, has approved the ***'General Guidelines for the Strategy to Prevent the Use of the Financial System for the Financing of Terrorism'*.**

[13] Pending final approval at the time of the NRA's adoption.

(VI) MAIN VULNERABILITIES IN MONEY LAUNDERING AND TERRORIST FINANCING.[14]

As indicated previously in other sections, prior to identifying vulnerabilities, it is necessary to define the concept of *vulnerability* in the context of money laundering and terrorist financing. Thus, according to the FATF:

"Vulnerability" *is any situation or circumstance that may be exploited or used by organisations or individuals seeking to carry out money laundering or* terrorist *financing activities*.

In a preliminary analysis, and irrespective of the specific vulnerabilities that may result from the study of each of the sectors of obliged entities described in the relevant chapter, there are a number of general areas of vulnerability which, on a cross-cutting basis, may have an impact on money laundering or terrorist financing activities across the various sectors.

(A) Vulnerabilities arising from the population.
(B) Vulnerabilities arising from geographical factors.

1. Transactions with high-risk territories or their citizens/entities.
2. Operations involving countries at higher risk in relation to jihadist terrorism.
3. Operations in the Gibraltar area.

(C) Vulnerabilities arising from the legal entity and the activities carried out.
(D) Vulnerabilities arising from payment methods, the use of cash and the informal economy.
(E) Vulnerabilities arising from technological innovations in financial transactions.

1. Vulnerabilities arising from the use of cyberspace
2. Vulnerabilities arising from the use of cryptocurrencies or crypto-assets.

(A) Vulnerabilities arising from the population.

There is undoubtedly a direct link between the number of foreign residents in a country and the volume of funds moving to and from abroad. This poses a vulnerability in terms of AML/CFT due to the greater risk of concealing funds of illicit origin, or intended for illicit purposes, through various channels, such as ordinary financial transfers, investment transactions in Spain, or simply through the inflow and outflow of funds carried by foreign or Spanish nationals.

More than 10% of Spain's population is of foreign origin (4.8 million), with the largest communities hailing from Morocco (714,000), Romania (670,000), the United Kingdom (287,000), Italy (244,000), Colombia (199,000), China (190,000), Ecuador (135,000) and Bulgaria (123,000)[15]. This significant presence facilitates the parallel existence of organised crime groups in Spain that use these communities to attempt to conceal their activities.

[14] Main source: 2017 National Security Strategy.
[15] INE data. Population figures as of 1 January 2019.

In the case of remittances, it is worth noting that there are some 2,100,000 migrant workers in Spain and, according to EUROSTAT 2017, 1.3 million of those in employment are non-EU citizens, who in many cases are separated from their families and regularly send funds to support their relatives or loved ones.

This high volume of international remittances and the use of cash by some immigrant communities in our country lead to greater vulnerability when it comes to concealing or disguising the movement or transfer of funds derived from illicit activities. It is important to highlight the fact that some of the countries with the largest immigrant populations in Spain are among the world's leading producers and traders of drugs or involved in illicit trade.

It is also necessary to take into account the vulnerability posed by the **high volume of cash** in circulation, which results from a combination of several factors: the immigrant worker's employment situation, their family circumstances and country of origin, the number and frequency of remittances they send, and the amounts involved. Immigrants whose families remain in their country of origin support them through small remittances. On occasion, the migrant's wage is the family's sole source of income, and the frequency and regularity of remittances to other countries is very high. This vulnerability has been exploited by money laundering networks as a means of transferring funds to third countries.

These vulnerabilities are exacerbated by the clear risk arising from the fact that other countries have implemented fewer prevention policies and that their authorities carry out fewer controls on operations involving the receipt of funds from Spain.

Another vulnerability exploited by criminal groups stems from the concentration in certain areas of our country, particularly in coastal regions, of large communities of foreign residents. This situation is exploited by criminals and criminal groups to disguise their presence amongst communities of citizens from their own country, to continue their activities from Spain, to launder illicit proceeds from other countries, or even to invest them once they have been laundered elsewhere.

(B) Vulnerabilities arising from geographical factors.

B.1. Conducting transactions with high-risk territories or with citizens/entities from those territories.

The vulnerability that may be exploited for ML/TF purposes is related to the frequency and number of transactions or customers linked to high-risk territories; in other words, the higher the frequency and volume of transactions, the greater the vulnerability.

Identifying all geographical circumstances that may influence potential ML/TF transactions requires a specific analysis for each sector and even for each entity based on its operations, taking into account various possible risk criteria. In any case, it is not possible to draw up a list that exhaustively enumerates the risk criteria for a country or a resident.

The high-risk jurisdictions for one sector do not necessarily coincide with those of other sectors, nor even among all institutions within the same sector, and this must be reflected in the risk analyses and in the adoption of enhanced due diligence measures to be applied by entities in the sector, as it is the responsibility of the obliged entity to carry out its own analysis to determine the risk involved in dealing with certain countries or with residents of those countries and, where appropriate, to apply enhanced due diligence measures.

The first element of geographical vulnerabilities stems from transactions with jurisdictions that have strategic deficiencies in their anti-money laundering and counter-terrorist financing systems. For this reason, the FATF and the European Commission draw up and periodically update lists of high-risk countries which must in all cases be taken into account by Spanish entities when applying their AML/CFT preventive measures.

In this regard, the lists of non-cooperative countries in tax matters, drawn up by Spain and the EU, must also be taken into account, as these jurisdictions may present a higher risk of money laundering due to their lack of transparency and their tax regimes.

Various criteria for identifying high-risk territories are set out in the Guidance on Geographical Risk in AML/CFT Matters, issued by the COPBLAC,[16] which aims to guide regulated entities in this area.

In any case, it is the responsibility of each obliged entity, depending on the sector in which it operates, the type and volume of transactions it carries out, its professional experience and, above all, its corresponding risk assessment, to determine the existence of other risks arising from operating with certain countries or their nationals.

The **main risk criteria** to be taken into account are that the countries:

a) Do not have adequate systems in place to prevent money laundering or terrorist financing.
b) Are subject to sanctions, embargoes or similar measures adopted by the European Union, the United Nations or other international organisations.
c) Exhibit significant levels of corruption or other criminal activities.
d) Provide funding or support for terrorist activities.
e) Have a significant extraterritorial financial sector (offshore centres)
f) Are considered tax havens.

Consequently, the nationality or residence of the customer or their beneficial owner, the origin and destination of the funds, and the involvement of any intermediaries, becomes risk factors to be taken into account; as such, institutions must exercise the utmost caution when analysing the risks associated with transactions in cases where the clients or their funds have links to countries considered to be of particular risk in each activity and carry out transactions with those jurisdictions.

[16] http://www.tesoro.es/sites/default/files/guia_riesgo_geografico_en_materia_de_bc_ft.pdf.

B.2. Transactions with countries posing a higher risk of terrorist financing.

In the case of Spain, in addition to activities with countries commonly identified as posing this risk, particular attention must be paid to transactions with countries in the Maghreb region, due to their geographical proximity and the significant presence of citizens from that area, which constitute clear vulnerabilities in terms of terrorist financing. The correct identification of the origin of funds received in Spain and, in particular, of the reasons for and recipients of such funds must form part of the preventive policy.

Furthermore, attention must be paid to the greater vulnerability of sectors that regularly operate with countries whose political systems may directly or indirectly support radical groups in their religious or ideological stances. This support can take various forms: directly or indirectly financing groups sympathetic to a radical environment, harbouring terrorist elements within the country, supporting their ideas in international forums, promoting their indoctrination, etc.

B.3. Activities in the Gibraltar area.

The region's geostrategic location poses a significant vulnerability, with clear exposure to the activities of organised crime groups engaged primarily in drug trafficking, smuggling, human trafficking and the movement of cash across the Spanish borders.

Specifically, in the Campo de Gibraltar area, criminal activities have been carried out by organised crime groups, primarily involved in drug trafficking and smuggling. These operations, which involve unloading, storage, distribution and/or transport, are characterised by the routine use of cash, both in transactions to pay for the goods and in the acquisition and maintenance of the infrastructure required for these operations, which leaves little trace for the traceability of transactions. The limited use of the banking system in connection with this criminal activity in the area does not prevent the capital, or a large part of it, from eventually entering the formal economy. A portion of the illicitly obtained funds is often used to purchase luxury goods intended for personal enjoyment or ostentation: high-end vehicles, boats, property, jewellery, watches and other high-value items.

In this geographical context, one must also take into account the vulnerability posed by the borders of Ceuta, Melilla and Gibraltar to the smuggling of goods (tobacco, mobile phones, electronic equipment, etc.) which generates significant cash flows.

Furthermore, in the nearby coastal area there is a significant presence of corporate and property transactions carried out by entities created or based in other jurisdictions, whose legislation allows them to provide corporate services or act as mere shell or holding companies in Spain, but which are incorporated under foreign laws, thereby creating greater vulnerabilities for concealing high-risk transactions.

(C) Vulnerabilities arising from the nature of the entity or activity carried out.

When analysing the vulnerabilities that may be exploited by criminal networks to use entities in different sectors to commit ML/TF activities, it is necessary to distinguish between endogenous and exogenous risks that may exist in each type of entity or activity.

Among the intrinsic or 'endogenous' risk factors arising from the entity itself or the activity carried out are:

a) The possibility of creating or acquiring entities or businesses for the purpose of concealing money laundering activities derived from illicit activities or for the purpose of committing terrorist financing (TF) activities. In Spain, almost all regulated entities belong to sectors subject to licensing, registration and compliance with authorisation requirements, and are subject to a regime of prudential supervision and AML/CFT prevention.
b) The possibility of direct or indirect control over an entity's operations by money laundering or terrorist financing networks.
c) The possibility that employees or agents of certain types of entities may be linked to criminal networks, which would enable the use of sophisticated and elaborate systems for handling illicit funds without the entity's knowledge and making such activities more difficult to detect.

Extrinsic or 'exogenous' risk factors are those that may allow networks to exploit an entity for ML/TF purposes; in other words, it is not that the entity itself poses a risk, but rather that an entity operating normally may possess a number of characteristics that make it vulnerable and susceptible to being used for ML/TF operations for various reasons, such as:

a) A possible lack of commitment to AML/CFT policies and measures on the part of the entity. This absence may be due to a deliberate failure to implement preventive policies for reasons of implementation costs, to negligent ignorance regarding the extent to which these measures have been developed within the entity, or to the importance attached to the revenue generated by allowing greater laxity in the implementation of the required controls.

b) An excessive flow of transactions with certain countries or the existence of a high number of customers of certain nationalities may be reasons for using a particular type of entity for AML/CFT operations.

c) The absence of information or adequate procedures enabling the authorities to obtain precise knowledge of the beneficial owners of clients that are legal entities.

In addition, there is the potential failure by the competent authorities to communicate risk factors and to update relevant guidelines and regulations. These are serious risk situations facing preventive policy, which require greater vigilance and rigour on the part of national authorities through the regulatory and supervisory mechanisms at their disposal.

(D) Vulnerabilities arising from payment methods, the use of cash and the informal economy.[17]

According to data from the Banco de España, cash remains the most common retail payment method. In 2018, 53% of citizens stated that they use cash as their most frequent payment method (57% in small towns), whilst 43% showed a preference for debit cards.

In other words, despite the growing use of cards as a means of payment in Spain – which in 2018 accounted for transactions totalling €147.431 billion (9% more than in 2017), the use of cash remains very common, which represents a clear vulnerability in the system due to its potential use for ML/TF purposes.

[17] Sources: "National Cash Survey" by the Banco de España (28/06/2019) 2018 Results; Payment Systems Department. Payment Monitoring and Supervision Division, Banco de España 2018; and Statistics on the Distribution of Small Payments in Spain. Banco de España. 2018.

Alongside cash (paper money and coins, whether domestic or foreign), bearer bank cheques (denominated in any currency) and any other physical means, including electronic ones, designed to be used as a bearer payment method are also considered means of payment.

Bearer bank cheques account for only 3% of the volume of retail payments (€347.631 billion) and, although they are still used by some companies accustomed to this type of instrument, their use has been declining for years. Their current use is very limited compared to other retail payment instruments, so their potential impact in relation to the risk of money laundering is negligible.

With regard to **electronic payment methods**, which allow funds deposited for this purpose to be accessed immediately, we are faced with a vulnerability to ML/TF activities insofar as criminals can exploit the difficulties faced by institutions in establishing appropriate control mechanisms for their use. New technologies have created new markets in which operators offer new instruments (such as mobile and virtual wallets, QR code payment applications, or the use of biometrics); payment methods (telephone payments, mobile payments) and payment services (cash collection at home to top up virtual wallets) which are systems based on electronic transactions by the customer that can be used or ordered from any terminal and anywhere in the world. In parallel, a very wide range of services has been developed which, in line with this philosophy, offer not only payment options but also services related to money transfers, currency exchange or the creation of virtual deposits.

These payment models are characterised by their flexibility, automation and immediacy – features that expose them to certain types of money laundering and terrorist financing linked to specific criminal activities. They are particularly well-suited to sending money via channels other than traditional banks or payment institutions, and to settling transactions involving the supply and demand of illegal goods and services.

The vulnerability of **cash** is determined by:

(i) The **frequency** of its use. Spanish financial and commercial culture shows a certain preference for cash in many transactions, which is why a significant number of transactions involving individuals and businesses still use cash.

However, the development of the banking sector, the widespread adoption of other forms of payment, and the ability to transfer funds using online banking services have progressively limited the use of this payment method. This trend is set to continue in the coming years, given that the European Central Bank ceased issuing the 500-euro note in January 2019, although it remains legal tender. It is estimated that since 2012, cash in circulation has fallen by 50%, and that by the end of 2018, the money in circulation in Spain amounted to some €30 billion in banknotes and coins of various denominations.[18]

(ii) Its characteristics of greater **exposure to risk**. As will be seen when analysing the risks associated with the movement of cash and its use for ML and TF purposes, cash possesses the key characteristics sought by criminals: it is anonymous, untraceable and easily transferable. This is why it is the traditional instrument, the most widespread and present in most criminal contexts, as it is usually the method of choice for paying for illicit goods or services, or the means used to facilitate their transport and hoarding, without requiring the involvement of third parties.

Criminal organisations obtain a considerable amount of funds from their criminal activities, so using physical cash (especially high-denomination banknotes) is doubly useful to them: on the one hand, it is advantageous as a payment or collection method due to its opacity and anonymity, and on the other hand, it is very convenient for the transfer or storage of the financial proceeds of their illicit activities due to the difficulties in tracing it.

[18] Estimated figures in a supranational monetary environment with different issuers, in which the circulation of euros is not limited to ECB issues and to movements recorded by financial institutions.

The **informal economy** also poses a significant vulnerability to being exploited for money laundering and terrorist financing**.** The widespread use of cash is directly linked to the size of the informal or 'underground' economy, leading to significant distortions in a country's economic and labour market data, reducing public revenue and causing inequalities in fair professional competition within the affected sectors.

It is not possible to determine with sufficient precision or reliability what the impact of the informal economy is on GDP, as there are no accepted methodological criteria for making such an estimate. However, there are some analyses and studies based on estimates[19] which place it at the European average, below Italy, Greece and the Eastern European countries, but above countries such as France or Germany.

The main effects that the informal economy may have on money laundering and the financing of terrorism are:

- The generation of illicit funds from tax offences and crimes.
- Greater ease in channelling illicit funds into the system.
- An increase in the use of cash, which entails greater risks in terms of both money laundering and terrorist financing, as analysed in the relevant section on sectoral risks.

(E) Vulnerabilities arising from technological innovations in financial transactions.

E.1 Vulnerabilities arising from the use of cyberspace.

Cyberspace is a unique environment characterised by its technological nature, ease of access, anonymity, high connectivity and dynamism. In the digital space, criminal threats take on a global dimension. In recent times, malicious activities in the field of cybersecurity have increased significantly in number, scope and sophistication. Such activities are becoming increasingly relevant for Spain, a highly interconnected country that occupies a leading position in Europe in terms of the roll-out of digital networks.

From a technological perspective, the digital transformation of society and public administrations, coupled with the growing reliance on information technologies, has increased their vulnerability to potential attacks and, consequently, the potential gains for attackers, in an environment where the right to the protection of personal data is an essential requirement in citizens' dealings with the Administration via electronic means.

With regard to cyber threats, there is growing activity by third countries, terrorist organisations, organised crime groups and individual actors. These groups exploit the anonymity offered by cyberspace to achieve their aims at minimal cost and with lower risk, given the difficulty of attribution. Data and information theft, ransomware and denial-of-service attacks, the *hacking* of mobile devices and industrial systems, and cyberattacks against critical infrastructure are examples of cyber threats.

The use of cyberspace as a means for carrying out illicit activities, disinformation campaigns, propaganda or terrorist financing, and organised crime activities, amongst others, impacts national security, amplifying complexity and uncertainty, and also jeopardises citizens' own privacy.

Spanish financial institutions, aware of the vulnerabilities arising from technological advances and, at the same time, of the need to make continuous progress in FinTech innovations, have significantly improved in the vulnerabilities arising from the use of virtual currencies and assets.

[19] IMF 2018 (F. Schneider and L. Medina).

E.2 Vulnerabilities arising from the use of virtual currencies and assets.

Regardless of the ML/TF risk analysis of virtual currencies and assets discussed in the relevant chapter, it is important to highlight the vulnerability that the existence of such instruments poses to the financial system, stemming from the opacity of both their holders and the origin of the funds used.

In accordance with Directive (EU) 2018/843 of 30 May (the Fifth Directive)[20], virtual currencies are digital representations of value not issued or guaranteed by a central bank or public authority, not necessarily linked to a legally established currency, which do not have the legal status of currency or money, but are accepted by natural or legal persons as a means of exchange, and can be transferred, stored and traded electronically. They use cryptography to ensure security in their storage and use. They rely on the use of a decentralised shared ledger or 'blockchain' in which all transactions leave a trace visible to all users, preventing manipulation whilst allowing for anonymity. The creation and widespread adoption of virtual currencies and assets has led to a radical change in certain criminal schemes and, consequently, in specific money laundering processes.

Of the approximately 2,500 types of virtual currencies in existence, with a crypto-market capitalisation of $325 billion at the end of 2019[21], the main one is Bitcoin, whose market capitalisation had fallen in 2018 from $280 billion in January to $65 billion in December, before recovering to $185 billion in 2019, reflecting extremely high volatility. Other common cryptocurrencies include Ripple, Ethereum, Bitcoin Cash, EOS and Stellar Ripple, all of which have a market capitalisation in excess of $1 billion.

Although their use is still very limited in Spain, the main advantage for holders and users is the cost savings and anonymity they offer. However, there is a lack of regulation and oversight of their use by the authorities, with the consequent risk to financial stability, consumer protection, and the potential for criminal activities attracted by the anonymity of these transactions. The foreseeable evolution of their use positions crypto-assets as a growing vulnerability susceptible to being exploited for ML/TF purposes, which must be monitored, as they concentrate the highest levels of opacity and anonymity, as well as being traded in transactions that have no direct link to legal or territorial jurisdictions, nor to regulated entities.

This growing use and the increasing existence of new secondary markets for their trading (on derivatives exchanges) presents challenges for the authorities due to the risks posed to investors, their potential use for fraudulent activities, and the growth of potential unregulated sources of funding. Specifically, activities such as tax evasion, money laundering, the financing of terrorism, and trafficking in drugs, arms or human beings may be facilitated by the use of cryptocurrencies.

Furthermore, this growth is also being driven by the issuance of virtual assets to finance new start-up projects. These issuances lack a defined legal status, are transnational in nature (most issuers are based outside the EU) and offer a high degree of opacity and anonymity to purchasers, making them a potential vehicle for tax evasion, fraud, market manipulation or money laundering.

This lack of regulation is international in nature, although the first regulations on the prevention of ML/TF already exist in the 5th EU Directive and the FATF Recommendations, which require national transposition, aimed at defining these activities, strengthening their control and supervision, and the registration or licensing of entities providing financial services involving virtual assets.

[20] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018, amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Fifth Directive).

[21] Cryptocurrency markets and blockchain, 2019. FUNCAS Financial Digitalisation Observatory.

(VII) SECTORAL RISKS: THE FINANCIAL SECTOR.

Within the Spanish financial system, there are various types of activities and transactions that may be carried out by different types of financial institutions in accordance with the regulations established for each activity and each institution. These financial institutions channel the various financial instruments or assets in accordance with the requirements laid down for that purpose in their specific legislation. For the purposes of this analysis, we shall proceed, in general terms and from the perspective of the risks of engaging in money laundering and terrorist financing activities, to analyse the financial transactions that may be carried out:

a) Financial services provided by credit institutions[22]

- Private banking[23]
- Corporate banking
- Bank deposits
- Institutional investment
- International money transfers
- Lending
- Cross-border banking correspondent services

b) Services provided by credit institutions
c) Insurance and pension funds
d) Securities investment services, managers of collective investment schemes and securitisation managers
e) Mutual guarantee societies
f) Money transfers by payment institutions
g) Other payment institution services
h) Electronic money transactions
i) Currency exchange activities
j) Crowdfunding platforms

The description of financial activities, their regulatory framework, the number of operators and the turnover corresponding to each is set out in the sections analysing the risks for each type of institution and its operations, as outlined below. However, it should be noted that, in general, the Spanish financial system is dominated by credit institutions, whilst the financial market share of insurance companies, securities firms and other types of institutions is considerably smaller.

[22] Risks arising from the provision of other financial services are addressed in the sections specifically designated for that purpose.
[23] Private banking services are not only provided by credit institutions; other operators, such as investment firms or asset management companies, may also provide similar services, although these do not include the custody of funds.

Financial Institutions[24] (31 December 2019)	Number		Balance sheet (millions of euros)	Assets under management (millions of euros)
	Subtotal	Total		
Banks (including savings banks)		52	2,237,057	
Banks	35		2,180,384	
Subsidiaries of foreign banks	17		56,673	
Securities (securities firms and agencies and portfolio management companies)		96		5,073
Securities (financial advisory firms)		140		
Insurance (life insurance) **(a)**		101		199,171
Credit unions		61	145,987	
Credit Institutions (CI)		36	60,951	
Collective investment **(b) (d)**		123		337,397
Pension funds **(c)**		80		115,264
Mutual guarantee		18	1,189	
Payment institutions		42	12,087	
Electronic money		7	177	
Private equity		145		10,041
Currency exchange		291	0	
Foreign exchange dealers	15		123	
Foreign currency purchasing entities **(e)**	276			
Branches of foreign financial institutions.				
EU banks		78	115,715	
Non-EU banks		3	3,615	
EU securities		65		91
EU insurance		18		4,181
EU collective investment		28		0
Payment institutions		12	15	
EU e-money		5	183	

(a) Insurance companies that are part of banking groups hold a 65% market share.
(b) Collective investment firms belonging to banking groups have an 85% market share.
(c) Pension fund companies within banking groups have an 82% market share.
(d) These figures include 17 investment fund management companies that also manage private equity vehicles with €3.731 billion under management.
(e) 2,819 registered. In the tourism sector, 2,804 companies are authorised to purchase foreign currency as an ancillary activity.

[24] Sepblac data 2019.

(a) Financial services provided by credit institutions.

Activity, context and regulations.[25]

Credit institutions are commercial companies whose main activity consists of receiving deposits or other repayable funds from the public and granting loans on their own account. This sector comprises banks, savings banks, credit cooperatives, and branches of foreign, EU and non-EU credit institutions.

All these institutions, insofar as they operate in Spain, are registered with the Banco de España and require official administrative authorisation to operate, subject to compliance with a large number of requirements of various kinds. The total number of credit institutions operating in Spain, according to data from April 2020, stands at 227. Specifically, the Banco de España's Register of Institutions lists 51 banks, 2 savings banks, 61 credit cooperatives, 33 representative offices of foreign credit institutions, 61 EU institutions without an establishment in Spain, 14 subsidiaries of EU institutions without an establishment in Spain, and 3 branches of non-EU credit institutions. Most of these institutions belong to the Spanish Banking Association (AEB), the Spanish Confederation of Savings Banks (CECA) and the National Association of Credit Cooperatives (UNACC), which act as a link between credit institutions and public administrations and have been playing a very significant role in the implementation of AML/CFT measures.

According to the latest Annual Reports from the Banco de España, the Spanish banking sector has undergone a profound restructuring since the start of the crisis in 2008, a year in which 285 operating institutions were registered. As a result, there has been a significant increase in concentration. Thus, the five largest groups went from accounting for 49% of total assets in the Spanish banking sector in 2008 to 70% in 2017, some twenty percentage points above the EU average. It should also be noted that credit institutions within the Spanish financial system hold around two trillion euros in deposits from private customers.

Until November 2014, all credit institutions were supervised by the Banco de España. Since then, under the Single Supervisory Mechanism (SSM) – a system comprising the European Central Bank (ECB) and the national supervisory authorities of the participating countries – the ECB directly supervises significant institutions (12 consolidated groups as at 31 December 2018), whilst the less significant institutions (58 as at December 2018) are supervised directly by the Banco de España under the oversight of the ECB.

Financial inclusion. In general, the Spanish population and residents in Spain[26] have easy access to financial products provided in a responsible and sustainable manner. However, the way in which these products are accessed—which was traditionally channelled through bank branches—has changed in the wake of the crisis. Thus, the restructuring of our financial system and the closure of 39% of branches open to the public between 2008 and 2017 (with 27,706 remaining operational at the end of this period) have forced institutions to develop other channels to facilitate access to their services. These initiatives range from the installation of ATMs outside branches, the promotion of online banking, the use of mobile branches ('ofibuses') or branches offering temporary services, as well as the development of networks of partner agents and seconded staff.
The sum of all these facilities means that less than 2% of the Spanish population does not have any financial services. In terms of the number of municipalities and populations, and specifically access to cash, we are talking about 3,402 municipalities — of which 2,976 have a population of fewer than 500 inhabitants — and 913,682 inhabitants.

[25] Banco de España, Register of Institutions, Annual Report and Financial Stability Report.
[26] The Basic Payment Account is a factor contributing to this inclusion. It is a non-interest-bearing current account that may be opened by any person legally residing in the EU, an asylum seeker, or a person without a residence permit who cannot be deported.

In any case, it should be noted that the level of financial inclusion in Spain stands at 98%, and that 92% of the population lives in municipalities with two or more bank branches, whilst less than 3% live in places without physical access to a bank branch.

Regime governing entry into the business. Authorisation to establish credit institutions in Spain is granted by the European Central Bank following a procedure handled by the Banco de España, based on documentation provided by the institution and a mandatory report from SEPBLAC on the adequacy of its anti-money laundering and counter-terrorist financing procedures. In addition, in order to grant such authorisation, a series of requirements are taken into account relating to the solvency of the new institution, the suitability of its shareholders and senior management, the professionalism of the latter, and the existence of sound administrative and accounting systems as well as adequate internal control procedures. Once authorisation has been obtained and following incorporation through registration in the Commercial Register, credit institutions must register in the Register of Institutions and register their directors, managing directors or equivalent in the Register of Senior Officers, both at the Banco de España.

Vulnerabilities and risks.

The **inherent risk** of the activities carried out by this sector is very high due to a combination of factors: the majority of the monetary flows circulating through the financial system are channelled through credit institutions, which means that their size, number of customers, number of transactions and deposits, the economic volume of transactions and their internationalisation make the credit institution sector highly attractive and highly vulnerable to ML/TF operations.

Furthermore, the characteristics of the financial services provided by these institutions offer significant advantages for concealing funds of illicit origin: security of deposits, appearance of legitimacy, transferability to third parties, speed and efficiency of transactions, and potential transfers to other countries, amongst others.

In any case, the inherent risk of the sector is also influenced by the diversity of institutions, their activities and their different risk profiles, which determine the existence of different inherent risks depending on the activity. Specifically, the risks will differ for:

- Current account deposit activities.
- Corporate banking activities.
- Investment banking activities.
- Private banking activities.
- International money transfer activities.
- Granting of loans.
- Cross-border correspondent banking.

Supranational Analysis of ML/TF Risks in the EU [27]. The conclusions of the SNRA report explicitly reflect this diversity in risk levels, which varies depending on the activities carried out by banking institutions. Thus, the risk faced by a corporate bank offering financial services to businesses, governments and institutions differs from that faced by a retail bank whose clientele consists of private individuals and small and medium-sized. The activities of a bank that focuses on treasury management are exposed to a different risk from that faced by an investment bank or a bank providing correspondent banking services.

[27] https://ec.europa.eu/info/sites/info/files/supranational_risk_assessment_of_the_money_laundering_and_terrorist_financing_risks_affecting_the_union.pdf.

This is why the sector faces a variety of AML/CFT risks that depend on multiple factors such as:

- Type of services provided by each institution.
- Size.
- Profile and nature of its clientele.
- Geographical scope (local, regional, national or international).
- Method of interaction (face-to-face, by telephone or online).
- Complexity of the products offered.
- Usual business activity.

Among these variable factors, both the FATF and the EU have paid particular attention to the level of risk posed by so-called **Politically Exposed Persons** (PEPs), particularly in financial activities. Initially, it was considered that the risk posed by these individuals stemmed from corruption-related activities committed in their countries of origin, the illicit proceeds of which were subject to money laundering in a different country. For this reason, all countries were required to establish measures directly aimed at mitigating the risks posed by potential customers classified as PEPs.

Subsequently, the international recognition of the use of family members and associates to conceal funds, as well as the existence of money laundering activities within their own countries, has led to countries being required to establish more stringent measures to monitor the activities of clients classified as PEPs and their associates, whose level of money laundering risk is considered higher. This risk is considered more significant in financial transactions linked to personalised wealth management and the making of international (and, to a lesser extent, domestic) investments and deposits through special purpose vehicles or holding companies.

The **residual risk** associated with the activities carried out is determined by the high level of regulation, control and supervision to which this sector is subject at national level by the authorities, both in terms of prudential supervision and the prevention of money laundering and terrorist financing. Furthermore, the credit institutions sector is the one with the greatest understanding of its preventive obligations and of the ML/TF operational risks that affect them.[28]

This high level of risk awareness, both at sector level and individually at institution level, means that institutions develop and implement internal control policies and procedures for AML/CFT prevention, which include the assessment and approval of their own risk analyses at institution level. These internal control procedures, which include early warning systems, decision-making procedures and customer onboarding policies, amongst other areas, are not static but are sufficiently flexible to address the evolving nature of ML/TF threats appropriately; furthermore, they must adapt swiftly to internal changes, as well as to external corporate processes such as mergers, takeovers or demergers.

In the case of financial groups comprising several entities, internal control policies and measures must be uniform and applied consistently. The quality of the prevention system will depend, in each entity or group of entities, on the internal control procedures and the resources allocated.

[28] Catalogue of Risk Operations: http://www.tesoro.es/sites/default/files/cor_entidades_de_credito.pdf.

To assess the quality of internal control systems and procedures for the prevention of ML/TF, the following are used: the risk self-assessment analysis carried out by each institution, the external expert's assessment, information from the Banco de España as the prudential supervisor, and the information available to SEPBLAC in the exercise of its supervisory role regarding AML/CFT and as a financial intelligence unit.

The interaction of inherent and residual risks according to the types of transactions will result in a different level of residual risk for each type of service or activity provided and for each individual institution; therefore, alongside the description of the risk elements arising from the sector's common vulnerabilities set out in the risk fact sheet, the specific risks posed by the various types of financial services provided must be taken into account.

In its dealings with the sector, the Banco de España has been conveying to institutions their responsibility for establishing appropriate governance and for the design and operation of their internal procedures and internal audit, with the aim of adequately identifying, managing and controlling ML/TF risks. Furthermore, and in line with the various measures recently adopted by EU legislators to clarify and strengthen the relationship between ML/TF prevention and prudential supervision, the Banco de España will take into account the implications that ML/TF prevention risks may have on the stability and solvency of credit institutions under its direct supervision and will act accordingly, within the scope of its powers.

Private banking operations.[29]

Private banking consists of the professional management of a client's assets, characterised by the provision of personalised services covering advisory, planning and wealth, financial and tax management.

ML risks. The very nature of private banking activities and the specific conditions under which they are managed mean that these services carry a high risk of being used for money laundering purposes. In most cases, **threats** relating to the misuse of these services stem from economic crimes, such as fraud, tax offences or embezzlement, but funds of illicit origin may be linked to any other categories of crime.

The main **vulnerabilities** stem from the very complexity of the operations involved in managing these funds and assets. This complexity may involve the creation of legal structures or companies for a client or group of clients and the purchase of financial products in the name of such structures, with the consequent difficulty in identifying the beneficial owner. The use of financial intermediaries in carrying out transactions is also common, which further complicates the practical difficulties in identifying the client and the source of the funds, as well as the exploitation of the international presence of certain entities in high-risk areas to carry out investments or transactions in these territories. Other factors to consider are the clients' own profile as well as the ultimate objectives of their relationship with the manager (banker) or entity providing the services.

Generally speaking, these are clients with a higher-than-average risk profile, greater purchasing power (sometimes holding substantial assets) or classified as politically exposed persons (PEPs), who seek the highest possible degree of anonymity and use corporate structures to achieve this. These services offer clients personalised treatment and preferential management, enabling them to achieve maximum returns on large sums of money. There is no legal reference to thresholds for the provision of these services, and generally, they are offered for the management of assets starting from 500,000 euros, although the thresholds and the names of the services (Personal Banking, Premium Banking, etc.) may vary depending on the institution.

[29] As indicated, private banking services are not only provided by credit institutions; there are other operators that also provide these or similar services, although these do not include the custody of funds.

Private banking services do not involve ordinary banking transactions, but rather the management and investment of funds, assets or securities of significant financial value, tailored to the client's needs or financial preferences, which usually involve complex procedures carried out through the institution itself, but which may also involve the use of third-party managers acting as intermediaries, with high levels of specialisation in different areas of the financial markets, as well as the use of legal structures that make it more difficult to ascertain the beneficial owners and the origin of the sums involved in the transactions.

Generally speaking, this is a service that offers significant benefits to the financial system, as it encourages capital investment whilst providing substantial advantages for clients, who are offered personalised and comprehensive services that instil greater confidence in their investment or wealth management activities. At the same time, it enables the management of substantial assets, often of a family nature, which are thus integrated into the financial and investment market within a framework of greater reliability and safeguards.

Precisely because it is such a personalised service, it requires the institutions providing these services to have a broader understanding of the client, their activities and their risk profile, establishing robust systems in their client onboarding and AML/CFT policies, thereby mitigating existing risks.

However, as noted, the complexity of fund and asset management operations, the difficulty in identifying beneficial owners, the high returns that can be generated for both the client and the manager, and the frequency of cross-border transactions and investments—including, on occasion, transactions and investments in which international financial centres, *offshore* jurisdictions and other higher-risk countries may be involved—are factors that mean private banking financial services maintain a **high** level of ML risk.

TF Risks. In the analysis of terrorist threats and their financing methods, no TF risks have been identified in private banking services, and the risk of their use for this purpose is **low**.

Corporate banking operations.

AML risks. This is a specialised banking area focused on corporate, business or investment banking operations, aimed at companies, multinationals or corporations. The services offered include loans and other credit products, treasury and cash management services, trade finance, real asset analysis, portfolio valuation, and debt and equity structuring, amongst others.

The **threats** are similar to those described for private banking, although with a higher incidence of activities linked to corruption in the private sector and, to a lesser extent, their use to circumvent international sanctions, countermeasures or dual-use goods. The main **vulnerabilities** associated with these services are linked to the complexity of the corporate structure and the ownership chains of client companies, as these can facilitate the concealment of their identity, hinder the identification of their beneficial owner and/or prevent full knowledge of their actual activity or the origin of the funds they handle, which results in a higher risk.

Furthermore, there are other associated risks, such as those arising from the significant sums involved in the transactions and products offered and, above all, from the clients of these services themselves. The EU SNRA echoes this view, highlighting that the greater level of sophistication required in corporate banking services makes them vulnerable to potential use in ML schemes through the involvement of legal and financial intermediaries with a higher degree of specialisation in this type of activity.

These complex corporate structures, insofar as they may lead to a reduced understanding of the actual business activity, the origin of the funds being handled and the true economic operations of the company, result in a **moderate/significant** residual risk of these services being used for money laundering purposes.

TF Risks. Although companies and business groups linked to TF activities have been identified in the past as having maintained client relationships with financial institutions, a precise assessment of the current risk—taking particular account of the high level of awareness within the credit sector regarding activities with a possible direct or indirect link to terrorist groups— and the implementation of specific preventive measures in this area, currently justify classifying the risk of this channel being used in TF processes as **low**.

Bank deposits.

The widespread use of bank deposits, which is the norm in Spain where financial inclusion and access to banking services is almost universal, and the fact that bank deposits are a very simple and effective system for introducing and moving funds within the national and international financial system, or for withdrawing or using them when necessary, make their use a very common practice with a high inherent risk for ML/TF purposes across all types of **threats** and offenders linked to all predicate offences.

The wide diversity of existing customers and the extremely high number of transactions related to bank deposits that take place daily throughout the financial system are, in turn, the main **vulnerabilities**, and require highly detailed and complex internal policies and procedures covering customers, types of transactions, amounts, destinations, types of transfers and customer/third-party profiles, amongst other measures.

Apart from these internal policies and procedures, the ease with which the use of bank deposits for ML/TF purposes can be detected obviously depends on the type of transactions carried out.

Thus, simple deposit transactions (deposits) carried out for ML purposes are easier to detect by banks' internal prevention and alert systems, whereas more complex transactions, including deposits, cash withdrawals or transfers, may not be.

As highlighted in investigations and prosecutions for ML/TF offences, or in reports of suspicious activity from the sector, there are customers who lend their accounts to make deposits (or carry out other transactions) involving funds from third parties, without having any connection to those funds; there are also customers who claim to carry out fictitious professional activities to justify deposits of illicit funds; or customers who hide behind complex corporate structures, sometimes with residence abroad, to conceal the origin and beneficial ownership of the funds; or who become part of chains of financial transactions between different account holders or jurisdictions that make it difficult to ascertain the source of the funds.

ML Risks. In this context, the level of ML risk associated with deposits in retail accounts is considered **significant,** as evidenced by various supervisory activities and investigations and prosecutions for ML offences, which justifies a higher degree of control by institutions in the sector and the implementation of specific measures to monitor the customer and their business relationship.

TF Risks. However, with regard to TF activities, it is considered that, given the high level of awareness that has existed for years among the authorities and the Spanish financial sector, the level of residual risk should be regarded as **moderate**. In fact, this awareness on the part of credit institutions has led to the progressive use of alternative means outside the banking system to conceal and move funds linked to TF activities in our country.

Institutional investment operations.

ML risks. The use of institutions that collectively invest large sums of money in securities or other types of investments, thanks to contributions from retail investors (insurance companies, investment funds, etc.) for money laundering purposes, carries a degree of risk exposure that is inherently high.

This is because the nature of the operation allows for the rapid integration of funds into the financial system and their immediate conversion into other securities, and the large volumes of funds associated with this type of investment, which allow illicit funds from organised crime to be better concealed with a higher level of sophistication. The **threats and vulnerabilities** would be similar to those indicated for corporate banking or, to a lesser extent, private banking. However, the risk is lower than in other similar investment services provided by the sector to private banking clients or in transactions by other financial institutions carrying out investment activities of a similar nature.

In any case, the complex regulatory regime applicable to this type of investment requires credit institutions to adopt additional AML/CFT prevention measures and controls involving an analysis of the transaction's consistency with the client's risk profile, which in practice entails a double verification of the suitability of the investment and the origin of those funds against the client's history and profile, which would lower the final risk rating to **moderate.**

TF risks. The volumes and characteristics of this type of product mean that the risk they pose to the financing of terrorism is considered **low**.

International fund transfers.

ML and TF Risks. The sending and receiving of funds to or from abroad, whether through customer accounts or directly without any corresponding debit or credit to those accounts, are financial services that carry a **high inherent risk** of being used for both ML and TF purposes, as indicated in other chapters of this National Risk Assessment (for example, in the section on services provided by payment institutions).

If we add to the above:

- The high number of foreign individuals and entities established in our country and the high volume of transactions carried out by these groups and by the numerous commercial entities that maintain fluid commercial relations with other countries make these transactions vulnerable to being used to disguise the transfer of funds of illicit origin.
- The identification of ML/TF schemes in which shell companies or entities with fictitious activities are used to move funds for illicit purposes; the presence of corporate structures created for the purpose of concealing the origin and beneficial ownership of the funds and to justify their transfer; and triangulation processes or the existence of chains of transactions between different individuals and jurisdictions that make it difficult to ascertain the origin of the transferred funds.
- The existence of different systems or types of fund transfers linked to ML/TF activities: splitting transactions to avoid detection of transfers; the use of complex payment chains involving multiple parties in various countries; cash deposits with immediate transfer to other countries; the use of entities with no real commercial activity; the use of 'back-to-back' systems, etc.

All of this justifies the view that, despite the increasingly strict and rigorous control measures adopted both by regulators and supervisors and through the banks' own policies and procedures, these services are considered to carry a **significant** residual risk of being used for ML/TF purposes. This necessitates greater monitoring and control by all relevant authorities and obliged entities, with particular emphasis on:

- The destination/origin of transfers.
- Any intermediaries involved.
- The amounts involved.
- The profile of the parties involved.
- The transaction or legal act giving rise to the transfer.

Granting of loans.

The activity of granting credit on a professional basis, although ordinarily carried out by credit institutions, is not an activity reserved for them. In other words, it may be validly carried out by any natural or legal person without the need for authorisation or a licence. However, in Spain, the market share of credit granting activities by credit institutions stands at 70% of the total.

Credit transactions in the broad sense may take various forms: loans, consumer credit, mortgage loans, financing of commercial transactions, the granting of guarantees or reverse mortgages, amongst other types. As indicated in other sections, credit granting and repayment activities involve risk exposure linked, on the one hand, to the possible illicit origin of the funds being repaid (ML purposes) and, on the other, to the possible use to which the loan amounts may be put (TF purposes). Credit services may be used by any type of threat linked to any predicate offence generating illicit funds, primarily those requiring the repatriation of illicit funds (in transactions of a certain value) or those seeking to integrate cash into the financial system (in loan repayments, either directly or following integration into the system in instalments).

ML risks. Lending activities and loan repayments are exposed to money laundering risks, primarily due to the possible illicit origin of the funds being repaid by the customer. There are certain types of ML risks associated with credit transactions that are forcing institutions to strengthen controls, particularly regarding the methods of repayment of granted loans, as cash payments of the debt incurred, loan repayments made well before the agreed maturity date, or those made via international transfers from other countries can be used as methods to launder illicit funds.

TF Risks. Obtaining funds through loans presents risks due to their potential use to finance activities linked to terrorism, particularly in the case of small-value loans where lending controls are less stringent.

Therefore, the inherent risk of **money laundering and terrorist financing** activities occurring in this type of contract must be considered significant. However, this level of risk is mitigated in various ways, as these are traditional banking business lines, credit institutions already have rigorous procedures in place for verifying and monitoring customers and their professional activities, both to ensure the repayment of the financing granted plus interest, and for the purposes of ML/TF prevention. Consequently, these transactions, when carried out by credit institutions, should be classified as **moderate** risk.

Cross-border correspondent banking.

ML and TF risks. The international correspondent banking network is a channel that can be exploited for ML/TF purposes, as the ease and speed with which large sums can be moved allows, through complex financial transactions, the dissociation of funds from their criminal origin, making it virtually impossible to trace them.

This difficulty in tracking is exacerbated by certain **vulnerabilities** specific to this service, such as the fact that banks participating in the payment chain are subject to the regulations of the country where they are domiciled and the existence of a multitude of corporate transactions that hinder greater control over the beneficial owners of the transfers ordered.

However, not all types of cross-border correspondent banking relationships present the same level of risk;

therefore, in each case, the stringency of the measures to be applied must be determined on the basis of the circumstances and potential risks.

It is necessary to assess the client institution's risk level in a detailed and specific manner, analysing, amongst other things, factors relating to:

- The jurisdiction: the country's regulation and supervision, anti-money laundering (AML) and countering Financing of Terrorism (CFT) framework, etc.
- The products offered by the client organisation.
- Correspondent banking services.
- FinTech systems and methods used.
- Transparency of payment operations.
- In particular, the consistency of specific transactions with the type of business relationship maintained with the client institution.

For all these reasons, without prejudice to the specific circumstances of each case, in general the risk associated with the correspondent banking service should be considered **significant**.

Conclusions.

The financial services provided by credit institutions often carry **high inherent risks** of **ML/TF**. However, these risks are mitigated by a wide range of factors and measures.

In fact, the credit institution sector has for many years been subject to extensive regulation and supervision in the area of ML/TF prevention, and these institutions have been adopting and implementing increasingly rigorous **internal policies, bodies and procedures**, investing in human and technological resources to strengthen their preventive systems.

This is the sector with **the highest level** of **awareness** of the risks associated with money laundering and terrorist financing, with numerous preventive measures and policies promoted and coordinated by AEB and CECA, and it has significant material and human resources dedicated to prevention. Furthermore, it is the sector with the highest number of suspicious activity reports and is subject to **ongoing supervision** by the competent authorities (the Banco de España and Sepblac).

All of this has contributed to a steady reduction in the high level of inherent risk that financial services provided by the credit institutions sector face of being used for ML/TF operations.

In any case, the analysis of the sector's common vulnerabilities reflects the existence of a number of residual risks that remain relevant to the financial transactions and services provided by the sector, although the threats and vulnerabilities that may increase the risk of ML/TF are not uniform, but vary depending on the type of financial transactions or services provided, which in turn affects the **different assessment of residual risks for each type of service** provided, as indicated in each case.

b) Lending services provided by credit institutions and by other persons and entities.

Activity, context and regulatory framework.

Under Spanish law, the business of granting loans on a professional basis is not a reserved activity; in other words, it may be carried out lawfully by any natural or legal person without the need to prior authorisation or a license.

Consequently, although it is most frequently 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 operations: granting loans, consumer credit, mortgage credit, financing of commercial transactions, granting guarantees, leasing (financial leasing with an option to purchase), reverse mortgages, factoring (assignment of a loan portfolio) and ancillary activities to ensure the administration and financing of the loans assigned to them.

(i) Credit Institutions (CI).

Outside the scope of credit institutions, lenders that meet the legal requirements may obtain a licence to operate as Credit Financial Institutions (CIs). These are entities which, subject to administrative authorisation, may also carry out the credit activities included in their authorised programme of activities. The use of the designation "Credit Financial Institution" or its abbreviation "CI" is subject to reservation, meaning it may only be used by those holding the relevant authorisation.

What distinguishes these institutions from banks is that they may not raise repayable funds from the public in the form of deposits, loans, temporary transfers of financial assets or similar instruments, whatever their intended use, and consequently, the legislation on deposit guarantees does not apply to them. However, they may issue securities subject to the Securities Market Act and securitise their assets subject to the general regulations governing securitisation funds.

The solvency and governance requirements are equivalent to those for credit institutions, as it is understood that these requirements serve as a guarantee for the stability of the financial system and for the users of the services it provides, including both businesses and consumers. Furthermore, the authorisation process for CIs is subject to the same 'fit and proper' checks and shareholder suitability assessments as credit institutions. In particular, it requires the issuance of a preliminary report by SEPBLAC regarding the adequacy of the AML/CFT bodies and procedures that the applicant institution intends to implement should authorisation be granted.

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, suitability of holders of significant shareholdings, commercial and professional integrity, statutory limitations on its corporate purpose to activities specific to an CI unless authorised as hybrid entities, internal control procedures, etc.

Following their registration in the Commercial Register, CIs must be registered in the Banco de España's Special Register of CIs, with such registrations being published in the Official State Gazette, Boletín Oficial del Estado (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 terms of regulations on significant shareholdings, suitability and incompatibility, the registration of senior officers, corporate governance and remuneration policy.

The CI sector, according to data from the Banco de España's register, as of December 2019 comprises 27 institutions and 9 hybrid CIs, i.e. those authorised to provide payment services (CI-PA) or issue electronic money (CI-EM), meaning that, in addition to special authorisations from the Banco de España and SEPBLAC, they are also subject to the regulations governing such institutions. According to data from the Banco de España, the volume of financing offered by this type of institution stood at €50.958 billion at the end of 2019, of which around 60% originated from subsidiaries of credit institution groups. The size of the sector is equivalent to approximately 2% of that of credit institutions.
The National Association of Credit Institutions (ASNEF) is a trade association that represents virtually all credit institutions and 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 guidelines and organises events on security in the conduct of its activities (personal data, cybersecurity, prevention of money laundering and terrorist financing, amongst others).

(ii) Lenders other than credit institutions and credit finance institutions.

As it is not subject to licensing requirements, 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 granting of mortgage credit are subject to requirements for access to the activity and a supervisory regime set out in Directive 2014/17/EU, which Law 5/2019 of 15 March, regulating mortgage credit agreements, transposes into our legal system, and which seeks to ensure, at European level, a higher standard of responsibility on the part of these lenders in their dealings with borrowers.

Under this regime, in order to operate, they must be registered with the Banco de España or the relevant Autonomous Community, depending on the geographical area in which they carry out their business. The supervision of these agents is further reinforced by the prohibition on registration in the Commercial Register without the corresponding administrative registration.

Vulnerabilities and risk.

As in the case of credit institutions, the granting of loans by other entities and the repayment thereof entail a risk linked, on the one hand, to the possible illicit origin of the funds being repaid and, on the other, to the possible use to which the loaned sums may be put, and therefore the **inherent risk** of both money laundering and terrorist financing occurring in this type of service must be considered significant, as it may be subject to abuse by any type of **threat** linked to any type of predicate offence or terrorist activities.

ML Risks. Given the aforementioned requirements for access to the activity, it is difficult for organised crime structures to gain control of CIs, as they are subject to strict regulatory conditions regarding authorisation and supervision. However, this possibility is less complex in the case of smaller lenders that do not have CI status and operate without a licence, registration or prudential supervision, as they face a less rigorous regulatory regime. In these cases, participation in ML schemes involving the granting of credit and the subsequent repayment of criminal funds is more feasible.

Furthermore, in the case of smaller entities, the implementation of overly rigorous control measures may lead to a reduction in or loss of business, meaning that certain customers may seek out similar entities with less stringent procedures. This may affect the rigour with which different entities in the sector implement prevention systems for fear of losing market share, thereby impacting the risk profile of some entities relative to others.

There is, therefore, a significant risk exposure for ML activities arising from the use of the lending services offered by these institutions, particularly for those that have not been classified as CIs or are not supervised. However, in quantitative terms, the ML risk posed by lending activities carried out by lenders other than credit institutions and CIs is not significant, as their market share is negligible.

TF risks. As noted in the case of lending operations for credit institutions, there are risks associated with TF activities arising from lending operations where the funds are ultimately used for purposes other than those stated in the application and linked to terrorist ends. These risks increase in line with the size of the institution, the amounts of the loans, knowledge of the customer and the purpose of the loan, and the degree to which preventive policies are implemented.

As for **residual risk**, due to the regulatory and supervisory requirements and controls applicable to CIs, the sector's awareness, and the fact that the majority of credit is held by institutions subject to controls and obligations, it is considered that the inherent risk is significantly reduced.

The CI sector's own association, ASNEF, has set up a Fraud and Money Laundering Prevention Service to advise CIs on these matters and to act as an intermediary with the competent authorities, providing guidance and regularly organising seminars on developments and the application of the AML/CFT regime they are required to implement. In this regard, CIs are a sector that plays a significant role through systematic reporting or reporting on the basis of suspicion and, furthermore, are subject to specific inspections regarding AML/CFT prevention.

Lenders that do not qualify as CIs have also been increasing their reports to SEPBLAC. However, the fact that many entities operate without a licence or prudential supervision prevents the same level of knowledge and control over these entities and individuals as is available for CIs, meaning they pose a greater risk than CIs.

Conclusion.

The sector faces **significant inherent risk** in relation to both money laundering and terrorist financing activities.

ML risks. In the case of **CIs,** it is considered that the stringent regime governing access to and the conduct of business, their financial links with banks, and the fact that entities in the sector have been adopting and implementing increasingly rigorous internal policies and procedures, mean that the **residual risk** of money laundering activities is classified as **moderate**.

However, in the case of **lenders that are not CIs**, due to the lower level of control over the provision of services, there is a greater risk both of them being used for money laundering purposes by criminal networks and of them being linked to the repayment of loans with illicit funds; consequently, it is considered that there is a **significant** residual risk.

TF Risks. A **moderate/significant** risk is considered to exist due to the potential use of CIs and entities that, without CI status, carry out credit operations through unrepaid loans whose funds are used in activities linked to terrorism.

c) Insurance and pension funds.

Activity, context and regulatory framework.

Insurance. The insurance sector's essential role in the economy justifies a high level of regulation and public intervention aimed at protecting policyholders, insured persons, beneficiaries and third parties under private insurance contracts, which consist of the exchange of a present and certain benefit—the premium—for a future and uncertain benefit—the indemnity.

In accordance with the regulations, insurance business may be carried out by entities taking the form of public limited companies, mutual societies, cooperatives and social welfare mutuals, although it is important to note that around

60% of the sector's volume corresponds to the activity of entities forming part of a banking group.

Sector figures: as of 31 December 2018, there were 215 entities registered in the Administrative Register of Insurance Entities, with the number of registered insurance intermediaries and reinsurance brokers standing at 75,444. Most entities in the sector are members of the Spanish Union of Insurance and Reinsurance Entities (UNESPA), which accounts for 96% of the business. According to statistics from the Directorate-General for Insurance and Pension Funds, Dirección General de Seguros y Fondos de Pensiones (hereinafter DGSFP), gross premiums written at the end of 2018 stood at €65,909 million, of which €29,143 million corresponded to the life insurance sector.

Pension schemes are defined in the sectoral regulations as the right of the individuals for whom they are set up to receive financial benefits in the event of retirement, the death of the scheme member, permanent disability, long-term care needs and death, and the obligations to contribute to them. The benefits provided by these schemes are private in nature and are supplementary to (never a substitute for) state pensions.

They are a long-term savings product with a specific purpose. The resources required for the financing, coverage and effectiveness of pension plans are held within **pension funds**. These pension funds, which have no legal personality, are administered by a management company with the assistance of a custodian. The benefits received will depend on the capital contributed by the participants and the returns generated by the Pension Fund in which the Pension Plan is held.

Sector figures: according to data from the DGSFP, at the end of 2018 there were 2,624 pension schemes managing total assets of €105,889 million.

The regulation of the insurance sector, set out in a variety of rules, establishes that it is subject to the prudential supervision of the DGSFP and requires prior administrative authorisation to operate. This authorisation process 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 preventive bodies and procedures that the entity being established intends to implement.

Insurance undertakings and insurance brokers, when acting in relation to life insurance or other investment-related services, and pension fund management undertakings are obliged entities in the field of ML/TF prevention under Law 10/2010 of 28 April.

Furthermore, the EU-level regulation known as Solvency II has led to a far-reaching strengthening of the governance system of insurance companies, which also has a significant influence on the AML/CFT prevention system. Solvency II contains rules requiring the development, documentation and approval of policies and procedures across all areas of the entities' operations, and raises the standards for the integrity, professionalism and training of the entities' directors, managers and employees. This regime defines the functions and systems that insurers must have in place, notably including internal audit functions and the verification of compliance with the adequacy and effectiveness of governance and internal control systems, which also encompass AML/CFT prevention systems.

For its part, the compliance function must direct its checks towards all areas of the entity's activity and assess exposure to compliance risk; consequently, it must also focus its attention on the design and operation of AML/CFT prevention procedures.

Vulnerabilities and risks.

The vulnerability of the life insurance sector has been assessed by the EU SREP as low or moderate and is in any case low in the case of ML for non-life insurance. In this regard, the FATF has also consistently affirmed the lower inherent risk of the sector when compared to other financial sectors.

Threats would stem mainly from the areas of economic crime and tax evasion, with no terrorist threats linked to these activities having been detected.

In the case of Spain, the data show that, despite the volume of transactions, the sector presents a low **inherent risk** of being used by money laundering or terrorist financing networks. This lower risk stems primarily from the lack of flexibility offered by most products of this type, where the payout depends on a verifiable event that may occur in the long term, such as death or retirement.

Money laundering requires a deep understanding of the sector and of related products that could facilitate anonymity, such as investment-linked services ("unit-linked[30]"). For terrorist financing activities, the scenario is less likely, and the knowledge and planning required to use the sector for such purposes, as well as the lack of immediate availability, make its use for terrorist purposes unfeasible, although some isolated transactions have been detected.

Notwithstanding the above, 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 (associated with stakeholders, associated with premiums and associated with employees), with single-premium life insurance and unit-linked products being the main risk products; however, in the Spanish case, the already low risks are mitigated by the due diligence measures applicable to the sector.

For its part, **residual risk** is characterised by the existence of strong regulation, accompanied by the corresponding control and supervision, both in the prudential sphere and in the area of ML/TF prevention. Additionally, the sector has a high level of awareness of both prevention obligations and potential risk operations, through, amongst other things, the documents issued by the regulator.

The sector's legal obligations include the development and implementation of internal control policies and procedures for ML/TF prevention, which involve the analysis and approval of their own risk assessments at the entity level and are applied in the corresponding due diligence measures. The adequacy and correct application of this risk-based approach applied by institutions is duly monitored both by the external expert's own assessment, as required by the regulations, and by the sectoral supervisor.

In its dealings with the sector and through the inspection of institutions' anti-money laundering systems, the DGSFP has been emphasising the importance of the responsibility that internal audit and compliance functions must assume in ensuring the proper functioning of such systems.

Conclusion.

The insurance and pension funds and schemes sectors, in general, have low inherent risks that may be moderate in relation to certain specific products, particularly single-premium life insurance and international unit-linked investments.

In any event, the application of AML/CFT regulations to the highest-risk products and entities, combined with the awareness-raising, supervisory and enforcement activities carried out by the competent authorities, leads to the inevitable conclusion that the sector in question poses a **low** residual risk in our country.

[30] Investments on behalf of the insurer in units of collective investment undertakings and other financial assets.

d) Investment services, collective investment undertakings and management companies.

Activity, context and regulatory framework.

Royal Legislative Decree 4/2015 of 23 October, approving the consolidated text of the Securities Market Act, regulates the financial instruments existing in the Spanish market. Specifically, it defines these instruments as negotiable securities issued by persons or entities, whether public or private, and grouped into issues. Any right of a financial nature, whatever its name, which by virtue of its specific legal structure and transfer regime is capable of being traded on a generalised and impersonal basis on a financial market, shall be considered a negotiable security.

Furthermore, the sector is also regulated by Law 35/2003 of 4 November on Collective Investment Institutions (CIIs) and by Law 22/2014 of 12 November, which regulates venture capital firms, other closed-end collective investment undertakings and management companies of closed-end collective investment undertakings.

These entities are subject to prior administrative authorisation by the CNMV. The authorisation process requires compliance with the obligations set out in the regulations and the issuance of a preliminary report by Sepblac regarding the suitability of the preventive bodies and procedures that the entity being established intends to implement should the requested authorisation be granted. The CNMV is the competent body for the prudential supervision of securities markets and their activities, whilst the supervision of anti-money laundering and counter-terrorist financing is also carried out by Sepblac.

Investment services. In Spain, alongside credit institutions, investment services may be provided by investment services firms (ESIS):

- **Securities firms and agencies**. The difference between the two is that securities agencies cannot carry out investment activities on their own account; therefore, their activity consists of providing investment services to third parties, whereas securities firms may also act on their own account, in addition to being able to provide the underwriting service and the ancillary service of granting credit for securities trading.
  According to data from the CNMV Register, as of 31 December 2019 there were a total of 39 securities firms and 56 domestic securities agencies. In addition, there are some 3,000 EU securities firms and agencies that can use the EU passport to operate in Spain under the freedom to provide services, and a further 65 EU entities with branches in Spain.
- **Portfolio management companies** (SGC). This is a virtually non-existent corporate form, as entities whose main business model is the management of client portfolios have preferred to operate as securities agencies because this is a more flexible type of entity. As at 31 December 2019, there was only one such entity.
- **Financial advisory firms** (EAFs) offer their clients, as their sole reserved activity, financial investment advisory services. They may not carry out deposit or fund intermediation functions. They must hold the requisite authorisation and be registered with the CNMV. They have a broad portfolio of retail clients, although their income comes mainly from advising large investors (€22 billion). As of December 2019, there were 140 EAFs, with total assets under management slightly exceeding €31 billion. Most EAFs deal exclusively with retail clients, whilst 22 of them deal with professional clients.

Collective investment. **Collective Investment Institutions** (CIIs) are financial institutions whose purpose is to invest in shared assets on behalf of a group and to distribute returns to investors based on the collective results. CIUs may be established as **investment funds** or as **investment companies**.

In both cases, is required for a financial institution to act as custodian of the invested funds, but investment funds must always have a management company (MCCIIs), as they lack legal personality, whereas investment companies may manage their own assets or use a management company. Almost all Spanish MCCIIs (investment funds and investment companies) are members of INVERCO, the Association of Collective Investment Institutions and Pension Funds.

a) **Investment funds** can fall into different categories:

- **Investment funds in financial assets**. These belong to a number of investors who subscribe to units in the fund. The units are held in custody by the custodian. This is the main collective investment vehicle. According to data from the CNMV, in December 2019 they had assets of €273.1 billion.

- **Real estate investment funds**. These invest in real estate assets with the aim of generating income from their letting. They are governed by the provisions applicable to financial funds. They must have a minimum of €9 million paid in.

- ***Hedge Funds***. Complex products in which the manager adopts different strategies to maximise returns for fund investors. They are aimed at qualified investors (high net worth individuals, institutional investors, professional entities). Their main feature is that they can invest without the restrictions faced by other funds (all types of assets, diversification of investments and leverage). Consequently, they offer the potential for higher returns, but also a greater risk of losing the investment. According to data from the CNMV, there are 63 open-ended collective investment schemes in Spain.

b) **Open-ended investment companies** (SICAVs). These are public limited companies whose corporate purpose is to invest in financial assets, and whose shareholders are the investors themselves. They require a minimum of 100 shareholders and €2.4 million. They are subject to a 1% tax rate. In December 2019, there were 2,600 SICAVs in Spain with assets of €28.366 billion, although their number has been declining in recent years.

Therefore, **collective investment undertaking management companies** (MCCIIs) are public limited companies that administer and manage the aforementioned investment funds and companies, acting in the interests of unitholders and shareholders. They may also act as administrators and managers of venture capital funds. SGIICs are subject to various requirements and must publish certain specific information for each investment fund (documents containing information for investors; prospectus; annual report with management accounts and annual accounts; quarterly/half-yearly reports on assets, number of units or shares in issue, securities in the portfolio, etc.).

At the end of 2019, there were 123 investment fund management companies registered with the CNMV, managing assets of around €300 billion in investment funds, mainly in financial investment funds. The sector is highly concentrated, as the three largest SGIICs have a combined share of approximately 40% of total assets.

Venture capital entities: Venture capital funds and companies. Their purpose is to invest temporarily in companies that are neither financial nor property-related, with the aim of increasing their value and obtaining a return on the investment made. They focus primarily on investments in companies in the technology and services sectors. They are managed by closed-end collective investment undertaking management companies (SGEICs) or by MCCIIs.
Management companies are engaged in the administration and management of venture capital funds and the assets of venture capital firms. According to the CNMV register, there are 159 venture capital firms (–SCR) and 215 venture capital funds (FCR). In 2019, investment in private equity and venture capital in Spain totalled nearly €8.5 billion, with 18 transactions exceeding €100 million [31]. International operators accounted for 80% of total investment, with a significant presence in large transactions.

Securitisation fund management companies (SGFT). These are companies that raise funds from clients (investors) in the market to invest in assets derived from credit claims of third parties (originators) through independent financial instruments (such as sub-participations, derivatives or redemption rights). These are complex financial products, but they can allow funds of illicit origin to enter the financial system through the acquisition of rights or securitisation bonds relating to existing loans or risks and, as such, may be used for ML/TF purposes.

Asset-backed securitisation funds are separate estates, lacking legal personality, managed by these management entities, comprising in their assets the financial assets and other rights they pool, and in their liabilities, the fixed-income securities they issue and loans granted by credit institutions. According to the CNMV's Official Register of Securitisation Funds, in December 2018 there were 78 securitisation funds and the number of management companies (SGFT) stood at 7.

Vulnerabilities and sectoral risk.

This sector is characterised by the diversity of its participants and products, which can give rise to different types and levels of risk. Furthermore, account must be taken of the interaction between the sub-sectors and, above all, the direct relationship with other parts of the financial sector, particularly the banking system, which carries significant weight both due to the direct provision of investment services and because a large proportion of the aforementioned entities providing investment services, collective investment services and others belong to banking groups.

Given the nature of the operations carried out by entities in this sector, their volume and the products they offer, the **inherent risk** is considered to be high, with a susceptibility to abuse from various types of **threats,** such as organised crime of various kinds and activities related to financial crimes linked to corruption, tax offences and fraud.

Supervisors, investigators and financial intelligence analysts highlight ML/TF risks associated with these activities, primarily in relation to the following **vulnerability** factors:

- The use of corporate structures that may hinder the identification of the beneficial owner of the securities.
- The use of complex channels that may hinder the tracing of the origin and flow of invested funds and that favour investor anonymity.
- The characteristics and origin of investors and their intermediaries, particularly where they have links to high-risk jurisdictions (*offshore centres*, tax havens, jurisdictions designated as non-cooperative in tax matters or in the fight against ML/TF), as well as clients who are public officials and cases where clients act through nominee holders.

As the EU SNRA points out, although the risk of terrorist financing is low, there is a growing risk of money laundering through capital markets, particularly via providers of such services or through the use of complex, cross-border schemes that facilitate the use of these products for the purpose of concealing the origin of funds and/or their owners.

In any case, when used for money laundering purposes, factors such as the financial viability of the product or the need to ascertain the quality of the investment act as a deterrent to the use of these instruments.

[31] Data from the Spanish Association of Capital, Growth and Investment (ASCRI).

However, when networks can rely on more complex financial planning and use professional facilitators for this type of service, there may be greater appeal for their use for money laundering purposes.

It is worth noting that in recent years there has been a growing awareness within the sector of the risks associated with money laundering and terrorist financing. Beyond regulation and legal due diligence obligations, investment firms and management companies are implementing increasingly comprehensive and complex internal control systems for the prevention of money laundering and terrorist financing. Custodian banks, which are essential to these services, also have preventive duties. Furthermore, the authorities have stepped up their supervision of prevention measures within these entities. Although the level of residual risk is generally considered moderate, this risk level rises to a significant level depending on the characteristics of the type of investment product managed and the profile of its clients.

Conclusion.

ML risks. The inherent risk of these services being used for money laundering activities is high due to the very purpose of generating financial returns on the invested funds and the existence of various vulnerabilities arising from the types of investment products and investment channels that can help conceal the origin of the funds and the identity of the beneficial owner. However, the regulation and supervision of these services, the awareness among sector entities regarding the implementation of AML/CFT 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 **moderate/significant**, depending on the product and the profile of its clients.

TF risks. Unlike ML risks, the very nature of this type of service—which is linked to the financial returns of products—makes it more difficult and less attractive to use for TF purposes and reduces exposure to such risks. Consequently, the residual risk of using securities investment services, the financial services provided by collective investment scheme managers, and securitisation fund management companies for TF activities is considered to be **low.**

e) Mutual guarantee societies.

Activity, context and regulatory framework.

Mutual Guarantee Societies (MGS) are non-profit organisations whose objective is to facilitate and reduce the cost of access to credit for small and medium-sized enterprises by providing guarantees (sureties or other forms, other than surety insurance).

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, who are institutions that provide resources to the MGS. Generally, these are public administrations, chambers of commerce, associations and credit institutions.

MGS have a re-guarantee system, provided through the public company Compañía Española de Reafianzamiento, S.A. (CERSA). The cover provided by this system, in addition to providing financial support for the operations of mutual guarantee societies, promotes the proper management of the risks assumed and improves their quality.

MGS 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.

As of 31 December 2019, there were 18 mutual guarantee companies listed in the Banco de España's Special Register. The guarantees granted by these entities amount to around €1.1 billion per year, and the outstanding balance of guarantees granted exceeds €4 billion.

Vulnerabilities and risks.

Given the nature of the activity and the volume of assets with which the sector operates, the **inherent risk** is considered moderate, since, although lending activity carries high risks, the requirements and internal controls imposed by mutual guarantee societies in order to grant guarantees for loans severely limit any potential access to funds for use in ML/TF purposes by any **threat**.

The overall standard of anti-money laundering systems is considered acceptable. However, this will depend on each company and on its internal control procedures for anti-money laundering and the resources allocated. The sector's association, CESGAR, organises training courses on anti-money laundering for its members, and SEPBLAC has carried out inspections at some institutions. Furthermore, as with other regulated entities, the quality of internal control systems and procedures for ML/TF prevention is assessed using the institution's self-assessment form, the external expert's evaluation, information from the Banco de España as the prudential supervisor, and that held by Sepblac in the exercise of its supervisory role regarding ML/TF.

Conclusion

Mutual Guarantee Societies have moderate **inherent risks**, but their subjection to regulation and supervision regarding the prevention of money laundering and terrorist financing, the adoption and implementation of increasingly rigorous internal policies and procedures by entities in the sector, the involvement of other regulated entities in the guaranteed transaction, the small number of MGS, and the requirement to hold membership to access the financial services they provide, are risk-mitigating factors. All of these factors lead to the **residual risk**, for both **ML** and **TF** operations, being assessed as **low**.

f) Money transfers by payment institutions.

Activity, context and regulatory framework.

Money transfers to or from abroad by payment institutions, commonly referred to as remittances and known internationally by their English acronym MVTS[32], are considered by the FATF and the EU SNRA report to be particularly vulnerable to ML/TF.

A payment service is considered a "money transfer" when it takes place without the involvement of any payment account in the name of the payer or the payee. In this case, the beneficiaries of the funds may receive them directly or through correspondent institutions established at the destination, this being a common practice for cash remittances sent from Spain to family members in the senders' countries, where there is a low level of banking penetration or where this is a traditional method of remittance.

[32] Money and Value Transfer Services.

Most of the customers of this type of institution are immigrants from Latin American, North African and Asian countries, and it is also common for some businesses acting as agents for payment institutions to be run by people of these nationalities, whilst simultaneously carrying out other non-financial economic activities in the same premises, such as so-called 'call shops'.

According to data from the Banco de España[33], the volume of activity of these institutions in Spain amounted to almost €8 billion in 2018 in remittances sent abroad (a figure higher than in previous years) and around €700 million in remittances received from abroad.

The ranking by destination country for remittances in 2018, which is the same as in 2017, is led by Colombia (€909 million), followed by Ecuador (€799 million), Morocco (€662 million), the Dominican Republic (€574 million), Bolivia (€472 million) and Romania (€452 million), with an average amount of €256 per remittance.

The sector comprises 42 payment institutions established in Spain. The sector is highly concentrated, with the ten leading institutions accounting for nearly 80% of the total volume. Almost half of these institutions (18) belong to the Spanish Association of Payment Institutions (AENPA).

Money transfers by payment institutions are subject to specific regulations, without prejudice to anti-money laundering (AML) and countering the financing of terrorism (CFT) regulations. They are subject to authorisation by the Banco de España, following a report from SEPBLAC regarding the suitability of the AML and CFT bodies and procedures. Once authorisation has been obtained, and following registration in the Commercial Register, the entity will be entered in the Special Register of Payment Institutions, in which its agents and branches must also be listed. Prudential supervision of compliance with and maintenance of the conditions of authorisation is the responsibility of the Banco de España, whilst AML/CFT supervision falls to Sepblac.

Vulnerabilities and sectoral risk.

The **inherent risk** in the payment institutions sector is very high for various reasons, related to both endogenous and exogenous factors.

In Spain, there are around 5 million registered foreign nationals (INE data), which facilitates the introduction of cash into the financial system and its transfer abroad through the vast number of remittances sent by emigrants to their countries of origin, amounting to some €8 billion annually.

Payment institutions and their branches and agencies present a higher risk than other regulated entities due to their ability to channel funds, making them an attractive system for transferring illicit funds. This is due, on the one hand, to the fragmentation of their operations, as a large number of customers carry out many small-value transactions, and on the other hand, to the existence of a significant number of small-scale establishments that handle money transfers on an agency basis (each payment institution may have thousands of agents). All of this makes it difficult for the authorities and the payment institutions themselves to exercise adequate control over these establishments, which in previous years has encouraged criminal networks to use agents and small establishments for ML/TF activities.

As investigations, prosecutions and supervisory actions have shown, the money transfer sector is vulnerable to exploitation by various types of **threats,** both for ML and TF activities.

Specifically, there are risks of misuse (or abuse) of the sector for **ML** activities by international organised crime groups, particularly those linked to drug trafficking, fraud and scams ("Nigerian letters"), smuggling of goods and customs-related tax fraud, which may use these money transfer services

[33] Department of Statistics and Special Register of Payment Institutions of the Banco de España.

to channel illicit funds to other countries (mainly in East Asia, South America and some countries in Central Africa).

Potential ML operations do not only involve splitting remittances among multiple senders to destination countries in order to avoid detection (activities known as 'smurfing'), but also involve networks taking control of these agencies (outside the institution), which allows money transfers to be made by impersonating senders or by forging their identities through agents linked to the money transfer networks themselves.

For their part, the risks associated with TF activities are generally linked to jihadist groups, whether national or international, which use these money transfer services as channels to funnel funds—in many cases small amounts of lawful origin—to their recipients in Spain or other countries. The small amounts involved and the legitimacy of the funds make it difficult to detect these TF-related transfers.

Residual risk. The implementation in recent years of risk-based AML/CFT preventive measures in the money transfer sector has led to increased monitoring and supervision of these transactions and the adoption of a series of specific preventive measures by payment institutions, which have resulted in a significant mitigation of risks. These measures include:

- The establishment of stricter customer due diligence obligations. Specifically, Spanish regulations require the identification and verification of the identity of the customer or any person carrying out an occasional money transfer transaction, regardless of the amount (unlike the requirement under the EU Directive – a threshold of €1,000).
- The adoption of specific obligations regarding internal control policies for the prevention of money laundering and terrorist financing (ML/TF) within the sector.
- Requirement for a more rigorous system of systematic reporting through the Mandatory Monthly Declaration submitted by these entities, which requires detailed information on their activities in accordance with different classification criteria.
- Creation of a register of high-risk agents by the sector itself, through its association AENPA.
- Intensification of supervisory actions and sanctioning measures.
- Measures aimed at raising awareness among organisations regarding the prevention of money laundering and terrorist financing.
- Existence of a Catalogue of ML/TF Risk Transactions in the money transfer sector[34].

For their part, payment institutions represent the second-largest group of obliged entities in terms of the number of suspicious transaction reports; specifically, the annual figures for reports from entities in the sector have averaged around 1,000 reports since 2014.

The result has been a substantial improvement in the implementation of preventive measures, with a strengthening and increase in controls and prevention policies, meaning that the risk associated with money transfers by payment institutions has now shifted from high to significant.

Under no circumstances should the risk posed by payment institutions in relation to their customers' activities be linked to the potential risk posed by payment institutions as customers of other regulated entities. In this case, the improvement in the quality and quantity of the internal measures, policies and procedures adopted in recent years by payment institutions, together with the measures implemented by financial institutions, and the growing collaboration between both types of institutions, mean that the overall residual risk has been significantly reduced and is likely to continue to do so.

[34] http://www.tesoro.es/sites/default/files/cor_entidades_de_pago.pdf.

Conclusion.

Money transfer activities carried out by payment institutions carry very high inherent risks of being used for ML/TF purposes. However, these risks have been mitigated through various actions and measures that have yielded very positive results in terms of the overall reduction of risks.

These measures, specifically aimed at money transfer operations, operate across various areas of action: strengthening the prevention regime by payment institutions; intensifying inspections; reporting obligations; engagement with the sector by the authorities and the joint compilation of lists of high-risk transactions; coordination between sector entities and the monitoring of high-risk agents, amongst other actions.

All these mitigation measures implemented in recent years in the payment institutions sector have led to a substantial improvement in the sector's risk profile, which has shifted from high to **significant** for **ML** and **TF**.

g) Other services provided by payment institutions.

Activity, context and regulatory framework.

Payment institutions are those authorised to carry out all or some of the payment services set out in Royal Decree-Law 19/2018, such as deposits and withdrawals from payment accounts; transfers, direct debits and card payments (debit or credit); the issuance of payment instruments or the acquisition of payment transactions; money remittance (discussed in the previous section of this report); payment initiation services or account information services. Payment institutions may not offer deposits or repayable funds, nor issue electronic money, amongst other restrictions on their activities.

As indicated in the previous chapter, the payment institution sector comprises 42 payment institutions established in Spain and registered with the Banco de España; in addition, 413 payment institutions without a physical presence, authorised in other European countries, are permitted to operate.

In Spain, payments are mainly 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 chapter, are in the minority, although they have been expanding in recent years due to their speed and lower cost.

The Payment Services Directive (PSD2) and its transposition now regulate certain services as services to be provided by payment institutions that were not previously subject to a specific framework. Specifically:

- Payment **initiation** services. These services allow a payment order to be initiated, at the user's request, in respect of a payment account held with another payment service provider. Therefore, a customer authorises the provider of these services to access their payment accounts to pay for their purchases or other services directly to the supplier, without the need to use a payment card or for the financial institution to act as an intermediary in the transaction.
- **Account aggregation** services**.** These services consist of consolidating information on balances and transactions from various payment accounts that a single customer may hold with different financial institutions.

The nature of these services means that payment institutions which act exclusively as payment "initiators" or account information "aggregators" need only obtain the customer's consent and the information

necessary to carry out their activities, without needing to act as administrators of payment accounts, as they do not manage their customers' funds.

All these payment institutions are subject to authorisation, supervision and registration by the Banco de España.

Vulnerabilities and sectoral risk.

Payment institutions can instantly transfer sums of money between individuals and entities, and may involve the opening of payment accounts, which present ML/TF risks insofar as vulnerabilities within the institutions can be exploited if appropriate control mechanisms are not established to prevent misuse, and entail significant **inherent risks**.

New technologies have created new markets in which operators offer new instruments based on electronic transactions by the customer, which can be used or ordered from any terminal and anywhere in the world. In parallel, a very wide range of services has been developed that go beyond payment activities.

With regard to payment initiators/account information aggregators, it should be emphasised that they must have the customer's consent to operate and that they act merely as intermediaries between the payee and the customer, without needing to act as payment account administrators. For this reason, the payment initiation and account aggregation activities carried out by payment institutions present clearly lower **inherent risks**, as they do not, under any circumstances, manage client funds.

Furthermore, given that no contractual relationship is required between these service providers and the account manager, the regulations on payment services require, in order to ensure the integrity of funds and the confidentiality of information: 1) that open, common and secure standards be used in communications between both parties, and 2) that all parties adopt security measures in their dealings.

In any event, in accordance with EU regulations, these entities are considered obliged entities for the purposes of AML/CFT and must therefore apply the same preventive controls to payment transactions and payment initiation services[35], thereby further reducing these risks.

Finally, with regard to payment institutions that issue credit and debit cards, a contractual relationship is required with retail customers and entities that make purchases using their cards and authorise the payment institutions to debit the credit institution where those customers hold a bank account, that credit institution being, in turn, an obliged entity. For this reason, the activities carried out by these payment institutions that issue credit and debit cards present lower inherent risks, although they must also establish appropriate control mechanisms to prevent their misuse.

Conclusion.

On the one hand, the existence of payment accounts at certain payment institutions poses a risk of use for ML/TF activities. However, their use for making payments is not widespread, the amounts involved are not significant, preventive measures for customer identification and ML/TF are required, and, in general, they operate with funds from other financial instruments (although some accept cash deposits), which leads to the conclusion that these services present a **moderate** residual risk of being misused (abused) for the purposes of ML/TF.

[35] In accordance with the interpretation of the EU authorities, account aggregation services must also be included as obliged entities.

However, the sector's rapid growth and its link to technological developments are risk factors that must be taken into account and monitored in the coming years.

On the other hand, the residual risk associated with payment initiation operations is **moderate to low**, 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 order 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, they inform the seller that the payment has been initiated.

As for the activity 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 to whom, as obliged entities, the AML/CFT preventive framework applies. However, 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.

Finally, as regards payment institutions that issue credit and debit cards, their residual risk could be described as **moderate**, as they generally operate with funds received from other regulated entities (via direct debits). However, as in the previous case, these are institutions that 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.

h) Electronic money transactions.

Activity, context and regulatory framework.

Electronic money institutions (EMIs) are those authorised to issue electronic money that is accepted as a means of payment by entities other than the issuing institution. Electronic money is understood to be the monetary value represented by a claim on its issuer. This value is stored on an electronic medium, is issued upon receipt of funds of an amount not less than the monetary value issued and is accepted as a means of payment by entities other than the issuer.

Its regulation is established by Law 21/2011 of 26 July on electronic money. The process of establishing electronic money institutions requires a series of conditions, such as a minimum registered share capital of 350,000 euros, a registered office in Spanish territory, and professional and commercial integrity, amongst others. Spanish electronic money institutions must obtain a prior report from SEPBLAC assessing the suitability of the bodies and procedures envisaged, in accordance with the documentation submitted regarding the AML/CFT structure and procedures they will apply once operational.

The procedure for opening branches and providing services freely in Spain by electronic money institutions from other EU Member States is subject to the Banco de España receiving notification from the supervisory authority of the electronic money institution's country of origin.

According to data from the Special Register of Electronic Money Institutions managed by the Banco de España, in December 2019 there were only seven registered EMIs in Spain (in addition, there are EU EMIs that may be operating in Spain without an establishment). With regard to the sector's activity, card top-ups amount to around 500 million euros per year.

Vulnerabilities and sector-specific risks.

The Spanish electronic money institution sector is currently in the process of development. The risk of infiltration by organised crime groups is high, as is the risk of such activity. Given that the payment institution sector is subject to very strict controls, there is concern about the high risk of funds linked to ML/TF operations being channelled into the electronic money sector.

The **inherent risks** of their use for both ML and TF purposes are greater than those of other payment systems. This is because these are instruments which, in some countries, though not in Spain, do not provide data on the holders of electronic money or on the origin of the funds held (unlike debit or credit cards which, in the case of Spain, contain information on the payer and their linked payment account), that they do not require the holder of prepaid cards to hold a current account or similar, and that they allow for rapid conversion into cash.

In Spain, identification is required in all cases at the time of depositing funds, but this identification requirement varies depending on the issuing country, which may set different thresholds, thereby influencing exposure to the risks of their potential misuse, both for money laundering (ML) and terrorist financing (TF) purposes.

As regards **threats**, it has been found that certain electronic money instruments, such as prepaid cards, have been used in various countries to finance terrorist activities, mainly linked to jihadist groups, due to the absence of customer identification requirements below certain thresholds. They are also instruments susceptible to use by threats originating from third countries where acquirer identification systems are less rigorous, which has led to an increase in regulatory restrictions in European countries on transactions involving anonymous instruments.

Spanish regulations require customer identification in all cases for transactions involving electronic money, regardless of the amount (unlike the requirements of EU Directives – a threshold of €150 – and international standards), although simplified measures are permitted in the following cases:

a) Where the electronic money cannot be reloaded and the amount stored does not exceed 150 euros.
b) Where, if it can be topped up, the total amount available in a calendar year is limited to €2,500, except where the electronic money holder requests a refund of an amount equal to or greater than €1,000 during that same calendar year.

Conclusion.

The electronic money institution sector faces very high inherent risks that are common to the entire sector. These risks are even greater in cases where electronic money is issued in other countries and where controls on the holder's identity and on transaction thresholds do not meet the requirements imposed at national level. However, as indicated, the specific regulatory amendments adopted to strengthen the AML/CFT regime in these institutions, the regulatory and supervisory authorities' engagement with the sector, and a substantial increase in the implementation of internal policies and procedures by institutions in the sector—including improved reporting of suspicious activity—have led to a substantial improvement in the sector's risk profile, which has shifted from high to **significant** for both **ML** and **TF**.

i) Currency exchange activities.

Activity, context and regulations.

The professional activity of exchanging foreign currency in establishments open to the public is subject to a specifically regulated authorisation regime, 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 against payment in euros. The regulations distinguish between entities for which this is their main activity and those for which it is an ancillary 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.

According to data from the Special Register of Owners of Foreign Currency Exchange Establishments, as of 31 December 2019, there were 16 entities authorised to buy and sell foreign currency. The remainder, in accordance with data protection regulations, are listed in another non-public register, also managed by the Banco de España, which includes 255 establishments for which the purchase of foreign currency is their main activity.

With regard to the 2,516 establishments where this activity is ancillary and is provided exclusively as an additional service to customers of the main business, the low level of risk involved justifies their exclusion from the status of obliged entities, provided they meet a number of restrictive conditions:

1) That the amount exchanged per customer does not exceed 1,000 euros in each calendar quarter.
2) That the foreign currency exchange activity is limited in absolute terms and may not exceed €100,000 per year.
3) That the foreign currency exchange activity does not exceed 5 per cent of the business's annual turnover.

Foreign currency buying and selling activity is estimated at around €1 billion per year. The four declarants with the highest volume of activity account for 16% of the total.

Vulnerabilities and sectoral risk.

The **inherent risk** of currency exchange operations is very high due to the very nature of the activity.

ML risks. Various national and international analyses (EU SNRA, FATF or EUROPOL) classify currency exchange as a highly vulnerable activity for money laundering. This is due to its close link to the movement of cash and the resulting difficulties in identifying its origin, its traceability, anonymity, ease of transport, etc., which make these transactions particularly attractive for such purposes. The exchange of illicit cash for another currency requires no specific planning, technical knowledge or experience for money laundering purposes.

As highlighted by the EU's Financial Intelligence Unit (FIU) and revealed by investigations carried out by law enforcement agencies, cases have been detected in which criminal organisations control or have infiltrated currency exchange establishments in order to carry out activities involving the conversion of illicit funds into another currency, thereby giving them the appearance of legality.

TF risks. The usual TF schemes of jihadist threats often rely on cash due to the numerous advantages it offers. Subsequently, it is necessary to carry out a currency exchange operation to convert

the funds – obtained in local currencies through various collection systems – into internationally used currencies. The EU SNRA report indicates that conversion operations are particularly attractive to terrorists on the move, as well as for obtaining funding for terrorist groups in third countries.

From the perspective of **residual risk** analysis, in Spain there are requirements and obligations for currency exchange establishments regarding both conduct and the reporting of information to the Banco de España for ML/TF prevention. All entities are subject to authorisation, controls and prudential supervision by the Banco de España and must be registered in the register of currency exchange establishments in order to commence operations.

Furthermore, currency exchange establishments are also subject to compliance with obligations regarding the prevention of money laundering and terrorist financing. Thus, there is a special regime for these establishments that requires enhanced due diligence measures in identifying customers who carry out transactions exceeding €6,000 in a single transaction or cumulatively over a calendar quarter. Awareness of and compliance with these obligations is high among larger entities, although among smaller ones, the level of implementation and awareness does not appear to be as developed.

In any case, the rapid development of technology is playing a decisive role in traditional currency exchange methods. The growing availability of electronic payment methods and apps that enable multi-currency payments is helping to reduce residual risk due to the gradual decline in physical currency exchange transactions, which in turn enables businesses to analyse and monitor transactions more effectively.

Conclusion.

The currency exchange sector carries very high inherent risks of being used in money laundering (ML) and terrorist financing (TF) operations. However, regulatory licensing and registration requirements, the monitoring of their activities by the Banco de España, growing technological development, the application of a strengthened customer due diligence regime, and the sector's entities' high level of awareness of their ML/TF prevention obligations and their supervision mean that the level of residual risk is progressively decreasing, although it is still considered **significant for both ML and TF.**

j) Activities of Crowdfunding Platforms.

Activity, context and regulatory framework.

Crowdfunding Platforms (CPs) connect project promoters seeking funds through the issuance of securities and shares or by applying for loans with investors or fund providers seeking a return on their investment. In other words, CPs have a financial component through which the investor expects to receive a monetary return on their financial contribution.

CPs must be distinguished from other forms of financing also grouped under the term **"crowdfunding"**, as the latter are conducted 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 schemes of the CPs.

In crowdfunding platforms, a group of investors contributes small amounts (up to €2 million) whilst taking on a proportionately high level of risk. Recently, professional investors, known as "accredited investors", have been joining the platform and can contribute up to €5 million. Only business, educational or consumer projects are eligible for crowdfunding; activities reserved for investment services and credit institutions, mortgage-backed loan or credit projects, or financial advisory services are prohibited.

There are **loan-based** crowdfunding platforms, also known as **"lending platforms"**, which allow individuals to apply for a loan to achieve a specific goal. The platform's managers 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 authorised, the project is advertised on the platform to raise funds from lenders.

Investment CPs, 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 CPs. These include projects for the purchase of homes or commercial premises.

CPs platforms require prior authorisation to operate 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, which will be made public following registration in the Commercial Register.

Sector figures: by the end of 2019, there were 28 CPs registered with the CNMV in Spain. The trend since their creation shows a clear increase in investment figures, with annual percentage increases of around 50%. However, the activity of this sector is of very little significance: total funding raised amounted to just €104 million in 2018 and €138 million in 2019, representing a 34% increase, but with fairly small absolute amounts.

Vulnerabilities and sectoral risk.

As highlighted by the EU's SNRA, the use of participatory financing platforms for 'crowdfunding' and 'crowdlending' activities can be considered high-risk activities in terms of both money laundering (ML) and terrorist financing (TF). However, due to their financial nature, PFPs carry a higher risk of being used for ML purposes than for TF operations, owing to 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 money laundering and terrorist financing operations, for several reasons. Firstly, because of the possibility of using illicit funds to make them appear as investments or loans to third-party recipients, who, in turn, may also submit fictitious projects. On the other hand, because CPs can be used by criminal organisations, either through projects submitted by criminal organisations for financing 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 financed with illicit funds.

The ML/TF risk is significantly heightened by the possibility of accepting transactions lacking transparency regarding the beneficial owners of the parties involved and the source of the funds. Consequently, the regulation of the sector—both in terms of business operations and ML/TF prevention—is of great importance.

In this regard, it should be emphasised that there is a lack of regulation regarding AML/CFT in this sector at a global level, meaning that entities can operate with the same degree of lack of control and supervision 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. The failure to include CPs as obliged entities under EU Directives and national legislation must also be considered a significant risk factor.

In Spain, following the definition and regulation of the operation of CPs, due to the risks highlighted, they will be incorporated as obliged entities and made subject to the obligations of the national AML/CFT regime, as well as to supervision.

Conclusion.

ML risks. When assessing the current risk that CPs platforms—whether for crowdfunding, crowdlending or equity crowdfunding—may be used for money laundering activities, the following must be taken into account: (i) current regulation of the sector is limited to prudential matters (definition of CPs platforms, conditions for establishment, registration and operating regime); (ii) they are not subject to anti-money laundering (AML)/countering the financing of terrorism (CFT) obligations, nor are they subject to supervision; and (iii) there are inherent risks that CPs services may be used for illicit purposes. These circumstances are offset by the fact that the number of entities, the volume of funds raised, and the activity carried out by these entities are currently of very little significance. For all these reasons, it is considered that, at present, the residual risk of being used for ML activities is **moderate/significant**.

TF risks. Given that the very nature of CPs operations relates to financial lending and investment activities that require an outlay to subsequently generate a return, TF risks are considered to be lower than those associated with ML. Crowdfunding systems linked to participatory financing procedures would be more susceptible to TF activities involving small sums. Therefore, there is a risk of use for TF purposes that should be considered **moderate**.

(VIII) SECTORAL RISKS: USE OF CASH AND VIRTUAL CURRENCIES.

This chapter analyses separately the ML/TF risks arising from the use of cash and virtual currencies.

a) Use of cash, cash movements and cash-intensive businesses.

Activity, context and regulatory framework.

As described in the chapter on vulnerabilities, cash transactions are very common in our country and, although other forms of transaction are becoming increasingly widespread, a significant number of cash transactions are still carried out involving individuals and, to a lesser extent, businesses.

These transactions and the physical movement of cash have been progressively restricted in Spain. Movements of payment instruments have been the subject of considerable attention from the perspective of ML/TF prevention, and evidence of the use of large amounts of cash in criminal schemes has led to greater restrictions and controls on its use since 2003, the year in which the legal framework governing capital movements and economic transactions with foreign countries, as well as certain ML prevention measures, was adopted.

The need to monitor cash movements has been reaffirmed at European level by various regulations concerning controls on cash entering or leaving the Union, progressively increasing existing obligations and coordination between Member States. Regulation (EU) 2018/1672 extends these obligations to gold, prepaid cards and cash sent by post or transported as goods or via courier services. If cash is sent by other means (unaccompanied cash), the competent authorities shall be empowered to require the sender or recipient to make a declaration of disclosure of information and to carry out checks on any consignment, parcel or means of transport that may contain cash.

At national level, persons carrying out movements of means of payment are subject to a declaration obligation (S1) when they reach or exceed €10,000 when leaving and entering Spain, or €100,000 when travelling within the national territory.

Declarations for cash movements exceeding €100,000 within Spain have been declining in recent years, and the use of cash as a legitimate means of payment is decreasing due to the progressive prevention and control measures adopted at national level in relation to payments made in this way.

Meanwhile, cash movements at the border are following the opposite trend, with continuous growth from 2014 to 2018 in both the number of declarations, which have since risen by 37% (17,000 in 2018), and the amounts declared, which have increased by 40% (€645 million in 2018). This increase in declarations of cross-border cash movements coincides with a decrease in the number of seizures (459 in 2019, 37% fewer than in 2014) and in the amounts seized (€19.2 million in 2019, i.e. 20% less than in 2014).

Furthermore, given the close link between the use of cash and economic crimes, as well as its potential use for money laundering and terrorist financing purposes, tax legislation has imposed limits on cash payments of €2,500 or more for commercial transactions and €15,000 or more where one of the parties is a non-resident and is not acting in the capacity of a business owner or professional, which has undeniable effects on preventing the use of cash for ML/TF purposes.

Vulnerabilities and risk.

The **inherent risks** of cash transactions and their potential use for ML/TF purposes are very high. As already noted, when analysing its vulnerabilities as a means of payment, the widespread use of cash in our country poses a significant risk that our system may be exploited for illicit purposes. The anonymity and lack of traceability of funds prevent verification of their origin (lawful or unlawful), allow their transfer to third parties for unlawful purposes, their laundering through the integration of such funds into the financial system, the acquisition of other illicit goods, or the carrying out of criminal activities.

Particularly serious is the link between cash and certain **threats** posed by organised crime. Networks involved in smuggling, drug trafficking, sexual offences, human trafficking, the smuggling of illegal goods, fraud and scams, etc., carry out their crimes largely through cash transactions, as this is the only way to ensure that the funds cannot be traced by the authorities responsible for investigating and prosecuting such conduct.

Inherent ML risks. The inherent risks associated with the use of cash in ML are very high. Restrictions, greater awareness amongst financial institutions and other regulated entities regarding the use of cash for ML purposes, and the growing difficulties in channelling cash into the national financial system are leading to a decline in its use as a means of payment. These measures also contribute to greater concealment and the outflow of large amounts of cash to third countries through various mechanisms, generally using **high-denomination banknotes**, as these offer an advantage in terms of storage and transport, taking up less space and being easier to conceal.

This **cross-border movement** of funds makes it very difficult for the authorities to trace the proceeds of crime and identify evidence of their illicit origin; furthermore, it allows the process of laundering those funds to be carried out more easily in another country where there is no evidence or suspicion that the cash is the proceeds of an illicit act. Even if the cash is detected in the destination country, the legal and practical implications can frustrate efforts to prosecute offenders and seize the cash.

On other occasions, funds from crimes committed abroad or committed in Spain and subsequently transported abroad are brought into our country with the aim of being used under the guise of legality (for example, by simulating income from commercial activities).

The EU SNRA report also highlights the appeal of cash movements for criminal organisations seeking to launder money of illicit origin. Generally, these individuals carry smaller amounts that are harder to detect and may not be subject to the declaration requirement applicable to individuals transporting €10,000 or more.

These risks of cash being used for money laundering purposes have also been identified in **businesses where there is greater use of cash**, as such entities or professions can be exploited by criminal networks to mix illicit cash with the legitimate cash received by these businesses. Despite the existing limits on the use of cash in commercial transactions (€2,500) described in this section and the awareness of the authorities and the financial sector of such practices, the risk of illicit cash entering the financial system via businesses that regularly handle cash remains high.

Inherent TF risks. As already noted, the special characteristics of cash (anonymity, ease of transport, lack of traceability, etc.) make it a key element in terrorist financing activities.

Cash funds are used to finance individual terrorists and terrorist groups, their cells, their routine living expenses (accommodation, transport, food, etc.), their activities (indoctrination, training, propaganda, use of social media, etc.), their support groups and, of course, the acquisition of weapons and materials for terrorist activities.

As in the case of ML, the movement of cash is of enormous significance, although its detection is even more complex due, on the one hand, to the fact that, as has been highlighted, the **amounts involved in TF are much lower than those for ML** and even below the international thresholds for reporting such movements (generally €10,000) and, on the other hand, because the funds intended for TF are sometimes of legitimate origin.

Similarly, as the EU SNRA also highlights, it has been demonstrated that terrorist groups have used various techniques to move cash across external borders, particularly in the case of larger organisations. This threat is particularly significant with regard to movements from the EU to third countries. Furthermore, cases have been identified in which foreign terrorist fighters have acted as cash couriers to finance their travel and stay in conflict zones.

With regard to **businesses where there is greater use of cash**, cases have been detected of such entities being used for money laundering purposes, and although this type of financing system requires greater technical expertise to launder funds from different sources and to cover initial investment costs, the level of risk is still considered to be significant.

Residual risks associated with money laundering and terrorist financing.

Awareness of the high risk associated with the use of cash has led to the establishment of certain regulatory restrictions to control its use, which are enforced by both the authorities and the private sector. Among other measures, the following are worth noting:

a) Individuals are legally obliged to submit an administrative declaration when carrying out physical movements of cash (or other means of payment), whether within the national territory (€100,000) or across Spanish borders (€10,000).
b) In the period 2014–2018, an annual average of 15,378 declarations of cash movements at the border were received (totalling €531 million annually), and 4,480 declarations of movements within the national territory (totalling €810 million annually, although this figure has been falling significantly in recent years).
c) A limit is imposed on cash payments of €2,500 or more where one of the parties is acting in a business or professional capacity, in addition to payments or deposits made at credit institutions, and of €15,000 where one of the parties is a non-resident.
d) There is an obligation to declare deposits and withdrawals at credit institutions amounting to €100,000 or more €100,000 in cash (or the equivalent in foreign currency). Between 2014 and 2018, there was an annual average of 13,131 cash deposits/withdrawals amounting to €100,000 or more.
e) Funds subject to administrative declaration at the border because they exceed 10,000 euros and which are not declared will be subject to automatic seizure. This task is carried out by customs or police officers when verifying compliance with the declaration obligation. In the period 2014–18, an annual average of over 21 million euros was seized due to this failure to declare.
f) Failure to comply with legal declaration obligations leads to the initiation of the corresponding penalty proceedings, with the applicable financial penalties being imposed. In the period 2014–18, the average annual number of penalties imposed for such breaches stood at 621 per year.
g) Credit institutions must report monthly on the number and value of transactions they carry out cash transactions exceeding €30,000 that are not credited or debited to the customer's account. This

obligation applies to obliged entities that carry out cash remittance transactions exceeding €1,500. In the period 2014–18, the annual average stood at 1,428,600 transactions.

Conclusion.

As indicated, cash movements carry very high inherent risks of ML and TF. However, there is a high level of expertise in this field, which has for years driven extensive regulation, monitoring and enforcement in the area of ML/TF prevention: sectoral risk analyses and the statistical data collected have made it possible to identify patterns, the main geographical points of entry and exit from the national territory, profiles (differentiated by entries and exits, by geographical location…), preferred destinations, routes taken, most commonly used currencies, etc. This has enabled the progressive specialisation of customs and police authorities and the adoption of measures targeted at the highest risks detected, as well as control measures aimed at ensuring proper taxation arising from the ownership and transfer of virtual currencies and the origin of the funds used to acquire them.

All of this has contributed to a continuous reduction in the level of risk of being used for ML/TF operations involving both the movement of cash and businesses with a high use of cash, with various measures having been adopted in this regard.

Cash movements. Despite the numerous measures adopted and the resources deployed, the number of travellers crossing Spain's borders is very high, as is the potential volume of funds transported; this, combined with the inherent risks of cash (anonymity, lack of traceability, ease of transport, etc.), justifies the **residual risk** of **ML** and **TF** associated with cash movements continuing to be considered **high**.

Businesses with regular use of cash. Due to the inherent risks of cash already noted, the risk of illicit cash entering the financial system through businesses with regular use of cash for **ML** purposes is **significant/high**. However, in the case of **TF** purposes, due to the circumstances noted above, this risk is lower than in the case of cash movements, but sufficiently significant to be considered **significant**.

b) Activities involving virtual currencies or assets.

Activity, context and regulatory framework.

The activities and context relating to virtual currencies and assets have already been described in the section on vulnerabilities common to all sectors and activities (Vulnerabilities arising from technological innovations in financial transactions. E.2 Vulnerabilities arising from the use of virtual currencies and assets).

It should, however, be borne in mind that these are digital representations of value issued by the private sector that use cryptography to ensure security in their storage and use. Most rely on the use of a shared ledger known as a blockchain, in which all transactions involving virtual currencies or assets leave a trail visible to all users, preventing tampering but making it difficult to identify the participants in the transactions.

In Spain, there is no obligation to accept them as a means of payment; in fact, according to information from the AEAT, there are very few payments made with virtual currencies and their circulation is very limited. Given that their value fluctuates sharply, they cannot be considered a good store of value or a stable unit of account.

Nevertheless, there have been investment-related transactions due to the high degree of fluctuation in their exchange rates, which led to significant gains by the end of 2017, followed by further declines.

Alongside virtual currencies, there have been efforts to raise funds from investors to finance projects through so-called 'initial coin offerings' (ICOs). The term ICO can refer both to the actual issuance of virtual currencies and to the issuance of various types of rights generally referred to as *'tokens*'. These assets are offered for sale in exchange for virtual currencies or official currencies (e.g. euros). In 2019, Security Token Offerings (STOs) have emerged with a similar objective, although in many cases they are aimed at qualified or high-net-worth investors.

At present, in accordance with official communications issued by the Banco de España and the CNMV, virtual currencies and "tokens" issued in ICOs, where their acquisition or holding takes place in Spain, cannot benefit from any of the guarantees or protections provided for in the regulations relating to banking or investment products. This situation makes them particularly vulnerable to fraud, price manipulation or other illegal activities, with criminal activities involving pyramid schemes having been detected.

In Spain, there are tax obligations relating to any capital gains realised on the buying and selling of cryptocurrencies and virtual assets; in this regard, the AEAT has highlighted the risk of money laundering stemming from tax offences that underlies the trading of crypto-assets. To address this threat, the AEAT has been promoting the use of new technologies for gathering and analysing information across all types of networks, and its guidelines contained in the 2020 Annual Tax and Customs Control Plan expressly include the implementation of appropriate control measures to ensure the correct taxation of these transactions, as well as the origin of the funds used in their acquisition.

The National Fraud Investigation Office, part of the AEAT's Financial and Tax Inspection Department, has carried out a comprehensive investigation project, identifying more than 77,000 taxpayers who have carried out transactions involving crypto-assets.

Alongside these measures, the AEAT has also reminded taxpayers of their obligation to declare the profits and capital gains generated from trading in crypto-assets.

However, despite these tax obligations on capital gains arising from the buying and selling of virtual currencies and assets, there is no prudential regulation or regulation regarding anti-money laundering (AML) and countering the financing of terrorism (CFT) obligations for entities providing virtual currency conversion or management services to the public.

Nevertheless, the Fifth Directive (EU) 2018/843 on the prevention of ML/TF, which is due to be transposed shortly, already includes a legal definition of "providers of services for the exchange of virtual currencies for fiat currencies" and of "providers of electronic wallet custody services". Both types of service providers must be regarded by Member States as obliged entities for AML/CFT purposes and be subject to registration and supervision by national authorities.

This progressive regulation of entities engaged in these activities has also been reflected in the FATF's inclusion of new international standards for the global network, which include a registration or licensing requirement for the entities mentioned in the previous paragraph, as well as for those acting as providers of exchange services between virtual currencies and those providing financial services for the issuance or sale of virtual assets equivalent to securities (*security tokens*).

A specific type of virtual asset is the so-called **'stablecoin',** which is one whose value remains directly or relatively stable in relation to an underlying asset or reference basket. In these cases, its value may be linked to the value of a fiat currency or a basket of assets that may include fiat currencies, virtual currencies, investment assets and/or commodities. Although their implementation is still very limited, in recent years international projects have been developed that may prove highly significant in the future.

Vulnerabilities and sectoral risk.

The **inherent risks** of virtual currencies being used for money laundering and terrorist financing are very high. Despite their limited use in our country, the growing global expansion of virtual currencies and assets has led to a significant shift in certain criminal methods and, consequently, in specific money laundering and terrorist financing processes, meaning the system is increasingly vulnerable to being exploited by any type of threat for these purposes.

Access to virtual currencies is straightforward; there is no need for a provider or intermediary – all that is required is a virtual or electronic wallet to store keys and to exchange legal tender for virtual currency. This makes it possible to quickly open anonymous virtual currency accounts into which illicit funds can be deposited, and to split and move those funds very rapidly within the virtual environment.

Until the next amendment to Law 10/2010 of 28 April, providers of these services are not obliged to carry out any form of customer due diligence or to keep customer records, although in some cases this is already standard practice. However, the regulation of these service providers will not be able to prevent virtual currency transactions taking place outside their scope.

The growing existence of new secondary markets for trading on derivatives exchanges and the exchange of virtual currencies for other virtual currencies makes it more difficult to identify the holder and to track illicit funds. The authorities face different challenges due to the risks posed by their use for potentially fraudulent activities and the growth of potential unregulated sources of funding.

Specifically, funds derived from criminal **activities** such as extortion, fraud, tax evasion, terrorism, and trafficking in drugs, arms or human beings can be shielded through the use of virtual currencies. Consequently, criminal networks are increasingly demanding illicit payments in virtual currencies, either by requesting these assets or currencies as a means of payment in cases of blackmail and extortion, or as compensation for a criminal operation. It is also common for them simply to convert the illicit funds obtained into virtual currencies.

These illicit funds in virtual currencies can be transferred to other holders within the criminal network or successively converted into other virtual assets (tokens) or into different types of virtual currencies, some of which are more opaque than others (there are virtual currencies that can only be acquired with other virtual currencies), making them even more difficult to trace. In turn, funds in virtual currencies can be used by criminal organisations as a means of financing new criminal activities.

Among these threats, the use by criminals and organised crime of the deep web for trafficking all kinds of goods and providing illicit services stands out, as does the use of cryptocurrencies as a means of payment.

Given the maximum level of opacity surrounding their holders and transactions (for example, through so-called “dark wallets” or privacy-enhanced coins such as “Zcash”) and as they can be exchanged in transactions that have no direct link to legal or territorial jurisdictions, nor to entities subject to AML/CFT obligations, the risks of them being used for these activities are very high, although quantitatively, only a few isolated transactions have been reported in our country.

The risks posed by the so-called “stablecoins” currently in circulation are no different from those associated with virtual currencies and assets, but we must remain vigilant regarding future designs of “stablecoin” projects that have the potential to reach a very large customer base and, consequently, achieve widespread adoption—the so-called “global stablecoins”.

In that case, preventive controls should be stepped up to ensure that their increased use is not accompanied by a rise in the risk of money laundering and terrorist financing. These risks may arise from:

- Designs that allow for unrecorded anonymous transactions (such as those carried out on encrypted applications or on the dark web).
- Anonymous users (for example, a user whose address is not linked to their real identity).
- Transactions between private individuals (i.e. without the intermediation of a duly registered or authorised provider, or which facilitate cross-border payments without clarifying how they will be supervised).

Conclusion.

For all the reasons set out above, the inherent risks of using virtual assets or currencies for ML/TF purposes are clearly high. The lack of appropriate regulation, the ease of access to this type of asset, the opacity of its operation and the anonymity of the parties involved, the cross-border nature of the phenomenon, the high risk of loss of invested capital, potential illiquidity issues, the extreme volatility that may affect this type of asset, and the possibility that the information provided may be inadequate are risk factors that must be taken into account.

However, in Spain, given that the total volume in circulation is low, their limited use as a means of payment, and the fact that the figures for the issuance of digital tokens are very small and subject to supervision by the CNMV, the actual risk of their use for ML/TF purposes should be considered mitigated in relation to the extremely high inherent risk.

Taking all this into account, **virtual currencies** pose a **significant/high** risk for use in both **ML** and **TF** activities, and this has been observed in some investigations analysing the use of virtual currencies and assets for these purposes. However, it must be reiterated that detecting and monitoring these transactions is difficult, which has only allowed for the identification of isolated cases and, for the time being, figures of little significance. In short, this is a sector that must be subject to close monitoring and greater regulatory restrictions and controls in view of its emerging risks and progressive growth.

These risks are lower when it comes to the use of **virtual assets:** although they involve a significant level of risk for **central banking** activities, they should be regarded as **moderate** for **financial technology** activities, since the very nature of this type of investment service is linked to the potential financial returns of products, which entails greater management complexity and lower risk exposure when used for financial technology purposes.

(IX) SECTORAL RISKS: NON-FINANCIAL ACTIVITIES AND PROFESSIONS.

The Spanish non-financial sector encompasses various activities regulated in accordance with different requirements determined by their specific legislation. For the purposes of this analysis, we proceed to analyse the potential ML/TF risks of non-financial transactions, both those expressly identified by the FATF and by the 5th (EU) Directive:

a) Money orders via postal services
b) Loan brokerage activities
c) Real estate transactions
d) Auditors, external accountants and tax advisers
e) Activities carried out by notaries
f) Activities carried out by land, commercial and chattel registrars
g) Specific activities carried out by solicitors and other professions
h) Provision of corporate services to third parties
i) Gaming sector
j) Professional trade in jewellery, precious stones and metals
k) Buying and selling of works of art and antiques
l) Professional trade in other high-value goods
m) Investment in tangible assets
n) Cash-in-transit services provided by private security firms

	NON-FINANCIAL ACTIVITIES AND PROFESSIONS	
	Subtotal	Total
Casinos and gambling		105 (a)
Casinos	53	
Lotteries and games of chance	52 (b)	
Legal professions		4,074
Notaries	2,794	
Registrars	1,280	
Solicitors	(c)	
Auditors		2,210
Accountants & Tax Advisers		1,215
Corporate service providers	(d)	
Real estate sector		4,219
Dealers in jewellery, precious stones and metals.		1,537
Art and antiques		2,965
……Galleries and antique dealers	2,845	
Auction houses	120	

(a) Casinos and lottery and gambling companies only.
(b) Number of companies (not points of sale).
(c) General Council of the Bar. 154,583 lawyers in Spain. The figures for members carrying out activities provided for in the AML/CFT Act (letters ñ) and o) have been estimated from surveys conducted by the General Council; some 400 firms or individual lawyers have declared that they carry out these activities.
(d) Further details regarding the forthcoming launch of the Register of Corporate Service Providers and Trusts.

a) Postal services.

Activity, context and regulations.

A postal money order is a service whereby payments are made to natural or legal persons on behalf of and at the request of others, via the postal network. In accordance with the law, this service is considered a financial service of general economic interest and must be provided, either directly or through third parties, by the operator designated by the State to provide the universal postal service, which is carried out by the Post Office in accordance with the regulations governing the provision of postal services.

This money order service can be provided both within Spain and abroad, and payments can be made either in cash or by cheque. Payments into current accounts are only possible within Spain. The maximum amounts permitted may not exceed €2,500.

Unlike banks or payment institutions, which also provide transfer services, postal services, when carrying out money order and transfer activities, are not considered financial institutions for the purposes of Law 10/2010 of 28 April. However, they are obliged entities and are therefore required to comply with the preventive obligations established by this Law and its Regulations.

Vulnerabilities and sectoral risk.

Although the **inherent risk** of money transfers for ML and TF purposes is initially high, the difference between money transfers via postal order and those carried out by other means is that the stages of the postal order service management process are necessarily carried out through the staff, resources and facilities of the public postal network managed by Correos, which considerably reduces the endogenous risk factor of its use for ML/TF purposes, notwithstanding the fact that, for technical reasons, certain stages may be contracted out to third parties.

This represents a significant reduction in risk exposure and makes it more difficult for criminal organisations to use the service for money laundering purposes, particularly in relation to postal orders originating from and destined for the service provided by Correos itself, and with regard to potential risks of networks accessing these services for ML/TF purposes, as is the case with other types of funds transfer services.

Conclusion.

The postal money order sector faces high inherent risks, particularly in activities linked to money laundering. However, the provision of the service by a public operator, the specific regulatory amendments approved for payment institutions that are applicable to postal money orders with a view to strengthening the prevention regime, the engagement of supervisory authorities, and the effectiveness of internal policies and procedures regarding ML/TF prevention, imply a substantial reduction in the sector's risk profile. This risk should be considered **low** for use in **ML** operations and for all postal money orders originating from and destined for the postal service provided by Correos itself, but it should be considered **moderate** in relation to possible links to **TF** operations in postal money orders where the money orders originate from and are transferred via other operators.

b) Credit intermediation activities.

Activity, context and regulations.

These are natural or legal persons whose work does not involve granting financing but rather acting as intermediaries to secure such financing. Credit intermediaries are those natural or legal persons who, on a professional basis and without being lenders themselves, offer credit agreements, provide advice or conclude credit agreements on behalf of and for the account of a lender.

This is a professional activity which, when carried out with the necessary levels of transparency and professionalism, can be of great benefit to consumers by enabling a more efficient search for the credit and loans available on the market. This intermediation activity may take place in the field of consumer credit or mortgage credit and is subject to a specific regulatory framework.

To ensure a high level of protection for consumers and users, guaranteeing transparency and fair competition, firms must comply with numerous pre-contractual information obligations towards the borrower and adhere to rules regarding the communication of changes in interest rates or the advertising they produce.

Professionals may carry out their activities on behalf of a single lender or several. When providing advice, this may be independent; in this case, the range of products is wider and the rules to prevent conflicts of interest are more stringent.

In the case of consumer credit, the activity of intermediation is not subject to a licence requirement and is therefore not subject to registration. However, in the case of mortgage lending, intermediation is a reserved activity, and intermediaries must be registered with the Banco de España or the body designated by each Autonomous Community, where they operate exclusively within the geographical area of an Autonomous Community, to which their prudential supervision is entrusted. Credit intermediaries may operate on the basis of the European passport principle, through a subsidiary, branch or under the freedom to provide services.

The former register of mortgage lenders and credit intermediaries managed by the Spanish Agency for Consumer Affairs, Food Safety and Nutrition had 155 individuals registered. Under the new Law 5/2019 of 16 March, it will be the Banco de España or the body designated by each Autonomous Community that carries out this registration function.

Vulnerabilities and sectoral risk.

The **inherent risk** of ML/TF activities occurring in the sector is assessed as moderate due to the nature of its operations, which carry a certain degree of exposure as they involve lending transactions that could allow funds to be repaid using illicitly obtained assets or, indeed, the non-repayment of the amounts granted and their use for activities linked to TF, as already described in other sections of this document devoted to credit activity.

However, the loan transaction is not carried out by the intermediary itself but by a lender, usually a financial institution, thereby strengthening anti-money laundering and counter-terrorist financing controls.

The **residual risk** in the sector is determined by the high level of regulation, control and supervision of the activity at national level, both in terms of prudential supervision, in the case of financial institutions, and in terms of AML/CFT prevention.

This regulatory and monitoring regime by the authorities is complemented by the sector's existing awareness of its AML/CFT obligations, potential risk operations and compliance with the legal duties of the institutions themselves to develop and implement internal control policies and procedures for AML/CFT prevention.

Conclusion.

The loan brokerage sector faces medium-level inherent risks; however, these risks are mitigated by various factors, such as the involvement of financial institutions in the transactions—which are ultimately responsible for granting the loan and setting its financing terms—following the implementation of the relevant measures required by AML/CFT regulations, thereby creating a dual preventive control system. This contributes to a reduction in the inherent risk that the loan brokerage sector faces of being used for money laundering operations and allows the **residual risk** in **ML/TF** operations to be assessed as **moderate-low**.

c) Transactions in the real estate sector.

Activity, context and regulatory framework.

The real estate sector is an economic sector of great importance in Spain for many reasons: for the resources it mobilises and, in turn, generates in other sectors such as construction or finance; for encompassing a wide range of economic transactions; and for having a significant social and labour market impact. Misuse of the real estate sector can lead to serious economic destabilisation and, consequently, affect the country's institutional and political stability.

According to data from the National Institute of Statistics (INE), property sales figures at the end of 2019 showed a decline compared to 2018, although they recovered at the start of 2020. In January, the total number of properties transferred and registered in the land registers was 184,688, a decrease of 7.7% compared to the same month of the previous year. Registered property sales (47,000) fell by 2.6% compared to January 2019.

In recent years, there has been a shift in the property market following the crisis in the sector, with house prices rising and property once again being seen as a safe, stable and highly profitable investment, attracting both domestic and foreign consumers and investors. Furthermore, there is a growing property rental market that is highly attractive to investors and private individuals seeking a means of generating immediate returns on their property assets.

This is a sector regulated by various authorities (at national, regional and local levels) and aimed at a global market, both domestic and international. Access to the property sector is not subject to any national or regional authorisation, as it is an activity that may be freely undertaken. However, the sector is subject to state regulations as an economic activity (as set out in the Land Law, the Condominium Law and the Urban Leasehold Law) and to technical regulations on building planning; in addition to the requirements and authorisations imposed by the urban development plans of autonomous communities and municipalities.

The range of professionals involved in the property sector is wide: from businesspeople and **commercial companies** engaged in the purchase of land and buildings for subsequent sale and/or letting, to **property developers** who purchase land and buildings for development, subdivision, construction or refurbishment, either directly or through third parties, for subsequent sale and, nowadays, also for letting.

In recent years, new operators have emerged in the real estate sector linked to property rental activities, such as Listed Real Estate Investment Companies (**SOCIMIs**), whose main activity is direct or indirect investment in urban real estate assets for rental purposes, including residential properties, commercial premises, care homes, hotels, garages and offices, amongst others. This nature and their operations in the property market present risks from a money laundering perspective similar to those of other operators in the sector, which is why they are soon to be included as obliged entities in the field of ML/TF prevention.

The objective of SOCIMIs is the acquisition, development and refurbishment of real estate assets such as buildings, flats, commercial premises, shopping centres or offices, to offer them for rent on the market. In recent years, this sector has undergone significant expansion, with a very substantial turnover and profit volume, and it benefits from a favourable tax regime, making it highly attractive from an investment perspective, although it remains a sector with a high level of concentration amongst a small number of companies.

Their involvement in the property market means that, like other entities operating in this sector—including those specialising in property lettings—they are subject to preventive obligations regarding their clients and transactions, given the risks involved in receiving funds of potentially illicit origin with a view to channelling them into the financial system.

On the other hand, there is the role of **the intermediary in** property **transactions** (property agent or agency), whose function is to manage a sale or purchase transaction on behalf of a client, resolving legal issues and, in many cases, financial matters as well. At present, no specific qualification is required to carry out this intermediary activity, which leads to fragmentation within the sector, partially mitigated by the existence of professional bodies such as the General Council of Official Associations of Estate Agents.

In 2012, in response to the economic crisis and the progressive decline in the value of real estate assets, the Asset Management Company for Assets Arising from Bank Restructuring (SAREB) was established. This has enabled the segregation of toxic or problematic assets from credit institutions requiring public aid, with the aim of removing them from their balance sheets. This portfolio of real estate assets carries certain inherent ML/TF risks, which are managed as the properties are sold. As indicated below, SAREB is subject to obligations regarding the prevention of ML/TF.

Preventive regulations in Spain go beyond those established in international standards by stipulating that "property developers and those who professionally engage in agency, commission or brokerage activities in the sale and purchase of real estate" are also obliged to comply with AML/CFT prevention measures.

Vulnerabilities and sectoral risk.

Due to the specific characteristics of the property market, this sector carries a **high inherent risk** and has traditionally been a target for money laundering activities. This is mainly due to the difficulties in identifying the ultimate owner of the property and the source of the funds, as well as the immediate use and appearance of legality that funds of illicit origin can be given within the real estate sector, and also to the inherent characteristics of real estate: it is durable, profitable, appreciating in value and necessary.

The real estate sector has been identified in the EU's National Risk Assessment (EU SNRA) as a sector highly vulnerable to ML/TF activities. Transactions involving real estate assets are considered a common channel for organised crime networks to invest funds of illicit origin and an attractive investment for proceeds from crimes committed both abroad and domestically.

This high exposure to risk varies depending on geographical areas and the profiles of those involved in the activity. Numerous investigations and legal proceedings have also highlighted a greater degree of links to threats arising from organised crime of various kinds: drug trafficking, criminal activities related to corruption, tax fraud, or international money laundering networks seeking to legitimise illicit assets obtained in other countries.

The sector's inherent risk of being used as a vehicle for money laundering is linked both to its endogenous and exogenous risks, as well as to a series of vulnerabilities:

- Ownership of real estate can take many different legal forms, both domestic and international, including forms of co-ownership based on time or space.
- It is common for real estate to be held through mere asset-holding or special-purpose companies or through legal structures that are sometimes not incorporated in our country.
- The valuation of real estate is highly subjective, linked to factors not directly derived from the property itself.
- It is a sector vulnerable to criminal behaviour related to bribery or other forms of corruption involving public officials linked to the sector.
- As highlighted by the EU SNRA, organisations of very different sizes and levels of awareness regarding ML/TF risks operate in this sector.

Furthermore, the sector's entities themselves face a high **endogenous** or **intrinsic risk** of being exploited by criminal groups, which may mean that these groups could become property developers or estate agents, involved in both sales and rentals; in this regard, it should be noted that the open-access regime for operating in the sector makes it difficult to detect such activities.

With regard to **exogenous risks**, the EU SNRA report notes that the heterogeneity and number of entities involved do not simplify the implementation of controls, the understanding of applicable obligations, or the supervision of the sector. Larger entities have been adopting measures in line with their ML/TF risks, developing risk analyses and assessments, internal manuals, alerts, information tools and training. Conversely, in smaller entities, the likelihood of them being set up for the purpose of legitimising assets is higher, and the level of awareness of the risk of being exploited by organised criminal groups—and the adoption of measures accordingly—is lower.

There are money laundering risks linked to the type of transaction, the means of payment used, or the parties involved in the property transaction. These types of risks can be detected through a series of indicators, including:

a) Risks associated with the transaction. For example: cases where the purchase price differs significantly from the real value of the property; instances involving successive transactions with very significant price changes; transactions formalised exclusively by private contract, amongst others.

b) Risks associated with the means of payment used. For example: the use of cash or negotiable instruments that allow for anonymity; payments made in instalments over very short periods of time; property rental payment systems; loans secured by cash or assets deposited abroad; financing with funds originating from countries considered tax havens or high-risk territories; the use of an intermediary account, bridge account or financial product held by the professional intermediary.

c) Risks associated with the parties involved: cases of individuals or entities from high-risk territories; PEPs; customers with no apparent sufficient financial capacity; recently incorporated legal entities whose assets are considerably lower than the transaction amount or which are involved in a transaction with no apparent connection to their business activity or corporate purpose; intermediaries attempting to conceal the identity of the beneficial owner, particularly if they originate from a foreign country, amongst others.

In order to address these risks, a culture of risk prevention has been implemented in large property developers and estate agents, but part of the sector—particularly smaller firms—could improve their awareness of ML/TF risks. The sector has a high level of understanding of its obligations and of ML/TF risk operations and maintains a detailed Catalogue of Risk Operations[36].

In Spain, the entire sector is subject to the AML/CFT regime, which includes the obligation to apply due diligence measures and enhanced measures in relation to certain customers (persons holding public office, non-resident customers, certain companies, etc.), as well as measures to verify the source of funds, identify the beneficial owner, impose restrictions on the use of cash, and supervise entities, amongst others.

Consequently, entities in the real estate sector, alongside clear progress in the implementation of internal policies and procedures and in raising awareness and training their agents, have seen an increase in the number of suspicious activity reports in recent years, which now stand at around 45 reports on average, compared to 13 reports in 2013.

There are, in turn, other factors that mitigate the inherent risk in the sector since, in addition to the preventive measures adopted by the entities themselves, other obliged entities involved in property transactions have established their own AML/CFT control procedures: notaries, land registrars or credit institutions, all of which have implemented specific AML/CFT prevention measures and units; consequently, the interaction of various obliged entities in property transactions contributes to the mitigation and subsequent reduction of risk.

Conclusion.

Transactions in the real estate sector carry a **high inherent risk** of money laundering, from both an endogenous and exogenous perspective. It is a traditionally vulnerable and high-risk sector, which is attractive for money laundering purposes and does not require specialised technical or financial knowledge. In recent years, the existence of money laundering schemes associated with both small and large real estate transactions has continued to be demonstrated.

Developments in the sector have led to the emergence of new operators who may be involved in money laundering activities, such as entities operating in the rental market, which have already been incorporated into the EU Directives as obliged entities, or those companies created specifically for investment in rental property assets, which must be included as obliged entities due to the risk being similar to that of other operators in the property sector.

In the face of these inherent risks, it is worth highlighting the increase in mitigation measures adopted by entities in the sector, as well as a greater understanding of the types of money laundering associated with geographical areas, parties involved, types of transactions, payment methods and associated financial transactions; all of which enables entities and operators in the sector to identify and, consequently, reduce the risks of transactions linked to money laundering.

The involvement of other regulated entities in property transactions—primarily credit institutions, notaries and land registrars—who are required to fulfil their preventive obligations, also helps to control and mitigate

[36]https://www.tesoro.es/sites/default/files/cor_sector_inmobiliario.pdf.

the ML/TF risk in the real estate sector.

ML Risks. Despite the measures and mitigating factors described, the high inherent risks of the sector, both endogenous and exogenous, the traditional and frequent use of the real estate sector in money laundering operations, as evidenced by investigations and court cases, and the diversity of operators and intermediaries who may participate in each transaction, helping to conceal the beneficial ownership of the properties and the origin of the funds, mean that, despite awareness of the risk and the widespread adoption of preventive mitigation measures, the residual risk of ML activities in this sector remains **significant**.

TF Risks. For their part, TF risks linked to real estate transactions are clearly less significant than in the case of ML, as the very nature of real estate assets and the sector's financial transactions makes it more difficult to dispose of funds immediately and to use the small amounts typical of current TF operations in our country. Nor have any real estate transactions linked to the financing of terrorism or terrorists been identified in our country; therefore, the existing TF risk is considered to be **low/moderate**.

d) Auditors, external accountants and tax advisers.

Activity, context and regulatory framework.

Within this section, a distinction must be made between different types of professional activities:

Auditing (both statutory and voluntary) consists of the review and verification of annual accounts, as well as other financial statements or accounting documents, prepared in accordance with the applicable financial reporting framework, provided that the purpose of such activity is to issue a report on the reliability of those documents that may have legal effect vis-à-vis third parties. This activity, regulated by the Audit Act, must necessarily be carried out by an auditor or an audit firm, who will issue the corresponding report subject to the requirements and formalities established in that Act.

The purpose of the regulations on the audit of accounts is to establish sufficient safeguards to ensure that the annual accounts or any other financial information that has been verified by an independent third party (the auditor) is accepted with full confidence by interested third parties. The effectiveness of these professionals' work is therefore based on their independence from the audited client. The Audit Act sets out very strict criteria to ensure independence, which are subject to supervision and control by the Institute of Accounting and Auditing (ICAC).

Auditors must meet a number of requirements in order to practise their profession, in addition to being registered with the Official Register of Auditors (ROAC) of the Institute of Accounting and Auditing and providing financial security. The requirements include having no criminal record for intentional offences, having obtained the relevant authorisation from the ICAC, and passing a professional aptitude examination organised and recognised by the State. Audit firms or auditors authorised in other, as well as those authorised in third countries, on a reciprocal basis.

Their work is essential for the confidence of financial markets and clients.

The sector's turnover in Spain[37] in 2018 was €692 million (€663 million in 2017), with around 61,000 annual audit engagements reported to the ROAC. Although there are some 2,300 individual auditors and 1,400 audit firms, in 2018 only 2,138 providers reported turnover (931 individuals and 1,207 audit firms). This sector is characterised by a high degree of concentration, given that the four major professional accountancy firms employ a large number of auditors and account for approximately 65% of the sector's total revenue.

External accountants and tax advisers are privately accredited professionals who offer services similar to those of an auditor, specifically through reports prepared by expert professionals. In this regard, the Register of Accountants has been established following the signing of a collaboration agreement between the General Council of Economists and the Institute of Chartered Accountants. This register brings together and represents a group of professionals who are highly qualified in accounting and have previously met pre-established requirements. According to figures from Sepblac, there are around 1,200 such professionals (2019).

Furthermore, the Spanish Association of Accounting and Business Administration has also established an accreditation scheme in the field of accounting with the aim of formally recognising the technical competence of accounting professionals and maintains a register of these experts.

Vulnerabilities and sector-specific risks.

In line with the findings of the EU SNRA, in Spain, the professions of external accountants, auditors and tax advisers are well organised and regulated, but exhibit certain shortcomings in terms of controls and risk management.

There is a clear **inherent risk** of misuse (abuse) of the sector, as criminal organisations find it attractive and profitable to use professionals of this nature to provide technical professional services and to lend an appearance of legitimacy to their corporate structures and the financial and commercial activities carried out by them.

In the case of external accountants and tax advisers, this inherent risk of the sector being exploited by criminal structures and organised groups is greater than in the auditing sector due to its endogenous risks; situations where these professional sectors are infiltrated for criminal purposes are more likely, not only to plan, advise on and facilitate money laundering activities (and to a much lesser extent TF) with funds derived from illicit activities that must be placed on the market, but also to carry out similar functions that enable the commission of other economic crimes, such as fraud of various kinds. Furthermore, the competition within this professional sector of external experts and advisers, and the ambiguous interpretation of the professional relationship of trust with the client, mean that these professionals are exposed to a greater risk.

For its part, the risk in the audit sector is lower insofar as these are services which, for the most part, are not freely sought by the auditee but are required by regulation, and which are specifically intended to verify the accounts prepared by the entity. However, risk in this activity does exist, in that, once a clean audit report has been obtained, the appearance of legitimacy of the activity and the funds it generates is enhanced.

[37] 2018 Report of the Institute of Accounting and Auditing and 2018 Annual Report of the Institute of Chartered Accountants.

The convergence of these risks justifies the inclusion of these professional categories as obliged entities in the field of ML/TF prevention, requiring them to apply preventive obligations. However, there is a gradation in their levels of compliance depending on size, turnover and number of employees, which reduces the residual risk.

Furthermore, as also indicated by the EU SNRA, greater difficulties have been identified in these sectors compared to other non-financial sectors with regard to controls and risk management, in particular concerning the application of obligations relating to the beneficial ownership of their customers and the identification of the source of funds.

Conclusion.

The services provided by these professionals carry a high inherent risk of being used to facilitate ML/TF activities. This risk is lower in the case of audit services due to their professional regulation, supervision and current market conditions, and in larger entities due to their lower intrinsic risk. The subjection of these professional services to prevention obligations, their internal controls and supervision in the area of ML/TF prevention contribute to a mitigation of their risks.

ML risks. The residual risks of ML schemes and transactions being used are considered **moderate** in the case of auditors, being lower in the case of larger entities, but **moderate/significant** in the case of external accountants and tax advisers, mainly due to the endogenous risk factors described.

TF risks. The very nature of the activities means they are considered **moderate/low** in all three sectors, although the risk of abuse for TF purposes is lower in larger entities and varies according to client type.

e) Activities carried out by notaries.

Activity, context and regulatory framework.

A notary is a public official of the State who is appointed following a competitive examination, and whose role is to provide citizens with the legal certainty enshrined in the Constitution in the field of extrajudicial legal transactions. They are legal professionals who practise on a competitive basis, although their fees are standardised across the board.

There are some 3,000 notaries spread throughout Spain, including in small towns, to ensure the service is available. They are organised into notarial associations, which support them in their work whilst also monitoring their conduct. The deans of these associations form the General Council of Notaries, which represents the profession at national level. Notaries report to the Ministry of Justice.

Law 10/2010 of 28 April establishes that notaries are obliged parties, although notarial and registration acts that lack economic or financial content or are not relevant for the purposes of preventing money laundering and the financing of terrorism are not subject to these obligations. A list of such acts is to be established by Order, although no use has been made of this regulatory provision and all notarial acts are subject to the preventive regulations.

In the exercise of their preventive obligations regarding ML/TF, Law 10/2010 of 28 April provides for the possibility of creating centralised prevention agencies (CPAs) for the regulated professions. The creation of CPAs aims to intensify and strengthen collaboration between regulated professionals and the judicial, police and administrative authorities, allowing for a higher level of specialisation in these tasks within the group of obliged entities. Their creation pursues a dual objective:

- To facilitate compliance by individual entities with preventive regulations, by having a specialised body responsible for administrative or procedural functions which also channels reports of suspicious activity, improving their quality and streamlining the process.
- To standardise the measures applied by the profession, avoiding potential divergent interpretations regarding the scope and meaning of the obligations.

The Centralised Anti-Money Laundering Body of the General Council of Notaries was established in 2005. Membership is mandatory for notaries.

Vulnerabilities and sectoral risk.

The risk of money laundering in notarial transactions stems from the fact that virtually all property and commercial transactions must be recorded or authorised before a notary and, as is the case with other public officials, from the appearance of legality that public deeds confer on the property and assets included therein in favour of those seeking to obtain the use of property acquired with illicit funds. Therefore, given that the objective of all types of threats is to obtain the formal legitimacy of transactions conferred by public institutions, the role of notarial deeds is key within this process of concealing illegality.

The endogenous risk factor of penetration within the notarial sector is very low due to the specialised nature of access to the profession and the conditions governing its practice. However, the exogenous risk factor of the abuse of notarial services for these purposes is very high. These risks stem from the need and ability of criminals to feign, before the notary, the legitimacy of the transactions they intend to carry out and the origin of the funds with which those transactions are conducted, with the ultimate aim of obtaining the notarial deed that lends an appearance of legitimacy to that ownership of property or assets.

This ML/TF risk in notarial transactions can be identified through a series of risk indicators, defined by the OCP, which are simply factual circumstances that experience has shown to be associated in practice, primarily, with money laundering schemes, as revealed by court rulings, the OCP's own risk analysis, or the classification exercises carried out by international bodies in general.

There is a considerable concentration of money laundering risk within a fairly limited number of transactions:

- The incorporation of limited liability companies and the transfer of their shares.
- The sale of real estate.

Of the nearly 400 different types of transactions carried out by notaries, these two types of transactions account for the bulk of the risk (around 40%), whether we are referring to transactions reported on a suspicion basis by notaries or to transactions analysed and referred to SEPBLAC by the Notarial OCP. This 40% of the risk generated is quite significant when one considers that the total sum of both types of transactions represents barely 10–15% of all notarial transactions.

Alongside the two transactions mentioned above, the three highest-risk transactions – which, when added to the previous two, would account for more than 70% of all reported high-risk transactions – are:

- Those relating to company capital increases.
- Loans and acknowledgements of debt.

- Notarial deeds.

In general, there is a considerable degree of correspondence between the types of risky transactions identified by notaries and those ultimately reported by the OCP to SEPBLAC. However, there are cases in which the significance of certain transactions increases following the OCP's analysis of the circumstances identified by the notary. The most striking case concerns notarisation deeds, in respect of which the OCP assesses a significantly higher level of money laundering risk than that typically perceived by notaries.

With regard to risk indicators, the levels generally remain the same as for transactions. However, the proportion of some of the indicators increases following a specific examination by the OCP, as in the case of the two indicators involving the presence of a high-risk territory (party acting and funds). The same situation occurs with the presence of individuals regarding whom there are reports of involvement in criminal activities, as a result of the additional investigation that takes place during the analysis phase at the OCP.

A general analysis of the risks associated with transaction types and indicators reveals the following:

- The sale and purchase of real estate with the highest level of risk occurs in cases involving persons or funds from high-risk territories, whether carried out between parties with some form of connection, or where significant discrepancies are observed in the declared price.
- The sales and purchases of shares with the highest level of risk are those where the price is considered abnormally low or those taking place within a group or sequence of transactions without any particular logical economic or commercial explanation.
- The highest level of risk associated with the incorporation of companies usually arises when multiple pre-incorporated companies are involved or, in particular, when the founder uses them for other purposes.
- In the case of capital increases, the highest risk arises when funds or assets from high-risk territories are used, or when such contributed funds or assets do not correspond to the characteristics of the company increasing its capital, or are difficult to value or verify, particularly in the case of contributions of claims against third parties or the company itself, and in the contribution of shares or holdings in companies from third countries.
- In the case of financing transactions (loans and acknowledgements of debt), the highest level of risk stems from the involvement of individual lenders other than credit institutions, and from instances where the same (private) lender or borrower is repeatedly involved in several transactions within a short period of time.
- It should be emphasised that transfers of shares in limited liability companies (S.L.) carried out by private deed and abroad fall outside the control of notaries, although in this case notarisation takes place at the relevant consular offices and the associated risks are being mitigated through the recently signed agreement for their monitoring by the OCP.
- Transfers of shares in public limited companies that do not have their private agreement notarised are also outside the scope of notaries' authority.

Conclusion.

Their status as public notaries, whose involvement is essential in numerous types of transactions, means that attempts by third parties to use them to legitimise money laundering operations are inevitable.

However, notaries in Spain have developed a highly advanced ML/TF prevention system following the establishment of the Centralised Prevention Agency within the General Council of Notaries, which employs sophisticated tools, such as the Single Computerised Index, which cross-references information on millions of notarised transactions across the country, duly analysed by the OCP's specialist team, or the Beneficial Ownership Database, which enables notaries, authorities and obliged entities to verify

veracity of the declarations made by the beneficial owners of legal entities carrying out transactions subject to public deed.

These highly developed tools, combined with the high level of knowledge and awareness among professionals—which has made this one of the sectors that reports the highest number of transactions to SEPBLAC on the basis of suspicion—enable the residual risk to be significantly reduced. For these reasons, and due to the very nature of the transactions subject to notarisation, the residual risk of being used for **TF** operations is assessed as **low/moderate**.

However, this 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. These transactions are numerically quite significant within the notarial profession, which is why the residual risk in **ML** is classified as **moderate**.

f) Activities carried out by land, commercial and movable property registrars.

Activity, context and regulatory framework.

Land, commercial and movable property registrars are civil servants of the State who are appointed to their posts through competitive examination and whose function is to maintain the land, commercial and movable property registers existing in Spain. Registrars shall, under their own responsibility, assess the legality of all types of documents on the basis of which registration is requested. For documents to be registered in the relevant registers, the registrar must give a favourable assessment.

Under the law, only documents formalised by public deed or by a judicial or administrative decision may be entered in the register; consequently, all registration procedures require the prior involvement of a notary, a judge or an administrative authority, subject to the exceptions provided for by law. This is the general rule in the Land Registers and the Commercial Registers, although there are also cases where private documents are entered in the register, albeit rarely in the Land Registers (applications by sole heirs, or distribution of mortgages) or more commonly in the Commercial Registers (appointment and removal of directors, or appointment of auditors). Meanwhile, in the Registers of Movable Property, the general rule is access via private documentation (approved model finance lease agreements).

In Spain, there are around 1,200 registrars (2019), who receive their fees in accordance with the scale of charges approved by the Ministry of Justice, which covers the costs necessary for the operation and maintenance of the registers. Registrars do not operate on a competitive basis but according to territorial jurisdiction, meaning that citizens do not have a free choice of registry. This unique feature provides an additional safeguard, as registrars are not subject to market forces in the performance of their duties, which has a positive effect on the prevention of ML/TF.

In the exercise of their preventive duties regarding ML/TF, as also mentioned in the analysis of notaries, Law 10/2010 of 28 April provides for the possibility of establishing centralised prevention agencies (CPAs) for the regulated professions. The creation of CPO aims to intensify and strengthen collaboration between members of professional bodies and judicial, police and administrative authorities, allowing for a higher level of specialisation in these tasks within the group of obliged entities. Its creation pursues a dual objective:

- To facilitate compliance by individual entities with preventive regulations, by having a specialised body responsible for administrative or procedural functions which, furthermore,

channels report of suspicious activity, improves their quality and streamlines the process.

- To standardise the measures applied by the group, avoiding potential divergent interpretations regarding the scope and meaning of the obligations.

The centralised prevention body for registrars, created in 2015, is called the Anti-Money Laundering Registry Centre (CRAB) and registration with it is mandatory.

In 2018, a Ministerial Order established the forms for the submission of annual accounts of commercial companies to the Commercial Register, requiring the mandatory declaration and updating of their beneficial ownership, which is subject to registration in the Beneficial Ownership Register (RETIR). This system has a very positive impact on national beneficial ownership control systems and on the level of awareness among authorities and obliged entities, in line with national and international requirements for combating ML/TF.

Vulnerabilities and sector-specific risks.

The public faith placed in registrars is safeguarded by the courts, with the principle of legitimation applying, whereby the holder of the registered right is presumed to be the owner vis-à-vis third parties – a situation highly sought after by those seeking to enjoy the use of property acquired with illicit funds. The ultimate objective of money laundering activities is to ensure that property and assets derived from illicit activities acquire the formal legitimacy conferred by public institutions; consequently, the role of entries in public registers is key within this process of concealing the origin of assets and seeking the appearance of legitimacy.

The **endogenous risk** factor of penetration within the sector is non-existent due to the specialised nature of the regime governing entry into the profession and the conditions regulating its practice. However, this function of public faith, publicity and guarantee vis-à-vis third parties means that the **exogenous risk** factor of criminal organisations abusing registry services for these purposes is high.

Therefore, the **inherent risks** stem from the actions of criminals seeking to give the appearance of legitimacy to the real estate and commercial transactions they intend to carry out, and from the origin of the funds used to carry out these transactions, with the ultimate aim of obtaining the registration entry that grants them formal validity vis-à-vis third parties. The main transactions subject to risk in registration operations are similar to those identified in the analysis of notarial activities (property sales, transfers of company shares, loan transactions, etc.).

For these reasons, in Spain, as in the rest of Europe, registrars are legally obliged to comply with AML/CFT prevention measures, despite not being one of the professions designated by the FATF. Their preventive functions, coordinated through the Anti-Money Laundering Registry Centre (CRAB), play a very significant role within the national prevention framework, significantly reducing the inherent risks associated with registry activities.

There are, therefore, numerous mitigating factors: access to the profession via a competitive examination, which guarantees a high level of legal training; the fact that they do not operate in a competitive environment; the existence of the CRAB, which specialises in anti-money laundering prevention and coordinates preventive policies, risk identification and the reporting of suspicious transactions; and the legal assessment carried out by registrars when reviewing judicial, administrative, notarial and private documents intended for registration.

Conclusion.

The professional functions assigned to them, the legal obligation to register certain transactions and the legal guarantee provided by the register for both commercial and property transactions mean that the registrars' involvement is essential to obtain the presumption of legality that the registry itself reflects, which inevitably impacts risk from an AML/CFT perspective.

However, the specific entry requirements for the profession and the strict regulations and conditions governing its practice mean that any inherent risks of attempts to involve the sector in ML/TF schemes can be ruled out. Furthermore, as regulated entities, they have established a centralised prevention body, the CRAB, which provides the entire professional body with a highly advanced prevention system.

The obligation to file beneficial ownership information with the Commercial Register alongside the filing of annual accounts, and the existence of the Register of Beneficial Ownership (RETIR), which is maintained by commercial registrars, provides automated access to data on company ownership in a structured format, which is, in turn, used by public authorities and regulated entities.

Finally, the registration requirement for all natural or legal persons who, in a business or professional capacity, provide services classified as corporate services (or corporate services provided by third parties), must be registered with the Commercial Registry competent for their place of residence, in accordance with the Commercial Registry Regulations.

TF Risks. The involvement of registrars in certain transactions and certain types of business susceptible to being used for TF activities affects the TF risk. However, the types of transactions that must be submitted for registration do not currently correspond to the TF risk operations existing in our country; therefore, in general, the residual risk level is considered to be **low/moderate**.

ML Risks. 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 that has not been recorded in the Commercial Registers since 1995, being reflected solely in the share and participation registers kept by companies, with access restricted to shareholders). All of these are common transactions in the practice of the profession, which is why the residual risk associated with their use is classified as **moderate**.

g) Certain specific activities carried out by lawyers and other independent professionals.

Activity, context and regulatory framework.

This section analyses only the ML/TF risk associated with certain activities expressly provided for in Article 2.1(ñ) of Law 10/2010 of 28 April, carried out by lawyers, solicitors or other independent professionals. Specifically, these are cases in which they participate in:

- The planning, execution or provision of advice on transactions on behalf of clients relating to the sale and purchase of real estate or commercial entities.
- The management of funds, securities or other assets.
- The opening or management of current accounts, savings accounts or securities accounts.
- The organisation of 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.

Furthermore, when these independent professionals carry out activities relating to the provision of corporate services, as provided for in Article 2.1(o) of Law 10/2010 of 28 April, the analysis set out in the following section must be taken into account.

A lawyer is an independent legal professional who acts as counsel and defender for parties in all types of proceedings or provides legal advice. A court agent is a legal professional who exclusively represents their clients before the courts and tribunals. Although both professions are free and independent, in Spain membership of professional associations (which are public-law bodies) is mandatory in order to practise as a lawyer or court agent, with access to the profession being regulated by law.

Both professions are subject to membership obligations and compliance with ethical standards. In the case of lawyers, their own Code of Ethics of the Spanish Bar, approved by the Plenary Session of the General Council of the Bar on 6 March 2019, reiterates compliance with AML/CFT obligations in the course of their practice.

It should be emphasised that, in accordance with current regulations, lawyers shall not be subject to AML/CFT obligations with regard to information they receive or obtain from their clients when determining the legal position or carrying out their duty to defend said client in legal proceedings or in connection with them, including advice on the initiation or avoidance of proceedings, regardless of whether they have received or obtained such information before, during or after such proceedings.

In Spain there are currently (2019) around 150,000 lawyers, but the group that meets the requirements to be considered a regulated entity under Article 2.1.ñ of Law 10/2010 of 28 April is much smaller, as it includes only those members of the bar who carry out the activities listed above and covered by the Law.

According to estimates by SEPBLAC and the General Bar Association, this group comprises fewer than 500 professionals, generally working in larger law firms, and the sector's turnover in these areas is estimated at around €1.5 billion a year, derived primarily from the revenue of large law firms.

Vulnerabilities and sectoral risk.

Criminals and organised crime groups of various kinds generally require advice on legal procedures that enable them to give illicit funds a legal appearance. The legal expertise of lawyers and other independent professionals, and the fact that this is a professional sector subject to free hiring, are factors that lead criminal structures to have an interest in and a need to recruit professionals from this group.

These risks exist both in terms of integrating them into their organisation (very high **endogenous** or penetration **risk** factor) and in terms of misusing their services (high **exogenous** or activity risk factor), without there being, in the latter case, any connection to or knowledge of the illegal activity or the illicit origin of the funds on the part of the professional who is hired. In other words, these are members of professional bodies whose willingness to act within the law is beyond doubt, but who are, or may be, used for illicit purposes by their clients.

In fact, in judicial investigations into money laundering offences or other economic crimes, the involvement of professionals acting on behalf of their clients in financial, corporate or property transactions has been detected, the purpose of which is to hinder the identification of the beneficial owners of property, funds or assets, or their origin, or in the design of fund management or shareholding arrangements between companies for such purposes, sometimes intentionally (in which case the matter falls within the remit of the police and the courts) and, in the majority of cases, without any intention of acting unlawfully.

This sector is one of those facing the greatest difficulties in complying with its legal obligations regarding the prevention of money laundering and terrorist financing, particularly with regard to the reporting of suspicious transactions, the number of which is among the lowest of all regulated entities (only 22 in 2018 and 24 in 2017). Difficulties are also evident in the application of client confidentiality, which must be understood as relating to the client's right to legal defence and representation, without affecting transactions of an instrumental nature that are expressly set out in the law and in the FATF's international standards for these professional groups when carrying out certain activities which, by their nature, carry a higher risk of being linked to ML/TF.

These **inherent high risks** are the reason for their inclusion within the sector of obliged entities, provided that their activity is aimed at providing those specific services that go beyond the client's legal defence, and which involve the management, advice or planning of financial, commercial or real estate transactions that may be directly or indirectly related to ML/TF activities. They are therefore subject to supervision by SEPBLAC, which in recent years has carried out inspections in this sector generally focused on compliance with their formal ML/TF prevention obligations and their internal implementation of policies and procedures in this area.

Conclusion.

Lawyers and other independent professionals providing the services listed above face, on the one hand, a high endogenous or intrinsic risk due to the interest organised crime groups have in utilising their technical and legal expertise as part of their operations. On the other hand, these professionals face a high exogenous or activity-related risk due to the potential misuse of their professional services for carrying out the specifically listed operations for ML/TF purposes, without their being aware of the preventive obligations entailed by these operations or of the possible illegality of the origin of the funds, property or assets that are the subject of the contracted operation.

A clear distinction must be made between the legal defence and client representation activities typical of an independent legal professional and the activities listed above. The latter are specifically set out in the law and in international AML/CFT standards, as, due to the risks involved, they are subject to preventive obligations on the part of these professionals. However, there is a certain degree of confusion within the sector itself regarding the distinction between cases where AML/CFT prevention obligations apply and the rest of their legal defence and client representation activities, in which they do not have the status of obliged entities.

ML risks. The high inherent risks of money laundering and terrorist financing associated with this type of activity carried out by lawyers and other professionals, together with the significant room for improvement that still exists in the sector's understanding of its own preventive obligations, combined with the freedom to practise the activities listed in the Act, which makes it difficult for supervisory authorities to identify those members of the professional body who are carrying out these activities on a professional basis, lead to the assessment of a **significant** residual ML risk in this sector when they carry out, on behalf of the client, the transactions listed in Article 2(1)(ñ) of Law 10/2010 of 28 April.

TF Risks. The carrying out of such transactions for the purposes of TF also requires the involvement of qualified professionals to conduct them or to obtain legal advice. The possible existence of business dealings and commercial transactions linked to TF organisations involving these professionals leads to the residual risk being classified as **moderate**.

Solicitors. In view of the above, the degree of exposure to ML/TF risk for solicitors should be considered **low**, given that their activity consists essentially of merely representing clients in legal proceedings.

h) Provision of corporate services to third parties.

Activity, context and regulatory framework.

This section covers certain activities involving the provision of corporate services to third parties on a professional basis by natural or legal persons. Specifically, the corporate services included are as follows:

- Incorporating companies or other legal entities.
- Acting as a director or non-executive secretary of a company, or as an external adviser to a company, as a member of an association, or performing similar functions in relation to other legal entities or arranging for another person to perform such functions.
- Providing 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.
- Acting as a trustee in a trust or similar legal arrangement or arranging for another person to act in such a capacity.
- Exercising shareholder functions on behalf of another person, except in the case of companies listed on a regulated market and subject to disclosure requirements in accordance with EU law or equivalent international standards or arranging for another person to exercise such functions.

These activities are not subject to uniform regulation or treated in a similar manner with regard to the exercise of professional activity. However, the ML/TF risks associated with them have led both European and national regulations to include those who professionally carry out these functions as persons subject to ML/TF prevention obligations.

Consequently, those professional natural persons, self-employed natural persons and legal persons who carry out any of the functions listed are considered obliged entities, regardless of whether they are also included as obliged entities in any other of the categories provided for in Law 10/2010 of 28 April.

Pursuant to the provisions of the European Directive, professionals carrying out these corporate activities must register in a national register of service providers to companies and trusts and must submit an annual declaration regarding the activity data relating to these operations.

In Spain, this obligation has been implemented through the amendment of Law 10/2010 of 28 April, by requiring the registration in the Commercial Register of all natural or legal persons who, on a commercial or professional basis, provide all or any of the services classified as services to companies. Thus, registration must be carried out in the Commercial Register competent for the service provider's place of business and constitutes an additional control measure in the prevention of money laundering.

Vulnerabilities and sectoral risk.

As with the activities described in the previous section, criminals and organised crime groups of various kinds generally require advice on the legal procedures that enable them to give illicit funds a legal appearance through the incorporation of companies and the carrying out of corporate transactions, as well as to conceal the true identity of the owners of the companies or of their shares or securities.

Therefore, given the knowledge related to the provision of the corporate services listed above that certain independent professions possess, coupled with the fact that these are professional activities subject to a system of free contracting,

criminal organisations of any kind have a strong interest in and need to recruit professionals, both to integrate them into their organisation (very high **endogenous** or penetration **risk** factor) and to misuse their services (high **exogenous** or activity **risk** factor), without, in the latter case, there being any connection to, or knowledge of, the illegal activity or the illicit origin of the funds on the part of the professional being engaged.

In investigations leading to prosecution for money laundering offences or other economic crimes, the services most frequently sought for money laundering/terrorist financing purposes involve the establishment of complex corporate structures, with entities registered in different jurisdictions, whose activities lack economic rationale. In fact, cases have been detected involving professionals or entities of various kinds acting on behalf of their clients, either voluntarily or without the professional's knowledge, to be used by their clients in the design of complex corporate transactions aimed at hindering the identification of the beneficial owners of the companies or the owners of the company's assets or securities, or the origin of these assets or securities. Their involvement has also been detected in the design of transactions involving the transfer or management of funds or shareholdings between companies, often of an international nature, for such purposes.

The creation of corporate structures specifically for ML purposes may involve complex corporate ownership arrangements and the emergence of chains of intermediaries, sometimes resident in designated countries or territories, or individuals acting as fronts with the aim of making it difficult to identify the beneficial owner. Furthermore, financial transactions may utilise payment channels that promote anonymity and make it difficult to trace the origin of the funds.

These clearly high **inherent risks** are the reason for their inclusion within the sector of regulated entities, provided that the activity is of a professional nature and is aimed at providing those specific corporate services to clients.

In Spain, these corporate services are provided by both professional individuals (lawyers, advisers, managers and other independent professionals) and by entities and business owners, but their exposure to risk is very high in all cases.

Currently, in Spain and the EU, there is no precise information on the individuals/entities carrying out these activities, their number, the types of entities and professionals involved, the turnover of such activities, etc. This lack of information also makes it difficult for AML/CFT prevention activities and their supervision to achieve the systematisation, coordination and level of awareness and implementation that exist in other activities and sectors in the non-financial sphere, which has a negative impact on the mitigation of the AML/CFT risks posed by these types of activities.

Their control through the aforementioned registration will facilitate this mitigation both through the dissemination of their obligations regarding AML/CFT prevention and through monitoring and supervision by the authorities. Their inclusion as regulated entities and the sector's growing understanding of the risks represent progress in reducing the high inherent risks.

Among the corporate services provided, special mention should be made of:

a) Corporate services provided on a professional basis by a lawyer or an independent legal professional. As with the transactions in the previous section, there is some confusion within the sector regarding the distinction between cases where there are AML/CFT obligations (cases under subparagraphs (ñ) and (o) of Article 2 of Law 10/2010 of 28 April) and activities involving the legal representation and defence of clients in which they do not have the status of obliged entities.

b) Trust service providers (or trustees) operating in Spain, which are examined in greater detail in the relevant chapter, are generally regulated entities resident in other countries from which they transfer funds or acquire assets or rights in our country. It is unusual to find Spanish who provide this type of trustee service in a trust, as this is a legal structure that cannot be established in Spain. However, there are representation services for such trusts in our country.

c) Professionals or entities that provide services to third parties involving the sale of pre-incorporated companies, or their shares or holdings. These companies are incorporated in advance, without any real economic activity, for the sole purpose of their subsequent transfer to third parties. The very nature of this service makes it one of the sectors most vulnerable to and at greatest risk of being used for ML/TF purposes.

Conclusion.

Professionals and legal entities that provide corporate services on a professional basis face, on the one hand, a **high endogenous risk** factor due to the interest that organised crime groups have in integrating them into their organisations to carry out the activities listed in the law.

Furthermore, these professionals and entities also face a high level of **exogenous** or activity-related **risk** due to the potential misuse of their professional services for carrying out the corporate transactions specifically listed for ML/TF purposes, without these professionals or entities being aware of the preventive obligations associated with these legally defined transactions to verify, amongst other matters, the possible origin of the funds, property or assets subject to the contracted transaction and the beneficial ownership of those securities or assets.

The risk in this sector is analogous to that of the transactions referred to in the previous section, as it is a non-reserved activity and it has not yet been possible to verify risk mitigation through the register of providers of these corporate services provided for by law, the operation and development of which is in its initial phase. Until this Register becomes fully operational and the obligations it entails are met, the provision of corporate services is entirely unregulated; indeed, the number of professionals and entities providing such services, the possible number of transactions carried out, or the type of transactions most frequently requested by clients in the sector are unknown.

ML risks. All of the above implies that this type of professional corporate services operation carries a **significant** residual risk. This risk is heightened in the case of services involving the creation of companies with the intention of transferring them, as these are pre-incorporated companies lacking any real economic activity, and the risk of ML activities in such cases must be classified as **high**.

TF risks. In the case of the potential use of these transactions for TF activities, the need for qualified professionals to carry out certain transactions or provide legal advice on specific types of business and commercial transactions linked to entities posing a TF risk means that the risk rating is **moderate.**

i) Gaming sector.

Activity, context and regulatory framework.[38]

The gambling sector in Spain comprises various types of activities which are grouped according to the level of jurisdiction in question: games at the state level and games at the regional level.

The Directorate-General for the Regulation of Gambling, Dirección General de Ordenación del Juego (hereinafter, DGOJ) is responsible for state-level 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 establish rules on the verification of identity details and the data provided by participants, regulating in great detail the procedures for identity verification and the documentation provided by online players.

With regard to gaming licences, authorisations and registrations, the regulation stipulates that SEPBLAC must assess, prior to authorisation by the Directorate-General for Gaming Regulation, the mechanisms for preventing fraud and the systems for preventing money laundering and the financing of terrorism.

At the 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 activities—which include casinos, bingo halls, gaming halls, betting shops, racecourses, and 'B' and 'C' type machines—are regulated in accordance with the provisions of each Autonomous Community; consequently, the supervision and control of these establishments and terminals fall outside the remit of the DGOJ.

In this area, the national regulations on the prevention of money laundering and terrorist financing apply since, on the one hand, they designate casinos as obliged entities and, on the other, the persons responsible for the management, operation and marketing of lotteries or other games of chance conducted in person or via electronic, computerised, telematic and interactive means (online gambling), without distinguishing whether the gambling is regional or national. In the case of lotteries, sports-charity betting pools, competitions, bingo and 'B' type gaming machines, this applies solely to prize payment transactions.

Therefore, all forms of gambling are subject to the provisions of the prevention regulations, although there is a different level of requirement regarding prevention obligations due to their varying exposure to ML/TF risk, as set out in the regulations.

The **gambling market** is a significant economic activity in Spain involving various types of entities, including large international groups, public bodies and private national entities of varying sizes, which are divided between land-based and online activities.

State-level gaming.

State-level lotteries.

Unlike betting, lotteries are not linked to any sporting or other event organised by a third party; rather, their winning numbers or combinations depend entirely on chance. They are marketed by two

[38] Sources: DGOJ Annual Report – DGOJ Strategy for the Supervision and Inspection of Gambling – DGOJ Report: Analysis of the Online Gambler's Profile – DGOJ Yearbook of Gambling in Spain (IPOLGOB).

operators: the State Lottery and Betting Company, Sociedad Estatal de Loterías y Apuestas del Estado (hereinafter, SELAE) and the National Organisation of the Spanish Blind, Organización Nacional de Ciegos Españoles (hereinafter, ONCE). In 2018, these lotteries reached €10.951 billion in wagers, mainly through in-person sales, although there is a growing online market.

€8.79 billion corresponds to SELAE games: the National Lottery (regular draws, El Niño, Christmas Draw) accounts for around €5.2 billion staked annually, and the active games managed by SELAE (Primitiva, EuroMillions, Bonoloto, Gordo de la Primitiva and Lototurf) generate around €3.56 billion annually.

Games marketed by ONCE reached (2018) 2.16 billion euros in turnover across remote and in-person channels. Alongside the various types of lottery tickets, which account for the bulk of its business, ONCE markets instant lotteries and certain active lotteries (Eurojackpot, Super Once), has a large network of sales outlets across the country (around 20,000) and a long-standing tradition in Spain.

National betting.

This market generates bets worth around €7.172 billion (2018) through remote and in-person gaming channels. In recent years, it has undergone a significant change, shifting from the absolute dominance of La Quiniela via in-person outlets (which handled around €550 million in 2008 and currently around €210 million) to a much broader range of gaming activities, as a result of the development of online betting.

Its management, as with other state-run online games, is carried out via national-level websites (.es) which must comply with strict requirements established by Spanish legislation aimed at preventing gambling operations from illegal platforms. These operators are authorised, regulated and monitored by the DGOJ, which grants them a seal of quality and security.

Other nationwide online games.

In the sector of nationwide online casino games, the amount wagered exceeded €8.215 billion in 2018, a figure that continues the upward trend seen in recent years. The main categories within online casino games are slot machines (around €3.444 billion) and roulette (€3.650 billion). Online poker is also significant, with €2.071 billion wagered in 2018, representing a notable year-on-year increase. Other games are of little significance: nationwide online bingo (€99 million) and game shows (€1.7 million in wagers in 2018).

Gaming and gaming establishments at regional level.

a) Betting and premises offering betting games.

Betting managed and controlled by the autonomous communities accounts for some €2.138 billion in wagers, of which €1.888 billion corresponds to in-person betting and the remainder to online betting, with an upward trend since 2014, as is the case at the national level. In terms of in-person betting, this form of gambling takes place in 13,391 specific betting venues, gaming halls or other gambling establishments, of which 9,575 are hospitality venues, 3,049 are gaming halls, 489 are betting houses, halls or parlours, and 235 are bingo halls, highlighting the most significant figures from the total amount.

b) Casino games and casinos.

Land-based casino games (blackjack, punto banco, roulette and poker, as well as 'C' type machines) have generated a total of 1.815 billion in wagers. These games can only be played in casinos.

In Spain, there are 50 open casino halls and 1,519 'C' type gaming machines, as well as a total of 466 casino gaming tables. In total, they attract over 5 million visitors annually. In addition to the casino games mentioned above, other types of games of chance ('B' machines, betting) are also available in casinos.

c) Bingo games and bingo halls.

There are 319 bingo halls in Spain, with a total of €2.029 billion wagered (2018). There is a growing trend towards the diversification of gaming activities in bingo halls (installation of 'B' type machines, sports betting), so it should be noted that the above figure does not include the amounts wagered on these types of games.

d) Gaming halls.

Although gaming halls are subject to strict requirements regarding the operation of their activities, they may offer different gaming activities depending on the autonomous community. There are 3,463 gaming halls, generally small in size, which mainly offer 'B' type gaming machines, sports betting or other types of betting, alongside other services such as a café or amusement machines. The potential impact from an AML/CFT risk perspective lies in the different gaming activities carried out by each hall.

e) Type "B" gaming machines.

These machines (although they have a different name in some autonomous communities) can award cash prizes in exchange for a stake via a probabilistic programme based on a cycle of games (not a random operation in each game as in the "C" type machines typical of casinos). These machines can be installed in gaming halls, casinos or bingo halls, but also in bars and restaurants. There are currently around 190,000 of them, and they generally serve as a complementary service to the main offering. The prize amounts are limited (most offer a maximum prize of €500), which virtually eliminates their vulnerability from a ML/TF risk perspective.

f) Lotteries.

There are also some lottery activities managed by regional administrations with a low turnover (in 2018, the regional governments' own lotteries stood at around €67 million in amounts wagered through in-person and online channels).

g) Regional online gambling.

Regional online gambling accounts for a very small percentage of the gambling market: €211 million in wagers in 2018 (most of which relates to sports betting).

Vulnerabilities and sectoral risk.

Inherent risks. The gambling sector, and casinos in particular, are traditionally exposed to an endogenous or intrinsic risk factor associated with the control of the company or its management, or the possible dishonest behaviour of certain employees who may take advantage of their internal position to facilitate or engage in activities related to money laundering and terrorist financing.

However, exogenous or extrinsic risk factors are more significant, namely those related to the characteristics of the operation and the behaviour of customers who attempt to exploit certain vulnerabilities in gambling to carry out ML/TF practices.

These risks vary depending on the type of game. Some games rely entirely on chance, with specific numbers or winning combinations determining the outcome; in others, the player's experience or skill is a key factor; whilst in others, it is possible to manipulate or rig the results, potentially leading to bets being placed with prior agreements regarding the outcome. However, sectoral risk analyses, regulation and prudential supervision of the sector (which are very strict in the case of casinos), and investigations by law enforcement agencies have not detected any particularly significant ML/TF criminal activities linked to the gambling sector. Operations that may be linked to ML/TF include:

- The purchase of winning tickets, particularly in the lottery sector, as part of a more complex money laundering scheme.
- Abuse of the sports betting system by organised criminal groups, linked to fraud and money laundering, who, through bribery, predetermine the results of sporting competitions on which they place their bets, sometimes using illicit funds.
- In certain casino games, mainly online games, situations may arise involving cross-betting or card games (mainly poker) in which participants are colluding or belong to the same organised group.
- In the land-based casino sector, although there is no evidence of significant money laundering operations, the exchange of unused gaming chips for cash is a traditional practice in the sector.
- With regard to FT activities, in the past, transactions linked to local raffles and prize draws were detected, used to raise funds by organisations linked to terrorist groups and their support networks.

Residual risks. Although internationally the gambling sector is considered high-risk for ML, in Spain it must comply with specific measures that make it less vulnerable:

a) It is subject to very strict sectoral regulation with various aims: combating tax fraud, preventing addiction, protecting the rights of minors, and safeguarding the rights of players and vulnerable groups.

b) Unlike in other countries, in Spain casinos are not permitted to carry out financial transactions, open accounts for customers, grant credit, make transfers, provide 'junket' services, etc.

c) All operators, platforms, websites and forms of in-person and online gambling operating in Spain are subject to an administrative licensing and/or authorisation regime with very strict requirements.

d) Sector-specific supervision carried out on a risk-based basis, in accordance with the guidelines set out in the DGOJ's document "Strategy for the Supervision and Inspection of Gambling" and the "Technical Note on Fraud Management among Gambling Operators" (both documents published on the DGOJ's website), together with monitoring by the authorities (for example, the casino police), significantly limit the vulnerability of these entities.

e) Gaming operators themselves carry out significant monitoring of gaming activities, both for economic reasons (counterparty games) and due to the sector's own awareness, which means that the control measures implemented are highly dissuasive. In the area of AML/CFT, there is a Catalogue of Risky Transactions[39].

[39] http://www.tesoro.es/sites/default/files/cor_casinos.pdf.

f) The statistical information on the sector is very detailed, enabling the identification of areas where activities may be linked to ML/TF or other criminal activities. In the case of casinos, the sectoral analysis provides data on the locations (rooms and/or geographical areas) where the highest level of gambling activity takes place, where the greatest increase in betting has occurred in recent years, and where the highest percentage of profits/losses is generated. Detailed analyses are also carried out periodically on customers, types of games, gaming tables and machines, casino rooms and seasonality, amongst other variables.

g) In 2019, the National Commission to Combat the Manipulation of Sports Competitions and Betting Fraud (CONFAD) was established, a collegiate body for cooperation between public authorities, sports organisations, sports competition organisers and representatives of the gambling sector, with the aim of preventing and eradicating corruption and the manipulation of competitions and betting.

For all these reasons, taking into account the regulatory and monitoring framework—both prudential and relating to AML/CFT prevention—and the understanding of its AML/CFT prevention obligations and potential risk operations, as well as the evidence resulting from investigations and supervision in this area, it is considered that the various forms of gambling present different levels of risk, with non-face-to-face activities posing a higher risk than face-to-face ones.

Within in-person forms of gambling, there is also a gradation of risk, in that betting and lotteries are classified as moderate risk, whilst bingo, casinos and 'B' type machines are considered low-risk activities.

Conclusion.

The gambling sector comprises various types of activities whose potentially high inherent risks are reduced by the existence of mitigating measures of a regulatory, supervisory, informational and awareness-raising nature within the sector, which limit exposure to such risks; however, the residual risk identified must be assessed differently depending on the type of gambling. This finding leads to the conclusion that we are dealing with a sector of **moderate/low** residual risk. However, an individualised analysis of the different forms yields the following conclusions regarding their risks of being used in ML/TF activities:

Risks in casinos (land-based).

The regulatory framework governing casinos in Spain has always been conservative in nature. The ban on casinos during the Franco era was followed by very strict regulations designed to ensure that the authorities retain control over casino operators and their activities. Restrictive measures have been adopted to control addiction, regulate access to gambling, safeguard players' rights and guarantees, ensure that gambling services comply with regulations, monitor the tax compliance of operators and the payment of winnings, etc.

Among these measures, the following are particularly noteworthy:

- The obligation to provide identification when accessing premises, regardless of whether gambling activities are taking place.
- A ban on certain financial activities (opening gambling credit accounts, transferring funds to bank accounts or other gambling operators, junkets, etc.).
- Very strict rules governing the granting of licences to operators (requires a report from SEPBLAC).
- Establishment of a specialised police force.
- Very active sectoral supervision.
- Subject to high taxes.

Therefore, the very nature of prudential regulation contains measures that have a very direct impact on the area of ML/TF prevention, hindering any potential control of these entities by criminal organisations. Furthermore, there are no significant cases and entities in the sector are well aware of their obligations and high-risk operations; consequently, the residual risk of casinos in Spain being used for ML/TF activities is considered to be **low**.

Risks associated with lotteries and "online lotteries"

The main money laundering risk associated with these lottery activities, including those marketed "online", relates to the practice of buying and selling winning tickets, which generally involves intermediaries. This well-known system, usually linked to tax fraud, has been identified in police investigations and presents a higher degree of vulnerability than other forms of gambling; consequently, it is estimated that there is a **moderate** risk in **ML**, whilst no such risks have been observed in **TF** operations**,** meaning the risk should be classified as **low.**

Risks in charitable sports pools (quinielas).

These bets are marketed exclusively by SELAE. When analysing ML/TF risks, given that they consist of bets on a multitude of unrelated events, the chances of manipulating all the results are remote. Similarly, the economic value is relatively low. However, knowledge of combinatorics and probability, together with computer programmes designed to facilitate such calculations, allows for the investment of illicit funds with a certain degree of return on profits. Furthermore, as in the previous case, there are a multitude of bettors and, therefore, potential transactions involving the buying and selling of winning tickets. For all these reasons, it is estimated that there is a **moderate** residual risk of ML for this specific type of bet. No risks of this nature have been identified in **TF** operations, so the residual risk should be classified as **low**.

Risks associated with in-person gambling operations.

The risk associated with in-person gambling activities carried out in bingo halls, gaming parlours, hospitality venues or dedicated betting shops (the range of in-person gambling establishments is diverse) is determined by the type of game played by the customer. On the one hand, there are forms of gambling that are more exposed to money laundering and fraudulent activities, such as betting (specifically sports betting), where the amounts wagered or won can be significant and where, furthermore, there is a risk that transactions may be rapid and anonymous. In this regard, certain police investigations linked to fraud have highlighted this, so for this type of activity related to the betting sector, a **moderate/significant** residual risk for **ML** activities is justified; however, no risks have been identified for operations linked to **TF**, so the residual risk must be classified as **low.**

On the other hand, there are other forms of land-based gaming, such as 'B' type machines and bingo itself, whose nature and the amounts wagered or won create conditions that are unattractive for criminal activities related to ML, resulting in low vulnerability and a **low** risk of being used for ML/TF purposes.

Risks of online gambling.

Online gambling operators must be authorised by an authority responsible for granting licences and monitoring activities in the gambling sector. The licensing procedure assesses the applicant, their good repute and the ML/TF prevention measures adopted, and Sepblac is required to participate in this process. Individuals or companies with a criminal record or with offences related to ML/TF cannot obtain such licences. This procedure includes an examination of the operators' beneficial ownership.

Due to the high risk associated with remote systems, centralised systems have been approved to identify and verify the identity of customers, based on cross-referencing with national identification databases accessible to operators.

Although online gambling companies adopt appropriate security measures in line with the state of the art, they are aware of specific risks, such as those arising from the use of prepaid cards, the use of different payment systems and the origin of funds, cross-betting or difficulties in verifying the player's true identity.

The system approval procedure carried out during the licensing process and through periodic audits enables compliance by operators to be assessed. Furthermore, it is equally important to note, as a risk mitigation measure, that financial transactions carried out in an online gambling environment are traceable from their origin, which facilitates the control and monitoring of this type of activity.

Therefore, in general terms, as a result of the various prudential control procedures and mechanisms implemented for this type of activity, briefly described in this section, together with the risk mitigation measures put in place, the residual risk associated with online gambling should be understood as **moderate/significant** for **ML** activities, whilst no risks have been identified for operations linked to **TF**, meaning that the residual risk should be classified as **low**.

Despite all these risk mitigation measures, police investigations into fraud in sports competitions reveal that **online sports betting** is being used as a means of carrying out criminal activities and **money laundering**, which justifies the assessment of a **significant** residual risk for this segment of online gambling**.** No risks have been identified for operations linked to **TF**, so the residual risk should be classified as **low**.

Contests are a form of gambling that is generally conducted via computerised, telematic, electronic and interactive means; they present a **low** residual **ML/TF** risk due to their very structure, the volume of amounts wagered and the prizes that can be won, which makes them unattractive for such activities.

j) Professional trade in jewellery, precious stones and metals.

Activity, context and regulations.

The professional trade sector in jewellery, precious stones and metals consists mainly of small and medium-sized enterprises engaged in industrial or artisanal manufacturing, distribution and retail trade. In many cases, they also carry out import and export activities.

According to data from the Spanish Association of Jewellers, Silversmiths and Watchmakers, the sector comprises approximately 8,500 small and medium-sized enterprises. Of these, some 1,900 are engaged in the production of jewellery, silverware or watches, including repairs[40], of which only around 400 companies would be classified as factories, with employees and the capacity for expansion. The remainder consists of a multitude of workshops sublet by larger units, including retail trade or repairs. The business scale of the sector's industry corresponds to the

[40] Data from the Spanish Association of Jewellers, Silversmiths and Watchmakers. http://www.xn--asociacionespaoladejoyeros-urc.es/joyapedia/pagina.php?id=28.

characteristics of the industrial fabric of neighbouring countries with a similar land area and population.

Most of its production consists of commercial jewellery aimed at social segments with average purchasing power, with some 6,500 points of sale distributed throughout the country and a turnover of approximately 1.7 billion euros annually. Specialised chains account for over 50% of the sales market due to the gradual closure of independent shops in recent years. Large retail outlets also play a significant role in the sector's trade (13% of sales).

These activities are carried out within a framework of free enterprise, subject to compliance with the requirements and procedures necessary for the conduct of any business activity (government operating licence, AEAT, Regional Ministry of Labour, Industry and Trade, local councils, etc.) and may be undertaken by both sole traders and large companies.

Spanish legislation, in accordance with EU Directives, stipulates that those who trade professionally in jewellery, precious stones and metals are subject to anti-money laundering and counter-terrorist financing obligations and must comply with the preventive measures established for this purpose.

Vulnerabilities and sector-specific risks.

Jewellery, precious metals and gemstones, and the trade in them, possess certain characteristics that entail an **inherent risk** of being used in money laundering and terrorist financing operations. This has led the FATF's international standards to expressly include professionals engaged in the commercial trade of precious metals and gemstones as obliged entities in the field of ML/TF prevention, and to issue risk assessments on this matter[41]. Member States are therefore required to designate them as obliged entities at the national level and to ensure they comply with the relevant preventive obligations.

The vulnerability of the jewellery, gold and diamond trading sector has led the EU, in its Supra-National Risk Assessment (SNRA), to classify the sector as posing a significant risk for ML/TF operations.

Jewellery, precious metals and gemstones are assets that can concentrate great economic value in a small volume, which can facilitate their transport. Furthermore, they do not lose value over time but appreciate, and their price often depends on the buyer themselves.

Gold and other precious metals and stones are ideal for certain forms of savings and investment and, as a result, are also attractive for concealing illicit funds (through their purchase with such funds, subsequent transfer and reconversion) or for making payments for criminal activities. For organised crime groups (the main threats in this sector), the use of precious stones and metals can provide a useful system for paying for illicit transactions, offering advantages such as ease of safekeeping, retention of value, untraceable origin, or the possibility of successive deliveries, amongst others.

The risks in the sector are mainly associated with the method of payment, the customer profile and the type of transaction. The frequent use of cash, instalment payments or the endorsement of other transferable means of payment facilitate anonymity and make it difficult to identify the final buyer. Transactions with customers from certain jurisdictions (not always classified as high-risk) may be indicative of specific ML operations linked to customs fraud or other forms of fraud. Police investigations have also identified certain patterns arising from the intrinsic risks of precious metal purchasing entities, particularly in relation to recycling activities, with implications for both ML and TF activities.

[41] FATF Report (July 2015) "Money Laundering and Terrorist Financing Risks and Vulnerabilities Associated with Gold".

In the face of these inherent risks, there are a number of factors and mitigating measures that significantly reduce the level of residual risk, including:

- **Awareness** among sector entities regarding the prevention of money laundering has improved substantially in recent years, with the work of the Spanish Association of Jewellers, Silversmiths and Watchmakers (AEJPR) towards its members and its dissemination of their obligations in the area of prevention being particularly noteworthy. This awareness is growing among larger organisations, specialist chains and department stores, for which there are higher preventive requirements than for smaller organisations.

- The application of **preventive obligations** depends on the level of risk that institutions face of being exploited by third parties for ML/TF purposes, which is directly related to their size. Consequently, larger institutions must comply with the standard regime of preventive measures, although retail operations are subject to a simplified regime due to the lower exposure to ML risk associated with these smaller-scale commercial activities. Furthermore, as in other non-financial sectors, there is a less stringent regime of internal policies and procedures for smaller entities, namely those with fewer than ten employees and an annual turnover or annual balance sheet total of less than two million euros, which are not part of a business group that, as a whole, exceeds these figures; such entities have less stringent obligations due to their lower risk exposure.

- In 2016, the COPBLAC published on its website a guide entitled **"Guidance** on compliance with obligations regarding the prevention of money laundering and terrorist financing"[42] specifically aimed at small businesses and retailers in the jewellery, precious stones and precious metals sector. This Guide was drawn up in collaboration with the Spanish Association of Jewellers, Silversmiths and Watchmakers (AEJPR) to facilitate compliance with and the implementation of the preventive measures set out in the regulations.

- Once again in collaboration with the AEJPR, the COPBLAC drew up and published an Illustrative Catalogue of **High-Risk Transactions** (COR)[(43),] aimed at the jewellery, precious stones and metals, art and antiques sectors, which is intended to guide natural or legal persons who trade professionally in these goods in identifying transactions that could be classified as high-risk.

There is smooth **cooperation** between the Administration and the sector through the AEJPR, as this association, in addition to participating in the drafting of the aforementioned regulations and guidelines, acts as a channel for conveying queries and consultations to the Administration. Likewise, sector entities maintain close collaboration with Sepblac regarding the detection of specific types of risk.

Conclusion.

The professional trade in jewellery, precious stones and metals comprises various types of operators whose inherent risks are potentially high: the economic value of the goods, their small size, ease of transport and transferability, the durability of the goods and their value over time, difficulty in tracking transactions, etc. These risks lead to greater exposure to being exploited by organised crime groups, either endogenously through the control of a commercial entity for illicit purposes, or exogenously, by abusing legitimate businesses that are used, without their knowledge, by criminal groups to carry out ML/TF operations through them.

[42]https://www.tesoro.es/sites/default/files/orientaciones_joyeros.pdf.
[43]https://www.tesoro.es/sites/default/files/cor_joyerias.pdf.

However, these risks are significantly mitigated by various regulatory, supervisory, informational and sector-wide awareness-raising measures that limit exposure to such risks, resulting in a clearly lower residual risk, a finding supported by the relatively low economic volume of transactions in our country. This finding leads to the conclusion that we are dealing with a sector with a **moderate** level of residual **ML** risk, whilst the residual risk of the sector being misused for **TF** purposes is lower and can be considered **moderate/low**.

k) Buying and selling of works of art and antiques.

Activity, context and regulatory framework.

In accordance with the definition for tax purposes of the assets to which the special tax regime for works of art and antiques applies[44], this chapter covers the purchase and sale of works of art (paintings, engravings, sculptures, tapestries, ceramics, enamels and photographs, as defined in the regulations) and antiques (objects over 100 years old that are not works of art or collectibles).

The professional trade in art and antiques involves natural and legal persons who act as intermediaries between the owner and/or producer and the buyers of the works. These functions are carried out by art and antiques galleries and auction houses, which may, on occasion, also be the owners of the works.

According to unofficial statistics[45], sales in the Spanish art and antiques market reached around €385 million, showing sustained growth since the economic crisis, during which the market suffered a substantial contraction. Despite these increases, the market in Spain is not particularly significant from an economic perspective, as it continues to have low market prices and a small share compared with other European countries. Specifically, its share of the global art market was just under 1% and accounted for little more than 2% of the value of art and antiques sales within the EU (compared to 5% for Germany, 20% for France and 63% for the United Kingdom).

Currently, Spain is a net exporter of art and antiques with a trade surplus of €14 million, as exports reached almost €94 million in 2016 and imports stood at €80 million. However, prior to the crisis, imports outweighed exports.

As for operators, in 2016 there were 2,965 companies operating in the Spanish art market, 2,845 in the gallery sector and around 120 auction houses. The **art and antiques gallery** sector includes antique dealers and/or resellers, amongst whom are small businesses and traders. There are some 650 art and antiques galleries that generate almost 70% of sales in the sector. Most galleries are concentrated in Madrid and Barcelona.

The majority of works sold (63%) in Spanish galleries were sold for less than €5,000, compared with 36% of such works worldwide, and only 1% were priced above €250,000 (compared with 5% worldwide), which highlights the risks of money laundering and terrorist financing. Online sales accounted for 5% of gallery sales.

[44] Chapter IV of Law 37/1992 of 28 December on Value Added Tax.
[45] Data from "The Spanish Art Market 2017". La Cai Foundation. Clare McAndrew.

There are currently around 120 auction houses, with some 50 located in Madrid and Barcelona. It is estimated that sales in the sector totalled €74.9 million (including public auctions, online sales and private sales), remaining relatively stable in terms of the number of sales. One of the key characteristics of the auction sector in Spain is the relatively lower market price. In 2016, 97% of lots sold for less than €50,000 and only 0.5% sold for more than €250,000.

Regulation of the sector is scattered across various provisions, and depending on the type of asset in question, there will be provisions, permits and licences of different kinds. From a tax perspective, the sale of works of art and antiques is subject to a special VAT regime designed to prevent the reselling trader from having to bear part of the input VAT not deducted by the previous owner of the asset.

As regards the regime for the prevention of money laundering and terrorist financing, in accordance with applicable European regulations and Spanish law, natural and legal persons who trade professionally in works of art and antiques (dealers, art galleries, auction houses, etc.) are obliged parties and must apply the ML/TF prevention measures provided for by law.

Vulnerabilities and sectoral risk.

This is a sector with significant **inherent risk** and, as expressly stated in the Supranational Risk Assessment (SNRA) produced by the European Union, this risk applies to both money laundering (ML) and terrorist financing (TF) operations. The greater exposure to ML/TF risk in the buying and selling of works of art and antiques is due to several reasons:

- The characteristics of this market and the use of intermediaries facilitate anonymity and the concealment of the identity of the true owner and the customer.

- The buying and selling of these items and their successive transfers hinder both the investigation of possible predicate offences from which the funds originate, and the traceability of those funds and the goods, which may change hands rapidly and, on other occasions, only apparently so, allowing for the execution of several high-value transactions in a simulated manner.

- It is a market that is difficult to control, in which informal channels for the sale of goods exist outside the normal trade of professionals. This type of unofficial operation may involve cash transactions, making it even more difficult to identify those involved.

- The identification and valuation of the items to be bought or sold is context-dependent and can prove particularly difficult and subjective.

- These are goods that may have a high economic value, making them particularly attractive in certain operations involving the concealment of funds or sales to third parties. As has been established in investigations and prosecutions, these are items that are attractive to organised crime groups, not only in Spain but globally: the concealment of illicit funds through the acquisition of these goods; investment in assets of assured value for subsequent sale and recovery of funds; payment of a premium for goods linked to operations to recover the amount by the buyer, amongst other types of schemes.

Certain segments of the art and antiques trade are particularly vulnerable due to the risk of being exploited for money laundering and terrorist financing purposes. These risks may include criminal activity (voluntary participation through high-value transactions or commissions for involvement) or the unwitting misuse of professional services (high exogenous or activity-related risk), without there being, in these cases, any connection to or knowledge of the illegal activity or the illicit origin of the funds.

In the face of these inherent risks, there are a number of factors and measures that mitigate the resulting risk: these are professional dealers, with a high degree of specialisation and a recognised code of ethics; there is a Catalogue of High-Risk Transactions, which provides a list of examples of transactions likely to be linked to ML/TF, with the aim of helping these professionals identify clients and transactions most likely to be linked to illicit activities; professionals in this sector are regulated entities and must comply with the preventive obligations expressly set out in the legislation.

This level of compliance and awareness of their obligations does not appear to be uniform across the sector, as evidenced by the supervisory reviews carried out and the extent and quality of transaction reporting, with differences in the application of preventive obligations depending on the size of the entities.

Larger entities (with a higher risk of abuse) must comply with the standard regime of preventive measures, although retail transactions are subject to a simplified regime due to lower exposure to money laundering risk. Furthermore, as in other non-financial sectors, there is a less stringent regime of internal policies and procedures for smaller entities (those with fewer than ten employees and an annual turnover or balance sheet total of less than two million euros) due to their lower exposure to the risk of money laundering.

With regard to the risks of terrorist financing, it is important to note the existence of trade in cultural goods originating from countries in conflict, with the aim of raising funds for terrorist organisations. In this regard, although European and national regulations establish a series of highly restrictive measures on the import and trade of cultural goods, commercial activities linked to these goods have been detected in informal channels, the origin and trade of which are connected to terrorist financing operations.

Conclusion.

The professional trade in art and antiques involves various significant inherent risks (identification of the true buyer and/or seller, the economic value of the item, the use of cash, its transferability and the difficulty in tracking transactions, durability, potential appreciation based on subjective criteria, etc.), which lead to greater exposure to being exploited by organised crime groups.

This misuse can occur in various ways: through the control of entities in the sector, through the participation or collusion of professionals, or through the abuse of entities that carry out legitimate commercial activities in this sector to conduct ML/TF operations through them without their knowledge.

However, these risks are mitigated by various regulatory, supervisory, informational and sector-wide awareness-raising measures that limit exposure to such risks, resulting in a lower residual risk, which is further supported by the small scale of transactions and the sector's relatively insignificant economic volume in our country. These regulatory measures governing transactions in the sector lead to the conclusion that in Spain we face a **moderate** level of residual **ML/TF** risk**.**

l) Professional trading in other high-value goods.

Activity, context and regulatory framework.

There are products not included in the previous sections which, due to their high value, may pose a ML/TF risk. Specifically, and primarily but not exclusively, these include high-end vehicles and motorcycles, pleasure craft, aircraft and high-cost accessories.

The professional trade sector for high-value goods consists of 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 high-net-worth clients, established in our country through franchises or subsidiaries. Compared to other countries, these types of companies are small, with an annual average turnover from luxury goods that is lower than in other countries.

Regulation of the sector is scattered across various provisions, and depending on the type of goods in question, there are provisions, permits and licences of different kinds. The regime for authorising and supervising the activity is assigned to various regional authorities. As regards compliance with AML/CFT obligations by entities in the sector, it should be noted that the regulations already include such obligations, with entities being required to comply with specific preventive duties expressly provided for in the legislation.

Sectoral vulnerabilities and risks.

The vulnerability of the high-value procurement sector has been assessed in the Supra-National Risk Assessment (SNRA) prepared by the European Union as significant/very significant, and its analysis and assessments are similar to those relating to the purchase of gold or diamonds. This document bases the risk level, above all, on the lack of organisation and knowledge within the sector and the possibility of cash transactions.

These vulnerabilities can be applied to a certain extent to the Spanish context, although it should be noted that the risk is geographically concentrated in tourist destinations with higher purchasing power, as well as in certain commercial areas of major cities, and, in particular, the fact that in Spain the use of cash has for some years been subject to significant restrictions in terms of the amount involved, which greatly hinders its use in this type of commercial transaction.

There is a high **inherent risk**, as this is a sector that deals in items highly attractive to organised crime groups, as has been confirmed by investigations and prosecutions, not only in Spain but globally: the concealment of illicit funds through the acquisition of such goods; investment in high-value goods for their subsequent sale and the recovery of funds; the mere possession of luxury goods; the payment for services using these goods; and so on.

The use of cash is a common practice in the types of offences detected and, in Spain, had been in use prior to the adoption of tax measures that limit the use of cash to payments below a threshold of €2,500 for residents. In addition, there are other obligations for those who trade professionally in goods, relating to the possible splitting of transactions into several operations that appear to be linked in some way.

These significant restrictions on the use of cash have led to a clear reduction in risk, prompting changes in the methods used by criminals to continue attempting to maintain the buyer's anonymity and, as far as possible, hinder their identification. To this end, there has been an increase in purchases made through legal entities, whether Spanish or foreign, acting as intermediaries between the actual buyer and the seller, or funds from accounts located in third countries are used for purchases; in some cases, these countries are considered high-risk territories or even tax havens, regardless of whether the customer is a resident of those countries or not.

Conclusion.

As noted in the SNRA, the inherent risk exposure in the high-value goods trade sector is considered very significant, as it has been found that criminal organisations repeatedly acquire such goods using illicit funds. Conversely, this sector is considered of little relevance with regard to terrorist financing.

Whilst regulatory restrictions on cash payments reduce risks, a lack of awareness of obligations regarding ML/TF prevention and the breadth and heterogeneity of the sector lead to an assessment that the residual risk level is **moderate/significant** for **ML** operations and **low** for **TF** operations.

m) Investment in tangible assets.

Activity, context and regulatory framework.

This refers to the non-financial activity of trading in goods with a price refund offer and, in most cases, with a revaluation offer, which is expressly regulated by the Consumer Protection Act on the sale of goods with a price refund offer. The goods covered in this section would be stamps, works of art, antiques, jewellery and other goods that "can be touched" and have market value, some of which are already covered in other sections of this NRA. Brokerage in the market for tangible goods is an activity subject to the rules on commercial agency set out in the Commercial Code, and this regime was supplemented in 2003 by consumer protection legislation.

Currently, the market for these services is minimal in economic terms.

Vulnerabilities and sectoral risk.

With regard to their use for money laundering purposes, the situation facing this type of entity is similar to that of investment firms, although the fact that they are not subject to prudential supervision exacerbates the risk. Consequently, the endogenous or intrinsic risk of being infiltrated by a criminal organisation engaged in fraud is high.

The specific legislation aims to put an end to the legal uncertainty highlighted by certain legal proceedings against entities in the sector that were involved in fraudulent activities. These legal proceedings revealed that such establishments did not carry out financial activities, were not subject to supervision, and that the clients of these entities were not protected by the established investment or deposit guarantee schemes.

Such entities no longer operate in Spain following the fraud scandals, the prosecutions and the media coverage. In general, investors have lost confidence in placing their funds with these investment firms; consequently, regardless of the level of risk, their exposure and impact are currently of little relevance in terms of ML and very low in TF.

Conclusion.

Due to the current very low level of activity in this sector, it is considered that at present the residual risk level for **ML** operations is **low/moderate** and **low** for **TF** operations.

n) Cash-in-transit services provided by private security firms.

Activity, context and regulatory framework.

Cash-in-transit involves the deposit, safekeeping and professional transport of cash or means of payment, carried out by private security firms contracted, either voluntarily or compulsorily, by individuals or entities for the protection of persons and property.

The Spanish legal framework views private security as a means of mitigating risks associated with industrial or commercial activity, providing additional security that is complementary to and subordinate to public security. Private security activities include, 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 the transport and distribution of such objects. This includes the cross-border transport of funds.

Private security companies must be authorised, subject to the system of sworn declarations, and automatically registered in the Ministry of Home Affairs' National Register of Private Security. To obtain administrative authorisation, it is necessary to comply with the legally established requirements. Six companies authorised to provide cash-in-transit services are listed in the National Register: four operating nationally and two at regional level. The majority of operations carried out involve cash-in-transit services for public administrations and financial institutions with a low risk profile, whilst the provision of services to other private sector entities constitutes a smaller part of their activity.

Vulnerabilities and sectoral risk.

The inherent risk is significant both due to the large amounts of cash that may be transported and the possibility that it could be used by criminal networks to move cash of illicit origin, disguised as proceeds from commercial activities or services, for subsequent deposit into financial institutions.

Given the current stringent regulation of this sector, the endogenous risk of being infiltrated by criminal organisations is virtually non-existent. However, there are significant exogenous risks of these entities being exploited by criminal organisations seeking to transport illicit funds for money laundering purposes. No operations, high-risk activities or patterns typical of terrorist financing activities using this type of service have been detected.

This is a sector with a high degree of compliance with the law, which is the essence of private security activity; it has a rigorous system of control measures in place for the conduct of this activity and, furthermore, is subject to ML/TF prevention obligations, meaning that the residual risk in this area is negligible.

Conclusion.

The cash-in-transit sector has significant inherent risks; however, given the stringent regulation, the high level of control, its very small scale and its status as an obliged entity with a proven high level of knowledge and compliance with ML/TF prevention obligations, the residual risk is assessed as **moderate** for **ML** activities and **low** for **TF** activities.

(X) RISKS BY TYPE OF COMPANY AND LEGAL INSTRUMENT. TRUSTS.

The current legal framework in Spain permits the incorporation of different types of legal entities. There are two main groups: on the one hand, commercial companies and their various forms of incorporation and operation; and, on the other, associations and foundations, which are analysed in the following chapter.

Both their purposes and the regulations governing their incorporation and requirements, their statutes, governing bodies, operating regimes, financial systems and supervisory models differ for the various types of legal entities, which undoubtedly affects their risk of being used for ML/TF.

Similarly, the extent to which they are established and developed varies greatly: in Spain, there are two main types of commercial companies that account for over 99% of all companies: limited liability companies (S.L.) and public limited companies (S.A.).

Specifically, the types of legal entities, their governing regulations and the approximate number of registered entities are as follows[46]:

	No. of registered entities (no. of entities incorporated in 2017–2018)	**Main legislation**[47]
Company of limited limited, S.L.	1.2 million (93,911 in 2017) (94,694 in 2018)	Royal Legislative Decree 1/2010 of 2 July, text consolidated Law of Companies of Capital (updated Dec 2018). Act 3/2009, of 3 April April, on structural to commercial companies (updated Oct 2014).
Public limited company, S.A.	80,000 (426 in 2017) (438 in 2018)	Royal Legislative Decree 1/2010 of 2 July, consolidated text Companies Act (updated Dec 2018). Law 3/2009 of 3 April on structural changes to commercial companies (updated Oct 2014).
Groups of Economic Interest (AIE).	3,000 (175 in 2017) (294 in 20108)	Law 12/1991 of 29 April on Economic Interest (updated July 2009). Council Regulation (EEC) No 2137/85 of 25 July 1985 on the establishment of a European Economic Interest Grouping (EEIG).

[46] Source: "Spain in Figures 2019", by the National Institute of Statistics (INE). Central Business Register.

(47) Furthermore, account must be taken of the relevant registration regulations (for example, Royal Decree 1784/1996 of 19 July, approving the Regulations of the Commercial Register).

General partnership.	155 (33 in 2017 – including limited partnerships) (1 in 2018)	Comercial Code (updated Dec 2018).
Limited p a r t n e r s h i p .	81 (33 in 2017 – including general partnerships) (4 in 2018)	Royal Legislative Decree 1/2010 of 2 July, consolidated text of the Companies Act (updated Dec/2018).
Cooperatives and Agricultural Companies of (SAT).	20,707 (1,148 cooperatives in 2017 and 1,228 in 2018) 12,348 SATs (76 created in 2017)	Law 27/1999 of 16 July on Cooperatives (updated April 2015). Order of 14 September 1982, implementing Royal Decree 1776/1981 of 3 August, approving the Statute governing Agricultural Processing Companies.
Mutual Guarantee Societies (SGR).	900 (1 in 2017 (1 in 2018)	Law 1/1994 of 11 March, on the Legal Framework for Mutual Guarantee Societies. (updated April 2015). Royal Decree 2345/1996, of 8 November, on administrative authorisation rules and solvency requirements for SGRs. (updated Feb 2008).
Associations.	48,000 (328 in 2017) (359 in 2018)	Organic Law 1/2002 of 22 March, regulating the right of association (updated Oct 2011).
Foundations.	14,000 (404 in 2017) (428 in 2018)	Law 50/2002 of 26 December on Foundations (updated Oct 2016).

a) Commercial companies.

Activity, context and regulatory framework.

(1) Limited Liability Company. S.L.

This is the most common form of company in Spain: there are around 1.2 million limited liability companies (92% of all companies). Around 94,000 new companies of this type are set up each year, with paid-up capital totalling around 5 billion euros annually. By sector, the creation of this type of company is most prominent in the construction sector (almost 30% of all companies and 65% of paid-up capital), followed by the hospitality sector (10% of the total).

The reasons for such significant figures stem primarily from the fact that in this type of company, the entity is liable to third parties, whilst the partner is not personally liable with their assets for the company's debts, their liability being limited to the capital contributed. Furthermore, although the procedures for their incorporation and operation require checks by the public authorities, they are relatively straightforward: they must be set out in a public deed drawn up before a notary and subsequently registered with the Commercial Registry. The capital requirements are lower than those of public limited companies (a minimum of €3,000 to be paid up upon signing the deed is sufficient) and the share capital is divided into shares, although there may be a single shareholder holding all the shares (Single-Member Limited Company).

The management structure is set out in the articles of association and may be carried out by a sole director, joint and several directors (where the actions of one bind all), joint directors (who must act jointly), or by the Board of Directors (three or more directors).

In this type of company, shareholders have priority in the transfer of shares, which limits access by third parties. The transfer of shares must be recorded in a public document, generally before a notary, but also in a judicial or administrative document, and even in a private document.

Capital increases must also be formalised in a public deed and duly registered. In 2017, there were capital increases in 28,187 limited liability companies, amounting to €20.338 billion, figures similar to those recorded in previous years (for example, in 2016 there were 28,530 capital increases in limited liability companies amounting to €18 billion).

Limited liability companies (S.L.) are required to have their accounts audited, unless, at the end of two consecutive financial years, they meet at least two of the following conditions: total assets do not exceed €2,850,000, the net annual turnover does not exceed €5,700,000 and/or the average number of employees during the financial year does not exceed fifty. As regards the preparation of the Annual Accounts, this is the responsibility of the directors, who must sign them, and must be completed within a maximum period of three months from the date of the financial year-end. However, the maximum period for the approval of the Annual Accounts by the General Meeting of Shareholders is six months from the financial year-end.

Once the accounts have been approved, they must be filed with the Commercial Registry for publication, together with the declaration of the company's beneficial owner. Failure to file them may result in various penalties, including, amongst others, the company's removal from the registry or a ban on contracting with the public administration.

(2) Public Limited Company (S.A.)

There are around 80,000 S.A.s in Spain, accounting for 7% of all companies. Certain activities, such as banking, pharmaceuticals, insurance and pension fund management, require this type of commercial company to operate. Over the last two years, there has been a decline in the number of annual incorporations (around 400 S.A.s were incorporated in 2017 and 2018, compared to 600 in 2014 and 2015 and 500 in 2012 and 2013).

In this type of company, the minimum capital contribution is €60,000 and must be divided into registered or bearer shares (in the latter case, these are an absolute minority). The share certificate and provisional certificates must meet a series of legal requirements:

- Relating to the company: name, registered office, share capital and identifying details.
- Relating to the characteristics of the share: nominal value, number, series, etc.
- Relating to whether they are registered or bearer shares.
- If the shares are registered, they must be recorded in the register kept by the company, in which successive transfers of the shares, and the possible creation of rights in rem and other encumbrances on each share, shall be recorded. The company considers a shareholder to be anyone registered as such in the register.

Shares may be freely transferred, subject to any restrictions provided for in the articles of association, and may be listed on the stock exchange (listed public limited companies) if they meet the legally prescribed conditions, thereby allowing access to third parties; however, this consequently prevents the company from controlling the presence of persons outside the company.

Where shares are bearer shares, the transfer requires (i) the existence of a legal transaction, (ii) an effective transfer of the document representing the shares and, (iii) in order to formalise the change of ownership vis-à-vis third parties, the involvement of a notary public.

As with limited liability companies (S.L.), the entity is liable to third parties as a separate legal entity from its shareholders, and liability is limited to the amount contributed. The procedures for its incorporation and operation are similar to those for limited liability companies (S.L.), as they require a notarised deed to be registered with the Commercial Register. Registration confers legal personality and prevents the transfer of shares until the company has been registered. However, its incorporation requires a minimum capital of €60,000. The accounting and filing obligations are similar to those of limited liability companies. Furthermore, S.A.s, like S.L.s, must accompany their financial statements with a declaration of beneficial ownership.

(3) Economic Interest Groupings (AIE).

The purpose of these legal entities is limited exclusively to an economic activity ancillary to that carried out by their members. The purpose of an EIG is to facilitate or carry out the economic activity of its members through joint projects of various kinds. It is a non-profit organisation, which has implications for the risks involved. They may only be formed by natural or legal persons engaged in commercial, agricultural or craft activities, by non-profit organisations engaged in research, or by those practising the liberal professions.

The partners are the beneficiaries of the entity's profits and are also directly liable for its losses. No minimum capital is required to be paid up, but a minimum of two partners is required to form the entity. If it has European partners, it will be a European Economic Interest Grouping. Registration is mandatory. Ownership cannot be transferred, and the partners simply need to withdraw to dissolve the grouping.

The EEIG may not hold direct or indirect shareholdings in companies that are its own members, nor may it directly or indirectly direct or control the activities of its members or third parties.

(4) General Partnership.

This is a partnership that acts and is liable to third parties as a separate legal entity distinct from its partners, engaging in commercial or civil activities under a single business name. There are partners who contribute assets to the business, known as 'capital partners', whilst those who simply contribute labour are 'working partners'.

The partners' liability is subsidiary, unlimited and joint, meaning they are personally liable for any losses of the company that cannot be settled. This is a very traditional form of partnership whose use has declined over the years, and there are currently only around 1,600 general partnerships.

(5) Limited Partnership.

It is similar to a general partnership, although it has two types of partners: general partners, who are liable without limit for the company's debts and participate in the management of the partnership, and limited partners or silent partners, who do not participate in management and whose liability is limited to the capital contributed or committed.

There are two types of limited partnership: the ordinary limited partnership and the joint-stock limited partnership; however, limited partners may not vote or take part in any management decisions of the company. To acquire legal personality, they must be registered with the Commercial Register. There are only around 200 companies in Spain.

(6) Cooperatives.

These are companies formed by three or more persons who join together on a voluntary basis to carry out business activities aimed at meeting their economic and social needs and aspirations, with a democratic structure and operation, in accordance with the principles formulated by the International Cooperative Alliance.

Any lawful economic activity may be organised and carried out through cooperatives, which are governed by their articles of association. There are different types of cooperatives: for associated labour, consumers and users, housing, agricultural use, community land use, services, seafarers, credit, insurance, etc.

The share capital shall comprise the contributions made by the members and may also comprise assets and rights subject to economic valuation.

Cooperative societies require that, as a preliminary step, the draft statutes be certified by the Register of Cooperative Societies. Subsequently, they shall be formalised by a public deed before a notary and must be registered with the Register of Cooperative Societies; this act confers legal personality upon them. They must also prepare annual financial statements and file them with the Register of Cooperative Societies.

Cooperatives may be first-degree (where members are natural or legal persons), second-degree (where members are first-degree cooperatives), third-degree (comprising second-degree cooperatives) and so on. The minimum number of members is three for first-degree cooperatives and two for second-degree cooperatives. In first-degree cooperatives, the total sum of each member's contributions may not exceed one-third of the share capital, except in the case of cooperative societies, non-profit organisations or companies in which the majority of shares are held by cooperatives. Ownership cannot be transferred. Members simply need to withdraw to dissolve the cooperative.

Vulnerabilities and sectoral risk.

Inherent risk.

The use of legal entities by criminals and criminal organisations to conceal illicit proceeds, to mix them with income from lawful sources or to hinder the identification of the beneficial owner of the funds or assets has been detected in numerous investigations and prosecutions for money laundering offences and also, to a lesser extent, for terrorist financing. The inherent risk of using companies for these purposes can be considered high, but variable depending on the type of commercial company.

An assessment of the risks associated with different types of legal entities, based on the legal framework, analyses carried out by authorities and regulated entities, and a review of certain court cases and reports filed on the basis of indications, reveals variations in risk levels depending on the type of company.

For their part, the law enforcement agencies and the Special Prosecutors' Offices against Drug Trafficking and against Corruption and Organised Crime have highlighted the existence of greater ML/TF risks in certain types of legal entities, the use of which by various categories of organised crime groups has been confirmed in numerous investigations and prosecutions.

Thus, certain forms of commercial company, by their nature and composition, do not pose a risk from the point of view of their use for ML/TF purposes (general partnerships, limited partnerships, economic interest groups, etc.). However, limited liability companies and public limited companies appear to be more frequently used for ML purposes by criminal groups involved in drug trafficking, economic crimes and those related to corruption.

Limited liability companies (S.L.), being by far the most numerous, are also more commonly found in corporate structures used for ML/TF purposes. Among the risks specific to these companies, the following are worth noting:

- Transfers of shares when carried out solely by private document (without being recorded in a public deed or in a judicial or administrative document).
- Transfers of shares carried out abroad, which make it difficult for notaries to monitor and apply direct ML/TF prevention measures.
- Situations in which the S.L., once formalised in a public document, does not complete its registration, which allows it to operate despite its irregular status.
- Acquisition in Spain by foreign nationals and, to a lesser extent, Spanish nationals, of real estate in the name of dormant companies whose sole activity is the holding and management of the property. These asset-holding companies created for this purpose generally take the form of limited liability companies. Although the shareholders must be identified, either in the company's articles of association or in the relevant deed of transfer of shares, it is difficult to identify the true owner of the property.
- Cases involving chains of ownership of companies located in various different jurisdictions, designed to structure the ownership of Spanish companies for various purposes, generally to conceal the company's beneficial owner or the source of the funds. The companies holding the property or assets are, in turn, other foreign companies, which are themselves owned by other companies, ultimately leading to companies registered in non-cooperative jurisdictions or those with restrictive legislation, all with the aim of ensuring the anonymity of the company's beneficial owners. However, the beneficial ownership register at the Commercial Registry helps mitigate this risk by providing information on the companies within the chain of control of others.
- Dormant companies that do not file annual accounts with the Commercial Register, whose composition and beneficial ownership are not fully known to the authorities. These companies pose a risk from an AML/CFT perspective even though they do not carry out any activity, as they must act through notaries and generally meet the dual condition of having their entry in the Commercial Register closed and their tax identification number (NIF) provisionally suspended by the AEAT, situations which can be ascertained by any interested party through the Commercial Register's public records.
- Money laundering operations involving illicit proceeds carried out through limited liability companies (S.L.) that engage in other legitimate activities. These activities may pose a higher risk if they routinely use cash, as analysed in the relevant section.

In the case of unlisted public **limited companies**, their use for concealing funds obtained from economic crimes and corrupt activities has also been observed, although on a much smaller scale than with limited liability companies (S.L.) due to their lower prevalence in our country.

As with limited liability companies, it is possible to formalise a public limited company in a public deed yet ultimately fail to incorporate due to the lack of the mandatory registration in the Commercial Register. Furthermore, there are difficulties in identifying the parties involved when share transfers take place that are not recorded in a public deed. Company law permits the transfer of shares in a public limited company (S.A.) by private deed, which can lead to a degree of opacity regarding ownership. This point is expressly mentioned in the Mutual Evaluation Report on Spain prepared by the FATF in 2014. The transfer must be evidenced to the company by presenting the share certificate, and once the regularity of the chain of endorsements has been verified, the registered shares are entered in a register kept by the company, in which successive transfers of the shares are recorded, stating the successive holders, so that the company will only recognise as a shareholder anyone who is entered in that register. The transfer of shares is no longer registered in the Commercial Register, which leads to a lack of transparency regarding ownership.

The use of bearer shares is extremely rare in Spain, as the majority of shares in public limited companies (S.A.) are registered. No amendments to the company's register are required for their transfer. The register merely records the number of bearer shares issued when the S.A. is formed and their serial numbers, without including details of their owners. This is the system offering the greatest anonymity to shareholders.

In any case, the transfer of shares is formalised through a legal transaction with effect against third parties, involving a notary public, a judicial or administrative authority, or by private deed. This involves the participation of parties with obligations regarding the prevention of money laundering (notaries, lawyers, etc.), which will mitigate this type of risky behaviour, limit its effects and help to increase knowledge of the owner.

Residual risks. The measures established with the aim of preventing and mitigating the risks of abuse of Spanish legal entities are in place from the company incorporation stage. Specifically, the transparency of legal entities has been significantly increased, ensuring not only that basic information is accurate and available to the public via the Commercial Register, but also that the beneficial ownership of entities, including information on their ultimate beneficial owner, is available via:

a) The existing database at the OCP of the General Council of Notaries, which is duly regulated and contains information on the beneficial owners of all entities that have carried out any type of procedure requiring a notarial public deed (there is currently information on some 2.7 million entities, of which 2.5 million are commercial companies). This information is easily and quickly accessible to the competent authorities (SEPBLAC, the Policía Nacional, Guardia Civil, the Public Prosecutor's Office, etc.) and to obliged entities that have signed the relevant agreement for the purposes of customer due diligence.
b) The Register of Beneficial Ownership (RETIR) forms part of the Commercial Register. It must contain details of the beneficial owners of registered companies, as well as information on companies within the chain of control of other companies. This information is public and must be updated at least annually by the directors of the entities when they submit their annual accounts, and also whenever there are changes in their beneficial ownership. The Association of Registrars of Property, Commercial and Movable Assets is responsible for its electronic systematisation, entering into cooperation agreements to allow access to the information by obliged entities to carry out their ML/TF prevention duties, and by the competent authorities (SEPBLAC, Court of Auditors, Policía Nacional, Guardia Civil, CNMV, etc.).

In addition, the standard due diligence measures that obliged entities must apply when dealing with clients that are legal entities include verifying their identity and that of the person acting on their behalf, as well as identifying the beneficial owner, their corporate purpose, activities and the source of funds.

These AML/CFT obligations extend to the incorporation of companies, the sale and purchase of real estate, capital increases and transfers of shares, amongst many other transactions requiring the involvement of regulated entities. Subject to the caveats set out above regarding the formalisation of this legal transaction, transfers of shares and holdings shall be documented either in a notarial, judicial or administrative document, and in the case of a notarial document, recorded in their databases.

Residual risks of companies incorporated in Spain.

Existing measures significantly reduce the risk of companies being used for ML/TF purposes. In fact, they are particularly effective for certain types of companies, such as **cooperatives, limited partnerships, general partnerships and economic interest groupings**, which may be considered **low-risk.**

However, in the case of limited liability companies (S.L.) and public limited companies (S.A.), financial intelligence reports, risk analyses by notaries and registrars, police investigations and prosecutions for ML/TF continue to reveal the creation of companies and corporate networks for illicit purposes by various types of national and international criminal organisations linked to organised crime.

In these cases involving companies incorporated in Spain for unlawful purposes, these are generally companies which, despite the existing controls, manage to be set up and used for the purpose of concealing the origin of the funds used to carry out transactions. In other cases, they are set up for purely instrumental or asset-related purposes to conceal assets or securities (for example, assets or property held in the name of companies) and to make it difficult to ascertain the true identity of the owner of the funds or assets.

The risks of companies being incorporated or acquired for such purposes are greater for commercial companies whose partners are themselves other companies. They are often incorporated in third countries and have other companies as partners, forming part of a chain or corporate network, since despite the legal obligations to identify the beneficial owners of each such company, the verification and validation of this information cannot be carried out based on the information held in national databases and registers, but must rely on the mere declarations received.

In any case, risks vary greatly within the same corporate form depending on various factors. Listed public limited companies do not pose a risk in themselves, whilst public limited companies with bearer shares carry a very high risk of being used in ML activities. Similarly, the risks associated with limited liability companies vary depending on circumstances relating to their owners, their method of incorporation and their corporate purpose. All of this implies that, for these company types, the residual risk will generally be variable, ranging **from moderate to high** depending on the specific characteristics of each company (see summary table).

Residual risks of companies incorporated abroad.

A distinction must be made:

- On the one hand, those incorporated in EU countries, particularly public-law entities (or those in which the public sector holds a majority stake) and EU financial institutions that are subject to regulation and supervision by their respective countries.
- On the other hand, those companies incorporated in high-risk jurisdictions or those controlled or partly owned

mainly by other companies incorporated in those high-risk jurisdictions.

The transnational nature of corporate transactions means that, on occasion, these are transactions carried out in our country by entities incorporated in third countries whose owners are, in turn, other companies established in third countries within a complex chain of companies and countries of incorporation. These companies are therefore subject to different incorporation and corporate transparency regulations, particularly regarding the application of customer due diligence and the identification of the beneficial owner, with a chain of incorporation acts and rules interposed within the chain of ownership that greatly hinders the tracing of these funds and their beneficial owners beyond the mere declaration of their legal representatives.

This risk increases if the legal entity is resident in jurisdictions whose incorporation requirements and supervisory policies and practices do not meet the minimum standards required in Spain.

This generally implies greater opacity, which makes it difficult to mitigate these ML/TF risks through the measures required of domestic companies. Consequently, these companies established abroad can be more easily used to conceal illicit funds or disguise the true owner of the funds or the beneficial owner of the assets through a company operating in Spain. In short, as is the case with companies incorporated in Spain, the risks vary greatly within the same type of company depending on various factors.

In general, transactions carried out in our country by the vast majority of companies incorporated abroad should be considered to be of **moderate** risk. However, this risk increases exponentially in the case of companies whose owners are chains of companies; when they are incorporated in certain high-risk jurisdictions; when they operate in our country for instrumental or asset-related purposes in certain sectors, amongst other situations. In such cases, the risks should be considered **significant or high** depending on their place of incorporation, chain of ownership, corporate purpose and the type of activity carried out in our country (see summary table).

b) Trusts and similar fiduciary structures.

Activity, context and regulatory framework.

A trust is a contractual legal relationship whereby a person (the *settlor*) transfers funds, property or assets owned by them to another person (*the trustee*) or entity (a trust company or fiduciary services provider) to be administered or managed for a specific purpose or to be delivered to a third party (beneficiary) should certain circumstances arise or specific time periods elapse.

Although the trust is the most widespread form of fiduciary structure internationally, there are similar instruments recognised by other legal systems, such as the fiducia or the treuhand, to which the obligations established in relation to trusts should generally be extended[48].

The persons or entities providing these services (fiduciaries or *trustees*) may be either professionals who are remunerated for their services as fiduciaries (for example, depending on the jurisdiction, a lawyer or a trust company), or non-professionals (for example, a person acting on behalf of a family without any remuneration).

[48] The European Commission has published a list of entities similar to trusts: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2020.136.01.0005.01.ENG&toc=OJ:C:2020:136:TOC.

Under Spanish law, the creation of trusts or other similar instruments or structures is not permitted fiduciary entities similar to trusts, nor entities dedicated to their formation; in other words, there are no Spanish trusts or fiduciary entities or *trustees* established in Spain that are dedicated to setting up or managing trusts or similar fiduciary structures. Our legal system provides solely for the existence of testamentary trusts, consisting of a provision in a will whereby the testator leaves their assets to a person (trustee) so that the trustee may use those assets for a specific purpose. It is a testamentary mandate based on trust, which bears no relation whatsoever to the characteristics of inter vivos legal transactions found in Anglo-Saxon trusts or certain international trusts of a similar nature.

Notwithstanding the above, there is nothing to prevent trusts or similar entities from acting in Spain as clients of regulated entities or as owners of property and assets in our country, nor are transactions by trust companies or *trustees* incorporated abroad that manage these trusts or fiduciary structures prohibited. This clearly increases the risk that these structures may be used in Spain for ML/TF purposes.

Consequently, given the existence of trusts or similar structures established in other jurisdictions and of fiduciary entities or *trustees* operating as clients of entities within our financial and non-financial system, these legal instruments are subject to AML/CFT regulations and are classified as obliged entities.

Furthermore, when a trust or similar structure acts as a customer, obliged entities must adopt a series of specific preventive measures and must assess the ML/TF risk associated with business relationships or transactions with them.

It is not yet possible to quantify the number of trusts and trustees operating in our country (the register is currently under development), but SEPBLAC has made an estimate using indirect methods, concluding that their presence as clients of obliged entities in Spain is negligible. Conversely, their involvement as senders of funds from abroad to Spain is greater.

The General Council of Notaries, through its OCP, has also carried out a study on the presence of trusts in notarial acts, revealing that the vast majority of notaries (2,918 out of 2,941) have never carried out transactions involving trusts, which has a significant impact from a risk perspective.

Furthermore, individuals who may act as trustees in a trust or similar legal instrument, or arrange for another person to perform such functions, have been required since 2019 to register with the Commercial Register as service providers to companies and trusts.

Vulnerabilities and sectoral risk.

Inherent risk. Although these are uncommon instruments in our country and their creation is not permitted under our legal system, the competent authorities at the preventive, supervisory and enforcement levels, and the regulated entities most closely associated with this type of entity, have highlighted the high risks inherent in ML in Spain arising from the potential misuse of trusts and similar structures established abroad.

This potential use by criminals, criminal groups and organisations engaged in money laundering would seek to conceal the identity of the owner of the assets and the origin of the funds and assets managed through these legal structures, which entails a high exposure to risk for these legal instruments.

The establishment abroad of these trust-type legal arrangements may be intended to operate in Spain or to send funds to Spain under conditions of greater opacity. They are created and registered in certain foreign jurisdictions because their legal systems facilitate the establishment of trusts or fiduciary structures by lawyers, companies or agents resident in those jurisdictions. These professionals, in turn, frequently act as trustees under legal conditions that differ from those established in our legal system, which allows them to

operate in Spain under conditions of less transparency than domestic companies and professionals.

This concern is even greater with regard to the risks arising from certain types of trusts or similar structures, such as those which:

- Involve one or more natural or legal persons or legal instruments in the chain of control, in most cases with the aim of obscuring the identity of the beneficial owner of that structure and the origin of the funds and assets managed.
- Are purely instrumental in nature, that is to say, they are structures that hold property and assets but do not carry out any asset management, commercial or financial activities, being mere asset holders.
- Have been incorporated in certain higher-risk jurisdictions without apparent economic justification (offshore corporate vehicles, shell companies, use of nominee owners, etc.).
- They hold funds or assets in those jurisdictions.
- They carry out transactions, including payments and receipts, with no clear connection to the purpose of the trust.
- They *are* structured as *asset* protection *trusts*.

In general, criminal organisations that use trusts or similar arrangements and companies providing such fiduciary services – trustees – for their operations or to send funds to our country, also tend to use shell companies or proxies, attempting to add intermediate layers that make it more difficult to identify the client.

The use of intermediaries is intended to conceal the existence of a trust established abroad, as its detection could trigger a more rigorous system of due diligence or reporting on suspicion by regulated entities in Spain, due to the mistrust these instruments arouse in our country owing to their limited tradition and presence.

Consequently, complex networks of companies and legal instruments have been detected which, on occasion, comprised trusts or similar fiduciary structures, established in offshore financial centres with various natural or legal persons or other legal instruments acting as intermediaries in the chain of control.

With regard to potential TF risks, the EU's Supranational Risk Assessment indicates that such legal instruments are not attractive to groups engaged in TF activities. The structure of trust arrangements does not allow for the rapid management or disposal of funds that typically accompanies TF activities and requires a series of conditions to be met in order to be implemented, which hinders the use of these structures for TF purposes and clearly reduces their exposure to risk in relation to such activities.

Residual risk. Awareness of these inherent risks has led to the incorporation into our ML/TF prevention regulations of a series of measures relating to these legal structures with a view to mitigating them. Specifically, obligations have been introduced such as the requirement to obtain the constitutive document (*deed of trust, trust instrument, trust will,* etc.) and the obligation to identify all parties involved in these trusts or legal instruments when they act as clients of regulated entities, whether financial or non-financial.

This identification obligation applies both to the manager of the corporate structure (fiduciary or *trustee*) and to the parties involved—the settlor, beneficiary and protector, if any—as well as to the beneficial owners of all of them.

In addition, the trustee is required to declare their status to the obliged entities involved in any transaction in which they act on behalf of the beneficiaries or in accordance with the terms of the trust. In this case, the obliged entities must require the trustee to provide the relevant documentation relating to the trust (deed of trust, endowment funds, powers of the trustee, etc.), the settlor (business activity, possible PEP status, etc.), the trustee's accreditation and the powers held by the trustee.

For further information on the risk indicators affecting the various elements and parties involved in trusts, SEPBLAC has drawn up a "Guide to compliance with due diligence obligations in relation to Anglo-Saxon trusts and other similar legal instruments", which details these indicators to facilitate a better understanding by obliged entities dealing with them and to better mitigate the risks involved in these activities.

The OCP of the General Council of Notaries has also issued instructions on the customer due diligence measures applicable to trusts and similar entities, which include the obligation to request the trust deed and to identify and verify the identity of the beneficial owners. Furthermore, guidance is provided, along with a series of risk indicators linked to the use of trusts.

Alongside the awareness that regulated entities have of the higher risk posed by such structures when acting as clients, they also have a high degree of awareness of the existence of additional risks, which leads regulated entities to generally adopt a defensive approach, being reluctant to have direct relationships with foreign trusts which, however, albeit in limited cases, operate through the intermediation of a commercial entity.

Thus, regulated entities, particularly those in the financial sector, are aware of the additional risks associated with the place of creation of these structures, such that, depending on the jurisdiction of origin, they are subject to more rigorous controls.

Conclusion.

The high risks inherent in trusts and similar structures stem mainly from the fact that they must be established in third countries whose legal systems allow such trusts to be set up under special conditions that differ from those required by our regulations. This enables them to operate in Spain as clients of regulated entities under conditions of reduced transparency, making it difficult to identify their beneficial owners and the origin of the funds.

All of this has led to the adoption of stricter specific regulatory measures regarding AML/CFT for trusts and similar entities when they operate in our country. Guidelines have also been drawn up for regulated entities, setting out guidance, and these entities have been implementing special risk-based measures.

Furthermore, the small number of trusts operating in our country means that, generally speaking, there is a certain degree of wariness about dealing with this type of entity, particularly when it comes to financial transactions, which significantly limits the ability of trusts to operate as clients in Spain and the potential risks involved. For all these reasons, it is considered that the residual risk for **ML** operations should be classified as **moderate/significant**.

As for TF risks, the very nature of this type of entity does not facilitate the use of entities established abroad for TF activities in our country, as there are clear difficulties regarding the availability and transferability of funds with the immediacy and agility required for TF activities. Currently, the establishment of such entities abroad for use in Spain by criminal organisations as a vehicle for **TF** is not considered a risk and should be regarded as **low**.

SUMMARY TABLE

(i) Risks by type of company in Spain

Type of company	Risk
Cooperatives.	**Low**
Limited partnerships.	**Low**
General partnerships.	**Low**
Mutual guarantee societies.	**Bass**
Economic Interest Groups (EIGs).	**Under**
Limited companies in general (1).	**Moderate**
Specific limited companies (2). Examples: Purely asset-holding or special-purpose companies; companies whose shareholders are complex corporate chains or networks; companies whose beneficial ownership cannot be verified by the authorities or by regulated entities through direct means; companies whose owners are nationals or residents of high-risk countries; companies with no public information on their activities; companies that frequently change their structures without apparent reason, etc.	**Significant/High**
Listed public limited companies.	**Low**
Public limited companies with registered shares.	**Moderate**
Public limited companies with bearer shares.	**High**

(ii) Risks associated with entities or legal instruments operating in Spain that are incorporated abroad

Type of company	Risk
Public-sector bodies from the EU or equivalent/similar countries, or entities in which such bodies hold a majority stake.	**Low**
Financial institutions domiciled in the EU or equivalent/similar countries (excluding payment institutions).	**Low**
Client companies whose owners are foreign legal entities domiciled in the EU or equivalent/similar countries.	**Moderate**
Corporate clients belonging to complex corporate structures with their ultimate domicile in the EU.	**Moderate/Significant**
Client companies belonging to corporate structures with a complex chain of companies incorporated in different countries.	**Significant**
Client companies incorporated or domiciled in high-risk jurisdictions.	**Significant/ High**
Client companies controlled or majority-owned by other companies incorporated in high-risk jurisdictions.	**Significant/High**
Client companies belonging to complex corporate structures with a complex chain of companies ultimately domiciled in high-risk jurisdictions.	**High**
Client companies whose activity is purely instrumental or asset-based.	**Moderate/Significant**
Client companies whose activity is purely instrumental or asset-based, incorporated in high-risk jurisdictions.	**High**
Client companies whose declared beneficial owner cannot be verified by the authorities or by regulated entities by direct means.	**Moderate/Significant**
Client companies whose declared beneficial owner cannot be verified by the authorities or by regulated entities by direct means, incorporated in high-risk jurisdictions.	**High**
Trusts and similar structures.	**Moderate/ Significant**

(XI) NON-PROFIT ORGANISATIONS (NPOs).

Activity, context and regulatory framework of the various organisations.

The concept of non-profit organisations (NPOs) encompasses organisations of various kinds, and according to the definition used by the FATF, it would include "persons, legal structures or organisations primarily engaged in the collection or disbursement of funds for charitable, religious, cultural, educational, social or fraternal purposes, or for the performance of other types of good works".

The non-profit sector in Spain is made up of legal entities of a non-corporate nature. By virtue of their purpose, they are a fundamental part of the social fabric, complementing public social action by channelling private efforts towards the achievement of objectives of general interest.

For the purposes of this analysis and in accordance with the FATF definition set out above, the following types of entities are considered non-profit organisations:

a) **Public benefit associations**.
b) **Foundations**.
c) Organisations in the so-called **"third sector"**, including non-governmental development organisations (NGDOs) as referred to in Law 23/1998 of 7 July on International Development Cooperation, provided they have one of the legal forms referred to in the preceding paragraphs. The "third sector" also includes humanitarian organisations and social action organisations.
d) **Religious associations**, federations, confederations and foundations registered in the Ministry of Justice's Register of Religious Entities.

Likewise, non-profit organisations also include the branches of foreign foundations registered in the Register of Foundations and the federations and associations of non-profit entities referred to in paragraphs (a) to (c).

NPOs must pursue objectives of general interest, such as, amongst others, the defence of human rights and of victims of terrorism and violent acts, social assistance and social inclusion, civic, educational, cultural, scientific, sporting, health, labour, institutional strengthening, development cooperation, promotion of volunteering, promotion of social action, defence of the environment, promotion of and support for people at risk of exclusion for physical, economic or cultural reasons, promotion of constitutional values and defence of democratic principles, the promotion of tolerance, the promotion of the social economy, the development of the information society, scientific research, technological development or innovation, and the transfer of such innovation to the productive sector as a driver of business productivity and competitiveness.

(a) Associations and public-benefit associations.

Associations are non-profit legal entities comprising three or more natural or legal persons who undertake to share their resources and operations in order to achieve the common interests set out in the statutes governing the association's operation. The relevant legislation (Organic Law 1/2002 of 22 March on the Right of Association) also applies to churches, religious denominations and communities, sports federations, professional associations, trade unions and political parties.

Associations, in turn, may group together to form federations, confederations and unions of associations, which are second-tier entities whose promoters and members are legal persons of an associative nature previously registered in the general registers of associations.

According to data from the Ministry of Home Affairs[49], at the end of 2018 there were 56,181 active associations, of which 21,612 were active in the educational, cultural and ideological sectors, followed by 20,380 in the economic, technological and professional sectors, and 5,303 in the health and environmental sectors.

Associations may serve a public or private interest. Only those that have been **declared to be of public utility** by the Administration, in accordance with the procedures and requirements laid down in the regulations, are eligible for the special tax regime provided for NPOs and for tax incentives for patronage. Specifically, they must have been registered as an association for a period of at least two years immediately prior to their application, which allows for an analysis of the accounts and verification that the association has the appropriate resources and organisation to fulfil its statutory purposes. To apply for the declaration of public utility, associations must submit two activity reports and the annual accounts for the last two financial years, certified by the AEAT and the Social Security Treasury.

At the end of 2018, there were 3,092 Public Utility Associations registered in the National Register of Associations, with their main areas of activity being education, communication, cultural and ideological associations, health, the environment, technology and disability.

Public benefit associations are required to submit annual accounts to the Public Administration and must keep their accounts in accordance with the General Accounting Plan for Non-Profit Organisations.

Associations must maintain an up-to-date list of members, submit accounts of their financial results, carry out an inventory of their assets and retain the minutes of meetings held by their governing bodies and representatives. Furthermore, each association is required to keep a register identifying donors and beneficiaries for a period of 10 years. This information is available to the Public Administration or the competent AML/CFT authorities.

b) Foundations.

Foundations are legal entities characterised by being non-profitmaking and having objectives of general interest that benefit the general public; it is expressly prohibited to act for the benefit of the founders, the board of trustees, their relatives or specific legal entities that do not pursue objectives of general interest.

They are subject to specific regulations (Law 50/2002 of 26 December on Foundations and its implementing regulations), and the tax regime for non-profit organisations and tax incentives for patronage apply to them.

According to the Spanish Association of Foundations, Asociación Española de Fundaciones (hereinafter, AEF), there are more than 14,000 registered and active foundations in Spain, of which over 8,000 are currently active. The main areas of activity are culture and leisure (40%), education and research (21%), the environment (10%) and social services (9%).

In terms of size by revenue, the majority are small and medium-sized foundations, as only 11.26% of active foundations have an annual revenue exceeding 2.4 million euros. It is worth noting that most foundations operate at a national level, particularly at a regional level. Only 12.17% operate internationally, and less than 5% state that international activity is their main focus.

As for sources of income, around 55% comes from donations and grants, with private sources predominating. Income from public sources accounts for 20%, whilst 10% comes from financial institutions.

[49] Statistical Yearbook of the Ministry of Home Affairs 2018.

Their establishment requires a public document drawn up before a notary and they must be registered in the Register of Foundations to acquire legal personality. Only entities registered in that Register may use the designation 'Foundation'. To carry out the initial registration of the foundation in the Register, a mandatory and binding report from the relevant Protectorate is required regarding the suitability of the foundation's purposes and the adequacy of its endowment. The registered office cannot be located abroad if its operations are domestic.

National foundations are registered in the Single Register of Foundations, which is also responsible for the registration, recording and filing of acts, legal transactions and documents relating to them. The Register is public and shall contain, amongst other information, the filing and publication of the action plan and the annual accounts, accompanied, where applicable, by the audit report and the annual report on compliance with the codes of conduct for making temporary investments. In August 2019, there were 4,900 foundations registered in the Register.

Throughout the life of a foundation, its governing body, known as the board of trustees, carries out a series of administrative and management tasks designed to comply with the provisions of current legislation on foundations. This is the foundation's governing and representative body, responsible for fulfilling the foundation's objectives and diligently administering the assets and rights that make up the foundation's estate, whilst maintaining their yield and utility. The board of trustees shall consist of a minimum of three members, who may be either natural persons or legal entities.

The State Foundation Protectorate provides advice, guidance and support to foundations that are already registered, or in the process of being established, regarding their legal, economic, financial and accounting frameworks.

Foundations, like public-benefit associations, must maintain their accounts in accordance with the General Accounting Plan for non-profit organisations. At the state level, the Protectorate is responsible for reviewing and monitoring the annual accounts and action plans that foundations are required to submit annually. Thus, once these have been examined and their formal compliance with current regulations regarding annual accounts has been verified, the Protectorate will file them with the Register of Foundations. Any person may obtain information from the documents filed.

Annually, the state-level Protectorate sends the AEAT the lists of foundations that have duly complied with the obligation to submit annual accounts and of those that have failed to comply with this obligation or have not responded to the Protectorate's requests aimed at ensuring compliance with the obligation to submit the said accounts.

The Protectorate and the Board of Trustees, in the exercise of the functions conferred upon them by Law 50/2002 of 26 December on Foundations, and the staff with responsibilities for the management of foundations shall ensure that these are not used for money laundering or to channel funds or resources to persons or entities linked to terrorist groups or organisations.

To this end, the State Protectorate of Foundations actively collaborates with other agencies and ministerial departments in its monitoring of foundations, in particular with the AEAT, the Guardia Civil and the Centro Nacional de Inteligencia (CNI).

With the aim of helping foundations to manage their own affairs more effectively and ensuring greater transparency in their operations, there are various initiatives, such as those run by the AEF, the Lealtad Foundation and the Coordinating Body of Development NGOs, which issue certificates attesting to a foundation's level of compliance or establish transparency indicators for foundations. These indicators are reviewed periodically so that foundations can not only meet the transparency standards set out in the relevant legislation (Law 19/2013 of 9 December) but also adapt to the sector-specific regulations in force at any given time.

Like associations, foundations are required to keep a register of donors and beneficiaries for 10 years. This information is available to the Public Administration or the competent AML/CFT authorities, in accordance with Article 39 of Law 10/2010.

c) "Third sector": Non-Governmental Development Organisations (NGDOs), humanitarian organisations and social action organisations.

In a nutshell, the "third sector" refers to those private organisations that are not aimed at generating profits for their owners but rather at carrying out activities aimed at the development of other countries and/or at carrying out humanitarian and/or social action activities.

Within the sector, Non-Governmental Development Organisations (NGDOs) stand out; these are private, legally constituted, non-profit organisations which have, amongst their aims or as their express purpose, in accordance with their own statutes, the carrying out of activities related to the principles and objectives of international development cooperation (Article 32 of Law 23/1998 of 7 July on International Development Cooperation).

NDOs may register in the Register maintained by the Spanish Agency for International Development Cooperation, Asociación Española de Cooperación Internacional para el Desarrollo (hereinafter, AECID) or in any registers that may be established by the Autonomous Communities, with the relevant cooperation procedures to be established to ensure the communication and standardisation of registered data. This registration is essential for receiving official aid to fulfil their development aid objectives and to obtain tax benefits; the suitability of the organisations must be verified, as well as the accuracy of the registered data, and the necessary measures must be taken to ensure that the information collected is kept up to date. This obligation to update falls on the NGDOs, which must submit their information within the first four months of each year or three months after the relevant specific changes occur.

There are more than 2,000 organisations registered in the Register; the majority of NGDOs are organised as foundations (54.3%) or associations (37%), whilst the remainder are federations of either of the two aforementioned types or have special legal forms. The organisational structure varies, with some NGDOs belonging to the AEF, others to the Coordinating Body of Development Cooperation Organisations, Coordinadora de Organizaciones no Gubernamentales para el Desarrollo España (hereinafter, CONGDE), which in turn has regional coordinating bodies, and others belonging to both associations.

In terms of size, medium-sized NGDOs predominate. However, there is a significant concentration of income in a small number of organisations. The nine largest account for 78.2% of income.

Some 70% of NGDO expenditure is allocated to development projects, 15% to humanitarian aid, almost 6% to development education, and the remainder is used to attract donors and cover structural costs.

Depending on the type of activity, there are various types of NGDOs, with certain areas such as education, health, gender and civil society standing out, accounting for 50% of projects carried out abroad. Geographically, the Americas and Africa are the main areas of action for NGDOs.

In many cases, third sector organisations not only carry out NGDO activities but also humanitarian aid and social action within their own country or in third countries. Humanitarian aid organisations are those focused on assisting people affected by human or natural disasters and wars. Aid focuses not only on the provision of basic goods and health services, but also on the defence of human rights, the protection of victims, social advocacy, political lobbying, inclusion and support.

d) Religious organisations.

As religious organisations in Spain enjoy full organisational autonomy, as guaranteed by the Organic Law on Religious Freedom, it is difficult to identify characteristics common to all of them. Thus, there are religious organisations that are not registered and therefore lack legal personality, as it is registration as a religious organisation in the Ministry of Justice's Register of Religious Organisations that confers legal personality on these organisations and enables them to act and carry out legal transactions, have legal representatives and recognised organisational rules.

The Register allows for the registration not only of churches, denominations and religious communities and their federations, but also of entities created by them and those dependent on other religious organisations established abroad. Furthermore, it regulates the procedures for registration, amendment of statutes, change of legal representatives, places of worship, ministers of worship, membership of a federation and the dissolution of all types of religious organisations.

This regulatory framework is complemented by the declaration of well-established roots of religious denominations in Spain, a declaration which must be linked to an active presence in Spanish society and their establishment across the territory of several autonomous communities, as well as a representative number of entities and places of worship registered in the Register of Religious Entities. Likewise, they must have an internal structure and representation appropriate to their own organisation.

According to data from the Register of Religious Entities, in 2019 there were 19,153 registered organisations, of which 13,800 were Catholic, 2,700 Evangelical, 1,744 Muslim, 141 Orthodox, 86 Buddhist, 34 Jewish, 2 Jehovah's Witnesses and 1 Mormon.

Generally, their statutes stipulate that they are non-profit organisations with very limited financial resources: income comes from membership fees, public grants and donations or legacies. In the event of liquidation, the clauses generally stipulate that the assets are to be transferred to similar organisations of the same denomination.

The Ministry of Justice has created a Directory of Places of Worship, where religious organisations can voluntarily register their details. In doing so, religious organisations that have signed agreements with the Spanish State and benefit from special tax regimes publicise the existence and location of their places of worship. According to data from the Directory, almost 80% of places of worship belong to the Catholic faith (23,071), followed by the Evangelical faith (3,750) and Muslim places of worship (1,525).

Sectoral vulnerabilities and risks of NPOs.

As a preliminary point, it should be noted that FATF Recommendation 8, concerning NPOs, requires countries to adopt a risk-based approach to identify the characteristics and types of NPOs which, by virtue of their activities or characteristics, are at risk of being used as a vehicle for terrorist financing. Furthermore, the FATF requires the identification not only of the specific **terrorist financing** threats/risks relating to NPOs, but also of the ***"various ways in which these organisations may be used"*** by terrorists.

Inherent risks.

It should be noted that the sector's wide diversity makes it difficult to analyse sectoral risks in a generalised manner. As indicated, in Spain the vast majority of NPOs take the legal form of an association or a foundation; however, the risk factors are not directly linked to their legal form, but rather to the type of activity and the various parties involved, elements and circumstances of their operations, which influence variations in their inherent risk of being used for ML/TF activities.

ML risks. The inherent risks relate to the possible establishment of entities with the deliberate aim of use them for activities related to economic crimes, primarily tax evasion. In this way, the aim is to divert funds deposited in these institutions towards other purposes, in breach of the institution's own objectives, or simply to separate certain assets from the assets of a natural or legal person.

On the other hand, charitable foundations and associations enjoy a more favourable tax regime, provided they meet the requirements set out in the law and submit Form 036 to the AEAT. Furthermore, membership fees and donations are partially deductible for personal income tax or corporation tax purposes, which may lead to cases where such entities are set up as a vehicle to channel income (or assets of another nature) into this tax system, thereby avoiding standard taxation. However, the risk arising from this special regime is, in turn, offset by the existence of a legal framework of enhanced substantive and tax obligations that increases oversight and requires registration, accountability, the maintenance of accounts, and the submission of an annual financial report to the AEAT.

Therefore, in practice, the inherent risk is determined by the endogenous factor of creating entities for the purpose of engaging in potential tax evasion or fraud. However, there is no evidence that existing NPOs operating in accordance with their statutory purposes are subject to abuse or misuse by criminal networks or third parties as mere tools for money laundering (exogenous risk factors).

TF Risks. As established by the FATF's international standards and the EU SNRA, the main inherent risk associated with NPOs relates to their use as a vehicle for financing terrorism.

In Spain, as reflected in the FATF Mutual Evaluation Report of Spain (2014), there is extensive experience in the fight against TF, which has enabled the detection of the misuse of NPOs and the fraudulent creation of non-profit associations of various kinds for TF activities.

According to the information and risk assessments provided by the specialist authorities, the risks of NPOs being used as a tool for TF purposes currently focus on:

- Cultural associations and entities that may hold radicalised views or be linked to jihadist groups, and in particular those locations and mechanisms capable of raising or distributing funds, which may come from a wide variety of sources, including public funds and donations.
- Money transfers from foreign NPOs to our country, which may be intended to develop cultural and religious associations and places of worship with the aim of promoting radicalisation.
- Abuse of the activities of those NPOs that provide, in good faith, humanitarian support and social assistance in conflict zones or high-risk areas.

In this context, the most important elements for mitigating the risks of abuse by NPOs are the proper implementation of due diligence measures regarding the ultimate beneficiaries of the activity and the counterparties on the ground, which include knowledge of their activities, structures and purposes, as well as the results ultimately achieved. Both are included as mandatory actions in current regulations and have also been incorporated into the self-regulatory procedures previously developed by the sector itself. It is also important to note that the foundations themselves are working on a risk map for the sector.

In accordance with the risk analyses of the competent authorities on TF, NPOs can be exploited by the main terrorist threats—which currently are jihadist organisations—both for fundraising and for transferring funds to terrorist organisations or to conflict zones where the funds can be easily recovered or utilised by these organisations.

Among the types and possible ways in which NPOs are used for TF purposes identified by the LEAs, and national

and international intelligence services; of particular note are:

- Cases in which terrorist groups set up their own non-profit organisations as a vehicle to facilitate the collection of funds raised by the organisation itself (for example, to be used as vehicles for depositing funds obtained through extortion).
- Cases of NPOs created to obtain funding from third parties aligned with their ideology, who make voluntary contributions to support the terrorist organisation, its related activities or campaigns to publicise its aims.
- Cases where NPOs are established with perfectly legitimate aims and appearances, and with no link whatsoever to the organisation's own ideology, for the sole purpose of attracting funds to be allocated to purported causes that are not actually fulfilled, as the funds are diverted to other purposes linked to TF. Although this option may appear to carry a lower risk, as it requires specific knowledge and skills to be carried out, the truth is that it is not uncommon to find NPOs established for the purpose of raising and channelling funds linked to TF activities.
- Cases of abuse involving certain types of NPOs linked to specific high-risk groups and/or territories, which are used without their knowledge and involuntarily for the same purposes as in the previous cases.
- Cases in which certain types of NPOs, established for lawful purposes and linked to certain at-risk groups and/or territories, are infiltrated by individuals affiliated with terrorist groups in order to manipulate their decisions and the allocation of the funds they manage.

With regard to the risk factors for NPOs that may indicate the existence of a direct or indirect link to TF activities, the following should be highlighted:

a) Factors linked to their activities and purposes.
b) Factors linked to the sectors in which they operate.
c) Factors linked to the procedures for raising funds for their activities.
d) Factors linked to geographical risk areas.

a) and b) Risks inherent to the activity and sectors of operation.

Low risk. Due to their activities, there are many types of NPOs that clearly have a lower risk of being used for TF activities. These include public-benefit foundations and associations whose statutory purposes are focused on areas of activity that do not involve any risk of such activities, such as research, sports, agricultural, industrial, food, environmental and legal foundations, amongst many other activities set out in their statutory purposes. This lower-risk category should also include third sector organisations, NGDO's and other public-benefit foundations and associations dedicated to humanitarian and welfare purposes both within and outside our country, which work with specific groups: the elderly, people with disabilities, drug users, social reintegration, children, the sick, the marginalised, those living in poverty, or animal protection, amongst others.

Higher risks. There are other organisations operating within Spain which, due to the nature of their activities and the groups they work with, pose a higher risk of being used for TF purposes. Specifically, risk analyses by the competent authorities in the fight against TF highlight certain NPOs with a purportedly cultural, humanitarian or religious character that work with specific groups, particularly those linked to Islamic communities susceptible to radicalisation, which may be used for the collection and delivery of funds, or for their transport or transfer to third parties. These purported humanitarian or cultural activities could also serve to conceal potential purposes related to radicalisation, such as indoctrination and proselytising; recruitment; training; movement to or from conflict zones and areas; hosting individuals from such zones; or the transfer of funds to persons or organisations operating in these regions.

c) Risks inherent in fundraising procedures.

Transparency in the identification of donors and in fundraising methods are key factors in determining the risk level of these organisations. The existence of internal procedures and requirements regarding proper identification based on contribution thresholds reduces the risk of abuse by third parties.

As indicated in the chapter on AML/CFT vulnerabilities in Spain, it is also necessary to take into account the cash that circulates within the NPO sector, generally through donations and hand-to-hand payments. These amounts are usually small and are not always deposited in a bank (and are therefore outside the control of the authorities and supervisory activities). However, the figures for cash funds used by the sector, according to surveys conducted for this purpose amongst the organisations themselves, show that the use of cash is very limited in relation to the total funds they handle.

In this regard, there are legal obligations to identify donors above certain thresholds, which helps to mitigate risk; however, there is a higher risk in organisations that receive large amounts of cash donations, as well as in those that provide small grants to migrants and unbanked groups from regions with a higher risk of radicalisation or who have not yet established a firm foothold in our country.

d) Risks inherent to geographical areas.

In Spain, there are some 750 third sector organisations dedicated to international cooperation activities[50], 565 to the defence of human rights, 800 to development education and 367 providing aid to immigrants, whose scope of action both in Spain and abroad may entail a higher risk of links to TF activities.

Lower risk. Given the importance of the social and humanitarian work carried out by third sector organisations, it is essential to distinguish the hugely positive work of the vast majority of these hundreds of organisations from the potential risk posed by a few isolated cases, and to proceed to analyse their activities and the sources and destinations of their funds in detail and objectively. The proper identification of the origin of the funds received, as well as the reasons for and recipients of such funds, must form part of the preventive policy of the non-profit sector.

It is therefore necessary to differentiate between those operating in high-risk geographical areas and those whose area of operation does not involve risks in this regard. Thus, NGDO's operating in Spain on behalf of groups residing in our country are considered to be of lower risk, with the exception of the possible cases indicated in the previous section regarding organisations linked to communities susceptible to radicalisation, where the risk is clearly higher.

NGOs carrying out their projects in Latin America and in certain areas of Africa and Asia generally face very low risks in this regard due to the nature and type of their activities: support for children, educational projects, aid for the sick and disabled; or fair trade, amongst many other activities.

Higher risk. Therefore, attention must be paid to the greater risk posed by organisations that operate, whether regularly or occasionally, in countries or geographical areas where there is a greater presence of organisations or groups of citizens radicalised in their ideological or religious stances, or in countries whose political system could directly or indirectly support such groups. This support, as indicated above, can take various forms: directly or indirectly funding groups sympathetic to a radical political milieu through a non-profit organisation; harbouring potential terrorists within the country; promoting their ideas in international forums through non-profit organisations ostensibly of a cultural or religious nature; encouraging indoctrination or promoting a greater presence of certain communities or ideas in specific geographical areas through NPOs, amongst other activities.

[50] Source: https://www.guiaongs.org/directorio/.

Furthermore, in the case of Spain, alongside the countries commonly identified as posing this risk based on the criteria outlined, particular attention must be paid to dealings with North African countries, due to their geographical proximity and the significant presence of immigrants from that region, which may facilitate the concealment of terrorist-related criminal activities or their financing.

A common way in which NGDO's implement projects in third countries is through close collaboration with third-party organisations established in the country or region of operation; these are sometimes public administrations in the developing country, but more frequently local organisations, which are usually private and non-profit. In such cases, as already indicated, a thorough understanding of the partner organisation is a key factor in assessing risk. Operations carried out in higher-risk territories through other foreign organisations whose reliability has not been fully verified significantly increase the risk that funds will be used for illegitimate purposes and, depending on the geographical area, the risk of possible links to TF activities.

These inherent risks arising from the geographical area of operation abroad are compounded by vulnerabilities stemming from the lesser implementation of prevention policies in other countries and the lack of oversight by their authorities regarding the receipt of funds from donor countries. In this regard, the sector itself has launched an awareness-raising campaign to ensure proper monitoring and control of funds granted to other foreign NPOs, even where these are subsidiaries of Spanish NPOs themselves.

Residual risks.

This exposure to risk for NPOs is mitigated by the prudential obligations applicable to the sector and by the long-standing duties to implement certain AML/CFT preventive measures established for these entities, which currently entail a robust system of regulatory and operational measures.

These regulatory systems include obligations for foundations and associations regarding registration, accounting, taxation, information on the entity's aims and objectives, and the full identification of directors and administrators, amongst others.

Among these obligations, it is worth noting that staff with management responsibilities within NPOs must ensure that these are not used for ML/TF purposes, and to this end, a series of due diligence and record-keeping obligations are established. In particular, it establishes the duty for all foundations and associations to retain, for at least ten years, records identifying all persons who contribute or receive funds or resources from the NPO free of charge and, where applicable, their beneficial owners.

With regard to mitigating risks specific to the third sector, the AECID concentrates its funding on so-called 'accredited NGDOs', which have undergone an accreditation process certifying their experience and capacity. Additionally, the AECID has drawn up an Evaluation Manual for NGDOs applying for public funding for development projects.

Many of these organisations are members of CONGDE, the NGO Coordination Committee for Development, a private organisation that promotes self-regulation and the adoption of a Code of Conduct to enhance transparency and good governance. The 17 Regional Coordination Organisations also belong to CONGDE, meaning that approximately 500 NGDOs are members, either directly or indirectly, and have adhered to this Code of Conduct.

For its part, the COPBLAC has drawn up and published a document setting **out best practices** aimed at protecting the integrity and reputation of NPOs in these areas[51] and SEPBLAC has drawn up the **Guidance** for bodies responsible for ensuring that foundations and associations are not used for money laundering or terrorist financing[52]. This guide proposes that NPOs adopt a series of measures to provide themselves with more effective protection against the threat posed by those who seek to use them for criminal purposes.

A key element in effectively preventing any abuse is for NPOs to analyse and assess the risks arising from the various activities they carry out and, on that basis, to focus and direct their controls, intensifying them according to their activity, geographical scope of operation or volume of funds managed.

The guidance for NPOs is based on three pillars of action:

1. Functioning of the governing bodies.

2. Planning and technical monitoring of activities.

3. Financial transparency.

The **AEF**, in collaboration with various foundations of particular significance in Spain, is drawing up a Manual of Good Practices for the Prevention of Money Laundering and Terrorist Financing (ML/TF) for foundations and associations to address ML/TF risks and typologies. In addition to defining a series of risks faced by organisations in the sector, it will include a series of mitigating measures for each of the identified risks, such as having a code of good governance, declarations of good repute (updated periodically), internal reporting channels, self-assessment forms for each foundation's ML/TF prevention systems, amongst other measures.

Many NPOs established in Spain hold the Good Practice certificate issued by the **Fundación Lealtad**. The purpose of this foundation is precisely to promote trust in NPOs and, to this end, it issues a certificate verifying the organisation's compliance with certain aspects relating to transparency, control of funds, internal policies and measures, and decision-making.

With regard to religious organisations, the supervisory measures taken by the authorities include the existence of a **Register of Religious Entities** at the Ministry of Justice, through which there is a high degree of awareness of the activities of religious organisations. This obligation is set out in greater detail in the case of Catholic institutions, pursuant to the Resolution of 3 December 2015.

The creation of the aforementioned **Directory of Places of Worship** or the "declaration of well-established roots of religious denominations in Spain", established by Royal Decree 593/2015, are highly significant measures from the perspective of mitigating the risk associated with these entities.

Conclusion.

ML risks. According to the available information, operational non-profit organisations are not subject to abuse by criminal organisations as a vehicle for money laundering, and the exogenous risk of the use of already established and operational non-profit organisations is **low**.

However, there are cases in which the creation of foundations and associations is intended for fraudulent purposes and the concealment of assets, breaching the purposes for which they were established and diverting funds, thereby engaging in tax evasion and subsequent money laundering, which implies that the creation of NPOs carries a higher risk and justifies

51https://www.sepblac.es/wp-content/uploads/2018/03/mejores_practicas_en_organizaciones_sin_fines_de_lucro.pdf

52 https://www.sepblac.es/wp-content/uploads/2018/03/guia_orientativa_para_los_organismos_de_control_de_fundaciones_y_asociaciones.pdf.

a **moderate** rating.

TF Risks. In accordance with the guidelines of the FATF and the EU AML/CFT Framework, the risks associated with NPOs are more closely linked to TF activities. In Spain, to mitigate such risks, there are numerous prudential and AML/CFT regulatory obligations, as mentioned above. Furthermore, the awareness of regulated entities regarding TF risks (a consequence of years of combating terrorism and its financing), awareness-raising efforts within the sector (Foundations Protectorate, AEF), the implementation of best practices and guidance, and the use of financial intelligence in this sector are all highly relevant factors in reducing such risks.

In practice, there is continuous monitoring and close collaboration between the Spanish authorities and the high-risk segments of the NPO sector on issues related to terrorism and its financing, and there are various cases that demonstrate the authorities' proven ability to detect, investigate, prosecute and bring to trial terrorist financing activities in the NPO sector, which highlights the need to maintain and promote this monitoring and inter-agency collaboration.

All of this leads to the conclusion that the current residual risk would generally be **moderate**. However, the risk of abuse of existing entities is lower than the risk of new organisations being created, and the TF risk of some NPOs linked to certain high-risk groups or countries (see summary table) must be considered **significant/high**.

SUMMARY TABLE OF RISKS IN NPOs

ML Risks in NPOs	Risk
Misuse of existing NPOs for money laundering purposes.	**Low**
Creation of NPOs for ML purposes.	**Moderate**

TF risks of NPOs	Risk
Misuse of operating NPOs for money laundering purposes.	**Low/Moderate**
Establishment of NPOs for the purposes of TF.	**Moderate**
The establishment or misuse of specific non-profit organisations linked to at-risk groups and/or areas: – NPOs operating in geographical areas of jihadist conflict or in areas of heightened radicalisation. – NPOs operating in Spain with groups originating from geographical areas of jihadist conflict. – NPOs operating in Spain with communities and individuals who are more susceptible to radicalisation and jihadist proselytism. – NPOs operating from, or with the participation of, countries whose political system could directly or indirectly support this type of radicalisation. – NPOs whose funding comes from citizens or organisations linked to countries whose political systems could directly or indirectly support this type of radicalisation. – NPOs that carry out projects and activities in other countries (particularly in areas at risk of radicalisation) through third parties, with one or more intermediaries in the implementation chain.	**Significant /High**

(XII) CONCLUSIONS.

The FATF Mutual Evaluation Report on Spain regarding the fight against money laundering and terrorist financing, carried out in 2014, highlights that the country "has a sophisticated risk analysis system" and "has a high level of awareness of ML/TF risks, and the national strategy addresses the identified risks". This report was the subject of a follow-up report in 2019, which once again gave a positive assessment of the Spanish system for the prevention and prosecution of these offences.

In Spain, various plans and strategies coexist and are interlinked due to the nature of the issues they address. Specifically, at national level, building on the National Security Strategy, the National Strategy against Organised Crime and Serious Crime and the National Strategy against Terrorism have been adopted, each of which is in turn implemented through a range of specific strategic plans.

Specific policies for action in these areas are drawn up and implemented in practice according to the risks identified; consequently, the entire national system for combating ML/TF is based on a risk-based approach. These national policies must be updated periodically and must be consistent with the risks identified in these areas.

From the perspective of investigation and prosecution, the law enforcement agencies, the public prosecutor's office and the judiciary have been adapting their structures and resources, establishing specific units and employing specialist staff for financial investigation and the prosecution of criminal activities linked to money laundering and terrorist financing.

In the area of prevention, the risk-based approach is duly enshrined in Law 10/2010 of 28 April on the prevention of money laundering and terrorist financing, which expressly establishes the obligation to apply risk-based policies by all obliged entities in the private sector, both in the financial and non-financial sectors, as well as by supervisory bodies, the financial intelligence unit and other public institutions with competence in this area.

The main conclusions of the national risk assessment on money laundering and terrorist financing include:

- The threats in money laundering stem, above all, from **organised crime groups involved in drug trafficking, customs and tax offences, and fraud and scams** of various kinds. In recent years, there has been an increase in activities linked to economic crimes related to **corruption**, as evidenced by investigations and prosecutions in these areas. There is also a risk of money laundering in our country from criminal groups whose illicit funds originate from **criminal activities committed in other countries**.

- In the area of terrorist financing, the main threat comes from **jihadist groups**, which tend to operate in small, unconnected cells, composed of citizens from North African countries residing in Spain or second-generation Spanish citizens. These cells require few financial resources to operate and are self-financed through both legal and illegal activities. They avoid the formal financial system, particularly banks, and carry out transactions in small amounts, which makes it difficult to detect them through alerts or checks.

- The widespread **use of cash**, despite existing restrictions, remains a significant source of vulnerability and risk in relation to money laundering and terrorist financing. Cash makes it impossible to ascertain the lawful or unlawful origin of funds and to trace them, making it difficult to identify those who transfer them and their owners, and allowing them to be transferred, transported and concealed. These characteristics mean that cash is frequently used in both types of criminal activity.

- The high volume of fund movements to and from abroad entails a greater risk of concealing funds of illicit origin through various channels, such as **international financial transfers**, **remittances** via payment institutions or alternative means, **currency exchange**, or simply through **cross-border movements** of cash carried by citizens.

- There are particularly complex financial transactions and products that make it more difficult to identify the beneficial owner of the funds and to verify their legitimate origin, which entails greater risks in terms of money laundering. These mainly involve the use of **corporate structures and legal instruments established for these purposes with the help of professionals**; transfers of funds, investments and the sale and purchase of company shares or property involving **intermediary companies of a purely instrumental or asset-holding nature**; and transactions involving high-risk jurisdictions or ***offshore*** **territories**.

- Despite greater awareness and understanding of the risk, and the adoption of preventive mitigation measures, certain sectors—such as the **property sector** or **cash-intensive businesses**—remain attractive and pose a risk for money laundering operations.

- Advances in **technology** in financial transactions and payment methods, and the growth of **new virtual instruments**, pose emerging risks of money laundering and terrorist financing, as they increase the anonymity of their holders and the opacity of the origin of funds and the transactions carried out with them.

In recent years, a wide range of measures of various kinds have been adopted in the areas of prevention, supervision and investigation with the aim of mitigating risks in these areas, the effects of which are now becoming apparent. These measures have involved new administrative and criminal legislation, and the creation and strengthening of units and procedures aimed at preventing and combating both offences.

Furthermore, the forthcoming adoption and implementation of a series of regulatory and other mitigation measures will help to further reduce the risks of money laundering and terrorist financing in our country in the coming years.

Glossary

AEAT. Agencia Estatal de Administración Tributaria (Spanish Tax Agency).

AEB. Asociación Española de Banca (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).

CECA. Confederación Española de Cajas de Ahorro (Spanish Confederation of Savings Banks).

CGI. Comisaría General de Información (General Information Directorate. National Police).

CGPJ. Comisaría General de la Policía Judicial (General Directorate of the Judicial Police. National Police).

CGPJ. Consejo General del Poder Judicial (General Council of the Judiciary).

CITCO. Centro de Inteligencia contra el Terrorrismo y el Crimen Organizado (Centre for Intelligence against Terrorism and Organised Crime).

CI. Credit Institutions.

CIU. Collective Investment Undertakings.

CN**I.** Centro Nacional de Inteligencia (National Intelligence Centre).

CNMV. Comisión nacional del Mercado de Valores (National Securities Market Commission).

CONGDE. Coordinadora de Organizaciones no Gubernamentales para el Desarrollo España (Coordinating Body of Development Cooperation Organisations)

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).

ECB. European Central Bank.

EAF. Financial Advisory Firms.

EBA. European Banking Authority.

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).

FIU. Financial Intelligence Unit.

FGE. Fiscalía General del Estado (Prosecutor General's Office).

FTF. Fichero de Titularidades Financieras (Financial Ownership Register).

FATF. Financial Action Task Force.

GOIF. Grupo Operativo de Inteligencia Financiera (Financial Intelligence Task Force).

ICAC. Instituto de Contabilidad y Auditoría de Cuentas (Institute of Accounting and Auditing).

ICO. Initial Coin Offering. Initial offering of coins (crypto-assets).

JI. Jefatura de Información de la Guardia Civil (Guardia Civil Information Directorate).

ML. Money laundering.

MGS. Mutual Guarantee Societies.

MVTS. Money or Value Transfer Services.

NRA. National Risk Assessment.

NGDOs. Non-Governmental Development Organisations.

NPO. Not-for-profit organisations.

OCP. Órgano Centralizado de Prevención (Centralised Prevention Agency).

ONCE. Organización Nacional de Ciegos Españoles (National Organisation of the Spanish Blind)

PEP. Politically Exposed Persons.

RETIR. Registro de Titularidad Real **(**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 Company)

SEPBLAC. Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (Executive Service for the Prevention of Money Laundering).

SGIIC. Sociedades Gestoras de Instituciones de Inversión Colectiva (Management Companies for Collective Investment Schemes).

SICAV. Sociedades de Inversión Colectiva en Activos Variables (Undertakings for Collective Investment in Transferable Securities).

S N RA. (EU) Supra-National Risk Assessment.

SREP. (EU) Supervisory Review and Evaluation Process.

SOCIMI. Sociedades Cotizadas de Inversión en el Mercado Inmobiliario (Listed Real Estate Investment Companies).

SVA. Servicio de Vigilancia Aduanera (Customs Surveillance Service).

TF. Terrorist financing.

UCO. Unidad Central Operativa de la Guardia Civil (Central Operational Unit of the Guardia Civil).

UDEF. Unidad Central de Delincuencia Económica y Fiscal. Policía Nacional (Central Unit for Economic and Fiscal Crime. National Police).

UDYCO. Unidad Central de Droga y Crimen Organizado. Policía Nacional (Central Unit for Drugs and Organised Crime. National Police).

UNACC. Unión Nacional de Cooperativas de Crédito (National Union of Credit Cooperatives).

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).

List of key legislative provisions.

- Law 19/2003 of 4 July on the legal regime governing capital movements and economic transactions with foreign countries.
- Law 4/2010 of 10 March on the enforcement within the EU of judicial confiscation orders.
- Law 10/2010 of 28 April on the prevention of money laundering and terrorist financing.
- Law 31/2010 of 27 July on the simplification of the exchange of information and intelligence between the security services of EU Member States.
- Law 13/2011 of 27 May on the regulation of gambling.
- Royal Decree 413/2015 of 29 May, approving the Regulations of the Commission for the Supervision of Terrorist Financing Activities.
- Royal Decree 948/2015 of 23 October regulates the Office for Asset Recovery and Management.
- Royal Decree 304/2014 of 5 May, approving the Regulations of Law 10/2010 of 28 April on the prevention of money laundering and terrorist financing.
- Order ECC/2402/2015, of 11 November, establishing the Centralised Body for the Prevention of Money Laundering and Terrorist Financing within the Association of Registrars of Property, Commercial and Movable Assets.
- Order ECC/2503/2014, of 29 December, establishing the personal data file known as the 'Financial Ownership File' (FTF).
- Order EHA/114/2008, of 29 January, regulating compliance with certain obligations of notaries in the field of money laundering prevention.
- Order EHA/2444/2007, of 31 July, concerning the external expert's report on the internal control and reporting procedures and bodies established to prevent money laundering.
- Order EHA/2619/2006 of 28 July, implementing certain anti-money laundering obligations for regulated entities engaged in currency exchange or the management of international transfers.
- Order EHA/1439/2006, of 3 May, regulating the reporting of movements of means of payment in the context of the prevention of money laundering.
- Order EHA/2963/2005, of 20 September, regulating the Centralised Prevention Body for money laundering within the General Council of Notaries.
- Order ECO/2652/2002 of 24 October and Order EHA/1464/2010 of 28 May, implementing the obligations to report transactions relating to certain countries to the Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offences.