PORTUGAL

NATIONAL RISK ASSESSMENT OF MONEY LAUNDERING AND FINANCING OF TERRORISM

SYNTHESIS

JUNE 2015

INTRODUCTION

MONEY LAUNDERING

Money laundering (ML) is a process which *transforms* the proceeds of criminal activities to hide their origin and allow their use as though from a legitimate source. The aim of the launderer is to permanently disguise the illicit origin of money gained through criminal activity in such a way that such proceeds can be used as though they resulted from legal activity. This aim is achieved by concealing the sources of the income, by changing the form of such proceeds or by sending them to jurisdictions where anti-money laundering prevention and combat mechanisms are less strict.

FINANCING OF TERRORISM

According to the International Convention for the Suppression of the Financing of Terrorism, the financing of terrorism consists of the provision or collection of funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, to carry out terrorist acts or any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organisation to do or to abstain from doing any act. According to the Convention, the term funds means assets of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, letters of credit.

NATIONAL ASSESSMENT OF ML/FT RISK

The review of the FATF Recommendations in February 2012 brought about a fundamental change in the fight against ML/FT, adopting a risk-based approach. Therefore, countries should first identify, assess and understand the risks of money laundering and financing of terrorism that they face, and then, based on the risks identified, adopt appropriate measures to mitigate those risks.

1) Under these circumstances, it was decided to undertake the first money laundering and financing of terrorism national risk assessment (NRA), not only to ensure Portugal's compliance with the new international anti-ML/FT standards, but in particular to provide the Portuguese authorities with an essential instrument to use the scarce resources available more efficiently and to enable them to apply preventive measures in proportion to the nature of the risks, thus optimising their efforts. Accordingly, the objective of the NRA is to identify which sectors present the greatest potential risks and which may offer the lowest risk, in order to mitigate or possibly eliminate such risks.

The identification, assessment and understanding of ML/FT risks is an essential part of the development and practical application of a national anti-money laundering and counter financing of terrorism framework. This framework assists the authorities in establishing priorities and efficiently deploying resources. The NRA can also supply useful information to financial institutions and designated non-financial businesses and professions (DNFBPs) enabling them to perform their own risk assessments.

2) The exercise covers all sectors of activity where ML/FT prevention obligations are already in force, including some where it is accepted that there is a need to extend or reinforce those obligations, and was undertaken by the Working Group set up as a result of Decision No.9125/2013, of 1 July 2013, by the Minister of State and of Finance.

This Working Group was based on the Portuguese Delegation to the FATF which, with the permanent participation of the Ministries of Finance and of Justice, the financial supervisory authorities and the Financial Intelligence Unit (FIU), has hitherto ensured the coordination of the Portuguese AML/CFT system, and included the following members:

a) The Coordinator of the Portuguese Delegation to the FATF, as chair;
b) A representative from the Ministry of Finance;
c) A representative from the Ministry of Foreign Affairs;
d) A representative from the Ministry of Economy and Employment;
e) The members of the Portuguese Delegation to the FATF (representing the Ministry of Justice, Banco de Portugal, the Securities Market Commission, the Insurance and Pension Funds Supervisory Authority and the Financial Intelligence Unit);
f) A representative of the Prosecutor-General's Office;
g) A representative of the Tax and Customs Authority;
h) A representative of the Bar Association;
i) A representative of the Chamber of *Solicitadores*;
j) A representative of the Order of Statutory Auditors;
k) A representative of the Order of Chartered Accountants;
l) A representative of the Institute of Registries and Notary;
m) A representative of the Institute of Construction and Real Estate;
n) A representative of the Gambling Inspection Service of *Turismo de Portugal*;
o) A representative of the Economic and Food Safety Authority.

In addition, from within the public sector, the exercise also involved the Security Intelligence Service (SIS) which prepared a general overview of the threat, covering organised crime's money laundering strategies and the financing of terrorism and proliferation.

In the private sector, associations subject to ML/FT prevention obligations representing entities from the non-financial sector took part, along with financial sector associations. Therefore, initial written surveys were carried out on risk factors in the different sectors, and thereafter on the vulnerabilities identified in those sectors and possible measures to be taken to eliminate or mitigate them. Face-to-face meetings were also held with financial sector

associations.

There were regular meetings of the full Group and subgroups. The following six subgroups were formed, always including a representative of the FIU and the Group coordinator:

i) Financial Sector – including representatives from the Ministry of Finance, Banco de Portugal, Insurance and Pension Funds Supervisory Authority, and the Securities Market Commission;
ii) Legal Professions – including representatives from the Ministry of Justice, Prosecutor-General's Office, the Bar Association, Chamber of *Solicitadores* and the Institute of Registries and Notary;
iii) Auditors – including representatives from the Ministry of Finance, Order of Statutory Auditors and Order of Chartered Accountants;
iv) Casinos, Betting and Lotteries – including representatives from the Ministry of Finance, the Ministry of the Economy and the Gambling Inspection Service of *Turismo de Portugal*;
v) High Value Goods – including representatives from the Ministry of Finance, the Ministry of the Economy, the Tax and Customs Authority and the Economic and Food Safety Authority;
vi) Real Estate – including representatives from the Ministry of the Economy, Institute of Construction and Real Estate and the Institute of Registries and Notary.

The participants in the Working Group carried out surveys on risk factors, discussed the data collected, exchanged points of view and agreed on the future activities of the Group. The long and comprehensive process of bringing together the NRA required a significant effort from all participants. The NRA was compiled using the information collected from each sector covered, which would later be used to produce the sectorial assessments in the Annex to this document. It was, therefore, a wide-ranging exercise carried out at governmental level and involved all the public sector entities with AML/CFT supervision or oversight duties, as well as associations from the financial sector and a significant number of associations representing DNFBPs, thus demonstrating Portugal's continued dedication to preventing and combating ML/FT.

3) Risk can vary according to three factors: threat, vulnerability and consequence. An ML/FT risk assessment is a product or process based on a methodology which seeks to identify, assess and understand ML/FT risks and is the first step in responding to them. Ideally, a risk assessment involves an assessment of threats, vulnerabilities and consequences.

The methodology used in the NRA closely followed the FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment, published in February 2013. Other available texts published by international organisations and the FATF were also used, namely the FATF Global Money Laundering and Terrorist Financing Threat Assessment of July 2010. Thus the national assessment was written using the various sectorial contributions.

In the banking sector, the annual self-assessment reports and the answers periodically given to an ML/FT survey could be used to identify the various risk factors and consequent threats,

the likelihood that a risk will materialise, the consequence if it materialises and the instituted methods for addressing those factors. Outside this sector, a survey was prepared on the same subject – risk factors, the likelihood that a risk will materialise, the consequence if it materialises, and control mechanisms created to mitigate such factors – directed at the other entities/associations representing entities subject to ML/FT prevention obligations. The data from the banking sector and survey contributed to a better understanding of the perception that the supervised/overseen institutions have of the intrinsic risks they face, as well as the perception that the sectorial associations have of the risks inherent to each specific sector of activity. Data held by the FIU and Prosecutor-General's Office were added to the aforementioned information in order to define the existing threats more clearly.

Vulnerabilities were identified in essentially the same way.

Concerning the analysis/assessment of the risks inherent to each institution and each sector of activity, and the creation of a corresponding threat matrix, although the perceptions of the obliged entities and sectorial associations were also taken into consideration, the perception of the supervisor/overseer had a fundamental role, based on the information collected from on-site or off-site inspections and on the subsumption of that information into a comparative matrix, offering a comprehensive overview.

The work carried out, which led to this report, took as reference essentially the data from 2012 and 2013, and is aimed to identifying, assessing and understanding the ML/FT risks existing in Portugal, ensuring full compliance with the 2012 FATF Recommendation 1. The description of the threats and vulnerabilities identified is based in elements with a reasonable degree of development, while the part related to the Assessment, in particular the analysis' matrixes, represents a first approach with a necessary revision in the future. Anyhow, the work developed allows already a definition of priority measures to be taken to reinforce the Portuguese AML/CFT system and ensure full compliance with the new Recommendations.

ML/FT PREVENTION

The crime of money laundering is defined in Article 368-A of the Criminal Code. This type of crime was defined using the United Nations Conventions and guidance from Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005, with the following specificities:

- Predicate offences are defined using two criteria: crime type and the quantum of penalty;
- The type of crime also includes self-laundering;
- There are no provisions for punishment of unwitting money laundering through negligence;
- The acts of mere holding or acquiring the proceeds of crime were not included as typical types of money laundering, as they could be confused with the crime of use of stolen goods – Article 231 of the Criminal Code;
- The penalty applied to money laundering cannot be higher than the highest penalty for the predicate offence, although the suspect need not be sentenced or prosecuted for a predicate offence;

- In the event of the legal procedure for the predicate offence being dependent on a formal complaint being lodged, the same is applicable for the crime of money laundering;
- Reparation for the losses generated by the predicate offence implies the mitigation of the penalty applicable for the crime of money laundering.

Therefore, the crime of money laundering is typified as a mere conduct crime, with autonomy in relation to the predicate offences, which are presumed to have occurred in order to generate the proceeds of the money laundering transactions.

The crime of financing of terrorism is currently provided for in Article 5-A of Law No 52/2003 of 22 August 2003, in accordance with the provisions in the International Convention for the Suppression of the Financing of Terrorism of the United Nations and in Framework Decision No. 2002/475/JAI of the Council, of 13 June 2002.

The ML/FT prevention framework is provided for in Decree-Law No 25/2008 of 5 June 2008, transposing Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005, and Directive 2006/70/EC of the Commission of 1 August 2006 into Portuguese law.

The legislator chose to oblige the entities subject to prevention duties to direct their formal STRs to the FIU and Prosecutor-General's Office. This option is based on the fact that the FIU is strictly a police intelligence organisation, producing reports which may be included in or give rise to inquiries, but not enough in themselves to substantiate the application of a transaction suspension measure. In tandem with the work carried out by the FIU, reporting to the Prosecutor General's Office aims to promote evidence-gathering which, when formally investigated, enables a judge to be provided with the basis for a suspension of financial or other transactions.

Article 4 (4) of Law No 5/2002 of 11 January 2002, allows account transactions to be suspended whenever necessary in order to prevent money laundering. This suspension of debit transactions (blocking), was developed in courts' jurisprudence to be valid for a renewable period of three months.

The parties in the ML/FT prevention procedure are therefore the FIU and the Prosecutor General's Office, without prejudice to the intervention of an Investigating Judge to uphold, or not, temporary transaction suspension measures. In terms of checking the relevant entities' compliance with the obligations in Article 6 of Law No 25/2008 of 5 July 2008, and other sectorial regulations, the supervisory and oversight authorities also participate.

Financial Intelligence Unit (FIU)

The Financial Intelligence Unit (FIU) was included in the structure of the PJ through Decree-Law No 304/2002 of 13 December 2002 and is currently defined by Law No 37/2008

of 6 August 2008, which approved the new structure of this police force, as a department under the auspices of the National Directorate. Its competences are described in Decree-Law No 42/2009 of 12 February 2009 and in the ML/FT legislation itself (Law No 25/2008 of 5 June 2008). The organisational structure of the FIU is defined by Standing Service Order No 6/2010.

Under the terms of the law, the FIU is the competent centralised national authority for the collection, analysis and dissemination of information related to ML/FT. It is also responsible for handling information relating to more serious tax offences. Decree-Law No 93/2003 of 30 April 2003 defines the conditions relating to information sharing between the FIU and the Tax and Customs Authority (AT), for which the Permanent Liaison Group (GPL) was set up at the FIU, including representatives from the PJ and AT.

In terms of cooperation, the FIU undertakes its competences at national level with the entities which have responsibilities within the ML/FT prevention system, and at international level with its counterparts and other similar structures. Under the terms of the aforementioned Law No 25/2008 of 5 June 2008, in order to undertake its ML/FT prevention duties, the FIU has access to financial, administrative, judicial and police information on a timely basis. As far as the publication of statistical data is concerned, the FIU is responsible for preparing and updating statistical data referring to the number of suspicions transactions reported and the referral and result of these STRs. The FIU is subject to confidentiality in terms of dissemination of information. The number of STRs sent to the FIU has shown an upward trend. In the financial sector, when analysing the years 2012 and 2013, the number of reports was 2020 and 2400 respectively. In the non-financial sector, there has also been an increase in the number of STRs received. In this sector, the FIU also receives a lot of aggregate and bulk data.

The Public Prosecution Service

As far as ML prevention is concerned, within the Prosecutor-General's Office, the competent department is the Central Department for Criminal Investigation and Prosecution (DCIAP), whose competences are delegated by the Prosecutor-General. At DCIAP, when a STR is received from an entity subject to ML/FT prevention duties, its content is analysed and registered as a prevention procedure. Within the scope of this procedure, the necessary documentation is requested in order to ascertain whether there was an illicit act generating proceeds subject to ML operations. Prevention procedures can give rise to an inquiry, even in the absence of a transaction suspension, or can the documents obtained within the scope of such an investigation be added to enquiries already open. In 2013 there were 39 decisions to suspend operations, all judicially confirmed, further to the new enquires open, and information sent to existing enquires.

Supervisory and Oversight Authorities

ML/FT prevention also involves the supervisory authorities of the financial sector and

oversight authorities of the non-financial sector, as identified in Article 38 of Law No 25/2008 of 5 June 2008. It is the main competence of these authorities to assess whether the financial entities and DNFBPs (obliged entities) comply with the duties foreseen in Article 6 of the aforementioned Law and other sectorial regulations.

Under Article 38 of the aforementioned Law No 25/2008, the competent authorities tasked with verifying compliance with the legal framework in force are, in the case of financial institutions and in terms of financial services related to this area of supervision, Banco de Portugal, the Securities Market Commission and the Insurance and Pension Funds Supervisory Authority, as well as the Ministry of Finance for the Treasury and Government Debt Agency. In the case of DNFBPs, the number of supervisory authorities is greater. Therefore, compliance with ML/FT prevention obligations by holders of gambling licences in casinos and entities which pay prize money from gambling or lotteries is the responsibility of the Gambling Inspection Service of *Turismo de Portugal*. In the case of property brokers and real estate agents, and property developers which sell their properties directly, the regulator is the Institute of Construction and Real Estate. The Economic and Food Safety Authority supervises high value dealers and, in the absence of any other competent authority, external auditors, tax consultants, service providers to legal persons, to other legal entities or to legal arrangements, and other liberal professionals. Lawyers, statutory auditors and chartered accountants are supervised by their respective professional associations; *solicitadores*, by their chamber, and finally, notaries and registrars by the Institute of Registries and Notary.

I. THREATS

MONEY LAUNDERING

One of the current main threats to the Rule of Law are transnational criminal organisations, due not only to their ability to infiltrate, erode and subvert political, economic, financial and social structures, but also to their sophistication, intelligence and adaptability to internal and external change. Indeed, these organisations are highly skilled in identifying vulnerabilities, creating opportunities and new tactics in pursuit of their direct criminal activities and in laundering proceeds obtained illicitly. These organisations have evolved over the last few decades, taking advantage of the opportunities offered by geostrategic changes, the globalisation of the economy and financial systems, and the technological revolution. And despite certain differences in the way transnational criminal organisations are organised and operate, they have one shared goal – to maximise profit and minimise risk.

Certain factors are now crucial to their activity:

- Adaptation to the economic models of globalisation: transnational criminal organisations have moved away from the classical model of family-based local operation and have adopted a corporate model and global reach, similar to a multinational organisation, aiming to minimise and contain risks both in transporting illicit goods and in money laundering processes, through *informal* representation in multiple countries and by subcontracting local logistical support networks;
- Incorporation of progress in technology, which is particularly relevant in money laundering, where the absence of states and jurisdictions in the online environment is serving to create new and ingenious mechanisms for the illicit layering of funds (e.g. alternative payment methods and/or digital currencies), which have become attractive due to their inherent anonymity. On the other hand, the transfer of human activity to the online environment means a transfer of criminal activity there: the 'deep web' is thus a growing space (for buying and selling illicit goods) and organised cybercrime, targeting the banking sector in particular, and also companies and citizens, is an increasingly central threat among states' concerns;
- Legislative arbitrage: the transnational nature of these organisations allows them to identify advantages in each of the territories in which they operate, constituting an additional challenge for the authorities in each country. To minimise risks, a structure may be based in one country, running direct criminal activities in others and laundering the proceeds of crime in still others, exploiting not only the advantages arising from different legislative frameworks, but also the authorities' operational limits, constrained by geographical borders. Regarding ML, whose control, investigation and combat continue to be somewhat related to the predicate offence, the distance (and/or geography) between the illicit capital and its predicate offences adds further difficulty to the identification of its illicit provenance and its final beneficiary;
- Transformation of vulnerabilities into opportunities: the optimisation of more favourable mechanisms offered by each State (of economic competitiveness, tax or financial environment, e.g., bank secrecy) and the identification of actors in the public and private sectors, with important positions and access, who might be lured in or corrupted, constitute

fundamental characteristics in the strategy of transnational criminal organisations;

- Exploitation of opportunities created by economic activity: transnational criminal organisations are intensely involved in economic activity, depending on it to create an appearance of legitimacy for the proceeds of their activities. This dependency is gaining a new dimension for ML, since, beyond the so-called traditional sectors in the integration phase – in particular, property, tourism and catering – there is a growing tendency to invest the proceeds of crime in other profit-making areas. Although at first the injection of financial flows into the economy may seem to benefit job creation, growth and economic stimulus, the fact is that the inclusion of capital may in the long term lead to a dominant position for the criminal organisations in the targeted sectors or even to the importing of the direct criminal activities that gave rise to the capital;
- But in this vein of apparently legitimate activities, transnational criminal organisations not only operate to protect and conceal their investments (as a rule preceded by ML transactions), but also run criminal continuity practices, normally relating to tax, corruption and financial fraud. Tax fraud thus holds a dual role, in particular in organisations from eastern Europe: to maximise the gains from those activities (e.g. private jet airlines, tourism companies, etc.) and to channel the gains to "exit points", in order to bring the funds back into the personal estates of the heads of the organisations and even into new investments in traditional criminality (e.g. drugs and arms trafficking, and smuggling). To this end they make frequent use of triangulation schemes (operating entity, invoicing entity, bank account holding entity), aiming to send the funds to offshore financial systems, and they may theoretically make occasional use of the Madeira Free Trade Zone.

Furthermore, aside from international criminal organisations, the external threat is often related to corruption practices, namely among high administration officials in certain African countries. This vulnerability lies in the growth and expansion of the Portuguese financial system into African markets in general. Thus, financial flows from corruption in third countries, whether domestic or from international trade, may find ways for layering and integration in the Portuguese financial system and economy, in the opposite direction to funds from Portuguese corruption, which search internationalization, and use concealment mechanisms in distant or highly complex offshore centres. Though these flows do not necessarily qualify as organised crime, they are nevertheless estimated to be worth more than the proceeds from traditional forms of organised crime in terms of the economic repercussion visible at global level.

As an external border for Europe and a member of the European Union and euro area, and benefiting from the advantages offered by the free circulation of people and capital, with political stability, solid institutions and, despite the economic context, a competitive economic and financial environment, Portugal will not be immune to the threat of transnational criminal organisations. Besides these, the country has certain features likely to be exploited by these organisations, including:

- An agile, modern and dynamic financial system, built on high-tech platforms with multiple interfaces with their customers, in which, however, the pressure for pursuing objectives may result in the mechanisms of due diligence and compliance with obligations being overlooked;

- The prevalence of tourism in certain regions and the consequent high circulation of people and capital;
- The fact that the Madeira Free Trade Zone carries out its activity in compliance with EU, OECD and WTO rules, which paradoxically may make it appealing for the criminal organisations' strategy of diversifying investments and minimising risks;
- The reduction of bureaucracy and simplification of various processes (e.g. creation of new procedures: '*Empresa na Hora*', '*Sucursal na Hora*', '*Marca na Hora*', '*Associação na Hora*', '*Casa Pronta*');
- The legislative mechanisms in favour of competitiveness and economic entrepreneurialism, with the consequent reduction of context costs and administrative expenses for companies, facilitating the establishment of companies[1];
- Various investment incentive programmes;
- Linguistic compatibility with South America and European and tax attractiveness for Asian countries
- Greater vulnerability of the economic actors, created by the economic and financial context, to the entry of capital of illicit origin, due to their inability to obtain financing to sustain their activity.

Under the circumstances, Portugal is not exempt from the risk of featuring in the strategies of certain transnational criminal organisations, and some of the following situations have been detected:

- Direct criminal activities, although undertaken by minor organisations, as the Portuguese market is insignificant in relation to other European countries;
- Use of Portuguese territory as a transit country to the European market, sustained by logistical support networks for transporting and moving products
- Use of Portugal as a potential safe haven for individuals associated with organised crime, when security pressure in their countries of origin becomes more intense;
- Use of the Portuguese economic and financial space to layer and/or integrate illicit capital;
- Use of Portuguese territory as a platform, if not final, at least transitional (namely via informal remittance systems and intensive use of IT) for funds resulting from financial crimes (e.g. forged credit instrument fraud, social engineering type fraud or 'Ponzi'/pyramid schemes), which often appear to be related to South American and Asian criminal organisations.

Traditionally, certain organisations associated with specific nationalities show a clear preference for repatriating capital, putting the threat of layering on top, while others operate effective capital integration strategies.

[1] For example, the measures adopted by Decree-Law No 33/2011 of 7 March 2011, which lays down the simplification of the processes for establishing private limited companies and sole proprietorships, with the share capital being freely defined by the owners. It also lays down that the owners of these companies may pay in their capital up to the end of the first year of economic activity. Under the new legislation, it is possible to establish private limited companies with share capital of only EUR 1 per owner.

Criminal Types with Higher ML Risk

The identification of the threats herein made focused on the available statistical data on crime in general and on the cases in which, after the analysis carried out, the suspicions that originated the communication to the FIU and the DCIAP by the entities subject to obligations to prevent ML/FT were confirmed. In most cases, the determination of the predicate offence results from the police and judicial information collected from the interveners in the reported suspicious transactions. Also taken into account were the data on the potential ML predicate offences, registered by the Public Prosecution Service and also by the Criminal Investigation Police. All of these data, as well as those for each of the specific threats, relate to the years under review, i.e., 2012 and 2013.

The statistics show that in 2012, 82 cases were filed with the Public Prosecution Service, and in the same year, there were indictments in 7 cases and 8 cases were dismissed. In 2013, 97 cases were filed; there were 15 indictments, and 4 were dismissed. On the other hand, the same statistics show that in 2012, there were 19 convictions, there having been 36 in 2013.

Crimes against property (robbery, theft and misconduct) are the ones that have the highest number of criminal cases in the years considered. The percentage of this type of crime in the total number of confirmed suspicious transactions is not, however, all significant, accounting for only about 2% of these confirmations.

The number of investigations in the field of computer crime (computer fraud) was significant. As far as the communications analysis is concerned, about 6% of the suspected cases are related to this type of crime.

Drug trafficking, in turn, continues to be one of the main illicit activities developed by transnational and transcontinental criminal groups and organizations, taking advantage of the multiple advantages offered by social and economic globalization and modern communication technologies. Approximately 8% of the communications in which the suspicion was confirmed were validated as operations that could be related to this type of predicate offence.

As far as prevention is concerned, tax offenses constitute the most serious predicate offence when analyzing suspicious communications. Approximately 60% of the operations in which the suspicion was reported were related to these crimes.

In the analysis of suspicious communications made by the FIU, no situations related to the crime of smuggling, were detected. There are, however, within the scope of the DCIAP, some situations related to funds suspected of originating in this type of crime.

Regarding qualified scams, communications received in the context of ML's prevention disclose about 8% with relation to this predicate offence. With regard to funds originating in fraud, it is important to highlight the significant relevance of crimes committed abroad, whose revenues are circulated or sought to get grounding in Portugal. Also highlighted are the funds that originate in fraud committed through Internet platforms, such as pyramid-type schemes, or social engineering cases, in which there are offended persons either in Portugal or abroad. Attraction for accounts of these schemes with banks in the national territory has been noticed.

Corruption is, by definition, a typical predicate offence to money laundering. Concerning the analysis of communications in ML prevention, only 3% of the total confirmed operations are related to this crime. On the other hand, at the international level, two cases of blocking of funds from former foreign officials suspected of corruption were registered during 2013. Regarding the crime of embezzlement, in relation to the analysis of the suspicious communications of the years 2012 and 2013, there were no reports of ML relations with this predicate offence.

With regard to counterfeiting, no links with this crime have been detected in the communications of suspected transactions that were confirmed, although it may be admitted that some of these cases may be redirected to tax fraud.

Finally, other types of crime, which in the abstract can be considered as a threat in terms of ML, include aid to illegal immigration, trafficking in vehicles, crimes against people (homicide and illegal acts of sexual nature), trafficking in protected species, sports-related crime, trafficking in persons and insider dealing and market manipulation.

Higher risk ML methods

In addition to the types of operations communicated, the reasons for the communication and the sectors of origin of the operations, it is worth mentioning some of the more risky methods most frequently associated with the ML and which, in some cases, are also a serious obstacle to the collection of information:

- Cash operations, especially those carried out in payment institutions;
- Carousel of VAT in the field of tax fraud;
- Use of private accounts for money transfers;
- Use of electronic banking;
- Accounts opened by non-residents, especially in border areas;
- Open accounts on behalf of clients (Madeira free zone);
- Use of branches of credit institutions in offshore centers.

CROSS-BORDER MONEY LAUNDERING

In the context of foreign-origin ML, an important area relates to funds potentially arising from corruption in third countries. Investigation of these funds has been particularly difficult however. This results firstly from the absence of criminal investigation in certain countries where the crime is allegedly carried out. Secondly, there is an absence of interlocutors in many of those countries or the established structures tasked with investigation of corruption and ML prevention are dysfunctional. Thirdly, funds from various origins, legal and illegal, amalgamate under the same concealment structures and legitimation schemes (for example, investments destined for Portugal and Europe). Besides this, fraud crimes are also significant, including 'phishing', committed abroad with the goal of laundering the proceeds in Portugal.

Data from the FIU identify the countries where transnational transactions occur, through the confirmed STRs. For the most part, these are countries with which Portugal has important economic and financial relations and significant migratory flows. Of all the suspicious cases reported to the FIU which are subsequently confirmed, 45% are transnational.

FINANCING OF TERRORISM

Regarding the financing of terrorism, the highest consequence level relates to the Islamist threat in the matrix of traditional types of threats of this kind (anarchist, separatist, revolutionary and Islamist). It finds justification in identity, historical and political factors, including the Judeo-Christian and 'Western' identification, the historical connection to Al-Andalus and Portugal's membership of international organisations such as NATO and the EU. Furthermore, entities linked with states and organisations deemed priority targets for transnational Islamist terrorist organisations are established in Portuguese territory.

EMERGING CATEGORIES WITH HIGHER-RISK OF ML/FT

As well as the expected continuation of the high-risk trend from the tax fraud predicate offence, fraud in the form of the 'pyramid', 'bubble' or 'multi-level marketing' methods is also expected to increase. Tax fraud is expected to take the familiar form of the VAT carousel method, with an increasingly high number of fictitious operators expected to be introduced into the circuit of potential transactions made, on web platforms, and with increasingly sophisticated methods. A further trend to watch relates to the increase in online gambling and virtual casinos.

II. VULNERABILITIES

FINANCIAL SECTOR

The economic and financial climate of recent years has brought about a lack of liquidity in the financial system on various occasions. Therefore, given that a key ML method uses the financial sector, the current pressure on banking institutions in need of liquidity necessarily increases the risk of lax enforcement of identification requirements ascertaining the legality and legitimacy of funds invested by customers and investors.

Those institutions in a more fragile financial state are more vulnerable to investments by new shareholders who enable those institutions to overcome their difficult situations by injecting significant capital. The financial climate could therefore be attractive to criminal organisation for ML strategies, as they could also exercise a certain level of control over the financial institutions whose shares they buy. Secondly, the growing adaptability of criminal organisations to AML mechanisms, their sophistication and diversification of resources, strategies and *modi operandi* are factors which coincide to give an air of legitimacy to the financial flows they transact, easing their introduction into the national financial system, bearing no apparent relationship to their illicit origin.

Furthermore, a highly restrictive lending policy has increased the risk for economic actors, forcing them to find alternative financing models, possibly using less demanding criteria that are more vulnerable to the entry of illicit capital. All this, combined with the high levels of technology inherent to the Portuguese financial system, including significant internet usage, a sophisticated ATM network, online banking and widespread access to digital payment systems, increases the risk of the existing digital platform and cyberspace being used in logistical and operational support for illicit financial transactions, increasing possible vulnerabilities.

In general, the following were identified as the main vulnerabilities:
- The ownership of the capital;
- The need for financing;
- The internal organization of the obliged entities;
- Human resources;
- Technological resources;
- The kind of products marketed;
- Means of distribution;
- The clientele;
- The commercial pressure / sales incentives;
- The impact of international norms on national legislation, making the legislative process particularly complex and difficult;
- The limitations inherent to territorial jurisdiction, to deal with cross-border operations and Financial Institutions (FIs) with a global presence.

NON-FINANCIAL SECTOR

The non-financial sector is a very fragmented sector, where there is an extraordinary diversity of obliged entities. The vulnerabilities identified here reveal an enormous multiplicity, from the online game to the acquisition of high value goods, including real estate, in which the transaction is made, in whole or in part, in cash, to the ignorance of ultimate beneficiaries of collective entities, to the lack of requirement of organized accounting, and to the management of client accounts.

III. ANALYSIS

METHODOLOGY AND ANALYSIS MATRIX

Having identified the threats and vulnerabilities, the likelihood and consequence levels are now analysed, using a three-point scale: high, medium and low likelihood/consequence. The following definitions are used in this context:

LIKELIHOOD: the probability of the vulnerability materialising;

CONSEQUENCE: the impact of the vulnerability materialising.

Given the final evaluation of the risk arising from the combination between likelihood and consequence level, an analysis matrix was drawn up, also based on a three-point scale: low risk, medium risk and high risk.

ML/FT RISK ANALYSIS MATRIX

		CONSEQUENCE LEVEL		
		LOW	MEDIUM	HIGH
LIKELIHOOD LEVEL	LOW	LOW	LOW	MEDIUM
	MEDIUM	LOW	MEDIUM	HIGH
	HIGH	MEDIUM	HIGH	HIGH

Thus, low, medium and high risk are defined as follows:

LOW RISK
Risk level with a low or medium likelihood of materialising and which may cause limited or very limited damage. As a rule, it does not require any action or only requires action to reduce the likelihood and/or consequence of it materialising.

MEDIUM RISK
Risk level with a variable likelihood of materialising and which may cause damage also of a variable size. Requires action as early as possible to reduce the likelihood and/or consequence of it materialising, as well as a suitable contingency plan for its mitigation should it materialise.

HIGH RISK
Risk level with a significant likelihood of materialising and which may cause damage also of a significant size. Requires immediate and prioritised action to prevent and mitigate the risk suitably

THREATS

Crime types with highest ML risk

In sum, given the analysis undertaken and the information arising from confirmed STRs, including that based on the police records of those mentioned, the following table presents the risk analysis for ML threats:

Predicate offence	Inquires 2012-2013		STRs confirmed 2012-2013 (Total 958)	Likelihood	Consequence	Risk
Tax offences	Fraud	1859	60%	**High**	**High**	**High**
	Tax evasion	310				
	Smuggling	74				
Drug trafficking		12380	8%	**High**	**High**	**High**
Fraudulent crimes (fraud)		2148	8%	**High**	**High**	**High**
Corruption and Misappropriation of money or property by public officers	Corruption	889	3%	**Medium**	**High**	**High**
	Misappropriation of money or property by public officers)	674				
Counterfeiting*		916	0%	**Medium**	**High**	**High**
Trafficking in human beings		67	0%	**Medium**	**Medium**	**Medium**
Cybercrime (fraud)		12548	6%	**Medium**	**Medium**	**Medium**
Insider trading and market manipulation		35	0%	**Low**	**High**	**Medium**
Facilitation of Illegal Immigration		128	0%	**Low**	**Medium**	**Low**
Motor vehicle trafficking and dismantling		273	0%	**Medium**	**Low**	**Low**
Homicides and– crimes of sexual nature	Homicides	876	0%	**Medium**	**Low**	**Low**
	Sexual exploitation	87				
	Sexual exploitation of children	451				
Trafficking in protected species		3	0%	**Low**	**Low**	**Low**
Sport related crime		-	0%	**Low**	**Medium**	**Low**
Crimes against property	Robbery	33022	2%	**Low**	**Low**	**Low**

	Aggravated theft	63826				
	Embezzlement	9746				

* Data from ASAE

Financing of Terrorism

Regarding terrorism in the Islamist matrix, the conclusion is that although it has been pointed out the passing through or the presence of individuals that sympathise with extremist organisations in Portugal, as well as the connection of certain members of the Portuguese Islamic communities to radical proselytising activities, the terrorist threat in the Islamist matrix identified above may not present a high risk for Portugal in the short term. This may result from other contrasting factors, namely the small scale of the Portuguese Muslim community, the moderate alignment of the Portuguese religious leaders, and the fact that neither terrorist cells nor individuals trained in jihadi contexts operating in Portugal have been detected to date. This does not mean however that Portugal is immune to possible operational developments, be they attacks from abroad, or attacks on foreign targets in Portuguese territory. Taking all the available data together however, the potential risk of financing of terrorism that Portugal faces in regard to terrorism from the Islamist matrix is assessed as medium.

In terms of separatist and nationalist terrorism, the data suggests that, aside from the fall in activities related to this in Portugal, the risk of financing of terrorism is low.

IV. VULNERABILITIES

Financial Sector

Regarding the banking sector, the assessment model of the ML/FT risks arising from the provision of financial services subject to Banco de Portugal supervision corresponds to a potential risk, i.e. the *intrinsic risk* inherent to the financial institutions' activity arising from the combination between likelihood and consequence, irrespective of the robustness of the respective prevention/mitigation systems. The analysis in the banking sector concluded that in relation to the institutional groups *Banking Institutions*[2], *Investment Firms*[3] and *Other Financial Institutions*[4] the global intrinsic risk is high, while for *Special Credit Institutions*[5] the global intrinsic risk is medium.

Regarding the provision of financial services subject to the supervision of the CMVM, the ML/FT risk assessment model showed that the risk is low in the Financial Institutions that provide Investment Services, and in the Collective Investment Schemes and Other Assets Management Companies.

Also with regard to the insurance and pension funds sectors, subject to ASF supervision, it was possible to conclude that the risk is low.

Non-financial sector

In the non-financial sector, the ML / FT risk assessment model, taking into account the vulnerabilities identified in the activity, allowed us to conclude that the risks are high in the real estate, notary and registry, and merchants of high value goods sectors, medium in the casinos, independent professionals (ROC, TOC, Lawyers and *Solicitadores*) and low in the betting and lotteries sector.

Other Vulnerabilities

On the other hand, in relation to other identified vulnerabilities, the model leads to the conclusion that there are high risks in the use of illicit capital in strategic sectors, the use of illicit capital in the Investment Incentive Programmes, in relationships with offshore centres and free zones, in the physical transportation of cash and in the circulation of information within financial groups; medium risks in the use of *gatekeepers*, non-profit organizations and direct public debt of the State - retail and low risk in virtual currencies.

---

[2] Including Banks, Savings Banks, Mutual Agricultural Central Credit Bank, Mutual Agricultural Credit Banks.
[3] Including Credit Financial Institutions, Financial Leasing Companies and Factoring Companies.
[4] Including Payment Institutions, Electronic Money Institutions, Bureaux de Change and Other Financial Services Providers.
[5] Including Brokers, Broker-Dealers and Asset Management Companies.

Terrorism Financing

Vulnerabilities have been detected within financing of terrorism that for the most part may also be exploited by non-terrorist criminal actors, namely the following:

- Absence of border controls within the Schengen area;
- Significant difficulty in identifying suspicious transfers in low amounts, given the huge number of these kinds of transfers made each day and the lack of alert mechanisms regarding this type of transfer;
- Ease in disguising transfers with terrorist goals in allegedly legitimate transactions with the scope of international trade or migrants' remittances;
- Difficulty in distinguishing between 'common' criminal activities and terrorism financing activities.

However, these kinds of vulnerabilities cannot be eliminated, and must be considered a constraint on a general AML/CFT strategy.

V - ASSESSMENT

For 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 a similarly global response will be effective, based on strong domestic and international cooperation mechanisms and the exchange of information at all levels between the various prevention, supervision, oversight and repression bodies.

The research and analyses undertaken for this NRA on ML/FT offer conclusions not only in regard to the most important threats hanging over the AML/CFT system in force, but also on the most critical vulnerabilities and greatest risks that Portugal faces in this area.

Threats

From an AML viewpoint, there is one clearly prevalent threat, although there are others that should not be ignored. Indeed, ML's most common predicate offences are tax offences, including tax fraud, tax evasion and smuggling. While it is clear that sometimes, prosecution and punishment for tax offences may 'hide' some other predicate offences, since it may be easier to prove their existence, the fact is that the percentage of confirmed STRs relating to tax offences is overwhelming: 60%. This justifies particular focus on this type of criminality, 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 to market or smuggling, in the simple form.

Aside from tax offences, high risk threats include drug trafficking, fraud, corruption and Misappropriation of money or property by public officers, and counterfeiting. Of these, in 1993, drug trafficking was the first to be deemed predicate to ML. Fraud and corruption and misappropriation of money or property by public officers have been ML predicate offences for a long time, thus becoming a focus for AML. Only counterfeiting is still not considered a predicate offence for ML, as it is not necessarily 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 recognised in this NRA, this situation should be corrected.

Medium-risk but non-negligible threats include cybercrime (fraud), trafficking in human beings, and insider trading and market manipulation. Cybercrime has recently increased significantly. Swift access to information held by entities responsible for storing IT data, international cooperation and appropriate training for those responsible for applying the law are the main control mechanisms, key for improving detection and investigation of these kinds of

crime. In relation to trafficking in human beings, although the data from STRs whose suspicion was confirmed do not suggest that this crime is relevant for the purposes of ML, other analytical elements, including the perception of the criminal investigation authorities, suggest that it is important. Similarly absent in the period under review are the crimes of insider trading and market manipulation, also suggesting low importance for ML purposes. However, the authorities' perception, upheld by more recent data, is that the threat carries a medium risk.

Finally, although the threat of financing of terrorism, and the more recent phenomenon of foreign terrorist fighters, cannot be considered high, it should not be underestimated. So with specific regard to financing of terrorism prevention and combat, aside from preventive action under the widely released UN lists and the restrictive measures of the EU, cooperation between domestic public and private entities should be encouraged, along with international organisations with this type of concern. In the context of this cooperation, prospective information has been produced and working groups have been set up for the adoption of counter-measures to the terrorist phenomenon, helping define best practice and running training sessions, both domestically and internationally. The key international initiatives needed, aside from bilateral collaboration and cooperation for preventive detection of the phenomenon and the effective exchange of information liable to detect, control and neutralise the transnational terrorist threat, include multilateral cooperation in the form of continued active participation in the events and conferences held by the Community of Portuguese-Speaking Countries (CPLP), the EU and NATO.

Vulnerabilities

This NRA has also identified various vulnerabilities, enabling a risk assessment. Thus, the analysis allows to identify key vulnerabilities related to the anonymity of transactions. Indeed, besides facilitating the parallel economy, anonymity makes it impossible to trace the funds, such that any illicit origin or use for criminal purposes goes undiscovered.

Therefore, the acceptability of the use of cash in very high amounts, both to make payments and for physical movement of value, is a clear vulnerability in AML/CFT. These kinds of situations suggest that, as is the case in other countries, an additional limitation on the possibility of using cash above a specific amount should be considered, when making any payments for goods or services, as well as for paying tax debts.

Another important aspect of the vulnerabilities caused by anonymity relate to the physical transportation of cash. The 'money courier' gains particular importance here, as the legislation in force makes no specific provision for a duty to identify the origin of the funds with which the carrier travels on public highways.

The widespread use of cash, aside from allowing the unregistered economy to develop, also allows another vulnerability to develop, related to informal payment systems. Replacing official mechanisms with informal systems, which has recently intensified due to international de-risking, means that the transactions are no longer made in a regulated space but move to 'grey' areas of anonymity and lack of controls, which should be avoided as far as is possible.

Similarly related to anonymity and the difficulty in tracing funds is the relationship with offshore centres, jurisdictions which usually have less stringent regulation and control, where bank secrecy rules usually prevail.

Somehow related with the vulnerabilities linked to anonymity is the ignorance of the beneficial owner, both of collective entities and of specific transactions. Indeed, the qualitative evolution of organised crime structures' strategy towards adopting an economic profile – with increasing use of complex corporate networks, with onshore and offshore ramifications, used to camouflage the links between the capital flows, their owners and their origin – has brought an air of legitimacy and credibility to their activities. One of the patterns detected in Portuguese territory in certain investments of illicit origin consists of the use of intricate networks of companies, normally with connections to other countries, namely offshore centres. These corporate networks and their owners (in certain cases, politically exposed persons (PEPs) or their spokespersons) are then used to conduct multiple trades, formally legitimate in appearance, but which in reality are ML transactions. Knowing who effectively is the beneficial owner of collective entities or transactions is key for a successful AML/CFT policy. This was recognised in the FATF Recommendations and, more recently, in the aforementioned Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015. The requirement to identify the beneficial owner and to register the beneficiaries is therefore essential, not only for compliance with the Recommendations but also the Directive itself.

Also among the vulnerabilities linked to anonymity are bearer securities, such as bearer shares. These instruments raise serious problems in regard to the identification of beneficial owners and the opaqueness that results from the 'invisibility' of their transfer. The definitive solution for the problem would be to ban bearer shares, converting current ones into another type of share. Other, less effective, solutions could involve limits on circulation, such as compulsoriness of inventory (at company level or in the record office), allied with a limit on transferability (e.g. need for a notary's participation for the deed to be valid).

Another important vulnerability, not the direct result of anonymity, but linked to it, is the consequence of the lack of information, including in the real estate sector and in the creation of collective entities.

Other vulnerabilities identified relate to lack of resources, to a certain ignorance of the law and/or a failure to consider its risks, as well as the misuse of specialists (gatekeepers) for ML/FT purposes.

Finally, still in the vulnerabilities side, attention must be paid to the existence of a non-profit organisations (NPO) sector. NPOs are not subject to AML/CFT obligations, even though their possible misuse for ML and above all FT is a recognised risk factor. In this field, strengthening and developing certain rules for associations, foundations and cooperatives on the compulsoriness of identifying donors and beneficiaries, as well as the filing of documents, allied to measures for ensuring the suitability of the managers and the creation of a duty of cooperation with the AML/CFT authorities, could contribute to an increased awareness of the risks in the sector and their reduction. It would also be advantageous to draw up Guidelines to allow this sector to defend itself from possible misuse.

Risk Analysis

This assessment also offers conclusions over the highest ML/FT risks facing Portugal, by sector and geography.

The highest-risk sectors include the banking sector, the heart of the financial system in most countries. Being the sector with the largest size and greatest operational complexity, it is not surprising that it is one of the preferred ways for criminals 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 affect the real estate sector and high value goods dealers.

In the real estate sector, the transactions offer considerable ML opportunities, not only because the values involved are normally high, but also because it is relatively easy to complete quick transactions and transfer property and because companies based in jurisdictions or territories with low levels of cooperation and information exchange may be used.

Besides this, a privileged geographical location with areas of strong tourism development makes Portugal an appealing place for investments in real estate, tourism and restaurants, among others. These investments ensure legitimacy and financial stability, which may be extremely useful for criminal organisations, as they successfully legitimise significant capital flows under cover of apparently legal corporate structures. These sectors offer twice the ML opportunities, firstly as a channel for significant sums in the construction and development phases, and secondly in exploiting capital-intensive activities, in which large cash sums are used, e.g. hotels and restaurants. Certain regions are particularly attractive and conducive to investments in these sectors, such as coastal areas with strong tourism and a high flow of non-residents.

In the current economic context, of scarce liquidity, financing and investment, there is a major vulnerability to the injection of funds of potentially illicit origin, which, in the medium term constitutes a significant threat to the Portuguese economy, not only due to the inherent illegality of the capital's origin, but also due to the market distortions (competitiveness and unfair competition) it causes and the pressure mechanisms it may entail.

Therefore, as real estate entities are family-owned or are small to medium in size, they may lead to a lack of control over compliance with general and specific duties imposed on them by Law No 25/2008.

The high value dealers sector is also an area with high ML/FT risks. This is not only due to the easiness of using cash in transactions, but also due to the high number of operators trading those goods and their huge geographical spread.

Priorities

As AML/CFT is a priority and measures deepening the various control and transparency mechanisms continue to be adopted, it is important to assure that the economic space has a preventive action strategy, capable of restricting the use of the various activity sectors for ML/FT purposes, making them less appealing to the actions of organised crime structures. This presupposes the continued exchange of information, to provide a more effective response, based on the prevention and early detection of any suspicious transactions, in order to reduce the risks found.

Furthermore, the threats and vulnerabilities identified and their inherent risk levels allow certain priority measures to be defined. Some of these relate to the coordination of the AML/CFT strategy and policies. Others relate to the key legislative changes and measures regarding the sectors with the highest risk – banking, real estate and high value dealers.

VI – MEASURES TO BE TAKEN – PRIORITIES[6]

COORDINATION

Since Portugal joined the FATF, **AML/CFT policy** has been coordinated by the Portuguese Delegation, which includes the relevant ministries and financial supervisors, as well as the Prosecutor-General's Office (PGR) for a long period. However, regardless of the requirements in the revised FATF Recommendations and Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015, the existing system is no longer fit for purpose. Thus an initial measure to be taken is the immediate establishment, at a suitable political level – Resolution of the Council of Ministers – of a mechanism to coordinate AML/CFT policy, in Portugal, to better mobilise and use resources, working towards an effective reduction in ML/FT risks. Without prejudice to subsequent reconsideration of the choice between mechanism and authority, as provided for in the Directive, this mechanism could at this stage include, a **Coordination Commission**, created within the scope of the Ministry of Finance, chaired by (at least) a Deputy Minister and including, at senior management level (Director-General, Deputy Director-General, Chairman, Deputy Chairman or member of the managing body), not only the entities represented in the Working Group created by Decision No. 9125/2013, but also the Security Intelligence Service (SIS) and the Ministry of Internal Administration. The Commission should have a more restricted executive committee, entrusted with accompanying its day-to-day work, and a small, permanent, technical team dedicated exclusively to the tasks it must undertake. The necessary logistical support may be provided by the supervisory authorities which comprise the National Council of Financial Supervisors (CNSF), without prejudice to the possibility of human resources from other entities being also allocated.

GENERAL LEGISLATIVE CHANGES[7]

1. When defining the crime of money laundering, **Article 368-A** of the Criminal Code uses two criteria to classify the predicate offences: the crime type criterion and applicable penalty criterion ('deprivation of liberty for a minimum of more than six months or for a maximum of more than six year'). Historical reasons explain this, associated with the fact that initially the crime of ML appeared only as a result of drug trafficking as predicate, and subsequently, European directives introduced sentence limits in its definition. However, this solution is unjustified today. On the one hand, this is because the broadening of the range of predicate offences to include fiscal crimes, under the FATF Recommendations, excludes certain predicate offences, for example

[6] These measures to be taken should be combined with the proposals presented by the Working Group created by Decision No 490/2014, of the Minister of State and of Finance and the Minister of State and Foreign Affairs. The Group assesses the implications of the restrictive measures in the domestic legal system and create legislative proposals to reinforce, in terms of criminal and administrative penalties, the existing legal framework relating to the infringement of the restrictive measures as defined by European Union Regulations and resolutions of the United Nations Security Council.

[7] The proposals made and which affect the AML/CFT system in its entirety must be integrated with the transposition measures of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 as well as the specific measures in the sectorial matrices.

customs offences, such as fraudulent introduction to market or smuggling, are not included. On the other hand, Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 reduced the limits of the sentences for ML predicate crimes, considering criminal activity for purposes of ML to be "all offences, including tax crimes […], which are punishable by deprivation of liberty or a detention order for a maximum of more than one year or […] all offences punishable by deprivation of liberty or a detention order for a minimum of more than six months." Therefore, taking advantage of the wording in the aforementioned Directive, **the definition of the ML predicate offences in Article 368-A of the Criminal Code should be changed to use only a penalty criterion** ('deprivation of liberty for a minimum of more than six months or for a maximum of more than one year'), rather than using both criteria currently in force to qualify these crimes: catalogue criterion and penalty criterion.

2 – A systematically identified vulnerability relates to the very frequent **use of cash**. Indeed, cash, with the anonymity it has, is an excellent facilitator of ML/FT transactions. Therefore, some jurisdictions, namely European ones, have introduced legislation to restrict its circulation and thus that is also a reason to review the Portuguese legislation.

3 – The existence of **bearer securities**, shares, warrants, redemption operations to the bearer, etc., as with the intensive use of cash, is an important vulnerability in terms of ML/FT. The revision of this legislation should also be one priority.

4 – The lack of information on the beneficial owner of legal persons, especially those not subject to commercial registry is a high-risk ML/FT vulnerability. It is therefore necessary to take measures to reduce this risk, as reflected in the FATF Recommendations and EU Directive.

5 – Finally, one reference to possible legislative measures for **non-profit organisations.** These are not, nor should they be, entities subject to ML/FT prevention requirements, although their possible misuse for ML and especially FT purposes is a recognised risk factor. Therefore, reinforcing the rules for associations, foundations and cooperatives would contribute to a reduction in risks.

FINAL NOTE

This ML/FT National Risk Assessment is the first exercise of its kind carried out in Portugal. The conclusion of this NRA, which took almost two years, required the 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 show room for improvement, reveal the present threats and vulnerabilities, as well as the risks the country faces in combating ML/FT. However, an exercise of this type is not definitive. It requires updating to match the responses to the threats which may arise and the risks which may worsen, redefining courses of action and priorities. In these circumstances, the NRA requires periodic review, looking appropriate, unless exceptional circumstances arise, that it will begin in 2018, following the fourth FATF evaluation of the Portuguese AML/CFT system, which will occur, predictably, between October 2016 and October 2017.