

PORTUGAL

NATIONAL RISK ASSESSMENT

MONEY LAUNDERING,
FINANCING OF TERRORISM AND
PROLIFERATION FINANCING

SUMMARY

INTRODUCTORY NOTE

Portugal carried out its first money laundering (ML)¹ and financing of terrorism (FT)² national risk assessment (NRA) in 2015.³ That exercise already anticipated that every three to five years there would be an update and improvement of the identification and understanding of the risks faced by the country.

Hence, in 2018, after the fourth Financial Action Task Force (FATF) mutual evaluation of Portugal, it was decided that the 2015 NRA would be revised, to identify – a few years later – the sectors presenting the greatest potential risks and those offering the lowest risk, in order to mitigate or possibly eliminate such risks. It was also decided that the NRA would be extended to the risks of financing of proliferation (PF)⁴ of weapons of mass destruction (WMD), so as to cover all areas currently governed by FATF Recommendations.

The exercise, covering all sectors of activity with ML/FT/PF prevention obligations, was led by the anti-money laundering and counter-terrorist financing (AML/CFT) Coordination Commission (hereinafter the Coordination Commission), and a Working Group was set up for the purpose,⁵ which held regular plenary meetings and had the crucial support of the Commission's Permanent Technical Secretariat. The NRA preparation process was carried out at governmental level and involved all the public sector entities with AML/CFT/CPF supervision or oversight duties, as well as powers to combat these activities, and also private sector associations, thus demonstrating Portugal's continued dedication to preventing and combating ML/FT/PF. In total 198 entities participated in the NRA, 49 of which from the financial sector and 149 from the non-financial sector. The number of obliged entities exceeded 236,000.

This document, which essentially uses data from 2015 to 2018 as a reference, responds to the need for the identification, assessment and understanding of ML/FT/PF risks in Portugal, as a result of FATF Recommendation 1. The work undertaken allows for measures and respective priorities to be updated, along with the corresponding decision-making to guarantee full compliance with the Recommendations and ensure improvement in the efficiency of the Portuguese AML/CFT/CPF system.

It also presents a description of the identified threats and vulnerabilities, assesses the ability of the country to fight them, evaluates the ensuing risks, and indicates a number of actions that should be taken to strengthen the Portuguese AML/CFT/CPF system.

¹ ML is a process which aims to hide the origin of the proceeds of criminal activities, to enable their use as though from a legitimate source. ML is a crime provided for in Article 368-A of the Criminal Code, as amended by Law No 83/2017 of 18 August 2017 (hereinafter Law No 83/2017).

This amendment is part of the legal framework on ML prevention and combat, which has evolved since the approval of the 2015 NRA Report.
² FT consists of the provision or collection of funds with the intention of using them to carry out terrorist acts or to prepare such acts, also including the subsistence of their perpetrators.

³ https://www.portalcft.pt/sites/default/files/anexos/pt_nra_synthesis.pdf

⁴ PF consists of the provision of funds for the development, transport, storage and export of WMD (nuclear, chemical or biological) and related material (including the knowledge and dual-use goods and technologies used for illegitimate purposes).

Law No 97/2017 of 23 August 2017 (hereinafter Law No 97/2017) allows for the immediate and full implementation of any restrictive measure approved by the United Nations Security Council, past or future, related to PF, not requiring national authorities' approval of any additional legislation or rules of procedure.

⁵ <http://www.portalcft.pt/pt-pt/content/grupos-de-trabalho>

EXECUTIVE SUMMARY

FATF Recommendations set forth the need for a risk-based approach to preventing and fighting ML/FT/PF. This NRA meets the need for the identification, assessment and understanding of ML/FT/PF risks in Portugal, as a result of Recommendation 1.

The NRA, carried out according to the methodology and instruments constructed from the “Guidance on National Risk Assessment” published by the FATF and other available tools, was led by a Working Group set up within the Coordination Commission, and involved all the entities represented therein. In the private sector, associations representing the financial sector were consulted, as well as associations representing entities from the non-financial sector subject to ML/FT/PF prevention obligations.

After an introduction on the AML/CFT/CPF institutional structure, its purpose and methodology, the NRA presents background information,⁶ identifies threats and vulnerabilities and their respective analysis, examines the country’s capacity for ML/FT/PF prevention and fight, and concludes with a risk assessment, setting out strategic guidelines, priorities and measures to be taken. The risk assessments of the different sectors subject to ML/FT/PF prevention measures are presented in various annexes.

As far as ML threats are concerned, the crimes in Portugal likely to generate ML proceeds were considered. A high threat level was detected in tax crimes (although these can mask other predicate offences), drug trafficking and corruption. On a second level, with medium-high risk are misappropriation of money or property by public officials, IT-related crime, fraud and counterfeiting. Various ML types and methods were analysed, including physical transportation of cash, concealment of beneficial owners, intervention of politically exposed persons (PEPs), use of virtual assets and crowdfunding. As to the FT threat, the conclusion is that its level is mostly medium-low, but nevertheless should not be underestimated. With regard to the PF threat level, the conclusion is that it should be considered low.

The NRA also identified the vulnerabilities, combining intrinsic vulnerabilities with the quality of the existing controls, so as to determine the degree of residual vulnerability. The use of cash, particularly insofar as it allows for the physical movement of value, the transnational nature of transactions and the absence of beneficial ownership information continue to be a cause for concern in the financial sector. Despite the legislative measures that have considerably restricted the use of cash in the non-financial sector, namely in payments, it is still a significant vulnerability. In addition, customer anonymity, the absence of beneficial ownership information and the signing of contracts without the physical presence of the customer are considerable vulnerabilities.

The country’s ability to prevent and fight ML/FT/PF was also analysed. Within this scope, 22 relevant attributes were examined for a robust and consistent AML/CFT/CPF system. Hence, although most attributes are assessed positively, there is clear room for improvement for some. This is the case, inter alia, of the regulatory framework governing the seizure and management of assets and sanctions for legal persons, of suspicious transactions reports (STRs) from the non-financial sector and of the capacity of the Financial Intelligence Unit (FIU), of training for investigation of cybercrime and digital crime, and internal cooperation.

⁶ The background information is based on public data on geography and population, political system, economy and legal and judicial systems. It was decided that its publication would not be relevant in the context of the release of a public NRA summary.

Finally, the risk analysis identified the highest ML/FT/PF **risks** by sector and geography, concluding that – given the country’s responsiveness – Portugal is subject to a **medium-low risk** of ML and FT and a **low** PF risk.

The NRA also makes it possible to respond to international requirements and identify strategic policy guidelines. In addition, it also presents the priorities and general and sectoral measures, which are key to strengthening the AML/CFT/CPF system as a whole.

As regards strategic guidelines, the NRA underlines the need to overcome the lack of statistical data on ML/FT/PF, as well as the fact that these data are insufficient, incomplete, not comprehensive and/or reliable. Additionally, it highlights the need to strengthen a culture of inter-institutional exchange of information, to raise the quality of the risk-based approach, to increase the efficiency of criminal investigation, and to deepen cooperation with the private sector.

As to global legislative initiatives, it is important to consider, inter alia, the introduction of counterfeiting as a predicate offence to money laundering and the need to improve the statutory framework governing the seizure, management and confiscation of assets. In sectoral terms, previously identified shortcomings are still visible, some of which become more marked in this new period under review: exercise of oversight powers, preparation and release of regulations and guidelines. Hence, overcoming these shortcomings necessarily involves considering AML/CFT/CPF a priority for supervisory and oversight authorities. This priority should be reflected in their annual activity plans or strategic plans, and its implementation should be set out in their respective annual reports. In addition, there is a general need for reinforcement of the suitability requirements for access to and exercise of functions in specific obliged entities, as well as for qualification actions of both supervisors and overseers and the staff of those obliged entities, including with a view to improving a risk-based approach.

Finally, to perform its policy guidance task, the NRA should be permanently updated. Hence, given that an automated updating mechanism is still not viable, there should be a substantial update at least every three years or where warranted under exceptional circumstances.

I – INTRODUCTION

Institutional structure for the prevention and fight against money laundering, terrorist financing and proliferation financing

Portugal has a structure for coordinating the prevention and fight of money laundering, terrorist financing and WMD proliferation financing: the AML/CFT Coordination Commission, set up under the auspices of the Ministry of Finance.

The Coordination Commission, which is chaired by a Deputy Minister appointed by the Minister of Finance,⁷ has the mission of monitoring and coordinating the identification, analysis and assessment of the ML/FT/PF risks to which Portugal is or will possibly be exposed, as well as contributing to the continuous improvement of the technical compliance and effectiveness of the national AML/CFT system.

The Coordination Commission has an Executive Committee⁸ and a Permanent Technical Secretariat (Portuguese acronym: STP).

Law No 83/2017, which sets forth measures to fight against money laundering and terrorist financing, assigns the Coordination Commission an extended set of powers, provided for in Articles 8, 9, 116, 120, 124, 131 and 145, and also applicable to proliferation financing [Article 123(6)].

In terms of disseminating AML/CFT/CPF measures, in order to raise awareness of the risks and increase knowledge of the prevention methods, trends and obligations in force, the Coordination Commission has created a website, which is permanently updated.⁹

Portugal also has an extended list of authorities with powers to prevent and fight money laundering, terrorist financing and proliferation financing.¹⁰

Among these authorities are those tasked with supervising or overseeing obliged entities' compliance with ML/FT/PF prevention obligations.

Hence, in the financial sector, the Banco de Portugal is the competent sectoral authority for the exercise of supervision in terms of ML/FT/PF prevention of the following five institutional groups: (i) credit institutions; (ii) specialised credit institutions; (iii) payment institutions and electronic money institutions; (iv) exchange offices; and (v) other institutions: CTT – Correios de Portugal, S.A., investment companies, Development Financial Institution and regional development companies. The CMVM is responsible for the ML/FT supervision of two institutional groups: (i) management companies of units of collective investment and other assets and (ii) investment service providers. The ASF is responsible

⁷ The Coordination Commission is composed of representatives from the following entities: Ministry of Finance; Ministry of Foreign Affairs; Ministry of Internal Administration; Ministry of Justice; Ministry of Economy and Digital Transition; Ministry of Labour, Solidarity, and Social Security; Prosecutor-General's Office; General Secretary of the Internal Security System; Criminal Police; National Republican Guard; Public Security Police; Internal Intelligence Service (SIS); Banco de Portugal; Securities Market Commission (CMVM); Supervisory Authority for Insurance and Pension Funds (ASF); Economic and Food Safety Authority ASAE; Institute of Registries and Notaries (IRN); Institute for Public Procurement, Real Estate and Construction (IMPIC); Gambling Regulation and Inspection Service of Turismo de Portugal, I. P. (SRIJ); Tax and Customs Authority; Bar Association; Order of Statutory Auditors (OROC); Order of Certified Accountants (OCC); *Solicitadores* and Enforcement Agents National Association (OSAE); Head of the Portuguese Delegation to the FATF.

⁸ The Executive Committee is composed of the Head of the Portuguese Delegation to the FATF, as chair, and a representative of each of the following entities: Ministry of Finance; Ministry of Justice; Prosecutor-General's Office; General Secretary of the Internal Security System; Financial Intelligence Unit (FIU); Banco de Portugal; CMVM; ASF; ASAE; professional Associations and Orders referred to in the previous footnote.

⁹ www.portalbcft.pt

¹⁰ The judicial and police authorities, the Central Department of Criminal Investigation and Prosecution (DCIAP) and the FIU. Financial sector authorities (supervisory authorities): ASF, Banco de Portugal, CMVM and General Finance Inspectorate (IGF). Competent non-financial sector authorities: SRIJ; Inspectorate-General of the Ministry of Labour, Solidarity and Social Security (IGMTSSS); IMPIC; CMVM (as regards the statutory auditors over whom the OROC also has specific duties); OCC, Bar Association; OSAE; the member of the Government responsible for justice, assisted by the IRN; and ASAE.

for the ML/FT supervision of three institutional groups: (i) pension fund management companies, (ii) insurance undertakings carrying out activities with respect to life insurance and (iii) insurance mediators carrying out activities with respect to life insurance. The IGF is the competent sectoral authority with respect to the Treasury and Debt Management Agency (IGCP).

In the non-financial sector, the SRIJ is the competent sectoral authority for the oversight of ML/FT/PF prevention measures of (i) casino operators and bingo operators and (ii) entities covered by the legal framework for online gambling and betting. The IGMTSSS oversees the games operated by the Gambling Department of *Santa Casa da Misericórdia de Lisboa* (SCML): (i) *Lotaria Clássica*; (ii) scratch cards; (iii) *Totoloto*; (iv) Euromillions; (v) *Totosorteio – M1LHÃO*; (vi) *Lotaria Popular*; (vii) Football pools and (viii) Odd-type sports betting – Placard. The IMPIC oversees ML/FT with regard to real estate activities: (i) real estate agency services; (ii) purchase, sale, purchase for resale or exchange of real estate; (iii) renting, and (iv) real estate development. The CMVM with regard to the statutory auditors (over whom the OROC also has specific duties). The OCC is the sectoral authority for certified accountants, acting both individually and as legal persons. In turn, lawyers, when they intervene or assist, on behalf of a client or under other circumstances, in certain types of operation as listed in the law, including acts other than those they are expressly authorised to perform by law, are subject to the legal framework governing AML. The Bar Association is responsible for the respective oversight. Such is the case for *solicitadores*, whose respective oversight falls under the OSAE. The member of the Government responsible for Justice, assisted by the IRN, checks notaries' compliance with the duties and obligations provided for in Law No 83/2017. Finally, the ASAE oversees seven sectors¹¹ and respective products, services and business.

In addition to the afore-mentioned obliged, supervised or overseen entities, it is also important to mention entities equivalent to obliged entities. These include management companies of lending and equity-based crowdfunding platforms, supervised by the CMVM, and management companies of reward and donation-based crowdfunding platforms, as well as non-profit organisations supervised by the ASAE.

Finally, there are supplementary entities in the prevention and fight against ML/FT: the registrars and registry officials. As regards these entities, the IRN is the equivalent to the sectoral authority.

National Risk Assessment

The 2019 National Risk Assessment, which revises and updates the 2015 NRA, continues the process of identification, assessment and analysis of ML/FT/PF threats,¹² vulnerabilities¹³ and main risks. It seeks to identify agents, methods and means used for laundering illegal proceeds, financing terrorism or funding initiatives to produce or trade weapons of mass destruction. Thus, it plays a role in the ability of the country, sectoral authorities and obliged entities to allocate their resources so as to strengthen preventive control systems and adopt proportionate measures to mitigate their risks.

It is a collective and comprehensive exercise that involves the private sector, focusing on a risk-based approach and encouraging its practical application by the different sectoral authorities and obliged entities. It also aims to ascertain the country's ability to prevent and combat ML/FT/PF threats and to

¹¹ Merchants trading in goods against payment in cash, tax consultants, imports and exports of diamonds, sales and acquisitions of rights over professional sportspersons, service providers to legal persons, to other legal entities or to legal arrangements, auction houses and pawnshops, providers of services to companies and legal arrangements, and the transportation, safekeeping, handling and distribution of funds and valuables.

¹² A threat is a person or group of people, object or activity with the potential to jeopardise, for example, the state, society or the economy. Within the context of ML/FT/PF, the term includes criminals, terrorist groups and their associates, and is the starting point to understand the ML/FT/PF risk.

¹³ Vulnerability encompasses anything that may be exploited by threat or that may support or even facilitate its activities, the consequence being the impact or harm that ML/FT/PF may cause.

limit the respective vulnerabilities. The exercise – covering all sectors of activity with ML/FT/PF prevention obligations – was led by the working group (WG) set up following a deliberation of the Coordination Commission. The WG’s plenary session, led by the Chair of the Executive Committee of the Coordination Commission was attended by 22 entities,¹⁴ including the collaboration of the Permanent Technical Secretariat.

Methodology and analysis matrices

The methodology used in the NRA followed the *FATF Guidance - National Money Laundering and Terrorist Financing Risk Assessment*, published in February 2013. Other available national and international instruments were also used. In this context, instruments for supporting the different work stages were devised.

These instruments aim to assess the **level of threats**, the **degree of intrinsic vulnerabilities**, the **impact or harm**, the robustness of AML **control systems**, the **degree of residual vulnerability** and the **sectoral and national risk**.

Assessment of the **level of threats and degree of intrinsic vulnerabilities** involves the assessment of probability and consequence. The **probability** of materialisation of the fact increasing ML is assessed, and considered **Low** when the fact materialises very rarely, **Moderate** when the fact may materialise occasionally, **Frequent** when it materialises often, and **High** when the fact materialises repeatedly. The **impact or harm** for the sector/sub-sector is assessed as **insignificant** when effects are negligible, **tolerable** when the harm has reduced effects, **important** when the harm is significant, and **critical** when the effects are very difficult to mitigate.

Assessment of the robustness of the AML control systems uses a four-level scale: **High, Medium-High, Medium-Low and Low**.

The **degree of residual vulnerability** results from the combination of the degree of intrinsic vulnerability with the robustness of the ML control system. The **sectoral and national risk** is calculated on the basis of the degree of (residual) vulnerability and the threat level.

The threats and the vulnerabilities were assessed by estimating the respective degree of probability and degree of consequence, each with a weight of 50%, according to the following matrix:

THREAT LEVEL AND DEGREE OF VULNERABILITY

¹⁴ Ministry of Finance, Ministry of Justice, Ministry of Foreign Affairs, Ministry of Economy, DCIAP, FIU, SIS, Immigration and Borders Service (SEF), Tax and Customs Authority, ASF, Banco de Portugal, CMVM, IGF, SRIJ, IGMTSSS; IMPIC, Bar Association, OSAE OROC; OCC, IRN and ASAE.

		CONSEQUENCE (the impact of the threat or vulnerability materialising)			
		Insignificant	Tolerable	Important	Critical
PROBABILITY (the likelihood of the threat or vulnerability materialising)	Low	Low	Medium-low	Medium-low	Medium-high
	Moderate	Low	Medium-low	Medium-high	Medium-high
	Frequent	Medium-low	Medium-low	Medium-high	High
	High	Medium-low	Medium-high	Medium-high	High

Low, medium-low, medium-high and high levels/degrees are considered according to the following:

THREAT LEVEL AND DEGREE OF VULNERABILITY	
Low	Level or degree with a low or moderate probability of materialising and which may cause damage with insignificant impact. As a rule, it does not require any action or only requires action to reduce the probability and/or consequence of it materialising.
Medium-low	Level or degree with a low, moderate or high probability of materialising and which may cause damage with insignificant, tolerant or important impact. Requires action as early as possible to reduce the probability and/or consequence of it materialising, as well as a suitable contingency plan for its mitigation should it materialise.
Medium-high	Level or degree with a low, moderate, frequent or high probability of materialising and which may cause damage with tolerable, important or critical impact. Requires action with relative priority to reduce the likelihood and/or consequence of it materialising.
High	Level or degree with a frequent or high probability of materialising and which may cause damage with critical impact. Requires immediate and prioritised action to prevent and mitigate the effects of it materialising.

The ML/FT/PF sectoral risk is assessed based on the intersection of the sectoral threat level, with a weight of 40%, and the degree of residual vulnerability, with a weight of 60%. The global ML/FT/PF risk is calculated by intersecting the threat with the vulnerability, the threat having a weight of 40% and the vulnerability 60%.

		ML/FT/PF RISK ANALYSIS MATRIX			
		DEGREE OF VULNERABILITY			
		Low	Medium-low	Medium-high	High
THREAT LEVEL	Low	Low	Medium-low	Medium-low	Medium-high
	Medium-low	Low	Medium-low	Medium-high	Medium-high
	Medium-high	Medium-low	Medium-low	Medium-high	High
	High	Medium-low	Medium-high	Medium-high	High

Assessment process

The different authorities conducted the assessment based on the available instruments, with the ability to set out and propose the measures deemed consistent and suitable to strengthen the AML/CFT controls, mechanisms and procedures and thus to mitigate the identified vulnerabilities. Furthermore, they were requested to establish priority levels for the measures proposed, so as to allow for the application of enhanced or simplified measures proportionate to the risk, and thus ensure the best allocation of human, financial and material resources.

Portugal's ability to fight ML was also assessed, involving 24 entities.¹⁵ Within their scope of action and sphere of competence, all the entities assessed the quality of specific attributes, taking as reference the FATF international standards on risk and context, the structural elements, the Recommendations and the Immediate Outcomes.

This NRA includes new entities equivalent to obliged entities, the so-called 'management companies of crowdfunding platforms', respectively of loan and equity-based platforms - assessed by the CMVM - and reward and donation-based platforms - assessed by the ASAE - and registrars and registry officials, in their capacity as supplementary entities in AML/CFT.

ML/FT/PF risk for legal persons operating for profit and other entities without legal personality was also assessed.¹⁶

Finally, the identification and assessment of ML/FT/PF risks for non-profit organisations is under way.

The FT/PF risk to which Portugal is exposed was assessed according to international benchmarks and FAFT guidelines, as well as to (geographic or demographic) background factors that may facilitate terrorism or proliferation and increase vulnerability to FT or PF.

The assessment of vulnerabilities both in FT and PF is the result of data collected regarding a wide set of indicators, which gave rise to a scale of impact on vulnerability, assessed on the basis of **low, medium-low, medium-high and high**.

The assessed factors and indicators were of a legislative, operational and political nature, as well as related to the geographic and demographic context.

¹⁵ Sectoral supervisory and oversight authorities, as well as the relevant competent Associations and Orders, within the scope of ML prevention, Supreme Judicial Council, DCIAP, FIU, police authorities (Criminal Police, National Republican Guard and Public Security Police), other relevant entities in the confiscation, seizure and management of assets [*Gabinete de Recuperação de Ativos* (GRA), the Assets Recovery Office and *Gabinete de Administração de Bens* (GAB), the Property Management Office) and other entities with AML operational powers (Tax and Customs Authority, SIS and SEF).

¹⁶ Also including foreign trusts in the Madeira Free Trade Zone.

II – IDENTIFICATION OF THREATS

Money laundering

In recent years, organised criminal structures have become increasingly fragmented, relying more and more on highly specialised cells in a specific activity niche, in terms of both the development of the direct criminal activity in which they participate and the setup of the necessary infrastructure to launder the resulting money.

Available information suggests that there is often no overlap between the geographies used for committing criminal activities and those where the money generated by such activities is placed or laundered.

Main predicate offences

As far as predicate offences are concerned, the main threats emanate from tax fraud, drug trafficking and corruption, extortion and misappropriation of money or property by public officials. Tax crimes are the most relevant predicate offences for the threat assessment of ML risks.¹⁷ Drug trafficking and IT-related crimes come next. When combined, crimes against the State and crimes which may result in financial gain for their perpetrators (corruption, misappropriation of money or property by public officials and trading in influence) rank second in importance.

Drug trafficking is still one of the main activities impacting on the Portuguese criminal environment, and is therefore the crime that is subject to the highest number of investigations opened by the Public Prosecution Service. The FIU confirmed that more than 10% of the total STRs are operations that may be related to this type of predicate offence.

With regard to **tax crimes**, 3,453 investigations were opened (between 2015 and 2018) in relation to these crimes, and it is therefore the main predicate offence to ML. When analysing STRs, this was also the most commonly detected type of predicate offence – over 50%, on average.

On the other hand, as regards **property crimes against the State** (corruption, misappropriation of money or property by public officials, harmful mismanagement of economically-independent public sector organisations), in the period under review, 3,225 investigations were opened related to corruption, 1,752 to the misappropriation of money or property by public officials and 115 to harmful mismanagement of economically-independent public sector organisations. Over this period, no STR was reported in relation to these three crimes.

Economic and financial offences committed in an organised manner, **involving the use of information technology**, were subject to 14 investigations, 8 charges and 78 STRs. It is worth stressing the high number of charges compared to the initial number of investigations.

With regard to **counterfeiting**, links with this crime are yet to be detected in confirmed STRs, although admittedly some of these cases lead to tax fraud. The ASAE reported 45 suspicious ML transactions (of which, three were specifically related to counterfeiting) and the Public Prosecution Service opened 1,390 investigations during this period.

¹⁷ Although it is admissible that, in some cases, later investigations may show that they are linked to other illegal acts.

Finally, turning to **other types of crime**, the most notable are the illicit trafficking in protected species, for which 268 investigations were opened, while no STRs were related to this category of crime, and the illicit trafficking in arms, for which 232 investigations were opened, while no STRs were related to this type of crime.

Terrorist financing

The occurrence in recent years of countless attacks and the dismantling of terrorist conspiracies on European soil show that the Islamist terrorist threat in Europe is still high, with the «Islamic State» terrorist organisation being one of the main threats to the European territory.

The latest attacks have strengthened the perception that the planning and commission of attacks may be performed by individuals acting alone, with no established connection to terrorist organisations. Moreover, the current pattern of attacks in Europe highlights the involvement of individuals who are part of extremist circles nurtured on European soil.

As a result of developments in the terrorist threat in Europe, European and national legislators have sought to make their territory hostile to the development of terrorist activities and other related activities. At present, there is a more comprehensive national legal framework governing the crime of terrorism – for instance, criminalising travel or attempted travel to a State other than one's own State of residence or nationality, for the purpose of joining a terrorist organisation or perpetrating terrorist acts. Consequently, the financing of such acts, which are typical conducts of the crime of terrorism, is considered FT.

Funding needs are ubiquitous among all terrorist individuals and organisations, given that without financial means, they are not able to achieve their ends. As such, the survival of terrorist organisations depends on their ability to obtain financing, to ensure the proper functioning of their leadership structure, its operability, the maintenance of its ranks of fighters, the propaganda and conversion structures, as well as to guarantee access to weapons and other military equipment.

The potential targets (countries) of the attacks need not necessarily coincide with the places of origin or movement of funds. The fact that a country is not targeted in attacks by a given terrorist organisation does not mean that it is not a target for FT. A country placed on a lower level of alert can be particularly attractive to terrorism-related activities, including for purposes of fund raising.

The *modi operandi* associated with FT differ by virtue of the capacity, geographical presence, supporters or militants, and the agenda of the terrorist groups and organisations.

In light of the current main ideological matrices (of terrorism) with (potential) impact on Portugal and the quantitative and, mostly, qualitative indicators released by the competent national authorities for the purposes of preventing and combating FT, the following threatening agents are the most notable:

- Islamic State terrorist organisation and affiliated groups.
- Foreign terrorist fighters (FTFs) of Portuguese nationality or with ties to Portugal. The issue around the possible return to Europe of these individuals still raises concerns.
- Al Qaida (AQ) and affiliated groups.
- Hizballah – Shiite (Islamist) terrorist organisation, considered to be the main agent in this type of threat.
- Individuals with extremist profiles.

Proliferation financing

The proliferation of weapons of mass destruction (WMDs) is still a high level threat to world security. Despite the efforts of the international community, high-risk countries continue to engage in covert activities, aimed at enhancing their military capabilities, particularly as part of their WMD programmes.

Alongside the underground networks dealing with the purchase of goods and equipment required for the development of WMD programmes, the devices used to conceal the capital flows spent on those goods and equipment are equally important. For this reason, issues related to the financing of operations have taken on increasing importance in the orchestration of means to counter the proliferation of WMDs. For international bodies committed to combating economic crime, the most notable of which is the FATF, PF has attracted growing attention.

The fact that there are countries which have yet to ratify the international treaties and conventions to counter the PF for WMDs and other countries which, despite having signed such acts, have struggled to implement them, undermines the effectiveness of the control measures and sanctions.

Portugal is an integral part of the various international instruments against the proliferation of WMDs. Given that information sharing is a key factor behind the effectiveness of these prevention instruments, national entities participate in a number of them.

Entities with PF prevention obligations adopt an integrated approach to the phenomenon, in any context associated with the manufacture, purchase or sale of nuclear, chemical or biological weapons and their means of delivery or related material, as well as goods, technology and knowledge bound for WMD programmes in high-risk countries.

III. IDENTIFICATION OF VULNERABILITIES (ML)

In the **financial sector**, the following major intrinsic vulnerabilities were identified:

- The use of cash;
- The transnationality of transactions;
- The type of products sold;
- The distribution methods and channels;
- Customer identification;
- The identification of the customer's beneficial owner;
- The record of transactions;
- Non face-to-face business;
- The regular use (at national or international level) of business for ML;
- The regular use (at national and international level) of business to commit crimes against the market or tax crimes;
- Exercise of activities by non-legally qualified (natural or legal) persons;
- The internal organisation of obliged entities (human and technological resources).

In the **non-financial sector**, the following major intrinsic vulnerabilities were identified:

- The use of cash;
- The use of agents, distributors or other forms of intervention in the pursuit of their activities;
- The anonymity of the customer;
- The anonymity of the customer's beneficial owner;
- The record of transactions;
- Non face-to-face business;
- The regular use (at national or international level) of business to commit tax crimes;
- Exercise of activities by non-legally qualified (natural or legal) persons.

As regards **equivalent entities**, in the sector of management companies of crowdfunding platforms, the following intrinsic vulnerabilities were identified:

- Investors and beneficiaries of funding;
- The regular use (at national and international level) of business for money laundering or to commit crimes against the market or tax crimes;
- The distribution methods and channels;
- The record of transactions;
- Exercise of activities by non-legally qualified (natural or legal) persons.

As to **supplementary entities** in AML/CFT - the registrars and registry officials - the following intrinsic vulnerabilities were identified:

- Certain means of payment;
- Acts conducted online.

Finally, it should be noted that, when examining **legal persons operating for profit and other entities without legal personality**, the following intrinsic vulnerabilities were identified:

- Corporate bodies;
- Subsidiaries;
- Corporate groups;
- Group control;
- Capital increase;
- Discrepancy between declared activities and the business pursued;
- Beneficial owner.

Following identification of the threats and vulnerabilities, the probability and consequence of the materialisation of threats and vulnerabilities are gauged, using the aforementioned four-level matrix on the level of threat and degree of vulnerability. Subsequently, upon assessment of the national response capability, the level of risk is determined.

Analysis of ML threats

The **STRs recorded by the FIU** indicate that tax fraud, embezzlement, drug trafficking and cybercrime are the four most frequently mentioned types of offence. In turn, the **investigations and charges point to tax fraud, drug trafficking, offences involving the use of information technology and corruption** as the four most common types of offence. In light of the identified threats, **let us look at the specific risk level of each threat.**

As already stated in the 2015 NRA, **tax crimes**, most notably, from the standpoint of ML predicate offences, tax evasion and tax fraud, despite creating considerable illegitimate wealth advantages, having a strong negative impact on tax revenues and potentially causing significant distortions of competition in certain sectors of activity, are not yet met with significant disapproval on the part of society at large (although a shift in attitudes in this respect has been noted). In this context, the threat resulting from transnational crime is still present, typically involving shell companies, in which the identification of beneficial ownership is extremely difficult.

Experience shows that this threat carries a **high probability of materialisation and is of critical consequence**. Indeed, **the vast majority of STRs that are subsequently confirmed by the FIU's analysis –** for example, due to a discrepancy between the declared tax situation and the economic and asset situation revealed by the transactions analysed –, **involve tax fraud as the predicate offence**. Under these circumstances, whilst it cannot be excluded that the transactions concerned constitute crimes other than tax crimes, **their level of threat must be considered high**.

According to the information arising from received STRs, in which the analysis confirmed the suspicion, **drug trafficking** was on a downward path between 2015 and 2016, to increase between 2016 and 2017, only to drop again in 2018. As stated in 2015, the analysis shows that “seizures of drugs and associated property and cash on Portuguese territory provide indicators of the proceeds that criminal organisations are earning, and suggest that the probability of materialising should always be deemed high for this type of predicate offence”.

The belief persists that drug trafficking is still carried out at two levels: national, aimed at satisfying the retail markets; and transnational, targeting the import of drugs mainly into Europe, with the Portuguese territory serving merely as an entry point and transit space to other countries. In terms of national trafficking, cash is moved mainly through the transportation of banknotes and coins and through payment institutions. In terms of international trafficking through Portugal, financial settlement occurs abroad in most cases, with the sums passing through or staying in the country bearing no relation to the ‘goods’ in transit. **For all these reasons, given that the probability is high and the consequence is critical, the level of threat should be deemed high.**

Fraudulent crime, including fraud relating to the State and social security, in the purchase of consumer goods, in contractual financing transactions, as well as those committed within the financial system, with a considerably high impact, presents a particular risk. On the other hand, counterfeiting

documents, insofar as it prevents compliance with ML/FT requirements, also adds to that risk. Furthermore, 18% of STRs have this kind of crime as their predicate offence, which, taken with the analysis, suggests a **great probability of materialisation and high consequence, due to which the level of threat in this case, is medium-high.**

Also facing a **medium-high level of threat** are **IT-related crimes**. According to the information arising from received STRs, in which the analysis confirmed the suspicion, their developments have been on an upward path, exceeding 10% in the past two-year period. The typical illegal acts associated with online banking have now been extended to activities associated with virtual assets. In fact, the pursuit of activities related to this type of asset fosters an increase in criminal acts, with this crime type expected to take increasingly complex and opaque forms that will be ever more difficult for the authorities to detect and combat.

Apart from these, it is also worth mentioning **corruption** as one of the most relevant predicate offences when assessing the level of ML threat in Portugal.

On the other hand, **there are certain methods** more often associated with ML. **Based on the qualitative information available, some types of action may be deemed particularly relevant in terms of ML:**

- **The physical transportation of cash**, traditionally used to layer capital of illegal origin, is made particularly easy within the European territory due to the free movement of people, goods and capital. Reality has shown that, due to greater difficulties in the swift introduction into the formal financial circuit of the amounts generated by illegal activities, organised crime structures continue to regard the physical transportation of cash as a viable alternative as part of their strategies to move and conceal funds. In recent years, the number of situations detected involving the transportation of large cash sums (both entering and leaving national soil) has risen.

- **Concealment of the beneficial owner**. As part of a ML process, strategies are outlined to conceal the beneficial owners of both legal persons and commercial operations or financial transactions, which reveal the circuit followed by capital flows up to their integration into the economy. The progressively increasing sophistication of transnational criminal organisations allows them to combine different financial instruments, by implementing them simultaneously across several countries while taking advantage of legislative vulnerabilities and gaps. In fact, the lack of reliable information on the beneficial ownership and control of the various entities (corporations, foundations, trusts, among others) appears to be one of the main AML challenges.

- **Recourse to intricate corporate networks covering different jurisdictions**. The management of assets derived from criminal activities is purposefully diffuse, often via recourse to different corporate vehicles, complex trust funds and a multitude of jurisdictions. Different strategies are employed to guarantee a greater opacity of the operations carried out.

- **Merge of legal and illegal profits**. The final stage of ML processes results from the need to integrate funds arising from proceeds of criminal activity into the formal economy. The transformation of these processes into profit-making activities is intimately related to the growing transition of organised crime structures into company-like entities, in an effort to integrate illegal activities into lawful economic activities. This is done by making investments in potential profit-making economic sectors which, in reality, conceal ML operations. Equally crucial is hiring specialists responsible not only for the creation of the necessary economic and financial infrastructures for ML processes, but also for their actual management.

- **Use of investment incentive programmes**, funded internally or through European structural and investment funds, particularly those designed to attract foreign capital. Given that the situations involving fraud, misappropriation of property, corruption or trading in influence have gained visibility,

the use of these programmes to integrate illicit capital into key sectors of the national economy is not at all negligible.

- **Politically exposed persons.** The growing involvement of PEPs in situations linked to financial illicit activities poses additional challenges to the detection and investigation of suspicious situations, not only due to the caution and discretion with which PEPs are typically addressed, but also due to the intricate networking and interests with high-ranking economic and political bodies in the respective countries.

- **Virtual assets.** The increasing range of solutions available on the various digital platforms for the placement and layering of capital, characterised by their global and decentralised reach, poses new challenges for the identification of the origin of funds and the identity of the persons who move them. The fact that they are deregulated and operate on a peer-to-peer (P2P) basis carries potential risk to the economic and financial system and presents a further possibility of being exploited for ML purposes. In fact, factors such as technical difficulties in tracking transactions, underdeveloped regulations or the absence of a legal framework, contribute positively to the perception of complementarity in ML processes offered by technological payment solutions.

- **Crowdfunding** with recourse to online platforms is a relatively recent phenomenon. Its potential for ML is due to the fact that these platforms are relatively easy to set up and that straw persons can be potentially used. Recourse to crowdfunding for ML purposes appears to be boosted by its use in conjunction with other methodologies or building on legitimate initiatives to facilitate any one of the typical ML stages.

Sectoral incidence

The sectoral incidence of ML threats is also analysed. In this context, in the **financial sector**, the impact of the regulatory and technological revolution on the traditional business model of **credit institutions** in Portugal will foster much greater competitive pressure, with the risk of commercial objectives overriding the necessary prevention mechanisms. Thus, it is anticipated that the growing complexity of technological solutions converging with the financial system will provide new opportunities for ML. On the other hand, the dissemination in Portugal of a multitude of small businesses authorised to transfer funds, as authorised agents for **payment institutions**, has become a source of concern. The exponential growth of this “business” has made it possible to signal already suspicious situations in which certain agents act as true repositories of considerable sums in cash, which are then integrated into the formal financial system.

In the **non-financial sector**, **real estate**, **tourism** and **food services** are typically used worldwide for ML purposes, as they are particularly attractive areas for investment, given that they are cash-intensive types of business. They are also potentially exploited in Portugal, to the extent that some regions present several factors making them particularly attractive and conducive to investments that may facilitate ML.

Moreover, the recourse to **gambling** in casinos – building on the nature of this activity which allows for the use of large sums of cash – is also internationally acknowledged as one of the means used in ML processes, particularly during their placement stage. In this context, the misuse of casinos for ML purposes is a risk factor, particularly in the following dimensions: exchanging proceeds, in cash, from illicit activities for gambling chips with a view to the subsequent “legitimate” redemption by the cashier; exchanging lower-denomination banknotes for higher-denomination banknotes, preferentially used in cash transportation and storage; business conducted by usury networks, exploiting individuals in a vulnerable financial situation and/or highly addicted to gambling. Also notable are the entry of new operators into the exploration of bingo parlours, which raises the threat level in the sector, and online gambling and betting risks, regarding which the approval of the corresponding legal framework in 2015 made an irrefutable positive contribution to the enhanced transparency, control and inspection of this

sector. Illegal gambling has also gained importance – within specific communities – which, in light of the large sums it moves, fosters an increase in other illicit acts associated with gambling, whose profits are subsequently integrated and diluted in apparently legitimate investments.

On the other hand, another sector – **football** – has grown exponentially, with countless aspects that may be exploited not only for tax fraud but also for more complex crimes, like ML. Transfers of players, particularly international transfers, are usually regarded as an example of such exploitation. The fact that there are complex networks involving different agents, the various financial strategies associated with the same operation, the relative absence of dedicated professionals in club management (notably smaller clubs or those in minor leagues), increased funding needs, the growing number of match fixing cases, the financial flows associated with contracts executed via offshore companies, and the implementation of changes in the beneficial ownership of some corporations evidence particular risk.

Moreover, **international trade** has become increasingly attractive for ML, specifically through the concealment of illicit funds in the marketing of goods and services. Recourse to intricate corporate networks, with offshore ramifications, makes it particularly difficult to gauge a clear perception of the legitimacy of the capital involved in the transactions concluded, adding layers of complexity and opacity to the respective financial flows and resulting in increased difficulties for the clear identification of beneficial ownership.

Using **professionals**¹⁸ is key to building the necessary structure for the placement, layering and integration of funds of illicit origin. Using them casts an air of legality on criminally-obtained capitals. Compared to agents in the financial sector – which have been involved in ML prevention for longer – entities in non-financial sectors are yet to show the same preparedness in terms of ML prevention and fight. Moreover, many agents in non-financial sectors are somewhat distrustful of AML efforts, as they fear possible losses resulting from compliance with obligations and the necessary rejection of suspicious transactions or customers. On the other hand, constraints caused by certain measures deemed as particularly intrusive, for instance as regards managing bonds of trust with customers and how this may eventually conflict with their duty to uphold professional secrecy, are further obstacles in AML.

In turn, the organised crime's ability to infiltrate the so-called **alternative energies** and **urban management** sectors is internationally acknowledged, as part of its strategy to progressively integrate capitals of illicit origin into apparently legitimate business models.

Finally, due attention must be given to the **non-profit organisations** (NPOs) sector. This sector comprises heterogeneous and diffuse realities – associations, foundations, religious organisations, among others – subject to less stringent legal regulations, which may facilitate their use as a front for organised crime structures posing as legitimate entities, or the concealment, misappropriation and use of legally obtained funds (subscriptions, donations by individuals and firms, and State financing) for purposes contrary to the organisation's mission or to enrich its members.

Analysis of cross-border threats

A country's geographical position, its cross-border context and close ties with other jurisdictions, be they economic, financial or other, are also particularly relevant to their potential use for ML purposes. Also relevant in this context is the country's participation in certain regional organisations, bodies or structures, whether due to the fact that there is a common language, that there are strong common economic or political interests or that there are long-standing links, as is the case between Portugal and the so-called Portuguese-speaking world. The analysis of existing data, specifically taking into account the origin of capital inflows and the destination of capital outflows, means that the level of cross-border

¹⁸ Lawyers, *solicitadores*, auditors, certified accountants and notaries.

threat, examined in relation to 17 countries, is deemed to be **medium-high**, stemming from a moderate to high probability of materialisation and estimated major consequence.

Analysis of FT threats

Portugal is exposed to the same international terrorist threat as Europe, and may be seen as a target by Islamist extremist/terrorist groups or individuals. According to intelligence and other information compiled by competent authorities, including through STRs, the main *modi operandi* are as follows: credit card fraud, soliciting contributions, receiving and forwarding remittances, donations from family members and use of own funds, use of human couriers to transport currency, and use of funds for capital investments. The small number of STRs does not in itself make it possible to establish trends or make in-depth interpretations. Nevertheless, the fact that there are FT-related STRs suggests that Portugal is not immune to this phenomenon. Under these circumstances, the level of FT threat is mostly **medium-low**.

Analysis of PF threats

Countries that develop WMD programmes use several methodologies to purchase the goods, technology and knowledge they need, in an attempt to circumvent the control mechanisms in place and hinder the work of the authorities involved in the fight against PF. Some of these methodologies include: recourse to illicit activities by central banks, bank transfers omitting information on the origin of funds, use of networks to purchase dual-use goods, concealment of the real entities involved and of the dispatched goods, use of third countries as a triangulation and evasion platform, trading of precious metals as a means to raise funds, use of virtual assets, splitting payments into several tranches and different territorial constituencies, purchase of products at various points, use of numerous intermediaries and differentiation between the financial transaction flow and the flow of goods. Looking ahead, high-risk countries will foreseeably continue to purchase dual-use or sensitive goods from Portuguese firms and gather knowledge and technologies from our universities and research centres, in breach of the international sanctions in force. However, while it is admitted that some agents pose an intentional threat, it may be concluded that, in light of the stringent control mechanisms currently in force [on the basis of national or European Union (EU) legislation], **the level of PF threat is Low**.

Analysis of ML vulnerabilities

The NRA analysed the intrinsic vulnerabilities and gauged the degree of residual vulnerability in the financial and non-financial sectors. In the **financial sector**, the analysis focused on vulnerabilities in the banking sector,¹⁹ management companies of collective investments and other assets and investment service providers, pension fund management companies, insurance companies carrying out activities with respect to life insurance and insurance mediators carrying out activities with respect to life insurance and the Treasury and Debt Management Agency (*Agência de Gestão da Tesouraria e da Dívida Pública – IGCP, E. P. E.*). The residual vulnerabilities detected were **medium-high** in credit institutions and in payment and electronic money institutions, but **low** in pension fund management companies and insurance companies (life insurance) and **medium-low** for the others.²⁰

¹⁹ Which includes credit institutions, institutions specialised in credit, payment and electronic money institutions, exchange offices, and other institutions.

²⁰ Institutions specialised in credit, exchange offices, other institutions, investment service providers, management companies of collective investments and other assets, insurance mediators, and financial services provided to the public by the IGPC.

In the **non-financial sector**, vulnerabilities were analysed in the gambling sector, real estate sector, liberal professionals,²¹ trade,²² equivalent entities,²³ ancillary entities²⁴ and legal persons operating for profit.²⁵ The residual vulnerabilities detected were **high** in the real estate sector,²⁶ **medium-high** in chartered accountants,²⁷ trading of gold and precious metals, antiquities and art, aircraft, vessels and cars, in the football sector²⁸ and in auction houses and pawnshops; **medium-low** in social gambling,²⁹ in the legal professions sector – lawyers, *solicitadores* and notaries –, the import and export of diamonds and the transportation of funds and valuables, equivalent entities, supplementary entities, legal persons operating for profit; and **low** in the others.³⁰

Analysis of FT vulnerabilities

The fact that FT mostly materialises through microfinancing or self-financing makes it considerably difficult to uncover. In effect, where, in principle, there are no warning mechanisms that make it possible to monitor low-value transfers efficiently and without overburdening the financial system – particularly due to the array of false positives that would be generated – the far more difficult it becomes to detect suspicious transactions. On the other hand, the ease in disguising transfers with terrorist purposes (directed towards terrorist groups or organisations) as legitimate transfers of funds within the scope of international trade, migrants' remittances, donations or other, constitutes a further obstacle to their detection. Particularly as regards Islamist-based terrorism, donations are one of the most common sources for FT, thereby maintaining an appearance of legality as, in theory, they are meant for legitimate activities. These vulnerabilities are often due to the structural aspects of the threat itself and are not easily eliminated. However, there is no evidence of companies based in Portugal being involved in FT activities.

As regards the quality of the control system, the legal framework in force is adequate, well-defined and exhaustive, which fully and comprehensively provides for FT prevention. In addition, there are effective information mechanisms on restrictive, control and monitoring measures. This intelligence is solid; cooperation, internal coordination mechanisms and international cooperation are efficient in cases of terrorism and FT; and there is political commitment for the prevention and fight against terrorism and its financing. **Consequently, the degree of vulnerability to FT is assessed as medium-low.**

Analysis of PF vulnerabilities

Portugal is not significantly affected by geographical or demographical factors that facilitate proliferation or PF or which contribute to increased vulnerability to either of them. The country does not produce or trade in WMDs, but rather produces and trades in potentially double-use goods, as well as technology and know-how that can be used in WMD development programmes. The geographical position of the country, namely as a gateway into and out of the EU and as a triangulation platform between the African, American and European continents, may be used as an outlet for those goods. However, to date, Portugal has not been a part of the main routes for the purchase of goods and services destined for WMD development programmes.

²¹ Statutory Auditors, certified accountants, lawyers, *solicitadores* and notaries.

²² Gold and precious metals, antiquities and art, aircraft, vessels and cars, imports and exports of diamonds, football, salesrooms and pawnshops, providers of services to companies, and transportation, safekeeping, handling and distribution of funds and valuables.

²³ Management companies of crowdfunding platforms (lending and equity-based or reward and donation-based).

²⁴ Registrars.

²⁵ Regarding tax consultants, available data are insufficient to change the 2015 conclusions and, therefore, it is maintained that they are subject to ML/FT prevention obligations under their actual profession (lawyers, *solicitadores*, ROCs, CAs), and therefore they should not be considered autonomous from those professions.

²⁶ Real estate agency services, real estate development, purchase, sale, purchase for resale, and exchanging and leasing.

²⁷ Accounting services, accounting and tax consultancy services, and other services.

²⁸ Sales and acquisitions of rights over professional sportspersons.

²⁹ Lottery, territory-based odd-type sports betting and other social gambling.

³⁰ Gambling in casinos, bingo parlours, online gambling, and auditors.

In terms of control quality, there is an adequate legal framework in place, as well as effective information mechanisms on restrictive measures, sound control and monitoring mechanisms, high-quality intelligence, cooperation and effective internal coordination mechanisms, efficient international cooperation and political commitment for the prevention and fight against PF. The supervision or oversight of financial and non-financial sectors focuses – not only, but also – on the verification of the implementation of restrictive measures, chiefly, the verification of the adoption of adequate means and mechanisms to comply with restrictive measures. **As such, the degree of vulnerability to PF is assessed as low.**

V. NATIONAL ABILITY TO PREVENT AND FIGHT ML/FT/PF

Sectoral ability in terms of prevention

Portugal has in place sectoral structures and capabilities to prevent ML/FT/PF, supported by a comprehensive statutory framework (legal and regulatory), with overall organised monitoring of its compliance, although there are still a number of functional asymmetries among the staff working at obliged entities.

With regard to obliged entities, their preparedness, the suitability of managers, directors, staff and professionals, the conditions and procedures for the taking-up of a business or profession, the qualification and experience, and, to a large extent, the influence that the actual application of criminal or administrative and disciplinary sanctions exerts over those officials and professionals, are features that contribute to the proper functioning of an AML/CFT/CPF system. Nevertheless, from a risk-based approach, it is necessary to better understand the many obligations incumbent on officials and staff, namely the identification of beneficial ownership, the filtering of PEPs, the monitoring of businesses and professions, the registration and filing of transactions, as well as to emphasise the importance of having a person responsible for interacting with the judicial, police and sectoral authorities.

On the other hand, the quality of supervision or oversight, the involvement of officials from sectoral authorities and obliged entities, the quality of information, sources, identification system and, above all, the access to information, have a decisive influence on the quality of the monitoring of compliance with the statutory framework. In this context, the quality of operations, occasional transactions and business itself is negatively influenced by the weak control and communication of suspicious transactions, particularly in the non-financial sector.

Anyway, the analysis shows that the sectoral quality of the AML/CFT/CPF control systems set up by sectoral authorities and obliged entities is good overall and, by FATF standards, indicates that these systems are able to tackle challenges. In effect, of all 25 sectors assessed against a background of ML/FT/PF prevention, the control system of 68% of this universe are of high or medium-high quality. The remaining 32% mostly show a medium-low quality, pointing to the need to draw up and apply measures and concrete actions to improve their level of effectiveness.

In this NRA, mitigating measures mostly target operational action, given that the statutory framework governing ML/FT/PF prevention, the statutory control (compliance) and the management body's degree of involvement and leadership are broadly positive, the tasks and powers assigned to sectoral authorities are comprehensive, sanctions are diversified and wide-ranging, control procedures for the taking-up of a business or profession focus on professional skill requirements to perform management and senior management functions, and transparency as to the identity of beneficial owners is required. Nevertheless, the analysis shows that there is room for improvement in the statutory framework, more specifically, among other factors, as regards asset seizure and management procedures.

The quality assessment of compliance with the statutory framework is positive for financial sectors and most non-financial professions. Indeed, this exercise is carried out in proportion to the existing ML risk, taking into account the size, complexity and nature of the business or profession, but its assessment as regards risk factors associated with customers, products, services, operations, distribution channels and geographical location is negative.

The control procedures for acceding an activity or profession are, as a rule, robust in designated non-financial businesses and professions (DNFBPs), except for the real estate sector and providers of services

to companies, other legal persons or legal arrangements. In effect, in this sector and in this profession, there are no such procedures or those that exist are deemed insufficient. In the real estate sector, the lack of quality in AML control and the substantial dispersion and number of obliged entities operating in the sector present a true challenge to the oversight authority, which is faced with a mostly unregulated sector.

National ability to combat ML/FT/PF

The national ability to prevent and fight ML/FT/PF is a prerequisite to assess the effectiveness of national systems. For this purpose, and based on the FATF Recommendations, 22 key quality attributes were analysed. They are as follows: strategy and policies to fight ML/FT/PF, legal definition of the money laundering crime, seizure of assets, effectiveness of FIU action, investigation of financial crimes, suitability and autonomy of criminal investigators, prosecution of financial crimes, suitability of prosecutors, ability to judge financial crimes, suitability and independence of judges, cross-border controls, transportation of cash, customs controls, internal cooperation, international cooperation, external audits, financial integrity, efficiency of the tax authorities, level of formalisation of the economy, national identification system, access to independent sources of information, and access to information on beneficial owners.

The assessment of most of the attributes is positive, with the Portuguese AML/CFT/CPF system possessing the qualities required to qualify it as a robust and effective system. In this context, some of the desired improvements are listed below.

- As such, it is incumbent on the Coordination Commission to **set up the national strategy and policies** to fight ML/FT/PF, as well as to coordinate them. Following the conclusion of the 2015 NRA, political commitment to ML/FT/PF prevention and fight became increasingly stronger. The national AML/CFT/CPF strategy and policies are broadly underpinned by the NRA and the subsequent tools to strengthen the efficiency and cooperation between sectoral authorities and competent authorities in their prevention and fight. **This NRA makes it possible to revise the national strategy and policies** to fight ML/FT/PF, focusing on where they are found to be unsuited to the identified threats, vulnerabilities and risks. Portugal also has a set of Strategies in place that contribute to ML/FT/PF prevention, such as the National Cyberspace Security Strategy (“ENSC 2019-2023”), together with the National Counter Terrorism Strategy, the Strategy for Public Administration’s Digital Transformation (“*Estratégia TIC 2020*”), as well as the Technological and Business Innovation Strategy for Portugal 2018-30.

On the other hand, although Portugal is a stable country, with a legal system based on the separation of powers and integrated into the EU, **it is important to eliminate the shortcoming concerning the lack, insufficiency, limited comprehensiveness or incompleteness of statistical data, and**, as part of the international judicial cooperation in criminal matters, **there is great need for improving the system managing the sent and received extradition and mutual legal assistance requests.**

- As regards the **legal definition of the money laundering crime**, despite its extent and the effectiveness in the enforcement of law, there is nonetheless room for improvement in the proportionality and dissuasion of the applicable sanctions, when compared to other major crimes. Note that the Report states that the criminal law framework in force can be strengthened, in particular concerning the **low maximum limit laid down for fines**, applicable to legal persons convicted of money laundering. This improvement is even more necessary in cases involving the so-called professional “money launderers”.

- The assessment of the **statutory framework governing the seizure of assets** is positive, given that it provides the competent authorities with a wide range of operational instruments, including the administrative forfeiture of property. Notwithstanding the positive assessment, several aspects could be improved, more specifically, by ensuring that frozen or seized assets are actually confiscated in favour of the State, so as to **ensure that criminals are definitely deprived of that property.**

Regarding GAB, major improvements are required. In this context, a project entitled Asset Recovery and Management System (RGA) is under way, aimed at, inter alia, increasing the efficiency of teams investigating and managing assets associated with investigations and court cases, via digitisation of records, the creation of a common information system for the Public Prosecution Service, the GAB and the GRA, which makes it possible to meet the efficiency and effectiveness goals and to increase efficiency due to a reduction in the time taken to prepare, undertake, record and access relevant information. Finally, the resources allocated to the seizure of assets must be increased, as well as their ability to help in the identification of assets that may be frozen, seized or confiscated.

- The **FIU's actions** are positively assessed as regards the measures aimed at ensuring the suitability of its members and the existence of rules and mechanisms to protect information, thereby guaranteeing proper security and confidentiality levels. However, **the FIU's capacity must be improved**, namely through: (i) the allocation of adequate human, financial and material resources, (ii) the improvement in the quality of the STRs received and (iii) the carrying out of strategic reviews, identifying ML trends and patterns.

- In the **investigation of financial crimes**, despite some positive features, a need for improvement was identified in the training for and the competence to deal with this type of crime, with financial transactions, products and services, as well as with criminal phenomena in cyberspace, in a digital environment, and the use of information and communication technologies. A general need for improvement was also identified in terms of the human, financial and material resources available. As regards material resources, there is a substantial shortage of technical means, hardware, software and analytical tools.

- **Prosecutions**, including in **financial crimes**, are incumbent on the Public Prosecution Service, which has sufficient human resources in place for such purpose. Its access to necessary information and documentation is also satisfactory, as well as the collection of any declaration or statement that may be relevant. However, the analysis points to the **need to strengthen capacity building within the Public Prosecution Service**, which involves the strategic coordination of its intervention and the establishment of priority areas to increase effectiveness in the fight against economic and financial crimes.³¹

- As to the **transportation of cash**, although the assessment is fundamentally positive, room for improvement was tagged, however, as regards the need to: inform travellers more effectively on (i) the limitations to the physical transportation of cash, (ii) the obligation to declare cash, and (iii) the legal consequences of non-compliance with this obligation; ensure that travellers declare the transportation of cash whenever it is mandatory; ensure that the authorities responsible for controlling this have the necessary material and human resources in place to guarantee effective oversight; ensure that the control mechanisms for the physical transportation of cash exiting national territory are equally effective as those for cash entering the territory, and improve the implementation of measures and sanctions in cases of unlawful transportation of cash.

- The effectiveness of **internal cooperation is asymmetrically assessed** by the various participating entities. Indeed, while it is positively assessed by supervisors and other sectoral authorities, its assessment by law enforcement authorities is negative. This fact points to the importance of not only establishing information exchange protocols, organised by the Coordination Commission, but also of creating a cooperation culture, which will definitively eliminate a culture of silos. Internal operational coordination needs to be improved, although there is a legal framework allowing for joint investigations

³¹ Without prejudice to the foregoing, the Prosecutor-General's Office has taken a range of initiatives to strengthen capacity building within the Public Prosecution Service, namely through the ETHOS platform, providing training in economic and financial corruption and crimes. By disseminating jurisprudence, doctrine and good procedural practices, the ETHOS platform seeks to support the running of investigations and to enhance the quality of the Public Prosecution Service's intervention, as well as to foster collaboration among magistrates in various areas.

by the various competent authorities – and such investigations are actually carried out where warranted.

On the other hand, as regards the **interaction between competent authorities and obliged entities**, there is significant room for improvement. This cooperation is key to raising the obliged entities' awareness of their ML/FT/PF prevention obligations, new risks and types, as well as for competent entities to better understand the sectors they supervise or oversee and to build on risk-based approaches.

Turning to international cooperation, while positively assessed, there are, however, some difficulties in the implementation of the mechanisms that the legal framework makes available to entities, in particular when international cooperation requests are urgent. Given that the timeliness of the collection of information or evidence is key to preventing and combating ML/FT, this aspect must be improved. The same applies to the timely exchange of information on the beneficial owners of legal persons and arrangements set up or managed in or from Portugal, in response to requests made by law enforcement authorities, tax authorities or foreign supervisors.

- An important feature in ML/FT/PF prevention and fight is the possibility for obliged entities, for the purposes of complying with the obligations of identification and due diligence, to easily **access independent and reliable sources of information**, which make it possible, among other factors, to obtain information on the financial history of customers or other aspects related to them which are relevant for the identification of the customers' transaction profile.

In this context, it is acknowledged that financial supervisors have easier access compared with oversight authorities in non-financial sectors and legal professions. **As such, access to independent sources of information is deemed insufficient and reflects negative quality.**

- Finally, it is essential that information on the **identity of beneficial owners** of corporate structures, trust funds and legal arrangements is centralised in a register or mechanism that may be easily accessed by competent authorities and obliged entities. This register exists (Central Register of Beneficial Ownership – CRBO) and is governed by rules intended to guarantee that this information is sufficient, accurate and up-to-date. However, given that **the CRBO is not yet fully functional**, it is not yet possible to ascertain whether those goals will be met. For this reason, it is equally premature to qualify the ease and timeliness of access to the CRBO by competent entities and the obliged entities that must comply with ML preventive obligations. As regards the proportionality and deterrent effect of sanctions applied to the natural and legal persons that breach CRBO rules, they are still unknown, given that no sanctions have been applied to date. Access to information on beneficial ownership was assessed as merely sufficient.

VI. RISK ASSESSMENT

As stated in the 2015 NRA, “[f]or several years, the fight against ML has been an absolute political priority internationally, both because the interruptions to financial flows created by the activity of organised criminal groups have proven to be a key driver of the strategy for combating these structures, and because of the need to protect the economic/financial system against misuse, compromising its reputation and stability and with repercussions at economic, political and social level.”

Organised crime has greater economic and financial resources, and increasingly complex and sophisticated mechanisms, making the detection of capital flows of criminal origin even more difficult. This has become one of the most serious obstacles in the fight against ML. Its transnational nature means that only an equally global response will be effective, based on strong domestic and international cooperation mechanisms and the exchange of information at all levels among the various prevention, supervision, oversight and repression bodies”.

As this remains unchanged, the analysis carried out under the 2019 NRA shows the major external threats affecting the AML/CFT/CPF system, the most critical domestic vulnerabilities and the highest risks faced by Portugal.

Money laundering

Concerning ML, the **threats** which have a **high risk level**, assessed by the probability of materialisation and the consequence that this may bear, which is, as a matter of fact, in line with the most relevant predicate offences, are tax fraud, illicit trafficking in narcotic drugs and psychotropic substances, and corruption.

Similarly to 2015, tax fraud is still clearly the prevalent threat. Particular focus on this type of criminality is therefore still justified, including certain crimes that are not necessarily considered predicate offences under the current definition of ML, certain customs offences for example, such as fraudulent introduction into the market or smuggling, in the simple form. Also presenting a high threat risk is drug trafficking, which accounts for around 46% of open investigations and a substantial number of confirmed STRs, and corruption, which, although with no confirmed STRs, represents approximately 8% of open investigations.

On a second level, facing a **medium-high** level of threat, are economic and financial offences involving the use of information technology, whose relative importance in Portugal has grown, namely in terms of the number of confirmed STRs, and the crimes of misappropriation of money or property by public officials and counterfeiting. Of all these, only counterfeiting is not considered a predicate offence for ML, as it is not covered by the penalty criterion which serves to define predicate offences, nor is it included in the catalogue of such offences. Given its importance as acknowledged in this NRA (and in line with the 2015 NRA), this situation should be corrected.

The identified and analysed **vulnerabilities** help to qualify the associated **risks** and highlight those that, by resulting in high or medium-high risk, warrant that the formulation and application of the necessary risk-mitigating measures be treated as a priority.

The anonymity of the customer’s beneficial owner of the activity and the use at both national and international level of said activity for the purpose of committing tax crimes are vulnerabilities common to both the financial and non-financial sectors. The use of cash in the activity and the transnational nature of transactions are also relevant vulnerabilities, namely in the banking sector. In this sector, the acceptance of deposits or other repayable funds, private banking, correspondent relationships in credit institutions, as well as money remittance and similar correspondent relationships in payment

institutions and electronic money institutions, are the largest intrinsic vulnerabilities.

Anonymity, from an abstract standpoint, and although increasingly on the downside, besides facilitating the parallel economy, makes it impossible to trace the funds, such that any illicit origin or use for criminal purposes goes undiscovered. However, not knowing the beneficial owners, whether of legal persons or of certain operations or transactions, is still a fairly major vulnerability. Indeed, although the CRBO has already been established, the fact that it is not yet fully operational, together with the somewhat insurmountable limitations of a system built on the self-declarations of the persons concerned, makes this vulnerability difficult to eliminate. In this context, the organised crime structures' strategy towards adopting an economic profile – using intricate, complex corporate networks, often with offshore ramifications – makes the fight against such structures far more difficult. These corporate networks and their owners (in certain cases, PEPs or the respective figurehead) are then used to conduct trades, legitimate in appearance, but which in reality are ML transactions.

Monitoring must be strengthened on transactions originating in or moving to certain offshore centres – jurisdictions which have less stringent regulation and control and where bank secrecy rules prevail – and jurisdictions listed by the FATF.

The use of cash, aside from allowing the unregistered economy to flourish, also encourages the development of informal payment systems, which, taking into account the plurality of immigrant communities in Portugal, must not be neglected, especially as, as stated in the 2015 NRA, replacing official mechanisms with informal systems means that the transactions are no longer made in a regulated space but move to 'grey' areas of anonymity. In addition, given that such use is normal for the business of some entities in the financial sector, it continues to be relatively important for a number of non-financial sectors of activity (for instance, accommodation and food service activities, maintenance and repair of motor vehicles, hairdressing and other beauty treatment, sports activities, musical events). Limits to cash payments, introduced by Law No 92/2017 of 22 August 2017, when duly implemented and monitored, being a highly restrictive legislative measure, considerably restricted the possibilities for ML.

Another important aspect in this context is related to the physical transportation of cash. One of the typical ways to layer funds of illicit origin, moving them away from where they were created, is through the physical transportation of cash. Of particular importance here are 'cash couriers'. However, it is acknowledged that anyone transporting cash must fill in a declaration stating the origin of those funds or justifying their transportation, more specifically to prevent the criminal prosecution of cash smuggling, which is provided for and punishable under Article 92 (1) (e) of the General Regime of Tax Offences (RGIT).

According to the analysis performed, **ML risk** in Portugal **is medium-low**, based on the fact that the overall level of threat is medium-high, but the degree of residual vulnerability, in light of its responsiveness, is medium-low. Despite the criminal law response to these crimes (38 convictions in 2015, 28 in 2016, 63 in 2017 and 70 in 2018), this must continue to be closely monitored, in terms of both prevention and enforcement.

Terrorist financing

The terrorist threat remained moderate, which could be translated into a medium-low level, given that specific references to the country continued not to appear in propaganda disseminated by terrorist organisations but, to date, no risk factors have materialised culminating in attacks.

FT risk in Portugal, based on a medium-low level of threat and a medium-low degree of vulnerability, where the probability of materialisation is reduced and the consequence is mostly critical, **is medium-**

low. In any case, it must not be underestimated, and cooperation with national (public and private) entities and international bodies must be further strengthened.

Proliferation financing

PF risk is low, due to a low level of threat and a low degree of vulnerability. Looking ahead, the threat of proliferation, which includes the PF aspect, will remain in Portugal, and high-risk countries will foreseeably continue to purchase dual-use or sensitive goods from Portuguese firms and gather knowledge and technologies from our universities and research centres, in breach of the international sanctions in force. However, while it is admitted that some agents pose an intentional threat, many doubts persist as to their real power in light of the control mechanisms currently in force and, as such, the level of PF threat is classified as low.

Sectoral and geographical risk

This NRA also draws conclusions on the highest ML/FT/PF risks, be they by sector or geography.

As was the case in 2015, among the sectors with the **highest** risk is, in the financial area, the **banking sector**, the *core* of the financial system in most countries. As the largest sector with the greatest operational complexity, it is not surprising that it is one of the preferred means to introduce illicit funds into the legal economy and to layer funds intended to finance an activity like terrorism.

In the non-financial sector, the highest risks, more specifically ML risks, still exist in the **real estate sector** and in **some categories of obliged entities subject to the oversight of ASAE**. In the real estate sector, transactions continue to offer considerable opportunities, not only due to the fact that the values involved are high, but also as it is easy to complete quick transactions and because companies based in jurisdictions or territories with low levels of cooperation and information exchange may be used. Moreover, the geographical location and tourism make Portugal an appealing place for investments, which may make it possible, under cover of apparently legal corporate structures, to successfully legitimise significant capital flows. As stated in the 2015 NRA, this sector therefore requires particular attention and stronger AML/CFT/CPF mechanisms, and must be a priority for the overseeing entity.

Turning to the areas in this sector subject to the oversight of ASAE, sales and acquisitions of rights over professional sportspersons are classified as having medium-high residual vulnerability. Overall, however, strengthening ML/FT/PF prevention and control requires boosting training, as well as the articulation between regulators and supervisors, with the active participation of the sector associations, to substantially improve their effectiveness.

As to the geographical risk, the highest risks stem from some of the countries with which Portugal has stronger commercial and financial ties.

VII. STRATEGIC GUIDELINES

To keep the national AML/CFT/CPF strategy up-to-date and to formulate the policies to strengthen the national AML/CFT/CPF system, and as a result of the reassessment of external threats and domestic vulnerabilities and the shortcomings in the country's capacity identified in this NRA, it is important to establish certain strategic guidelines.

I – Address the lack, insufficiency, incompleteness, limited coverage and/or poor reliability of statistical data

The drafting of a coherent AML/CFT/CPF strategy requires the full, in-depth knowledge of the environment in which this combat takes place. In this context, it is key that the relevant statistical data are produced and released, not only to draft the NRAs, but also to assess the effectiveness of the ML/FT prevention and combat systems. They are also needed to meet a number of international obligations of the Portuguese State. It is therefore necessary to: (i) produce, compile and process all relevant data for the purposes mentioned and (ii) enhance the quality of the information produced, compiled and processed.

II- Strengthen a culture of inter-institutional exchange of information

Internal cooperation between competent authorities is crucial for the ML/FT/PF prevention and combat system. In this context, exchanging available information is a key factor. It is therefore important to (i) encourage the strengthening of internal cooperation, specifically through the conclusion of information exchange protocols and (ii) boost operational cooperation, in particular by increasing joint investigations and workshops to share experiences and knowledge.

III - Raise the quality of the risk-based approach

A risk-based approach for supervisors, overseers and obliged entities is absolutely essential for the proper management of necessarily scarce resources. On the other hand, regulating access (particularly in the non-financial sector) to DNFBPs may help reduce risk factors. As such, it is important to (i) strengthen the allocation of resources to higher risk and (ii) strengthen the regulations governing access to businesses and professions.

IV - Increase the efficiency of criminal investigation and prosecution

Given the scarcity of available resources, the effectiveness of criminal investigation and prosecution must be strengthened so that the response to ML/FT/PF can be adequate. Therefore, it is important to (i) strengthen the existing human resources' ability to monitor developments in the ML/FT/PF phenomenon, to identify new types, including those concerning virtual assets and (ii) increase the FIU's capacity, specifically as regards strategic analysis.

V - Deepen cooperation with the private sector

The private sector's involvement and participation is a prerequisite for an effective ML/FT/PF prevention and fight system. In this context, it is important to (i) promote regular sectoral and national fora and foster operational and informal cooperation and (ii) release Guidelines for the various sectors of obliged entities, in particular on ML/FT/PF types and best practice in the fight against them.

VIII. PRIORITIES – FUTURE ACTION

The conclusions drawn from the NRA on the risks faced by Portugal warrant that priorities be set and action be taken to mitigate or limit them.

The analysis discloses many differences between the contexts and the environments where supervisors and overseers play a role and monitor prevention obligations. However, these differences must not justify the substantial asymmetries between the financial and non-financial sectors. Therefore, this inconsistency between approaches must be overcome, using the necessary and advisable proportionality in the action taken, in increasingly complex, dematerialised environments, with multiple relevant risk factors and vehicles, in less formal, less costly and less bureaucratic circuits. For such purpose, supervisors and overseers must respond with effective cooperation, by disseminating good risk control practices among obliged entities and setting up enhanced or simplified due diligence, taking into account their obligations.

The difficulty in explaining control methods and procedures shows that it is still necessary to improve the joint work of oversight authorities and obliged entities for the effective detection, reporting and suspension of suspicious transactions.

The detection, reporting and suspension of suspicious transactions constitute a key step in the process of preventing the use of obliged entities for illicit purposes. Bearing this in mind, the risk stemming from the under-preparedness of obliged entities and, likewise, of the supervisory or oversight authorities must be mitigated or even eliminated, be it due to the lack of qualifications, the absence of experience or the failure to act by virtue of the lack of human, material or financial resources. On the other hand, the nearly non-existent number of STRs in non-financial sectors, including in legal professions, warrant an increase in training, mostly to develop qualifications and raise awareness among managers, directors and staff.

Finally, to obtain greater effectiveness in prevention, it is important to further cooperation between law enforcement authorities and supervisory or oversight authorities, disseminating good practices and improving knowledge on risks.

To this end:

Legislative priorities

- To include the crime of counterfeiting in the list of ML predicate offences;
- To improve the statutory framework governing asset seizure and administration and management procedures;
- To establish that legal persons not yet subject to registration must be so;
- To introduce administrative simplification and red tape cost-reducing measures, using technological solutions that enhance “instant knowledge” on the simultaneity of the establishment of legal persons and of their administrators, managers or other officials.

Operational priorities

- To promote the conclusion of information exchange cooperation protocols;
- To routinely send information to the sectoral authority on crimes related to their business or profession;
- To enhance the skills and experience of officials and staff of sectoral authorities and obliged entities;
- To strengthen the sectoral authorities’ capacity, by reallocating or procuring resources;
- To prepare institutions for the effective follow-up on new digital business models;

- To improve the timeliness of statistical information reporting on the management of assets administered and managed by the GAB;
- To raise awareness among each sector's professional associations of the inherent potential of sharing IT solutions to meet ML/FT/PF prevention obligations.

Sectoral measures

The analysis shows that, in sectoral terms, previously identified insufficiencies remain, some of which are more prominent in this new period under review – for instance, the exercise of oversight powers, the preparation and release of regulations and guidelines, and the lack of risk-based approach models. In fact, after some years, in very relevant sectors (football – sales and acquisitions of rights over professional sportspersons –, real estate, diamonds – imports/exports –, among others), inspections are still nearly non-existent, although they are unquestionably necessary. Thus, overcoming these insufficiencies necessarily involves considering AML/CFT/CPF a priority for supervisory and oversight authorities. This priority should be reflected in their annual activity plans or strategic plans, and its implementation should be set out in their respective annual reports.

Consequently, the NRA provides for specific measures for the following sectors: banking, securities, insurance, government debt, gambling, social gambling, real estate, statutory auditors, certified accountants, lawyers, *solicitadores*, notaries, trade, imports and exports of diamonds, auction houses and pawnshops, football, and transportation of funds and valuables.

FINAL NOTE

This ML/FT National Risk Assessment is a review of the first exercise of its kind carried out in Portugal in 2015. Conclusion of the 2019 NRA required an enormous cooperative effort of the entities that participated in the Working Group as well as the motivation, which was not always fully achieved, of the associations representing the private sector entities subject to ML/FT prevention obligations. The results obtained, based on the existing data and which, as stated in 2015, show room for improvement, reveal the present threats and vulnerabilities, as well as the risks the country faces.

However, this exercise requires updating to match the responses to the new threats which may arise and the risks which may worsen, redefining courses of action and priorities. In these circumstances, the NRA requires a periodic review, and unless exceptional circumstances arise, 2023 appears to be a suitable date, upon conclusion of the FATF follow-up evaluation (five years after the fourth round of evaluation, which, for Portugal, ended in November 2017).

Annex to the English Version
Glossary of Acronyms

Acronyms	English designation	Portuguese designation
GRA	Asset Recovery Office	Gabinete de Recuperação de Ativos
DCIAP	Central Department of Criminal Investigation and Prosecution	Departamento Central de Investigação e Ação Penal
CRBO	Central Register of Beneficial Ownership	Registo Central de Beneficiários Efetivos
DNFBPs	Designated Non-financial Businesses and Professions	Atividades e Profissões não-financeiras Designadas
ASAE	Economic and Food Safety Authority	Autoridade de Segurança Alimentar e Económica
EU	European Union	União Europeia
FIU	Financial Intelligence Unit	Unidade de Informação Financeira
PF	Financing of Proliferation	Financiamento da Proliferação
FT	Financing of Terrorism	Financiamento do Terrorismo
SRIJ	Gambling Regulation and Inspection Service of Turismo de Portugal	Serviço de Regulação e Inspeção de Jogos do Instituto de Turismo de Portugal
IGF	General Finance Inspectorate	Inspeção-Geral de Finanças
SEF	Immigration and Borders Service	Serviços de Estrangeiros e Fronteiras
IGMTSSS	Inspectorate-General of the Ministry of Labour, Solidarity and Social Security	Inspeção-Geral do Ministério do Trabalho, Solidariedade e Segurança Social
IMPIC	Institute for Public Procurement, Real Estate and Construction	Instituto dos Mercados Públicos, do Imobiliário e da Construção, I. P.
IRN	Institute of Registries and Notaries	Instituto dos Registos e do Notariado, I. P.
SIS	Internal Intelligence Service	Serviço de Informações de Segurança
ML	Money Laundering	Branqueamento de Capitais
OCC	Order of Certified Accountants	Ordem dos Contabilistas Certificados
OROC	Order of Statutory Auditors	Ordem dos Revisores Oficiais de Contas
PEPs	Politically Exposed Persons	Pessoas politicamente expostas
GAB	Property Management Office	Gabinete de Administração de Bens
CMVM	Securities Market Commission	Comissão do Mercado de Valores Mobiliários
OSAE	<i>Solicitadores</i> and Enforcement Agents National Association	Ordem dos Solicitadores e Agentes de Execução
ASF	Supervisory Authority for Insurance and Pension Funds	Autoridade de Supervisão de Seguros e Fundos de Pensões
STRs	Suspicious Transactions Reports	Comunicação de operações suspeitas
IGCP	Treasury and Debt Management Agency	Agência de Gestão da Tesouraria e da Dívida Pública - IGCP, E. P. E
WMD	Weapons of mass destruction	Armas de destruição em massa