COMMITTEE OF EXPERTS ON THE EVALUATION
OF ANTI-MONEY LAUNDERING MEASURES AND
THE FINANCING OF TERRORISM (MONEYVAL)

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

MONEYVAL(2019)27

# Anti-money laundering and counter-terrorist financing measures

# Cyprus

## Fifth Round Mutual Evaluation Report

December 2019

**The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism - MONEYVAL** is a permanent monitoring body of the Council of Europe entrusted with the task of assessing compliance with the principal international standards to counter money laundering and the financing of terrorism and the effectiveness of their implementation, as well as with the task of making recommendations to national authorities in respect of necessary improvements to their systems. Through a dynamic process of mutual evaluations, peer review and regular follow-up of its reports, MONEYVAL aims to improve the capacities of national authorities to fight money laundering and the financing of terrorism more effectively.

The fifth-round mutual evaluation report on Cyprus was adopted by the MONEYVAL Committee at its 59th Plenary Session (Strasbourg, 2-6 December 2019).

## CONTENTS

## EXECUTIVE SUMMARY

1. This report summarises the AML/CFT measures in place in Cyprus as at the date of the on-site visit from 13 to 24 May 2019. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Cyprus's AML/CFT system and provides recommendations on how the system could be strengthened.

### *Key Findings*

There are some elements in the Cypriot AML/CFT regime which are functioning adequately:

1. Cyprus understands the money laundering/terrorist financing risks that it faces to a large extent, albeit understanding of terrorist financing risk is less comprehensive. A number of measures have been deployed to mitigate some of the main risks effectively.

2. There is a good level of domestic co-operation and co-ordination between the competent authorities both on policy issues and at an operational level.

3. The banking sector has become more effective in mitigating risks. This is largely due to the increasingly sound supervisory practices of the Central Bank of Cyprus.

4. The financial intelligence unit has the ability to support the operational needs of competent authorities through its analysis and dissemination functions.

5. Cyprus has developed mechanisms which are capable of delivering constructive and timely assistance to other countries both on a formal and informal basis.

However, there are various major shortcomings which hinder the effectiveness of the Cypriot AML/CFT regime:

1. The competent authorities are not yet sufficiently pursuing money laundering from criminal proceeds generated outside of Cyprus, which pose the highest threat to the Cypriot financial system.

2. The competent authorities have not been very proactive at freezing and confiscating foreign criminal proceeds at their own initiative, although they have been instrumental in assisting other countries.

3. Cyprus has not conducted a formal assessment of risks posed by legal persons, despite having a developed company formation and administration business. This has reduced the authorities' ability to implement more targeted mitigating measures to ensure the transparency of legal persons.

4. There are weaknesses in the implementation of preventive measures by the trust and corporate services sector as a whole. This has major implications for the availability of beneficial ownership information of legal persons/arrangements registered in Cyprus and the reporting of suspicions transaction reports.

5. While significant strides have been made by Cyprus to implement a comprehensive supervisory framework for trust and corporate services providers, further progress is required, with certain areas requiring major improvement.

6. The risk in the real estate sector has increased exponentially since it has become the

preferred choice of investment vehicle to acquire citizenship under the Cyprus Investment Programme. These risks have not been properly been mitigated – the implementation of preventive measures by, and the supervisory framework of, the sector display significant weaknesses.

7. The risks related to the Cyprus Investment Programme have not been assessed comprehensively.

8. Administrative service providers did not demonstrate a uniform level of understanding of the risks of TFS evasion. Given Cyprus's status as an international financial centre and the role played by administrative service providers as gatekeepers, the fact that some service providers may not always be in a position to identify individuals or entities who may seek to conceal their identity behind complex structures to evade sanctions constitutes a significant vulnerability.

The application of a risk-based approach to the non-profit sector was still at a nascent stage at the time of the on-site visit.

## Risks and General Situation

2. As an international financial centre (IFC), Cyprus is primarily exposed to external money laundering (ML) threats as non-residents may seek to transfer criminal proceeds to or through Cyprus, particularly through the Cypriot banking system or may seek to use trust and company service providers, known in Cyprus as administrative service providers (ASPs), to facilitate their aims. The Cyprus Investment Programme (CIP) is inherently vulnerable to abuse for ML purposes, as is real estate, both in general and as the apparent preferred investment to acquire citizenship. Although the terrorism threat is considered to be low in Cyprus, the authorities rate terrorist financing (TF) risk as medium due to the fact that the country is an IFC and its proximity to conflict areas.

## Overall Level of Compliance and Effectiveness

### *Assessment of risk, coordination and policy setting (Chapter 2; IO.1, R.1, 2, 33 & 34)*

3. There is good understanding of ML risks at the national and sectorial level; in some aspects, particularly where the Central Bank of Cyprus (CBC) is involved, understanding is very good. FT risk is understood to a good standard. Understanding of both ML and FT is greater than that represented in the NRA. Overall, understanding is partly reduced by a range of factors, including the historic nature of the statistics used, and areas where assessment coverage is not fully developed or up to date (including, for example, the Cyprus Investment Programme (CIP), the real estate sector, legal persons and arrangements and NPOs). There is scope for more in-depth assessment, including deeper interrogation of information in relation to FT more generally.

4. A national strategy for AML/CFT and an associated action plan have been recently introduced. The strategy and action plan flow from the NRA findings and are in line with understanding of risk. There have been a series of national initiatives which specifically address the risks faced by Cyprus - for example, the issue of binding directives in relation to shell companies, increased standards for introduced business, and requirements for banks to meet customers who have been introduced and beneficial owners (BOs) of legal persons which are customers.

5. The Advisory Authority is a long-standing body which is the main coordination mechanism for AML/CFT. The role of the FIU at the heart of the AML/CFT system has been a significant positive influence for the development of the system. There is a good level of co-operation and co-ordination between the competent authorities both on policy issues through the Advisory

Authority and at an operational level between the various competent authorities.

### *Financial intelligence, ML investigations, prosecutions and confiscation (Chapter 3; IO.6, 7, 8; R.1, 3, 4, 29–32)*

6. The Police have frequently accessed and made effective use of financial and other information to further their investigations into domestic, and some foreign, ML, associated predicate offences, and FT. Until 2018, the Police did not make extensive use of intelligence generated by the financial intelligence unit (FIU) as expertise was not significantly developed. Conscious of this shortcoming, measures were implemented by the Police, and, as a result, the use of FIU intelligence saw a healthy increase in 2018. However, very few of the investigations initiated on the basis of FIU intelligence relate to stand-alone and third-party ML related to foreign predicate criminality. This is not in line with the risk profile of the country as an IFC.

7. Many suspicious transactions reports[1] (STRs) submitted by banks contain relevant and accurate information and are in line with the risks that Cyprus faces. A good portion have resulted in either an investigation domestically or served as a catalyst for the FIU to disseminate spontaneous information to foreign FIUs. Since most of the cases reported by banks involve legal persons/arrangements which are generally administered by ASPs, it is surprising that the reporting level of ASPs is not higher. It is of concern that, while banks have been able to identify suspicious activity on the basis of their ongoing monitoring procedures, ASPs have failed to do so in relation to clients common to both types of reporting entity. This would also suggest that, where legal persons/arrangements administered by an ASP do not have a bank account in Cyprus, the likelihood of a suspicious client or activity being identified in Cyprus is lower. The low level of reporting by the real estate sector also raises concern given the risks it faces.

8. The FIU has the ability to conduct multi-layered analysis of sophisticated ML cases involving the use of complex corporate structures spread over different jurisdictions, multiple bank accounts and extended ML networks. As a matter of good practice, the FIU spontaneously disseminates complete analysis packages to foreign FIUs that have proved to be critical in securing a conviction/confiscation abroad. The significant increase in STRs has put a strain on the limited human resources of the FIU and may have, to a certain degree, had an impact on the analysis and dissemination function.

9. The authorities appear to have adequate resources in place for ML investigations, but some units of the police are more resourced and more experienced than others for investigating ML, particularly when it is more complex. There is some uncertainty regarding when ML/financial investigations are triggered and on what basis they are taken over by the specialised Economic Crime Investigation Office of the Crime Combating Department. There are not any particular issues in legislation or procedurally, known to the assessors, which unduly hinder/delay investigations or prosecutions.

10. Cyprus has a reasonable record as regards pursuing ML in relation to domestic criminality, (albeit the overall numbers might arguably be said to be on the modest side if compared to the number of convictions for high-risk predicate offences). The number of prosecutions and convictions foreign proceeds generated ML is low, but the number of investigations is on the increase. Cyprus is aware that the low number of law enforcement activity regarding foreign proceeds does not correspond to its risk profile as an IFC and has taken positive steps to ameliorate this issue, for example by increasing targeted resources. Amendments have also been made to legislation to address an issue with the judiciary requiring the identification and proving of the predicate offence, but the same has yet to be tested before the courts. Whilst sentences for ML have often been subsumed into the higher sentence for a predicate offence (served concurrently), the

[1] STRs in this report refer to both suspicious transaction reports and suspicious activity reports. The Cypriot FIU receives both types of reports. The distinction between the two is not made in the law but in FIU Guidance.

jurisdiction has encouraging examples of where the sentence for ML has been higher.

11. In the review period, Cyprus has frozen EUR 115 Million and confiscated some EUR 13 Million in total, including the enforcement of foreign confiscation orders. This overall figure is encouraging but there is still a lack of activity in domestically initiated freezing and confiscation of foreign proceeds. However, in some instances the Cypriot Authorities on their own initiative have informed foreign counterparts of the existence of proceeds/equivalent property and have provisionally frozen such property pending the receipt and execution of an MLA Request. Cyprus is developing and improving its approach to financial investigations, yet these are still not being done a systematic basis. Nonetheless, the scope of the financial investigations when they are carried out is wide and the LEAs have access to a wide range of sources to aid and enhance such investigations. There is strong co-operation between the relevant authorities and the FIU in particular plays an important role in applying for freezing order and when necessary utilising postponement of transaction powers.

12. The customs authorities are very conscious of risks associated with the jurisdiction's frontiers. The authorities apply effective measures by monitoring movements including potential smurfing, by referring matters to the FIU where there are ML/TF suspicions, and by compounding offences to confiscate the amounts when the context of the case allows for it. However, there are concerns over the level of penalties imposed in some cases and the authorities acknowledge the maximum penalty for failure to declare/disclose cash above the statutory limit is a deficiency. The authorities apply strong procedures to target and search passengers, their luggage, mail and cargo (notwithstanding there is no declaration/disclosure requirement for mail/cargo) and have achieved some good results although there appears to have been a greater focus on money leaving the jurisdiction.

### *Terrorist and proliferation financing (Chapter 4; IO.9, 10, 11; R. 1, 4, 5–8, 30, 31 & 39)*

13. There have been some terrorism convictions with financial elements to them, and in addition there have been TF investigations, some of which are ongoing. There have, as yet, been no TF prosecutions/convictions. The jurisdiction does not have a considerable TF threat originating from domestic terror but, as an IFC, it is conscious of the risks associated with its international business. The jurisdiction is certainly not complacent and has a strong counter-terrorism infrastructure, in particular the Fusion Centre (an inter-governmental body) which meets and assesses threats associated with terrorism including TF. The jurisdiction has taken steps to increase training awareness of TF risks within both the public and the private sector and to target resources at seeking to harvest more TF investigations from incoming MLA.

14. Cyprus implements TF-related targeted financial sanctions (TFS) without delay through a combination of supranational (at EU level) and national mechanisms. Cyprus has not identified any targets for designation or proposed any designations to the 1267/1989 Committee or the 1988 Committee. It has never put forward a designation on its own motion, nor received a request from another country to give effect to freezing measures pursuant to UNSCR 1373. For both regimes, Cyprus relies entirely on the EU supranational framework. However, an informal mechanism exists within the Cyprus government to develop materials capable of supporting proposals for the designation of specific targets of financial sanctions for terrorism-related activities through the EU autonomous sanctions regime.

15. The supervisors have effective channels to communicate new designations to obliged entities. They also communicate the seriousness of compliance with TFS through regulations, notifications, and examinations. Compliance with relevant requirements is verified during on-site inspections, with the exception of examinations by supervisory authorities of real estate agents and the casino. In general, checks on compliance with TFS form part of full scope AML/CFT audits. While the CBC has devised a detailed on-site checklist, other supervisory authorities' manuals are less developed.

16. No funds or other assets have been frozen in Cyprus to date under TF-related TFS. However, in general, all obliged entities are aware of TF-related TFS screening obligations and the requirements to freeze funds/assets and have systems in place that allow them to implement TFS. There are

elements which are indicative of a functioning system e.g. identification of partial matches, matches with non-TF related sanctions regimes. Obliged entities screen customers against sanction lists. However, the frequency and depth of screening varies widely: from real time screening of customers, incl. customer-related persons such BOs, all the shareholders in entire ownership chain and transaction counterparties, to screening checks of customers and BOs conducted on a periodic basis.

17. Banks articulated a sophisticated understanding of the sanctions evasion risk, expressing concerns about complex structures of legal persons and about activity on behalf of designated persons by associates of their customers. Consistent with this risk understanding, banks appear to apply adequate measures to mitigate sanctions evasion risk. Given the materiality of the banking sector, these findings would suggest that Cyprus is taking measures in line with the risks it faces. Other obliged entities, especially ASPs, did not demonstrate the same level of understanding of the risks of TFS evasion as banks. The fact that some obliged entities may not always be in a position to identify individuals or entities who may seek to conceal their identity behind complex structures to evade sanctions constitutes a significant vulnerability in Cyprus given its status as an IFC and the role played by ASPs as gatekeepers.

18. At the time of the on-site, Cyprus started conducting a review of the NPO sector and, as such, has been in the process of identifying the subset of organisations which by virtue of their activities or characteristics are likely to be at risk of TF abuse. None of the measures taken so far by Cyprus have been based on an in-depth understanding of the risk of TF faced by NPOs in Cyprus and no aspect of the oversight mechanism relates to ensuring that they are not abused for the purposes of TF. A positive aspect of the system is the online Register of NPOs, and a comprehensive legal framework enacted in 2017. Authorities are in the process of building a comprehensive database on NPOs that shall be used for the future assessment of the NPO sector and implementation of a more in-depth risk-based approach.

19. Implementation and communication of TFS related to proliferation financing (PF) follow similar processes as with TF-related TFS. No funds or other assets have been frozen in Cyprus to date under PF-related TFS. There are domestic processes in place to issue export licences for dual-use goods and military equipment and exercise controls on the exportation of sensitive goods.

20. As with TF-related TFS, obliged entities are generally aware of the need to have protocols in place to freeze any assets without delay as part of the implementation of PF-related TFS. However, most obliged entities that were asked, including sophisticated banks, had difficulty in articulating differences between TF and PF, in terms of geographic risks, transaction typologies, or other types of distinctions. In the absence of a manifest geographical link, obliged entities might be less effective at identifying and taking action with respect to PF transactions and proliferator clients. Limited initiatives to raise awareness of obliged entities in relation to PF issues have been taken by supervisory authorities. The supervisory measures for monitoring compliance with PF-related TFS are similar to TF-related ones. The on-site methodologies developed by the supervisory authorities do not specifically distinguish between PF-related TFS and other TFS regimes. Apart from the CBC, the competent authorities do not appear to be prepared to monitor PF-related TFS requirements as such.

### *Preventive measures (Chapter 5; IO.4; R.9–23)*

21. Obliged entities' understanding of risk is somewhat uneven. Banks have a generally sophisticated understanding of both the ML and TF risks they face. Larger banks in particular can articulate their own sectoral and institutional risks and appropriately identify the different ML/TF risks of different types of products, lines of business, and types and identities of customers (including customers brought to banks by professional introducers). Non-bank financial institutions (FIs) all have an understanding of ML risk comparable to that of the banks. They demonstrated a general understanding of TF risk but are less consistently able to articulate how their business can be misused for TF purposes. The majority indicate that more guidance is needed. Among designated non-financial businesses and professions (DNFBPs), the larger ASPs, which have

significant international risk exposure, have a sophisticated understanding of risk. Smaller ASPs, real estate agents, and the casino are less sophisticated in their assessments and less articulate in their ability to describe their ML/TF challenges.

22. Obliged entities' understanding of their AML/CFT legal obligations is also uneven. Among financial institutions, particularly banks, understanding of AML/CFT legal obligations is very high, and in addition banks are aware of international best practices and prudential considerations that go beyond legal obligations. Among non-bank FIs and DNFBPs, awareness of AML/CFT obligations appears to be a function of size and international exposure. Most of the larger institutions and those with foreign clients, such as ASPs, have a detailed, sophisticated understanding of their legal obligations. The casino operator understands its own legal obligations and has limited direct interaction with most other obliged entities. Real estate agents know that they have legal obligations but are not always clear about what those obligations are.

23. Obliged entities refuse to engage in business with clients and customers that do not provide requested information for customer due diligence (CDD) purposes, but there is a widespread perception that banks are particularly intense in their collection and evaluation of CDD information. Bank customers, including other FIs and DNFBPs, believe that banks are applying CDD measures without real regard to risk distinctions. Most non-bank financial institutions consider bank CDD, perceived to be more rigid, as a supplement to their own risk-based compliance measures. Only a few sophisticated non-bank institutions with significant international business, including a few large ASPs regulated by CySEC and ICPAC and a money and value transfer service with a multinational location network, appear to have compliance practices that are designed to establish a completely free-standing structure to protect against ML/TF risk, without consideration of bank practices. Reliance on bank diligence with respect to some transactions such as large real estate transactions is explicit. This places undue risk-mitigation expectations on the banking sector and weakens the overall compliance effectiveness of the Cyprus financial system.

24. FIs generally apply specific and enhanced measures appropriately to correspondent accounts, new technologies, wire transfers, higher risk countries and targeted financial sanctions. With regard to PEPs, FIs generally screen aggressively for PEP status or associations but are still in the process of developing a reliable understanding of PEPs' source of wealth. Most DNFBPs appear to be at a comparable level of compliance, but real estate agents have not demonstrated that they apply enhanced measures appropriately.

25. Banks file STRs far more frequently than other types of financial institutions (including the MSBs met on-site) and DNFBPs. Even among banks, both the frequency with which internal investigations of suspicious activity are instituted and the frequency with which internal investigations lead to STR filings vary greatly.

26. The casino is currently operating at or beyond the limits of its ML/TF compliance and risk management system. An action plan prepared by an outside consultant, which is nearing completion, will identify mitigating steps that are needed to address current deficiencies, but it is unclear whether the plan is intended to identify steps that will need to be taken to accommodate anticipated growth.

### *Supervision (Chapter 6; IO.3; R.14, R.26–28, 34, 35)*

27. The supervisory authorities of FIs, the CBC, the Cyprus Securities Exchange Commission (CySEC) and the Insurance Companies and Control Service (ICCS) apply comprehensive controls in relation to preventing criminals from owning or controlling licensees.

28. There is a good understanding of ML risks; in some cases, there is very good understanding, for example, where specific risk exercises have been undertaken by the CBC. Overall, there is good understanding of FT risks although this is less developed than for ML. The supervisory authorities use risk-based approaches to focus AML/CFT programmes. The approaches used by the CBC for banks and CySEC for securities market participants are the most robust and sophisticated although there is scope for these to be refined (ie for minor changes to be made). The CBC's approach to non-

banks is not as comprehensive as for banks. These sectors are still at the development stage.

29. Inspections by the CBC and CySEC are very good quality and they always require breaches to be remediated. Sanctions have been imposed by the CBC and CySEC. There are strong elements of effectiveness and dissuasiveness, but the CBC process is not streamlined and, overall, the frameworks are not wholly effective for either authority. Sanctions have not been imposed by the ICCS. For the CBC and CySEC shortfalls in staff resources are limiting the efficiency of the licensing process (but not its quality beyond this) and for all three authorities, shortfalls in staff resources are limiting the volume of supervision, linked work on risk assessment, and sanctioning that can be undertaken.

30. The authorities have demonstrated that they have made a positive difference to the level of compliance by FIs. The authorities have promoted a clear understanding by FIs of their AML/CFT obligations, with a greater emphasis on AML.

31. All DNFBP supervisors apply market entry measures albeit with varying degrees of intensity. CySEC and the Institute of Certified Public Accountants (ICPAC) apply comprehensive controls in relation to licensing; the Cyprus Bar Association's (CBA) verification checks are more limited. There is no routine exchange of information between the three ASP supervisors on applications which have been rejected applications and licences that have been withdrawn. This may result in situations where persons who are deemed to be unsuitable by one supervisor are not precluded from seeking a licence elsewhere. The Estate Agents Registration Council applies market entry measures, although certain registration or licence renewal requirements for real estate agents could not be substantiated. The Casino Commission has applied appropriate market entry measures for the casino operating in Cyprus.

32. The ASP supervisors have a good understanding of the ML risks of the sector, while the understanding of TF risks is less developed. A similar risk assessment approach exists between the three ASP supervisors. However, there are differences in risk assessment methodologies and all of them require further enhancement or refinement (e.g. expansion of the set of AML/CFT risk data to be collected). The ML/TF risks of the real estate sector are underestimated by the Estate Agents Registration Council. The Casino Commission has a comprehensive understanding of ML risks to which casinos are exposed and has a general understanding of TF risks. All DNFBP supervisors (with the exception of the Estate Agents Registration Council) apply a risk-based approach to supervision with different degrees of intensity. The resources allocated to AML/CFT supervision within all supervisory bodies (except for ICPAC's onsite inspections) are not yet sufficient to ensure the implementation of a fully effective risk-based supervision. The number of on-site inspections conducted so far by all DNFBP supervisors (except for the ICPAC) is at the lower end of the spectrum. Very few sanctions for AML/CFT infringements have been imposed by DNFBP supervisors.

### *Transparency and beneficial ownership (Chapter 7; IO.5; R.24, 25)*

33. The authorities understand that Cyprus, as a company formation and administration centre, is exposed to ML/TF risks associated with legal persons created in the country. However, given that the country has not formally identified and assessed those risks, the precise nature and extent of the risks are not yet understood. This reduces the authorities' ability to implement mitigating measures which specifically target identified risks.

34. As a way of ensuring transparency of non-resident owned/controlled legal persons and legal arrangements, which pose the highest ML/TF risk, Cyprus uses a combined approach: (1) implementing a regulatory and supervisory framework for ASPs for both prudential and AML/CFT requirements; (2) imposing a requirement for non-resident owned/controlled legal persons or legal arrangements to engage the services of an ASP licensed and resident in Cyprus; and (3) placing an obligation on the ASP to obtain and hold adequate, accurate and current BO information on such legal persons/arrangements.

35. Significant efforts were made by the supervisors to establish a comprehensive ASP regulatory

and supervisory framework, which have resulted in an increased level of compliance by the ASP sector and improved the quality of BO information maintained by them. However, further progress is required, with certain areas requiring major improvement. In addition, there is no comprehensive mechanism in place to verify that the requirement to engage the services of a Cyprus-licensed ASP is applied for all non-resident owned/controlled legal persons/arrangements.

36. In order to obtain BO information, competent authorities mainly rely on information maintained by ASPs and banks by applying their information gathering powers. These powers are adequate and ensure timely access to information. Reliance by competent authorities on BO information maintained by ASPs, which are seen as the primary repository of BO information, may be problematic for two reasons: (1) the application of BO-related requirements by ASPs was not uniformly convincing; and (2) there are some concerns about the effectiveness of supervision of ASPs. This constitutes a gap in transparency of BO information of legal persons/arrangements. This gap is to some extent mitigated where the legal person/arrangement holds a bank account with a bank in Cyprus. Banks were found to apply BO-related requirements soundly. In 2018, Cyprus introduced provisions in the AML/CFT Law which provide the legal basis for setting up of a BO registry. At the time of the on-site visit, arrangements had been initiated to set the registry up.

### *International cooperation (Chapter 8; IO.2; R.36–40)*

37. Overall, Cyprus has been effective in executing requests in a timely and constructive manner in response to all types of formal requests from countries with which it cooperates most actively. The FIU has been instrumental in freezing and confiscating assets on behalf of foreign jurisdictions. Extradition requests have been processed effectively to extradite a number of high-profile, non-Cypriot fugitives wanted for prosecution in other countries. The Police have overcome challenges in responding to an increasing number of incoming requests by establishing the Office for the Execution/Handling of MLA Requests, which, however, is still in the process of removing a backlog of requests.

38. Cyprus has proactively sought legal assistance and extradition in relation to domestic ML and proceeds-generating offences committed in Cyprus with a foreign link. This has resulted in freezing and confiscation of assets abroad and assisted the Cypriot authorities in securing domestic convictions. Since there have not been many investigations domestically concerning proceeds of crime generated outside of Cyprus and laundered in/through Cyprus (e.g. layering activities through banking transactions) international cooperation in these types of cases was sought to a much lesser extent. This is not in line with the type of threats that Cyprus faces as an IFC.

39. The FIU is generally effective in providing and seeking informal cooperation. Due to a heavy workload and limited human resources the FIU may not have always managed to meet the deadlines, particularly where the case involved the collection of significant volumes of information. On a positive note, the FIU spontaneously shares fully-fledged analysis products with foreign counterparts, which have been critical in assisting foreign counterparts in securing convictions and the seizure and confiscation of proceeds.

40. The Police, Customs and the supervisory authorities have mechanisms in place to provide and seek information informally in a swift, constructive and confidential manner.

41. The authorities have been constructive in providing basic and BO information on legal persons and arrangements which is available to them.

## Priority Actions

1. The competent authorities should be more aggressive in pursuing money laundering from criminal proceeds generated outside of Cyprus.
2. The competent authorities should be more proactive at freezing and

confiscating foreign criminal proceeds at their own initiative.

3. Cyprus should conduct a formal and comprehensive assessment of risks posed by legal persons and arrangements.
4. Cyprus should ensure that ASPs take action to enhance their ML/TF risk understanding and apply preventive measures commensurate with the risks, including by providing more guidance, training and feedback.
5. The CBA should strengthen its authorisation procedure. All ASP supervisors should continue developing the application of the risk-based approach to supervision. Effective and dissuasive sanctions should be imposed for breaches of AML/CFT requirements.
6. The supervision of the real estate sector should be significantly enhanced, and measures should be taken to increase the level of compliance with preventive measures by real estate agents.
7. Cyprus should conduct a comprehensive ML/TF risk assessment of the Cyprus Investment Programme.
8. Measures should be taken to increase ASP understanding of the risks of TFS evasion.
9. Cyprus should proceed with the implementation of a risk-based approach framework to the non-profit sector.

## Effectiveness & Technical Compliance Ratings

**Effectiveness Ratings[2]**

| IO.1 | IO.2 | IO.3 | IO.4 | IO.5 | IO.6 | IO.7 | IO.8 | IO.9 | IO.10 | IO.11 |
|---|---|---|---|---|---|---|---|---|---|---|
| Substantial | Substantial | Moderate | Moderate | Moderate | Moderate | Moderate | Moderate | Substantial | Moderate | Moderate |

**Technical Compliance Ratings[3]**

| R.1 | R.2 | R.3 | R.4 | R.5 | R.6 | R.7 | R.8 | R.9 | R.10 |
|---|---|---|---|---|---|---|---|---|---|
| LC | LC | C | C | LC | LC | LC | PC | C | LC |
| R.11 | R.12 | R.13 | R.14 | R.15 | R.16 | R.17 | R.18 | R.19 | R.20 |
| C | LC | PC | C | LC | LC | C | LC | LC | C |
| R.21 | R.22 | R.23 | R.24 | R.25 | R.26 | R.27 | R.28 | R.29 | R.30 |
| C | LC | LC | LC | LC | LC | C | LC | C | LC |
| R.31 | R.32 | R.33 | R.34 | R.35 | R.36 | R.37 | R.38 | R.39 | R.40 |
| PC | LC | C | LC | C | C | LC | C | C | C |

[2] Effectiveness ratings can be either a High- HE, Substantial- SE, Moderate- ME, or Low – LE, level of effectiveness.

[3] Technical compliance ratings can be either a C – compliant, LC – largely compliant, PC – partially compliant or NC – noncompliant.

# MUTUAL EVALUATION REPORT

## *Preface*

1. This report summarises the AML/CFT measures in place as at the date of the on-site visit. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of the AML/CFT system and recommends how the system could be strengthened.

2. This evaluation was based on the 2012 FATF Recommendations and was prepared using the 2013 Methodology. The evaluation was based on information provided by the country, and information obtained by the assessment team during its on-site visit to the country from 13 to 24 May 2019.

3. The evaluation was conducted by an assessment team consisting of:

- Ms Elizaveta Churilina – Leading Consultant in International Cooperation Department, Rosfinmonitoring, Russian Federation (legal expert)
- Mr Albert Kaufmann – Deputy Head of Supervision Section DNFBP, Financial Market Authority, Liechtenstein (financial expert)
- Mr Steven Meiklejohn – Legal Advisor, Law Officers Department, Jersey (legal expert)
- Mr Davide Quattrocchi – Attaché from the Guardia di Finanza at the Italian Embassy for Spain, Italy (law enforcement expert)
- Mr Jacob Thiessen – Senior Counsel, Office of the Assistant General Counsel for Enforcement and Intelligence, Department of Treasury, United States of America (financial expert)
- Mr Richard Walker – Director of Financial Crime Policy and International Regulatory Advisor, Policy Council, Guernsey (financial expert)
- Mr Jérémie Ogé – AML/CFT Advisor, Ministry of Justice, Grand Duchy of Luxembourg (financial expert)

MONEYVAL Secretariat

- Mr Michael Stellini – Deputy Executive Secretary
- Ms Kotryna Filipaviciute – Administrator
- Mr Aleksei Samarin – Administrator
- Mr Uwe Wixforth – Administrator

4. The report was reviewed by the FATF Secretariat, Mr Richard Berkhout (IMF) and Mr Borja Delgado, Prosecutor (Andorra).

5. Cyprus previously underwent a MONEYVAL Mutual Evaluation in 2011, conducted according to the 2004 FATF Methodology and was placed in biennial follow-up. The 2011 evaluation and 2013 and 2015 follow-up reports have been published and are available at:

https://rm.coe.int/report-on-fourth-assessment-visit-anti-money-laundering-and-combating-/1680715f1f

http://www.law.gov.cy/law/mokas/mokas.nsf/99C7BBAB7610163EC2257B6E002AA836/$file/PROGRESS%20REPORT%20ON%20THE%204TH%20ROUND%20EVALUATION%20OF%20CYPRUS%20DEC%202103.pdf

https://rm.coe.int/moneyval-moneyval-2015-47-4th-round-evaluation-of-cyprus-biennial-upda/16807358f7

6. That Mutual Evaluation concluded that the country was compliant with 12 Recommendations; largely compliant with 28; and partially compliant with 9. Cyprus was rated compliant or largely compliant with 14 of the 16 Core and Key Recommendations.

# 1. ML/FT RISKS AND CONTEXT

7. Cyprus is an island situated in the north-eastern basin of the Mediterranean Sea at the crossroads of Europe, Asia and Africa. It is the third largest island in the Mediterranean, after Sicily and Sardinia, and has an area of 9.251 square kilometres. The population of Cyprus (Government-controlled area) was estimated at 864,200 at the end of 2017.

8. Cyprus is an independent sovereign Republic with a presidential system of government. The President is elected by universal suffrage for a five-year term of office. Executive power is exercised through a Council of Ministers appointed by the President. The legislative authority in the Republic is exercised by the House of Representatives. Justice is administered through the Republic's independent judiciary. Since 1974, the northern part of the island has not been under Government control[4]. This report only covers the AML/CFT regime in those parts of the island which are under Government control.

9. The country has been a member of the European Union since 1 May 2004 and a Euro Area member since 1 January 2008. Cyprus is also a member of numerous international organisations, such as the Council of Europe, the United Nations (UN), the Organisation for Security and Co-operation in Europe (OSCE), the World Trade Organisation (WTO), the International Monetary Fund (IMF), the World Bank (WB), the European Bank for Reconstruction and Development (EBRD), Europol and Interpol.

## *1.1. ML/FT Risks and Scoping of Higher Risk Issues*

### *Overview of ML/FT Risks*

10. As an international financial centre (IFC), Cyprus is primarily exposed to external money laundering (ML) threats as non-residents may seek to transfer criminal proceeds to or through Cyprus, particularly through the Cypriot banking system or may seek to use trust and company service providers, known in Cyprus as administrative service providers (ASPs), to facilitate their aims.

11. Domestic ML threats, particularly those deriving from fraud, corruption and drug smuggling, while less significant than foreign threats, are not negligible.

12. The Cyprus Investment Programme (CIP) is inherently vulnerable to abuse for ML purposes, as is real estate, both in general and as the apparent preferred investment to acquire citizenship.

13. Despite Cyprus's continuing exposure to external threats, the risk landscape of banks has considerably changed following the financial crisis in 2013. The total assets of Cypriot banks reduced drastically from EUR 122.9 billion in 2012 to EUR 60.5 billion in 2018 and non-resident deposits declined steadily. Figures shown to the assessment team indicate that the transactional volume has also significantly contracted. The level of non-resident business has shrunk although it has stabilised in recent years. Many banks which were previously exposed to international business reported changing their business model and seeking a share of domestic business. This reflects pressures imposed by foreign correspondents to mitigate risk combined with banks' conscious adoption of strategies not to take on risk that cannot be managed.

14. The risks related to ASP business have also experienced some fluctuation. Using the number of new Cypriot companies as a proxy[5], there was a dramatic reduction of new registrations between 2012 and 2013 as a result of the financial crisis. The business increased slightly during 2014 and 2015, exhibiting some further growth thereafter up until 2018 with a downturn from 2019 onwards.

15. Although the terrorism threat is considered to be low in Cyprus, the authorities rate terrorist

[4] Referred to in this report as the occupied areas.
[5] There is no data on the number of companies administered by ASPs.

financing (TF) risk as medium due to the fact that the country is an IFC and its proximity to conflict areas.

### *Country's risk assessment*

16. Cyprus published its first National Risk Assessment (NRA) in October 2018[6] with the participation of all relevant competent authorities and the involvement of private sector entities. The NRA is based on the World Bank methodology. The project was managed by the Central Bank of Cyprus and the Cyprus FIU. The NRA consisted of an assessment of the threats facing the country and the analysis of the vulnerabilities both at a national level but also from the point of view of the main financial and economic sectors. The combination of the level of threat and vulnerabilities produced the overall assessment of ML/TF risks.

17. During the process, information, including statistical data, was provided by stakeholders across the public and private sectors. Reports issued by MONEYVAL and other relevant reports from independent sources were also taken into consideration. The information was analysed and assessed during workshops and meetings. Threats and vulnerabilities were identified based on a number of risk factors relevant to each sector: the nature and scale of the sector, products and services of the sector, investigations, prosecutions, court orders, activity in the area of international cooperation, etc.

18. The NRA finds that the international engagement of the financial system heightens the risk of ML. The sectors primarily exposed to external ML threats were found to be the banking sector, followed by Trust and Company Service Providers, known in Cyprus as Administrative Service Providers (ASPs), and the real estate sector.

19. TF was analysed separately from ML and the findings are presented in a separate module. It was concluded that Cyprus faces a medium threat level since, despite the low number of any indicators[7], as an IFC the country faces an elevated exposure. The proximity of the country to areas of intense conflict was also taken into account.

### *Scoping of Higher Risk Issues*

20. The assessment team identified those areas which required an increased focus through an analysis of information provided by the Cypriot authorities (including the NRA) and by consulting various open sources.

- Banking sector – The banking sector is the most vulnerable in Cyprus due to its exposure to external ML/FT threats. The banking sector engages in non-resident business, which often features complex corporate structures, cross-border wire transfers with counterparties in various jurisdictions, introduced business, the use of nominee shareholders/directors, trusts and client accounts. The assessment team focussed on the banks' ability to effectively mitigate these risks through the application of mitigating measures. Particular attention was paid to the implementation of recommendations made by MONEYVAL in a special assessment of the effectiveness of customer due diligence measures conducted in 2013 (see section below 'the Special Assessment').
- Administrative Service Providers (ASPs)[8] – Given that international business is largely

[6] The NRA was concluded in 2017, covering the period between 2011- June 2016.

[7] such as mutual legal assistance (MLA) requests relating to TF, suspicious transactions reports (STRs), investigations, prosecutions and convictions for TF, freezing of funds of persons and entities designated under TF-related sanctions

[8] The term "Administrative Service Providers (ASPs)" is Cyprus-specific and includes those persons and entities that are licensed to provide administrative services as listed in Section 4 (1) of the Administrative Services Law. On the basis of the FATF terminology, administrative service providers are equivalent with the so-called "Trust and Company Service Providers (TCSPs)" (see Rec. 22). Additionally, administrative services may also be provided by advocates and Lawyers' Companies. However, the service of acting as a formation agent of legal persons is exclusively reserved to advocates and Lawyers' Companies.

introduced to banks by ASPs (including advocates and lawyers' companies), this sector plays a crucial gatekeeping role in Cyprus. ASPs also act as nominee shareholders and/or directors for Cyprus-registered companies owned/controlled by non-residents. Based on these and other considerations, the NRA considers the sector as the second most vulnerable sector of being misused for ML/FT purposes. The sector falls within the responsibility of three different supervisors: the Cyprus Bar Association, the Institute of Certified Public Accountants of Cyprus and the Cyprus Securities and Exchange Commission. The assessment team examined the effectiveness of supervision to determine whether policies, supervision and monitoring processes of the three supervisors are sufficiently harmonised to ensure consistency in the implementation of preventive measures by the ASP sector as a whole.

- Transparency of legal persons – Significant levels of international business involve the setting up of companies where the ultimate control is exercised outside of Cyprus by the beneficial owner (BO). Usually, such companies take the form of private limited companies, whose shares may be held by ASPs on behalf of foreign BOs. The assessors analysed the effectiveness of the country's mechanisms aimed at ensuring the transparency of these entities.
- Citizenship Investment Programme (CIP) – The CIP is managed by the Ministry of Interior (MoI). However, this is cross-cutting issue, which involves various public and private stakeholders. The assessors evaluated whether the ML/FT risks attached to such schemes are understood by the authorities and private sector entities which come in contact with applicants (e.g. banks, ASPs, etc) and whether appropriate risk-mitigating measures are being applied (e.g. criminal background checks, source of funds and wealth of the applicants and measures to ensure that the funds or assets involved are not directly or indirectly owned by UN and/or EU designated persons and entities).
- Real Estate Sector – One of the most common investments to acquire citizenship is real estate. The assessment team examined whether real estate agents involved in transactions related to the CIP understand the risks and apply effective preventive measures. The role of real estate developers in this context was also considered.
- Casino – During the on-site visit, it became clear to the assessment team that AML/CFT compliance by the casino had weaknesses. Given that the casino is planning aggressive expansion, including significantly increasing the size of the gaming operations, attracting foreign junket operators, and attracting foreign VIP customers, the assessment team deemed it necessary to focus on and weight more heavily the implementation of AML/CFT requirements by the casino. Online casinos are prohibited from operating in Cyprus.
- Money Service Businesses (MSBs) – in discussion with the authorities, it was determined that Cyprus hosts a fairly large population of temporary resident workers from South East Asia and that a considerable amount of outgoing remittances flow through MSBs. The assessment team weighted the measures implemented by the sector and the supervision of the sector by the CBC more heavily than those of other financial institutions.
- International cooperation – Cyprus is an international financial centre facing a high foreign ML/TF threat. The extent to which Cypriot authorities provide and proactively seek assistance, both formal and informal, from their foreign counterparts to initiate and carry forward domestic ML/FT investigations received additional attention by the assessment team. Assessors looked at possible challenges in providing formal and informal assistance to foreign counterparts (e.g. access to information, timeliness of handling requests, appropriateness/comprehensiveness of the information exchanged). Another important area in the context of Cyprus is the provision of assistance in the identification, freezing and confiscation of illegal assets traced or channelled through Cyprus and requests concerning BO of Cypriot companies owned by non-residents. Since Cyprus hosts many branches and subsidiaries of banks licenced abroad, attention was also paid to international cooperation

between supervisors, particularly between the Central Bank of Cyprus and banking supervisors in other countries.

21. The areas which were identified for reduced focus were the following:

- The insurance sector mainly services domestic clients and is small in terms of assets under management compared to the other financial sub-sectors.
- At the time of the on-site visit, dealers in precious metals and stones (DPMS) were prohibited from conducting any transaction in cash exceeding EUR 10,000 and therefore were not subject to AML/CFT requirements.

### *1.2. Materiality*

22. Cyprus is a small open economy. Services sectors like tourism, business and financial services are critical for the economy. In 2017 and 2018, the economic growth rate was 4.5% and 3.9% respectively. The GDP in 2018 accounted for EUR 20.730 billion. According to its national accounts, the largest share of Cypriot GDP in 2018 was wholesale and retail trade, followed by real estate activities and financial activities. Tourism, even though not specifically captured in national accounts, contributes significantly to the GDP through national account captured services such as accommodation, recreation, retail trade and associated services.

23. Cyprus is an IFC with an important company formation and administration sector. The expansion of the international business sector in Cyprus is largely due to the country's strategic geographical location, at the crossroads of three continents, its advanced professional services sector, its legal framework which is closely based on the English common law, as well as on the existence of a wide network of treaties with other countries for the avoidance of double taxation.

24. The Cyprus Investment Programme is material within the economy of Cyprus. The total volume of the funds invested under the CIP for the period 2013-2018 was EUR 6.64 billion. Real estate property is by far the most common type of investment.

### *1.3. Structural Elements*

25. Cyprus has all of the key structural elements required for an effective AML/CFT system including political and institutional stability, governmental rule of law, and a professional and independent judiciary.

### *1.4. Background and other Contextual Factors*

26. Cyprus has an increasingly mature and sophisticated anti-money laundering/counter-terrorist financing (AML/CFT) system, albeit there is room for improvement in sensitive areas.

27. Financial exclusion is not a widespread issue in the country, as according to the G20 Financial Inclusion Indicators in 2017 about 89% of inhabitants dispose of a bank account, whereas 80% above the age of 15 engage in digital payments.

28. The GRECO evaluation report on Cyprus (fourth evaluation round - Corruption prevention in respect of members of parliament, judges and prosecutors) adopted in June 2016, states that "*…It would appear that general awareness about corruption in Cyprus has increased over the years but although Transparency International's Corruption Perception Index has ranked Cyprus among countries less affected by corruption (32 out of 168), other surveys indicate that corruption is perceived to be widespread in the country;…*". A National Strategy against Corruption was approved by the Council of Ministers in Cyprus on 28 June 2017 with the objective to demonstrate the magnitude of the current actions against corruption, to identify the high-risk areas and to increase full transparency.

#### *Special Assessment of Cyprus*

29. In response to a request by the Eurogroup in 2013, MONEYVAL conducted a special assessment

of the customer due diligence measures applied by the banking sector[9] as a condition for granting the Economic Adjustment Programme by the Troika Institutions (the European Commission, the European Central Bank and the IMF). The assessment gave rise to a number of recommendations which were followed up by MONEYVAL under a special follow-up procedure[10]. This report, where appropriate, examines the implementation of those recommendations, particularly under IO 4. The recommendations were also included in the action plan of the Economic Adjustment Programme which was completed in 2016[11].

### *AML/CFT strategy*

30. Cyprus effectively formulates its national AML/CFT policy and strategy through the Advisory Authority for Combating Money Laundering and Terrorist Financing. The Advisory Authority is presided both by the Ministry of Finance and the FIU. Its role is primarily to inform the Council of Ministers of any measures taken and the general policy applied against ML/TF and to advise the Council of Ministers about additional measures which, in its opinion, should be taken for the better implementation of the AML/CFT Law.

31. A national AML/CFT strategy was adopted by the Advisory Authority in January 2019 and endorsed by the Council of Ministers in March 2019. The strategy is based on the findings of the NRA and contains the following nine pillars:

a. Minimise the threat and further strengthen supervisory processes in the banking sector;
b. Upgrade the supervisory processed of the ASP sector;
c. Upgrade the structure, training and capacity of investigators and prosecutors;
d. Build on the international cooperation procedures and systems;
e. Improve data collections and statistics procedures;
f. Enhance supervisory processes and procedures in other sectors;
g. Increase transparency of corporate entities and legal arrangements;
h. Enhance counter TF measures;
i. Monitor the implementation of anti-corruption measures.

32. The strategy is expected to be subject to ongoing review based on the experience of the authorities involved in its implementation, changes in legislation, developing best practices and the findings of future NRAs.

### *Legal framework*

33. The Prevention and Suppression of Money Laundering and Terrorist Financing Law of 2007-2018 (the AML/CFT Law) is the central piece of legislation on AML/CFT matters. It sets out the preventive measures but also provides for the establishment and functioning of the FIU, criminalises ML, includes provisions on the identification, tracing, freezing and confiscation and regulates the international exchange of information, among others. Other relevant pieces of legislation include the sectorial laws regulating the financial and DNFBP sector, the Criminal Code (CC), the Code of Criminal Procedure (CPC), the Suppression of Terrorism Law, the Implementation

[9] https://rm.coe.int/special-assessment-of-the-effectiveness-of-customer-due-diligence-meas/168071611d
[10] https://rm.coe.int/moneyval-interim-report-submitted-to-moneyval-by-cyprus-on-progress-in/1680716144
https://rm.coe.int/moneyval-report-submitted-to-moneyval-by-cyprus-on-progress-in-respect/1680716125
https://rm.coe.int/moneyval-report-submitted-to-moneyval-by-cyprus-on-progress-in-respect/1680716143
[11] https://ec.europa.eu/info/business-economy-euro/economic-and-fiscal-policy-coordination/eu-financial-assistance/which-eu-countries-have-received-assistance/financial-assistance-cyprus_en

of UN Security Council Resolutions and EU Restrictive Measures Law, the Control of Cash Law, the Companies Law, the Law Regulating Companies Providing Administrative Services and Related Matters (The ASP Law), the Trustee Law, The International Trusts Law and the Law on Societies and Institutions and other related Matters Law (LSI). The AML/CFT Law is supplemented by various directives issued by the supervisory authorities.

*Institutional framework*

34. The institutional framework involves a broad range of authorities. The most relevant ones are the following:

*Co-ordination and co-operation and ministries:*

- **The Advisory Authority for Combating Money Laundering and Terrorist Financing** (the Advisory Authority) serves as a mechanism for co-operation among all AML/CFT stakeholders and co-ordination for the development and implementation of policies and activities. It is a body established by the Council of Ministers composed of a representative from the FIU, the supervisory authorities, the Ministry of Finance, the Ministry of Justice and Public Oder, the Ministry of Foreign Affairs, the Customs and Excise Department, the Cyprus Police, the Company Registry, the association of international banks, the association of commercial banks, the Inland Revenue Department (the Tax Department), the Casino Commission, the Betting Authority and the Estate Agents Registration Council.
- **The Fusion Centre** is an intergovernmental strategy body which analyses trends and provides quarterly threat assessments on terrorism threats and comprises representatives of the CIS, Police, National Guard and officials of the MFA and the MoI.
- **The Ministry of Finance** co-chairs the Advisory Authority.
- **The Ministry of Foreign Affairs (MFA)** represents Cyprus on issues pertaining to the imposition of UN and EU sanctions.
- **The Ministry of Interior (MoI)** is responsible for the oversight of non-profit organisations (NPOs)
- **The Ministry of Energy, Commerce and Industry (MECI)** issues export licences for dual use goods and military equipment following consultations with, *inter alia,* the MFA, where necessary.
- **The Department of Registrar of Companies and Official Receiver (DRCOR)** within the MECI serves as the company registry.

*Criminal justice and operational agencies*

- **The Cyprus FIU** is an independent body within the Law Office of the Republic's Public Prosecutor Office. It discharges the functions set out under R. 29, but also executes MLA requests related to freezing and confiscation.
- **The Cyprus Police** has the general power for investigating all offences in Cyprus, including ML, predicate offence and TF.
- **Law Office of the Republic's Public Prosecutor Office (PPO)** is responsible for the prosecution of ML, predicate offence and FT.
- **The Customs Department** is responsible for investigating customs-related offences and the implementation of the declaration system for cash/bearer negotiable instruments entering and leaving Cyprus. It is also responsible for controlling the exportation and importation of sensitive goods.
- **The Tax Department** assesses tax and combats domestic tax evasion and provides assistance to overseas tax authorities.
- **The Ministry of Justice and Public Order (MJPO)** is the central authority for the receipt of

MLA (including European Investigation Orders (EIOs)) and extradition (including European Arrest Warrants (EAWs)) requests.

- **The Asset Recovery Office (ARO):** The FIU serves as the Asset Recovery Office set up pursuant to the requirements of the relevant EU legislation[12] concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds.
- **The Cyprus Intelligence Service (CIS)** is the intelligence-gathering body of Cyprus.

*Financial and non-financial supervisors*

- **The Central Bank of Cyprus (CBC)** licences and supervises banks, payment institutions, electronic money institutions, credit acquiring firms, currency exchange offices and financial leasing companies.
- **The Cyprus Securities and Exchange Commission (CySEC)** licenses and supervises the capital and stock exchange market, including investment firms, funds and fund managers. It also licenses and supervises ASPs which do not fall under the supervision of the other ASP supervisors (see below).
- **The Insurance Companies and Control Service (ICCS)** licenses and supervises life insurance undertakings.
- **The Institute of Certified Public Accountants (ICPAC)** supervises accounting professionals and licenses and supervises accounting professionals who provide administrative services.
- **The Cyprus Bar Association (CBA)** supervises legal professionals and licenses and supervises legal professionals who provide administrative services.
- **The Estate Agents Registration Council** took over competency from the FIU in May 2018 and since then supervises real estate agents.
- **The National Gaming and Casino Supervision Commission (Casino Commission)** licenses and supervises the only operational casino.

*Financial sector and DNFBPs*

35. An overview of the financial and non-financial sector is provided in the table below.

**Table 1: Overview of financial and non-financial sector**

| Type of Entity | No. Licensed / Regulated / Registered | Size of sector (EUR, billion) |
|---|---|---|
| Financial Sector | | |
| Banks (credit institutions): | 31 | 60.5 (total assets) |
| - Domestically authorised | (7) | 48.2 |
| - Foreign authorised | (24) | 12.3 |
| Investment Firms | 229 | 7.2 (total assets)<br>1.5 (trading income) |
| Life Insurance | 10 | 0.37 (insurance premiums) |

[12] COUNCIL DECISION 2007/845/JHA concerning co-operation between Asset Recovery Offices of the Member-States in field of tracing and identification of proceeds from or other property related to crime

| Type of Entity | No. Licensed / Regulated / Registered | Size of sector (EUR, billion) |
|---|---|---|
| Payment institutions | 10 | |
| - acquiring companies | (1) | 4.2 (total value of transactions) |
| - payment accounts | (3) | 0.53 (total value of transactions) |
| - money service businesses (MSBs) | (6) | 0.03 (inward transfers)<br>0.25 (outward transfers) |
| E-money Institutions | 13 | 0.72 (total assets)<br>0.11 (total value of transactions) |
| Currency exchange (of which 2 were not operational) | 4 | 0.01 (total estimated value of currency purchases)<br>0.08 (total estimated value of currency sales) |
| Credit acquiring companies | 5 | 6.5 (total assets) |
| Internally Managed Investment Funds | 66 | 1.3 (total assets under management) |
| External Investment Fund Managers | 34 | 4.5 (total assets under management) |

| Non-Financial Sector[13] | |
|---|---|
| Casinos | 1 |
| Real estate agents | 353 |
| Advocates | 3,808 |
| Lawyers' Companies | 689 |
| Accountants/Auditors | 671 |
| ASPs: | |
| licenced by CySEC | 159 |
| licenced by ICPAC | 326 |
| licenced by CBA | 1,555 |

36. The assessors ranked the sub-sectors on the basis of their relative importance in Cyprus given their respective materiality and level of ML/TF risks. The assessors used these rankings to inform

[13] The notarial profession does not exist in Cyprus. At the time of the on-site visit, dealers in precious metals and stones (DPMS) were prohibited from conducting any transaction in cash exceeding EUR 10,000 and therefore were not subject to AML/CFT requirements

their conclusions throughout this report, weighting positive and negative implementation issues more heavily for important sectors than for less important sectors. This approach applies throughout the report but is most evident in IO.3 and IO.4.

37. The **banking sector** is weighted as being the most important in Cyprus based on its materiality and risks. Most of the big banks offer fully-fledged banking services for commercial and private customers. The aggregated assets are – even after a considerable reduction following the financial crisis – about two and a half times the GPD of Cyprus. The banking sector is highly consolidated with the two largest banks accounting for two thirds of the overall assets. The NRA identified the banking sector as being at high ML risk as its relative size and openness to international business make it attractive to criminals seeking to hide the proceeds of crime among the huge volumes of legitimate business. Investments with the purpose of obtaining residence or citizenship under the CIP require the involvement of banks.

38. **ASPs,** which provide administrative services under the Administrative Services Law, are rated as medium-high risk by the NRA. ASPs play a critical gatekeeping role since international business is largely introduced to banks by ASPs. ASPs also act as nominee shareholders and/or professional directors for Cyprus-registered companies owned/controlled by non-residents and administer and manage trusts. Based on these considerations, the assessment team weighted ASPs as the second most material sector.

39. **Real estate agents** are weighted as the third most important sector given their exposure to international risks. As noted, one of the most common investments to acquire citizenship is real estate.

40. There is one licensed land-based **casino operator** currently in Cyprus (license issued in July 2018), with plans to expand its activities significantly to become an integrated casino resort by the end of 2021. Additionally, the licensed casino operator intends to introduce junket services. The enlargement of the temporary casino structure, the extension of the services (including possibly junket services) and further satellite casinos will undoubtedly increase the ML/TF risks and require a number of further mitigation measures. For this reason, the casino was weighted fourth in terms of materiality. Online casino services are prohibited in Cyprus under the Betting Law (2012).

41. The other sector which was weighted as relevant for the purpose of this assessment is the **money service business** sector; fifth in terms of priority. Although the sector is not a significant contributor to the economy, representing around 0.02% of GDP, it may be relevant for FT purposes. This is because it was found that relatively significant migrant remittance outflows mainly by household workers from the Far East are typically done via the money service business sector.

### *Preventive measures*

42. The preventive measures are set out under the AML/CFT Law and are broadly compliant with the Standards. At the time of the on-site visit, dealers in precious metals and stones (DPMS) were prohibited from conducting any transaction in cash exceeding EUR 10,000 and therefore were not subject to preventive measures. The notarial profession does not exist in Cyprus. The AML/CFT Law does not exempt any sectors or activities from these requirements. It extends to certain activities which are not covered by the Standards i.e. auditors and tax advisors.

### *Legal persons and arrangements*

Legal persons

43. The types of companies that may be established in Cyprus are provided under Chapter 113 of the Companies Law of Cyprus, namely companies limited by shares and companies limited by guarantee (with or without share capital). Both types of companies can be either private or public. Additionally, the Companies Law contains provisions on the establishment and registration of a place of business of foreign companies in Cyprus (so-called overseas companies). Provisions on the European Company (SE) are made by the Council Regulation (EC) No. 2157/2001, which is directly applicable to Cyprus.

44. Limited and general partnerships and general partnerships can also be established. Partnerships are governed by the Partnerships and Business Names Law. According to the Partnerships and Business Names Law, general and limited partnerships do not have a separate legal personality. For the purposes of this assessment, partnerships are subsumed under the definition of "legal persons" (cf. FATF Guidance on Transparency and Beneficial Ownership, October 2014, page 12).

45. The other forms of legal persons that may be established in Cyprus are societies, federations and associations, which are governed by the LSI. Further information on these types of legal persons is provided under R.8.

**Table 2: Number of registered legal persons as of December 31, 2018**

| | **Types of entities** | **Number** |
|---|---|---|
| 1. | Private companies of limited liability by shares | 215,346 |
| 2. | General partnerships | 5,736 |
| 3. | Societies | 4,929 |
| 4. | Overseas companies | 1,075 |
| 5. | Limited partnerships | 832 |
| 6. | Public companies of limited liability by shares | 562 |
| 7. | Public and private companies of limited liability by guarantee without share capital | 552 |
| 8. | Private companies of limited liability by guarantee with share capital | 39 |
| 9. | European companies (SE) | 21 |
| 10. | Public companies of limited liability by guarantee with share capital | 3 |
| 11. | Federations and associations | 0 |
| | ***Total number*** | ***229,092*** |

46. Private companies of limited liability by shares are by far the most common form of legal person. These companies comprise about 94 % of the total number of registered legal persons as of December 31, 2018. Such private companies have several benefits including tax benefits (as long as the company is considered foreign-owned no corporation tax is imposed) and a limitation of liability to the contributions of the members.

47. By way of context, the number of newly registered companies experienced a sharp decrease between 2012 and 2013 due to the economic slowdown (from 17, 999 in 2012 to 10,847 in 2013). The number of registrations steadied in 2014 (11,169) and 2015 (11,270) followed by a growth rate of about 20% in both 2016 (13,645) and 2017 (13,677). In 2018, there was a further modest increase of around 6% (14,526). In the first five months of 2019, new registrations decreased by 12.7% in comparison to the first 5 months of 2018.

48. The authorities attribute the increase in registration of companies between 2016 and 2018 to an increase in economic activity in Cyprus. They state that the number of new registrations is highly correlated with GDP growth rate, which was over 4% during those years. An additional factor explaining some of the increase (around 4% according to MECI calculations), relates to companies being re-registered by a court order after having been struck off the Register (see core issue 5.2).

Legal Arrangements

49. Cyprus is a signatory to the Hague Convention on Laws Applicable to Trusts and their Recognition. Cyprus has two pieces of trust legislation, namely the Trustee Law of 1955 and the International Trusts Law 1992. The latter is not a self-contained law on trusts, but it builds on the existing trust legislation (The Trustee Law of 1955). The law applies only to "international trusts" which are broadly defined as those trusts whose settlor and beneficiaries are not residents of Cyprus. At least one resident trustee is a statutory requirement, which ensures that the Cyprus Courts have effective jurisdiction over the trust.

50. According to Section 25A of the Administrative Services Law, the CySEC, the CBA and the ICPAC each establish and keep a trust register with respect to each trust governed by Cyprus law and where one of its trustees is a regulated entity resident in Cyprus and supervised by the CySEC, the CBA or the ICPAC in its capacity as a competent supervisor.

**Table 3: Number of registered trusts and institutions as of December 31, 2018**

| | **Type of trust/legal arrangement** | **Number** |
|---|---|---|
| 1. | Trusts – registered with CySEC | 1,796[14] |
| 2. | Trusts – registered with CBA | 1,547 |
| 3. | Trusts – registered with ICPAC | 653 |
| | ***Total number*** | ***3,996*** |
| 4. | Institutions | 406 |

51. In addition to trusts, the LSI provides for the incorporation of institutions. According to Section 2 of the LSI, an institution includes assets with a value above EUR 1,000 appropriated by a founder to serve a certain non-profitable object. The incorporation of an institution is effected either by an *inter vivos* trust instrument or by a will or testament. As from the incorporation of the institution, the founder is bound to transfer to it the property as promised by him (Sections 26 (3), 27 (1) and 30 of the Societies and Institutions Law). Since Rec. 25 broadly applies to "legal arrangements" meaning express trusts and other similar arrangements, institutions are qualified as legal arrangements for the purposes of this report.

*Supervisory arrangements*

52. Sec. 59 of the AML/CFT Law designates the relevant authority to supervise FIs and DNFBPs subject to AML/CFT requirements. The CBC supervises banks, payment institutions, electronic money institutions, credit acquiring firms, currency exchange offices and financial leasing companies. CySEC supervises the capital and stock exchange market, including investment firms, funds and fund managers, and ASPs which do not fall under the supervision of the other ASP supervisors. The ICCS supervises life insurance undertakings. ICPAC supervises accounting professionals and ASPs. The CBA supervises legal professionals and ASPs. The Casino Commission supervises the only operational casino. The Real Estate Registration Council supervises real estate agents.

*International Cooperation*

53. Cyprus has a broadly comprehensive framework for international co-operation, with incoming and outgoing MLA and extradition requests coming from/going to a wide range of jurisdictions both within and outside of the EU. The MJPO is the central authority for the receipt of MLA and extradition requests. Requests are transmitted by the MJPO to other domestic authorities for execution, depending on the nature of the request (except for requests dealing with Tax and

[14] This figure includes 119 trusts in which the trustees benefitted from the exemption to be licensed according to Section 4 (3) and (4) of the Administrative Services Law.

Customs matters, that go directly to relevant authorities). The Police execute requests for the collection of evidence, such as bank information, etc. Requests relating to freezing and confiscation are executed by the FIU. Extradition requests and EAWs are executed by the Police and the Attorney General's Office. Requests may also be executed by the courts if these relate to the taking of testimonies on oath for cases the hearing of which is ongoing before a foreign court.

## 2. NATIONAL AML/CFT POLICIES AND COORDINATION

### *2.1. Key Findings and Recommended Actions*

**Key Findings**

1. There is good understanding of the most serious ML risks at the national and sectorial level; in some aspects, particularly where the CBC is involved, understanding is very good. FT risk is understood to a good standard, although there is scope for more in-depth assessment, including deeper interrogation of information in relation to FT more generally. Understanding of both ML and FT is greater than that represented in the NRA;

2. There are some areas of risk understanding where assessment coverage is not fully developed, including, for example, the CIP, the real estate sector, legal persons and arrangements and NPOs;

3. The AML/CFT Law provides for a limited exemption in relation to electronic money. This has been directly transposed from the 4th AML Directive, but the NRA concludes that electronic money presents a low risk in Cyprus .There situations in which obliged entities are required to apply enhanced due diligence and permitted to apply simplified due diligence are consistent with the risks identified in the NRA;

4. A national strategy for AML/CFT and an associated action plan have been recently introduced. The strategy and action plan flow from the NRA findings and are in line with understanding of risk;

5. There have been a series of national initiatives which specifically address the risks faced by Cyprus - for example, the issue of binding directives in relation to shell companies, increased standards for introduced business, and requirements for banks to meet customers who have been introduced and BOs of legal persons which are customers;

6. The Advisory Authority is a long-standing body which is the main coordination mechanism for AML/CFT and comprises representatives from all relevant bodies, except for the MoI and the MECI. The role of the FIU at the heart of the AML/CFT system has been a significant positive influence for the development of the system. There are coordination mechanisms in place in relation to countering PF, which could be improved further.

7. Bilateral and multi-lateral cooperation and information exchange is strong, with examples of very good liaison and information exchange between the Cypriot authorities being provided;

8. There has been outreach to the private sector, except by non-ASP DNFBP supervisory authorities.

**Recommended Actions**

1. In its next iteration of the NRA Cyprus should conduct a more comprehensive assessment of the following areas: the vulnerability of the real estate sector; the Cyprus Investment Programme, legal persons and arrangements and a more in-depth TF assessment;

2. The existing coordination framework in relation to PF should be strengthened;

3. Membership of the Advisory Authorities should be extended to the MoI and MECI;

4. Cyprus should communicate the results of national risk assessments to real estate agents and the casino.

55. The relevant Immediate Outcome considered and assessed in this chapter is IO.1. The

Recommendations relevant for the assessment of effectiveness under this section are R.1, 2, 33 and 34.

## *2.2. Immediate Outcome 1 (Risk, Policy and Coordination)*

### *2.2.1. Country's understanding of its ML/TF risks*

56. Cyprus concluded its first National Risk Assessment (NRA) at the end of 2017 (published in October 2018) with the participation of all the competent authorities (with the exception of the MoI[15]) and private sector entities. Sources of information outside Cyprus were also used. As a result of this exercise, the authorities have a good understanding of the ML threats and vulnerabilities at the national and sectorial level. In some aspects, where the CBC is involved, understanding is very good.

57. The NRA report includes statistics up to the end of 2015, with the cut off point for use of qualitative information being mid-2016. Based on operational experience and liaison between the authorities, the Cypriot authorities advised that the pattern of risk has generally remained consistent with that described in the NRA. The main differences appear to be in relation to increased activity and risk in the real estate sector and more cases of corruption (evidenced by more STRs referring to this criminality underlying ML and increased identification of cases by the authorities). There was also a significant increase in the quantity and quality of information available at the time of the assessment team's visit to Cyprus compared with post 2013. For example, banks have more in-depth information on their customer relationships, including economic profiles; there is more analysis of transactions; IT systems have had a demonstrable influence; the number and quality of STRs has increased; and analysis overall has improved. More generally there is scope for more in-depth analysis to be included in the NRA reports so as to reflect the higher level of assessment and understanding articulated by the authorities to the assessment team.

58. The assessment team considered whether Cyprus understands the risks arising from both foreign and domestic threats. However, it has focussed most of its discussions and analysis on the understanding of cross-border risk, given Cyprus's exposure as an IFC. The authorities understand very clearly that the main ML/FT risks derive from foreign criminality, with the openness of the Cypriot economy to international business being the key factor. The banking sector is regarded as presenting the highest ML threat, followed by ASPs. These service providers are considered to pose a medium high ML threat. The real estate and remittance sectors were concluded as having a medium threat. The ML threat for the securities sector was evaluated as medium low. The main domestic predicate crimes for ML are regarded as being fraud (high threat), corruption and drug trafficking (all medium to high threat), with the various sources of information used such as STRs, investigations and MLA presenting a consistent picture.

59. For the purposes of the NRA process, given the materiality of the banking sector, bank products and services, private banking, deposits, loans, cash deposits, wire transfers (in and out), credit cards, trade finance, client accounts and correspondent banking accounts) were analysed in detail. For each product, analysis included a number of factors such as its materiality, the average transaction size, the profile of the customer base, the level of cash activity, the frequency of international transactions. Other factors were also used such as the possibility of anonymity, omnibus use of the product/service, ML/TF typologies, the possibility of use of the product/service for criminality (including fraud or tax evasion schemes), use in non-face to face business. The CBC has also been able to use its risk-based tool and onsite and offsite supervision (see IO.3) to inform understanding. The riskier products have been concluded as being deposits, loans and wire transfers.

60. A significant proportion of this cross-border risk, for banks and more generally, was considered to arise through the use of introducers, with that risk now being reduced and well

[15] Responsible for the supervision of NPOs

understood by ASP supervisory authorities and the CBC. The ASP supervisory authorities demonstrated good knowledge of the way in which the risks had reduced, including in relation to customers from third countries, customers for whom the ASP has relied on a third party to perform elements of CDD, third parties that ASPs have relied on to perform elements of CDD and non-face to face customers. In relation to introduced business, the CBC has been augmenting its measures regarding reliance on ASPs since 2013. These measures have made it easier to understand risks. Furthermore, the CBC has been receiving BO information from banks since 2014 and is aware of the patterns of business as between countries, both in terms of the current position and how it has changed. The CBC was confident in demonstrating how the information available in and from banks has changed and its understanding of the implications of this information. Linked with the foregoing, the CBC has also undertaken separate risk exercises in relation to shell companies and complex structures.

61. The vulnerability of the real estate sector now appears to be a little downplayed in the NRA, although the risk landscape of the sector changed significantly after the adoption of the NRA report. At the time it was in a poor economic position after the economic crisis but there has since been a boom in construction and property for sale. The authorities understand there is work to be done to fully understand the current risks but the risks are generally understood. Given the developing nature of the risks in the sector, the authorities were in the process of collecting data and information at the time of the on-site visit to conduct a more comprehensive assessment.

62. The assessment team has considered the CIP from the perspective of whether ML and FT risks are understood (and not from any other perspective). Risks of the programme are understood by Cyprus to some extent, although it has not been subject to a "whole of government" comprehensive AML/CFT assessment. Such an assessment has been recommended within the AA by the FIU. Some mitigating measures had been put in place from the scheme's inception to address risks; these included a requirement for applicants not to have a criminal record, a requirement for investments within the scheme to be transacted via a Cypriot bank account and provision of application information by the MoI to the Police, the local Interpol office and the FIU. There has also been a basic assessment of the application by the MoI, including use of a commercial database. In addition, the MoI uses the same database to monitor those who have received citizenship. The measures have recently been enhanced as a result of concern and input at EU level. In addition, the MoI is shortly to appoint three firms to assist it with undertaking due diligence on applicants. By way of wider context, applicants are high net-worth individuals (HNWIs), including some PEPs and few applications have been rejected. From time to time the FIU has received STRs and other negative financial intelligence on applicants or those who have received citizenship. Those receiving citizenship and who are also resident in Cyprus are no longer considered to be non-resident by reporting entities. However, this might not have a significant effect EDD is applicable in all cases where a reporting entity considers a customer to be high risk. The vast majority of applicants have used an ASP although it is not known to what extent source of funds and wealth is subject to due diligence. Overall, the level of information required, the checks undertaken and the flow of information between authorities leaves a gap which is vulnerable to exploitation.

63. There were multi-authority responses (including the FIU, the CBC and the ASP supervisory authorities), to international issues, in particular the Panama Papers, well-known Laundromat scheme. These have enabled exposure by and cross-border risks to Cyprus of these cases being well understood.

64. With reference to the Panama Papers, there was a highly proactive multi-agency approach involving all members of the Advisory Committee. In April 2016, the FIU and the supervisors required licensed institutions to provide information on direct or indirect links with the law firm at the heart of the Panama Papers; business relationships introduced by or representing that firm; and any business relationship with any person represented in the Papers; advise what actions had been taken in response to the release of the Papers; and findings by the entity. The information provided, including STRs received by FIU, provided a detailed picture of the risks in Cyprus arising from the data in the Papers. One relevant case had frozen funds of EUR 15 million. Further actions were

taken by the CBC and the ASP supervisors, such as onsite inspections to a number of entities to assess internal controls. In addition, supervisors as a whole enhanced their onsite and offsite supervisory processes in light of the Papers for example in relation to a refined focus on tax issues. The Tax Department also undertook a major exercise to interrogate its databases based on the names in the Papers; this led to a limited number of additional assessments.

65. There was a proactive multi-agency response to the Laundromat cases. In connection with the case, in June 2017 the CBC required all entities it supervised to inform it whether it maintained any business relationship with any person referred to in the case and whether an STR had been made. Further information was required on specific accounts and transactions when necessary. The FIU received a number of STRs from banks; analysis led to the spontaneous provision of information on several occasions to other countries. The FIU continues to be involved with examining the relevant case files for potential further action. The vast majority of companies in the case with a link with Cyprus were registered abroad with foreign BOs and in most cases the relationship had been closed prior to the emergence of the case. Another case, involving a Lithuanian bank, has been ongoing since 2013 and also enabled Cyprus to demonstrate its understanding of cross-border issues and risks to the assessment team.

66. There were also initiatives to address the issues raised by a Danish bank. Following the emergence of issues in connection with this bank, the CBC requested data from all supervised entities to seek to identify any connections with the case. Data for a period of eight years was obtained so as to allow in-depth analysis. This included data on the level of flows between the Danish bank and Cypriot banks; STRs had also been made.

67. The lessons learned from the responses to the international events mentioned above are the importance of close domestic cooperation and information exchange, the importance of proactively considering negative information such as the events, and the importance of strong preventive measures. The totality of information and assessment of it by the authorities has allowed them to have a good understanding of cross-border risks, with very good understanding in some areas.

68. Cyprus has not formally assessed the risks of legal persons and arrangements. It is understood that Cyprus faces a heightened risk as an international company formation and administration centre. The provision of information to the CBC on the countries of residence of BO of Cypriot companies which are the customers of banks, together with information on flows of funds from and to banks, is positive. Useful information is also held by other authorities such as CySEC and ICPAC. Relevant thematic ML assessments of risks have been considered at institutional level in some cases such as the risks to Cyprus of business relationships specified in the Panama Papers and other ML/FT-related events that received public attention.

69. FT has clearly been considered and assessed but it appears that not all potential avenues (e.g. an assessment of money flows to and from high risk areas, the implications associated with the country of origin or of continuing family ties for an apparently large population of temporary resident workers) have been explored to the greater depth which would be necessary to gain a more complete understanding. The assessment team is also mindful that there has not yet been a distinct assessment of risks of abuse to and by the NPO sector. Some authorities, particularly the CIS, appear to have a better grasp of FT risks based on operational experience and the Fusion Centre, which CIS is a part of, carries out quarterly counter terrorism risk assessments because of its status as an IFC and the risks of funds being transited through Cyprus or being managed within Cyprus.

### *2.2.2. National policies to address identified ML/TF risks*

70. There is strong political commitment to AML/CFT, the work of the Advisory Authority and of individual authorities. This commitment has been demonstrated by the support provided to AML/CFT initiatives since before the period under review. There is a positive relationship between the Advisory Committee (via its two Co-Chairs) and the Council of Ministers.

71. In light of the membership of the Advisory Authority, the work of the Advisory Authority can

be considered to comprise part of a national policy and strategy process to address identified risks. It was developed as a mechanism to formulate, discuss, agree and promote national policies. Where policies require more than bilateral or multi-agency operational activity or agreement, endorsement of the Council of Ministers, to which the Advisory Authority reports, is sought. Prior to 2019 national ML policies arose from this mechanism. Legislative initiatives have been discussed by subcommittees of the Advisory Authority, considered by the Advisory Authority and presented to the Council of Ministers for endorsement.

72. The Advisory Authority has also established subcommittees to consider projects, such as the establishment of the register of BOs. In addition, the supervisory authorities have established a special technical committee to inform supervisory approaches to AML/CFT, inform implementation of the actions pertinent to them and where appropriate align approaches such as the issue of directives. Input is also provided by the FIU on trends and typologies. Individual authorities also promote initiatives, such as the register of bank payment accounts and safe boxes initiated by the CBC.

73. There have been a series of initiatives which specifically addressed the particular risks faced by Cyprus. The risks in the banking and ASP sectors have reduced (significantly in the case of the banking sector) since the global and economic crisis. This is also due in very large part to strategic decisions taken by the supervisors to take strong counter measures to mitigate the risks in the sectors identified during the crisis, during the NRA process and during day to day supervision. The assessment team attaches significant weight to these collective efforts.

74. Specific measures include the issue by the CBC of guidance in relation to shell companies and tax evasion; upgrading of the CBC's requirements in relation to introduced business; and the CBC's requirements to meet customers who have been introduced to banks and the BOs of legal persons. This package of measures, and the enormous effort required to address the requirements of the special assessment and the action plan agreed with the Troika, represents a significant and successful national commitment to understand and address the risks faced by Cyprus.

75. In addition, measures have been taken in relation to the particular risks of ASPs, for example, the introduction of the ASP Law in 2013 to regulate persons providing administrative services and related matters (including the application of fit and proper standards), requiring all ASPs to be subject to the AML/CFT Law, measures in relation to introducers and reliance on third parties such as the provisions in ICPAC's AML/CFT directive and endorsement by ASP supervisors of the CBC's guidance in relation to shell companies and application of it to ASPs.

76. Measures have been taken by the FIU and the Police to address the risk of ML from foreign proceeds of crime. The FIU updates its reporting guidance to the private sector to reflect the changing risk landscape, issues typologies and provides feedback to ensure reporting is consistent with the risk profile of the country. This has had a positive effect on the reporting patterns by banks. It has also resulted in an increased level of reporting by ASPs although further progress is needed within this sector. The Police have started to shift their focus away from ML related to domestic predicate criminality and targeting stand-alone ML by undertaking various measures described under core issue 1.4. While these measures were implemented close to the date of the assessment and it is too early to assess their success, they are a clear indication that the Police are taking measures to mitigate the risks identified.

77. With regard to FT, several of the goals within one of the four pillars (prevent, protect, pursue and respond) of the 2014 counter terrorism strategy relate to CFT. Under the "protect" pillar there are goals to enhance measures to prevent the misuse of the financial system and nay other networks for the purpose of FT and combat the exploitation of non-governmental organisations for FT. In addition, under the "pursue" pillar there are goals to report and investigate suspicious transactions for FT and to enhance information exchange by improving the cooperation and coordination between national competent authorities. Under the strategy a fusion centre was established to create a forum for regular meetings to ensure timely exchange of information and the development of a quarterly risk assessment. Compliance with the counter terrorism strategy is

monitored by the Ministry of Justice.

78. The Advisory Authority has developed an AML/CFT action plan to address the NRA; this was agreed in 2018. Progress has not been monitored formally by the Advisory Authority (an update to the plan, showing progress in meeting the actions, was provided to the assessment team during its visit to Cyprus) although individual authorities are conscious of what is required of them under the plan and have been working to address the actions. A substantial number of the actions have been addressed. Positive measures which have been undertaken in fulfilment of the action plan or otherwise to address risks include: the provision of more sophisticated requirements for banks, including more recently the requirements removal of reliance on introducers, the setting up of an office within the Police to expedite the execution of mutual legal assistance requests from foreign authorities and harvest intelligence. Some matters relevant to addressing the plan's actions have been raised by the CBC at Advisory Authority level such as the CBC's issue of guidance on shell companies, and trends and typologies.

79. More recently, the Advisory Authority has developed a national AML/CFT strategy, which was endorsed by the Council of Ministers in March 2019. This strategy complements the counter terrorism strategy and includes: minimise the threat and further strengthen supervisory processes in the banking sector; upgrade the supervisory processes of ASPs; upgrade the structure, training and capacity of investigators and prosecutors; build on international cooperation procedures and systems; improve data collection and statistics procedures; enhance supervisory processes and procedures in other sectors; increase transparency of legal persons and arrangements; enhance CFT measures; and monitor the implementation of the planned anti-corruption measures.

The Advisory Authority has been active, meeting 16 times during 2016 to 2018. Coverage of issues has included not only the development of legislation and the registers mentioned above but also, for example, shell companies, the Panama Papers and actions taken, the designation of new supervisory authorities and the organisation of training seminars.

### *2.2.3. Exemptions, enhanced and simplified measures*

80. A limited exemption from some CDD requirements (identification and verification of identity requirements) exists in relation to electronic money. This is subject to conditions, namely that the obliged entity has determined that the risk is low; ongoing monitoring of transactions and business relationship is carried out for the purpose of identifying and reporting suspicious transactions; the payment instrument is not reloadable or has a maximum monthly limit of payment transactions of EUR 250; the payment instrument is used for payment transactions only within Cyprus; the maximum amount stored electronically does not exceed two EUR 250; the payment instrument is used exclusively for the purchase of goods or services; the payment instrument cannot be financed with anonymous electronic money; and redemption in cash or a cash withdrawal of the monetary value of electronic money does not exceed EUR 100.

81. While the exemption has been directly transposed from the 4th AML Directive, the NRA includes some consideration of the risk of electronic money and concludes that it presents a low risk in Cyprus. No financial intelligence such as STRs or other information suggests that the limited exemption is other than low risk.

82. FIs and DNFBPs are required to apply enhanced due diligence measures in the following circumstances: when dealing with natural persons or legal entities established in high risk third countries identified by the European Commission (EC) as high risk or identified by the FI or DNFBP as high risk; with respect to cross-border correspondent relationships with a third-country respondent institution; in relation to national and foreign PEPs; and in other cases that present a high risk of ML/TF. In addition, the AML/CFT Law also provides a list of factors for potentially high risk situations that a FI or DNFBP must take into account when assessing risk. These risk factors cover many of the risks identified in the NRA. Although obliged entities are not expressly required to take into account the higher risks identified in the NRA, the list of factors of potentially higher risk situations cover the higher risk areas identified in the NRA (e.g. introduced business, use of nominee shareholders/directors, etc).

83. Under the AML/CFT Law, a FI or DNFBP is permitted to apply simplified due diligence (SDD) measures, provided that it has previously ensured that the business relationship or the transaction presents a lower level of risk, and provided that the obliged entity carries out sufficient monitoring of the business relationship and transaction and business relationship to enable detection of possible unusual or suspicious transactions. The law also provides a list of factors for potentially lower risk scenarios. These scenarios have been transposed from the 4th EU AML directive and largely reflect scenarios which have been in place in Cyprus for some years without concern. While a comprehensive assessment has not been carried out beyond consideration of the impact assessment of the European Commission, the scenarios are consistent with the NRA and issues have not arisen in relation to them. In any case, the scenarios are permissive and may only be used after risk assessment by institutions and a substantiated conclusion that SDD is applicable in each case.

84. In practice, the factors to be taken into consideration when applying enhanced and simplified measures are consistent with the results of the NRA.

85. The assessment team also considered the extent to which there might be situations in the investment sector where a firm such as a financial intermediary is the registered owner of shares or units in a collective investment scheme and is acting on behalf of and pursuant to instructions from third parties. This arrangement is well described in European Supervisory Guidelines. While such situations were not formally considered as part of the NRA process, CySEC was well aware of the EU-level guidance on this matter and customer relationships with these characteristics are extremely limited.

### *2.2.4. Objectives and activities of competent authorities*

86. The national AML/CFT strategy and the action plan developed on the basis of the results of the NRA, serve as policy tools which shape the objectives and activities of competent authorities. The strategy, which is endorsed by the Council of Ministers, is an expression of Cyprus's political commitment to implement an effective AML/CFT system. The action plan contains twelve overarching themes each including specific corrective actions by the relevant authorities to address identified weaknesses and a timeline for their implementation. At an institutional level, the activities of competent authorities are governed by a strategy which is generally consistent with evolving risks and address the risks identified in the NRA.

87. The Police strategy for the years 2019 to 2021 comprises five pillars, which include combatting terrorism and radicalisation and combatting serious and organised crime. The activities under the latter pillar concern in particular actions aimed at combatting organized crime and corruption, combating of economic crime (including ML), systematic action against narcotic drugs, combating cybercrime and combating trafficking in human beings. These offences correspond to the highest threats identified in the NRA. The strategic plan also places an emphasis on strengthening the mechanism for the tracing, seizure and confiscation of proceeds of crime and international cooperation. On the basis of the strategy, measures have already been taken to enhance financial investigations, identify and investigate the laundering of funds originating from foreign predicate criminality and expediting international cooperation. The setting up of the Office for the Handling and Execution of MLA Requests is a clear example of evolving objectives to meet specific risks. Ongoing investigations into possible complicity by ASPs with criminals for criminal purposes and into foreign persons who have acquired Cypriot citizenship under the CIP demonstrate that the Police are increasingly focussing on the highest risks. The adequacy of these measures is assessed under IO 2, 7 and 8.

88. The FIU has focussed its attention to three particular areas identified in the NRA as a vulnerability in the national implementation: improving the quality of STRs, increasing the number of disseminations to the Police and enhancing the framework for the seizure and confiscation of proceeds of crime in cooperation with the Police and the Prosecutor's Office. To achieve these aims, among other activities, the FIU has: issued guidelines to the private sector to assist them in submitting better quality reports, provided training to the Police, prosecutors and the private

sector; initiated a recruitment process[16] to enlarge the analysis department as a measure to boost the number of disseminations to the Police; and has issued guidance and circulars for the Police and prosecutors on seizure and confiscation, as well as on stand-alone ML offences. The FIU's work plan includes the drafting and dissemination of more strategic reports for submission to other authorities and the private sector. The important role of the FIU in co-chairing the Advisory Authority will continue, since the FIU has, from its establishment, a central role on policy and coordination issues within this Authority which is the appropriate forum for co-operation and co-ordination among the FIU, Ministries, Police, Supervisory Authorities and the Private sector.

89. The Customs Department has a strategic plan for the period 2017 to 2019, one of the objectives of which is cooperation with competent authorities on security and safety matters related to terrorism. It follows the EU Handbook of Guidelines on Cash Controls, which places importance on AML/CFT issues related to the movement of cash. Customs is cognisant of the issues potentially giving rise to ML/TF associated with cross border movements, particularly regarding cash. It applies effective measures, and these are generally consistent with the risks.

90. Most supervisors are in the process of addressing the specific measures set out in the AA's action plan in order to strengthening the supervisory framework. In 2018 the CBC established a strategic plan with five pillars, including safeguarding a sound financial system, increasing trust in the financial system, enhancing the CBC's role in international organisations and fora.

91. All three FI supervisory authorities use risk-based approaches to focus AML/CFT programmes. The models used by the CBC for banks and CySEc are the most robust. The supervisory measures being taken by CBC and CySEC are broadly in line with the risks present in the country. The CBC has a strategy for the period 2019 to 2021. It has five pillars, including safeguarding a sound financial system and increasing trust and respect in the financial system. The safeguarding of the financial system is regarded as aligned with the FATF standards. Each department has specific objectives within the overall strategy and the AML/CFT department's plan includes ensuring a high level of compliance by supervised entities and enhancing international and national cooperation and coordination. The CBC's supervisory measures have been driven by external and internal assessments of risks and the NRA action plan. CySEC has a multi-annual strategic plan to establish the Cyprus securities market as one of the most secure, reliable and attractive investment destinations. Within the plan there are strategic objectives, which include improvement of the regulatory framework, maintaining high levels of compliance by supervised entities, and upgrading and streamlining CySEC. The objective on compliance explicitly includes implementation of the AA's action plan. Projects undertaken have been developed on the basis of the NRA, and AML/CFT strategy and action plan. This has included an emphasis on AML/CFT (such as the development of the risk-based supervision framework, improvements in the quality of data/statistics received and developments in relation to risk assessment).

92. All DNFBP supervisory authorities, are seeking to meet the action plan issued by the Advisory Authority. ICPAC operates within a strategic plan for the years 2019 to 2021, which includes objectives for strengthening the role, reputation and credibility of the Institute and strengthening organisational structure and efficiency of the Institute. Goals have been set under each objective, which include reinforcement of the AML/CFT supervision team; the introduction of advanced IT systems to facilitate more sophisticated risk based models and checks on licensees and their controllers; the introduction of an AMLCO examination; a new sanctions policy; the improvement of statistical information; implementation of the actions emanating from the NRA project; and cooperation with all stakeholders for the benefit of the country's reputation and economic growth, with particular emphasis on AML and compliance. CySEC's strategic approach is referred to above. The CBA has a strategic plan to reinforce its presence as a supervisory authority and enhance supervision and the effectiveness of measures applied by its members. It is based on three pillars, namely training, licensing and a risk-based approach. Objectives include the establishment of a policy for sanctions; installation of more developed systems for statistics and

[16] Which was completed shortly after the on-site visit.

data; establish more stringent criteria for AMLCOs; strengthen cooperation with other supervisory authorities; and recruit employees to strengthen the CBA as a supervisory authority.

93. The Real Estate Registration Council was established in 2018. It conducts inspections, although its programme is not risk based. The Casino Commission also became operational in 2018; there is only one casino and onsite inspections have been carried out to a limited extent.

### *2.2.5. National coordination and cooperation*

94. The Advisory Authority is a long-standing body which serves as the main coordination mechanism for the development and implementation of AML/CFT policies and activities at national level. It is co-chaired by the FIU and the MoF, and comprises all relevant AML/CFT stakeholders (see c. 2.3). It meets regularly, three or four times a year, or more if the need arises. The Advisory Authority advises the Council of Ministers on AML/CFT matters; the Council has followed the advice provided by the Advisory Authority. It has been the catalyst for the legislative proposals and structural changes necessary to enhance the AML/CFT system.

95. In recent years, the Advisory Authority has been instrumental in undertaking work to transpose the latest EU instruments, co-ordinating the NRA process and proposing the adoption of a national AML/CFT strategy to the Council of Ministers. In addition, it has overseen the development, though not the monitoring, of an action plan based on the outcome of the NRA. It has also engaged in proactive engagement on topical issues, most recently meetings with the Minister of the Interior to discuss issues concerning the CIP programme. The work of the AA would benefit from more focus on the proactive monitoring of actions taken to meet the action plan and the risk-based approaches of the authorities and how these are consistent with addressing national risks. It has not considered the risk implications of the CIP to a significant extent and plans for future developments, such as the expansion of the casino.

96. The FIU coordinates the Advisory Authority in practice and occupies a central role within the AML/CFT system; it undertakes significant engagement with the other authorities. This role has been a significant positive influence for the development of the system. Both Co-Chairs of the Advisory Authority meet routinely with other authorities to take forward the Authority's work.

97. At the operational level, co-operation is underpinned by provisions in the AML/CFT Law and MOUs. A memorandum of understanding exists between all financial sector supervisors. All supervisors (including those of DNFBPs) have set up a Special AML/CFT Technical Committee to develop common supervisory practices on the implementation of AML/CFT requirements, the discussion of issues arising from FATF and EU requirements which need to be addressed consistently, the coordination of AML/CFT supervisory activities and training for supervisory staff and staff of supervised institutions. This committee was first established by the FI supervisory authorities in 2010; it was extended to cover DNFBP supervisors in 2013. It is chaired by the CBC and meets at least quarterly. During the period under review the committee has considered common supervisory practices and methods of implementation of supervisory practices, coordination of supervisory activities, the NRA, and the delivery of training to officers of supervisory authorities and licensed entities. The committee has demonstrable benefit in bringing the authorities together routinely and in facilitating prioritisation and joint approaches. It supports the frequent contact between the supervisors at operational level.

98. Practical arrangements also facilitate cooperation. For example, officers of the Police and the Customs Department are seconded to FIU. The FIU has direct access to various databases held by other public authorities (see R. 29). In addition, an internal affairs service has been established within the Police, inter alia to investigate potential corruption within the Police; the competencies and powers of the service are subject to the direct supervision of the Attorney General. The authorities as a whole, not only the supervisory authorities, also cooperate in relation to the provision of training. By way of illustration: FIU regularly holds joint training with the Police and prosecutors and provides guidelines on ML/FT and confiscation; ICPAC provides annual training to the Police in relation to forensic accounting investigation, fraud investigation and financial interrogation techniques; and the CBC and FIU provide training together for the private sector.

99. Cooperation on both ML and FT between authorities is strong and there are very good examples of bilateral and multilateral cooperation between the authorities, both at the policy level (for example, the NRA and the work of the Advisory Committee), dealing with international issues which arise and the operational case level (including in relation to the CIP). The FIU receives full cooperation, and cooperation between the LEAs and the FIU and between supervisory authorities is particularly good. By way of illustration, the FIU and the Police work closely together on investigations and it has worked closely with the Police and prosecutors on freezing orders and with the Attorney General and prosecutors on policy and guidance on freezing orders, the FIU seeks information from foreign FIUs to assist the Police, for example, to seek to trace and freeze assets abroad. Close cooperation also exists between the FIU and the Tax Department; as part of this there is a dedicated liaison officer within the Tax Department for matters involving the FIU. The same cooperation and liaison arrangement apply in relation to the Cyprus Intelligence Service. In addition, the FIU has provided information to supervisory authorities on potential violations of preventive measures.

100. There is also strong co-operation within the Police, and between the Police and other authorities such as the CIS, Customs, FIU and the Tax Department. For example, the Police and Customs have a Memorandum of Understanding (based on an EU model) which sets out the co-operation and the operational arrangements between the two agencies, there are Police officers seconded to customs, and there are instances of joint operations.

101. In addition, there is strong operational cooperation within the supervisory community. For example, the CBC has provided information to the CBA, ICPAC, CySEC and the ICCS in relation to issues/cases where there are licensees in common (for example the CBC has invited members of ICPAC to participate in an onsite inspection) and the three ASP supervisors (ICPAC, CySEC and the CBA) have shared information on applications for licences. Supervisors have also been cooperating with other authorities. By way of illustration, the CBC and the Police have worked together on cases, including the FBME case and CySEC has provided close cooperation with the FIU and the Police in providing expert assistance and proving representatives to be expert witnesses.

102. Cyprus has mechanisms in place to coordinate national efforts in combatting the proliferation of weapons of mass destruction and some aspects of PF; the National Committee for the Implementation of the Convention on the Prohibition of Chemical Weapons and the Committee on Export Control of the Ministry of Trade and Industry. More specifically, action is coordinated through the Coordinating Unit to Combat International Terrorism, which was set up for the purpose of coordinating the activities of the relevant Ministries and Departments in the fight against terrorism and in the suppression of illegal activities, but also co-ordinates the combating of trafficking of harmful chemical substances and dual-use goods. There are also two bodies dealing specifically with aspects of PF-related TFS. The first is the Advisory Body on Financial Sanctions[17], set up by the Council of Ministers and chaired by the MoF dealing with (1) requests for the release of funds and financial resources falling within the exceptions/derogations provided for in the relevant resolutions and decisions of the UNSC and the EU and (2) the notification via the MFA of the release of funds and financial resources to the relevant UNSC Sanctions Committees, as well as the European Commission and EU Member States as necessary. The other body is the Unit for the Implementation of Sanctions in the Financial Sector[18], which is chaired by the MoF and deals with the examination of requests pertaining to UN and EU restrictive measures that fall within the financial sector.

103. In addition, the Advisory Authority also serves as a platform for the discussion of PF issues, since the public authorities with ML/TF competences also deal with PF-related matters. However, discussions on PF issues at the Advisory Authority have been around the implementation of TFS in

[17] Membership includes representatives of the MoF, the FIU, the MFA, the CBC, CySEC, the MJPO and the Ministry of Energy, Commerce, Industry and Tourism, which includes both the Company Registry and the Trade Services (Imports/Exports Licensing Section)

[18] Membership includes representatives of the Ministries of Finance, Foreign Affairs and Energy, Commerce, Industry and Tourism, the AG's Office, the CBC and CySEC

general, without necessarily distinguishing between TF and PF as subjects of competent authorities' concern. The Ministry of Energy, Commerce, Industry and Tourism, which issues export licences for dual use goods and military equipment, is not a member of the Advisory Authority, and has therefore not contributed to the development of PF-related policies. Information from individual competent authorities on activities in their area of competence which are relevant to PF has not been discussed at the Advisory Authority. Overall, a more active and joined up approach, intelligence and information-sharing on PF is needed.

### *2.2.6. Private sector's awareness of risks*

104. The private sector was involved to an appropriate extent in the elaboration of the NRA through a data collection exercise and the participation of various associations and professional bodies representing FIs and DNFBPs in some of the working groups. Most private sector representatives met onsite were aware of the contents of the NRA and confirmed their participation in the NRA.

105. A concise version of NRA report was published in November 2018 and is accessible on the MoF website. Following the publication of the document, the NRA report was communicated to all the members of the Advisory Authority and other relevant competent authorities. All supervisory authorities except for the Real Estate Registry Board and the Casino Supervision Commission, circulated the concise version of the NRA to the private sector. This was confirmed by the private sector entities interviewed on-site.

106. Some authorities took additional actions in relation to dissemination of information about the NRA. The CBC has advised compliance officers of all licensed institutions of the results of the NRA at two meetings. ICPAC has notified its licensees in writing of the results and required its licensees to incorporate the NRA in their risk assessments; in their annual report compliance officers have been required to confirm their understanding of the NRA and of its incorporation in risk assessments. The NRA is also referred to in onsite inspections and routine contact with licensees. The CBA increases awareness of the NRA through it onsite inspection programme. CySEC has also notified its licensees of the results of the NRA and conducted outreach through meetings and circulars.

107. Looking more widely at the dissemination of information, the CBC has provided further risk information to its licensees by presenting the results of the EU Supranational risk assessment to all its licensed institutions at the meetings referred to above.

*Overall conclusions on IO.1*

108. **Cyprus is rated as having a substantial level of effectiveness for IO.1.**

## 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

### *3.1. Key Findings and Recommended Actions*

**Key Findings**

**Immediate Outcome 6**

1. The Police have frequently accessed and made effective use of financial and other information to further their investigations into domestic, and some foreign, ML, associated predicate offences, and FT.
2. Until 2018, the Police did not make extensive use of intelligence generated by the FIU as expertise was not significantly developed. Conscious of this shortcoming, measures were implemented by the Police, and, as a result, the use of FIU intelligence saw a healthy increase in 2018.
3. Very few of the investigations initiated on the basis of FIU intelligence relate to stand-alone and third-party ML related to foreign predicate criminality. This is not in line with the risk profile of the country as an IFC.
4. No concrete action has been taken by the Police in relation to the strategic reports produced by the FIU.
5. Many STRs submitted by banks contain relevant and accurate information and are in line with the risks that Cyprus faces. A good portion have resulted in either an investigation domestically or served as a catalyst for the FIU to disseminate spontaneous information to foreign FIUs.
6. The low level of reporting by ASPs and the real estate sector raises concern.
7. The FIU has the ability to conduct multi-layered analysis of sophisticated ML cases involving the use of complex corporate structures spread over different jurisdictions, multiple bank accounts and extended ML networks.
8. As a matter of good practice, the FIU spontaneously disseminates complete analysis packages to foreign FIUs that have proved to be critical in securing a conviction/confiscation abroad.
9. The significant increase in STRs has put a strain on the limited human resources of the FIU and may have, to a certain degree, had an impact on the analysis and dissemination function.
10. There is a good level of cooperation between the FIU and the other competent authorities, especially on an informal basis.

**Immediate Outcome 7**

1. The majority of ML investigations and prosecutions are generally parallel to domestic predicate offences, and for self-laundering, which is not fully consistent with the jurisdiction's risk profile as an IFC. Very few ML investigations have been harvested from incoming MLA. However, the number arising out of SARs referred to the Police has seen an appreciable improvement and the jurisdiction has demonstrated that it is increasing its efforts to investigate possible ML, including that with a foreign element, from sources such as MLA and SAR disseminations.
2. The authorities appear to be well resourced to tackle financial crime, in particular with the creation of the Economic Crime Investigation Office and specific Economic Crime units in Limassol and Nicosia. However, the expertise within the police generally to deal with ML investigations may still be said to be in its infancy but the experience of some cases so far are helping to further the development of this

expertise.

3. Cyprus is developing and improving its approach to carrying out financial investigations and/or ML investigations, yet there are no specific written guidelines on what indicators to consider before initiating a financial investigation.
4. Notwithstanding the expectancy for more third-party, stand-alone ML prosecutions, particularly as regards foreign proceeds, the jurisdiction has a reasonable record as regards pursuing ML in relation to domestic criminality, albeit on the modest side if compared to the number of convictions for high-risk predicate offences. Within those convictions, Cyprus has had some good examples of tackling financial crime and going after the money, for example in fraud, drug trafficking and corruption cases.
5. The jurisdiction has taken, and is continuing to take, steps to meet the aims of increasing its ML investigations and prosecutions (qualitative as well as quantitative) by way of enhancing resources and training, and also the creation of the Office for the Execution/Handling of MLA Requests set up to mine incoming requests for domestic investigations.
6. The jurisdiction has encountered at least one instance of failing to achieve a stand-alone ML conviction without a predicate offence also being identified and proven. The result of this case and the impression formed from meeting some members of the judiciary on-site was that this prior identification and proving of the predicate offence was required. However, the authorities have taken steps to address this by way of an amendment to the AML/CFT Law and are taking additional steps through increased seminars for the judiciary and guidance issued through the FIU to the prosecutors and police, which resulted in more stand-alone cases being investigated and prosecuted.
7. ML has generally been prosecuted together with its underlying predicate offence and the sentences are served concurrently, and therefore the ML sentence is often subsumed within the sentence for the predicate. There are however some good examples of the ML sentence being more punitive than the predicate, showing a recognition by the prosecutors and judiciary of the seriousness of ML, even when it is a bolt-on to a predicate.

**Immediate Outcome 8**

1. In the review period, Cyprus has frozen EUR 115 Million and confiscated some EUR 13 million in total, including the enforcement of foreign confiscation orders. This overall figure is encouraging and not insignificant for a jurisdiction the size of Cyprus.
2. The FIU plays a significant role in executing the requests from other jurisdictions regarding the confiscation of foreign proceeds held in Cyprus. Given the risk profile of Cyprus, there is an expectancy for more proactive freezing and confiscation of foreign proceeds (without the prior trigger of a foreign request for assistance). In some instances, the Cypriot Authorities on their own initiative have however informed foreign counterparts of the existence of proceeds/equivalent property and have provisionally frozen such property pending the receipt and execution of an MLA Request.
3. The confiscation amounts have varied and there are appreciable gaps as compared to the value of assets frozen.
4. When the Police conduct financial investigations, they conduct the investigation in a

wide manner, following trails and looking at associates/connected persons, and not just narrowly focussing on the principal. They have relatively convenient access or direct access to central registries and may apply for disclosure and/or production orders.

5. As mentioned under IO 1, there is generally strong co-operation amongst the law enforcement authorities (including the FIU which has some limited quasi-law enforcement competencies), enhanced through many examples of secondment arrangements and the ad-hoc formation of Joint Investigative Teams.
6. The recovery rate for assets confiscated is particularly strong.
7. As the jurisdiction does not have physical borders per se, the jurisdiction is in a better position to control its frontiers at its ports (sea and air). The authorities apply strong procedures and controls at the "green line", in addition to the declaration system.
8. There are more confiscations regarding undeclared cash leaving the jurisdiction, which is not particularly in line with the profile of an IFC.
9. The Customs authorities apply effective measures by monitoring movements including potential smurfing, by referring matters to the FIU where there are ML/TF suspicions, and by compounding offences to confiscate the amounts when the context of the case allows for it. However, the figures provided showed a wide variation in the confiscation amounts and in some cases the amounts do not appear particularly punitive.
10. Despite there being no declaration/disclosure requirements for cash above 10,000 EUR for mail/cargo, the customs authorities nonetheless monitor mail/cargo appropriately and have demonstrated this by way of a recently uncovered large amount of cash thought to be proceeds of crime which were concealed in children's toys.

**Recommended Actions**

**Immediate Outcome 6**

1. The Police should continue developing its expertise to effectively handle complex analysis cases generated by the FIU.
2. Priority should be given by the Police to those cases disseminated by the FIU which relate to the laundering of foreign proceeds of crime in Cyprus.
3. Concrete action should be taken by the Police in relation to the strategic reports produced by the FIU.
4. The authorities should continue taking measures to improve the quality and quantity of both ML and FT STRs, especially in the ASP and real estate sectors.
5. The FIU should take measures to further enhance its analysis and dissemination functions: automate aspects of the prioritisation system; implement a more sophisticated case management system; assess whether the number of STRs under analysis is appropriate in proportion to the number of STRs received; complete the recruitment process of 5 new analysts to reinforce the Analysis Department ; produce strategic analysis reports on a yearly basis; increase the dissemination rate of reports to the Police and other competent authorities.

**Immediate Outcome 7**

1. Cyprus should be more aggressive in proactively pursuing all types of ML and particularly regarding foreign predicate proceeds, instead of merely adopting a

reactive approach to investigate ML parallel to domestic predicate criminality.
2. The efforts already shown in exploring and harvesting all existing avenues of potential identification for ML, including disseminations from the FIU and incoming MLA, should continue and be enhanced further.
3. It is recommended that clear guidelines are issued by the Police to clarify when the Police should initiate an ML investigation, and on what basis the Crime Combating Department/Economic Crime Investigation Office should be consulted or be required to take over the case.
4. The authorities should also ensure the Police are fully equipped, resource-wise, to investigate more sophisticated and complex ML.
5. The continued and systematic early involvement of the prosecutors in investigations of ML is to be encouraged given their expertise and their invaluable input into the sufficiency of evidence, and the prospects of success.
6. The issue regarding the need to identify and prove the predicate offence in stand-alone ML cases is one which the authorities should monitor very closely now that the AML/CFT Law has been amended and consider the further seminars to be given with the judiciary, and the actions to be taken by prosecutors in court, to ensure that this issue has been remedied.
7. The statistics on prosecutions should be better recorded, in terms of the bare numbers and also on the underlying predicate offences.

**Immediate Outcome 8**

1. Where financial investigations are to be carried out at local level, or by the separate central units such as the Drug Law Enforcement Service or the Operations Office, the authorities should ensure these units have sufficient resource and capacity for this.
2. Cyprus needs to increase the overall number for freezing and confiscation generally, but specifically it should proactively pursue, on its own initiative, more financial investigations regarding foreign criminality proceeds, and then tracing, freezing and confiscating such proceeds or their equivalent value property. Such property should also proactively be repatriated to the originating jurisdiction.
3. Cyprus is encouraged to explore the benefits of utilising its non-conviction-based forfeiture regime more regularly and amending legislation to remove practical obstacles to its effectiveness.
4. Consideration could be given to a permanent asset management unit, particularly if the jurisdiction begins to target more complex assets and legal structures.
5. More dissuasive penalties or confiscations when compounding the offence should be imposed for false/failed declared cash, where there is a suspicion of ML/TF.
6. Cyprus should introduce a declaration system for cash/BNI in excess of €10,000 entering or leaving the jurisdiction by way of mail or cargo, as otherwise this may hamper the effectiveness of detecting ML/TF in significant cash movements through such means of conveyance. Additional technical changes which are recommended are increasing the maximum penalty for false/failed declarations and empowering customs officers to stop/restrain cash where there is a suspicion of ML/TF (without there necessarily being a false/failure offence).

109. The relevant Immediate Outcomes considered and assessed in this chapter are IO.6-8. The Recommendations relevant for the assessment of effectiveness under this section are R.1, R. 3, R.4 and R.29-32.

## *3.2. Immediate Outcome 6 (Financial Intelligence ML/FT)*

### *3.2.1. Use of financial intelligence and other information*

Access and use of financial information

110. The Police access financial and other information fairly frequently in the course of their investigations through court disclosure orders. There are no legal or practical restrictions to the Police's access to information. The Police seek information from a wide variety of sources throughout a criminal investigation. In particular, the Police acquire banking, beneficial ownership and other CDD information from banks, ASPs, lawyers and accountants. Information is requested from the CBC on licenced entities, the Land Registry on real estate property, including purchase agreements deposited with the Department, the Tax Department on tax declarations and VAT information, the Registrar of Companies on company information including financial statements of companies, the Social Insurance Services on the income/salary of individuals and other financial information with respect to companies/individuals acting as employers, the Customs Department on cash declarations and other taxes, the Cyprus Stock Exchange (CSE) on CSE listed companies, the Civil Aviation Department on the ownership of aircrafts and the Merchant Shipping Department on the ownership of vessels. Information is also sought from foreign counterparts both formally and informally (see IO 2).

111. The Police have direct immediate access to the following governmental databases: database of temporary vehicle imports of the Customs Department; database of the Road Transport Department on the owners and details of motor vehicles, driving licenses including professional driving licenses, insurances and road taxes; database of the Registrar of Companies and database of the Civil Registry and Migration Department, including data concerning entry/exit.

112. Information-gathering is part of Police's daily work and has been used in numerous serious cases (see all case examples under core issue 6.1 and 7). The Police provided some statistics on disclosure orders, all of which relate to ML and associated predicate offences, except for 3 which relate to FT. There are no other statistics available but upon a review of case-examples furnished by the Police, the assessment team was satisfied that all types of information are obtained, according to the needs of the investigation.

**Table 4: Disclosure orders**

| **Police statistics** | | | | | | |
|---|---|---|---|---|---|---|
| | **2013** | **2014** | **2015** | **2016** | **2017** | **2018** |
| **Disclosure orders** | 127 | 160 | 124 | 106 | 105 | 174 |

113. A case example on access and use of information by the Police is presented below:

**Box 6.1: Access and use of information by the Police**

The case related to corruption offences committed by the President, members, the director of the Sewerage Board of Paphos (CIPA) and other persons in the tendering process for the renovation of the Paphos sewerage system.

During the corruption-related investigation, a large volume of data and information were obtained by the Police from banks, the Land Registry, Tax Department, Registrar of Companies and the Road Transport Department. The data and information were obtained on the basis of court disclosure orders. On the basis of an examination of financial and other information, it was concluded that the members of the sewerage board of Paphos had received bribes from applicant companies. The data and information was also used to trace and identify the proceeds of crime.

Seven persons were prosecuted before the Assize Court for the offences of Conspiracy to commit felony, bribery, abuse of power, corruption, illegal acquisition of property benefits by officials and public servants and money laundering. Data and information obtained through court disclosure orders proved critical in securing a conviction for all the accused persons. A confiscation court

order was issued for the total amount of EUR 750,000, EUR 371,500 and immovable property.

114. The Police may also obtain information from the FIU which may be of assistance in ongoing investigations of predicate and ML/TF offences as well as the tracing of criminal proceeds.

**Table 5: Requests sent by the Police to the FIU**

| **Police statistics** | | | | | | |
|---|---|---|---|---|---|---|
| | **2013** | **2014** | **2015** | **2016** | **2017** | **2018** |
| **No. of requests** | 17 | 31 | 59 | 53 | 48 | 71 |

115. These would generally include requests to determine whether the suspect is known to the FIU, assistance in asset-tracing and obtaining information from counterpart FIUs. A case example is presented below:

**Box 6.2: Police request to the FIU**

The Police was investigating a case of cyber theft on the basis of a formal complaint made by a Cypriot company involved in wood processing and imports of parquet flooring in Cyprus. In June 2016, unknown persons hacked the e-mail conversation between the Cypriot company and their supplier from Country A. The Cypriot company was provided with misleading instructions to transfer money to another bank account instead of the supplier's. The money was sent to a bank account in Country B. The FIU made an urgent request to Country B to enquire about the bank account. On the basis of these measures, the money was returned to the bank account of the complainant in Cyprus.

116. The Customs Department also accesses information frequently in the course of its work. Apart from the information obtained from the Cash Declarations System, for which it is the competent authority, the Customs Department has direct access to the databases of the Registrar of Companies, the Department of Road Transport, the Criminal Records of the Police and the Cyprus Ports Authority. It also has access to a number of European (AFIS, RIF, Europol-SIENA) and international (Interpol 24/7, WCO-CEN, RILO) databases from which it may obtain financial information. Furthermore, the Customs Department closely cooperates with the FIU, the Police, the Tax Department, the Land Registry and all the FIs in cases involving financial investigations. Requests to the FIU (statistics below) relate to the involvement of physical and legal entities in ML cases or whether they are adversely known to the FIU.

**Table 6: Requests sent by the Customs Department to the FIU**

| **Customs statistics** | | | | | | |
|---|---|---|---|---|---|---|
| | **2013** | **2014** | **2015** | **2016** | **2017** | **2018** |
| **No. of requests** | **4** | **5** | **37** | **26** | **28** | **8** |

Use of financial intelligence

117. While other authorities have the competence and powers to obtain and analyse financial and other information, financial intelligence is largely the preserve of the FIU in Cyprus. It is the structure within the country which has the most expertise to produce the required level and depth of financial analysis on ML, associated predicate offences, and FT. This is not unusual in a country the size of Cyprus. This section, therefore, focuses mainly on the use of FIU financial intelligence by the Police and to a lesser extent by the Tax Department and the Customs Department.

*The Police*

118. The Police is the main recipient of FIU disseminations. Reports are generally received by the Director of the Crime Combatting Department (CCD), who will review the case and determine which Department within the Police would be best suited to take the case forward. The decision could be based either on the complexity of the case, where the Economic Crime Investigation Office would take charge, or issues of territoriality depending on the jurisdiction of the District Police. Statistics on the use of FIU disseminations by the Police are presented in Table 7.

**Table 7: Dissemination by the FIU to the Police and use of FIU intelligence by the Police**

| ML and/or Predicate Offences | | | | |
|---|---|---|---|---|
| | **Dissemination** | **Investigation** | **Prosecution** | **Conviction** |
| 2013 | 10 | Not available | 5 | 3 |
| 2014 | 13 | Not available | 6 | 5 |
| 2015 | 25 | Not available | 3 | 3 |
| 2016 | 72 | 15 | 3 | 2 |
| 2017 | 84 | 20 | 2 | 1 |
| 2018 | 64 | 56 | 0 | 0 |

119. As apparent from the figures in the table, until 2018, the Police did not make extensive use of intelligence generated by the FIU. A simple comparison between the numbers of reports disseminated by the FIU and the investigations initiated by the Police points towards an underutilisation of financial intelligence. There are various factors which have hindered the Police from fully exploiting and maximising the benefits of financial intelligence. Expertise to effectively handle complex analysis cases was not significantly developed at the beginning of the period under review. This was noted as a national vulnerability in the NRA, which concluded that better use by the Police of FIU cases was needed. Furthermore, the large majority of cases viewed by the assessment team involved domestic predicate offences and/or ML. This does not correspond to the main threat identified in the NRA relating to the laundering of foreign proceeds of crime in Cyprus. It was also pointed out that no concrete action is taken by the Police in relation to the strategic reports produced by the FIU.

120. The authorities accept that this area requires major improvement to the extent that the first action item of the NRA action plan calls for better use of financial intelligence. In order to address this point, in 2018, guidance was issued by the Chief of Police to all Police Departments and Units with specific instructions on the handling of STRs. The guidance has already had a positive impact as reflected in the increase in figures for 2018 in Table 17, where 87.5% of reports disseminated by the FIU resulted in an investigation. The authorities have also taken measures to enhance the expertise on the handling of complex cases for example through the creation of the ECIO within the CCD and financial crime units within the districts of Limassol and Nicosia (see IO 7). These measures, in combination, have enhanced the capacity of the Police to use FIU financial intelligence although it is still early to measure their full impact.

121. The Police did provide some case studies which illustrate how, on the basis of a FIU report, they were able to proceed with the successful investigation of a foreign ML and/or predicate offences, enabling the prosecution to eventually secure a conviction (see Box 6.3 below and Boxes 7.1, 7.8 and 7.9 under IO 7).

**Box 6.3: Use of financial intelligence by the Police**

The FIU received a large number of SARs/STRs (approximately 56) from banking institutions in Cyprus, regarding a number of persons as an organized group from other EU countries who were acting in an organized manner to commit internet fraud. In many instances they used forged passports or identity cards and other forged documents. They received small amounts of money from abroad in their bank accounts which were subsequently withdrawn within the same day in cash from ATMs in Cyprus.

The FIU conducted an analysis of the contents of SARs/STRs and additional information from reporting entities. Information was also received from law enforcement which indicated that complaints had been filed to the Police by victims, relating to this organized fraud, which were under investigation by the Police.

The FIU provided the Police with detailed and extensive financial intelligence which was subsequently used for the investigation of the case. All the intelligence and other material submitted by the FIU was considered by the Police and used to obtain court disclosure orders. The information, which included bank transactions, bank documentation and forged documents, was

then used as evidence before the Court to prove the charges.

Two persons, EU nationals, were charged before the Court for conspiracy to defraud, forgery of documents, impersonation, illegal transfer of property and money laundering. They were convicted on 11.5.2018 on all offences and received the highest penalty for the ML offence i.e. 6 years imprisonment.

122. As noted under IO 9, there has been a very limited number of FT investigations (7) in the period under review. Four of these cases were disseminated by the FIU on the basis of STRs. To some extent, the Police demonstrated the ability to make use of this intelligence to initiate investigations as explained under Box 9.3.

*Tax Department*

123. The statistics on FIU disseminations to the Tax Department are presented in the table below. These involve domestic natural and legal persons in relation to cases which may give rise to domestic tax implications not ML. The Tax Department advised that it carefully analyses FIU disseminations and communicates with the FIU requesting further clarifications and/or additional information. The investigation of cases is done by using established audit techniques or any other method considered appropriate in the case.

**Table 8: Disseminations by the FIU to the Tax Department**

| 2016 | 2017 | 2018 |
|---|---|---|
| 20 | 49 | 14 |

124. The end result of such investigations could be an additional assessment of tax and/or criminal proceedings.

**Table 9: Use of FIU intelligence by the Tax Department**

| | 2016 | 2017 | 2018 |
|---|---|---|---|
| Total number of cases | 20 | 49 | 14 |
| Under investigation | 6 | 23 | 11 |
| Examined | 14 | 26 | 3 |
| Result of examination - tax assessment | 0 | 2 | 0 |
| Result of examination - no tax assessment | 14 | 24 | 3 |

*Customs Department*

125. Very few cases have been disseminated to the Customs Department. Whenever the Customs Department receives disseminations from the FIU, they are investigated according to the circumstances of each case and always in combination with the intelligence kept by the Customs and/or obtained from the Police.

**Table 10: Disseminations by the FIU to the Customs Department**

| 2016 | 2017 | 2018 |
|---|---|---|
| 1 | 2 | 1 |

126. The Customs Department provided a brief outline on how financial intelligence was used to further its investigations in the four cases received from the FIU.

**Box 6.4: Use of financial intelligence by the Customs Department**

Case 1 (2016): The FIU disseminated a case concerning a specific sale of products effected by a Cypriot to a foreign company and requested verification of the customs clearance of the goods and

whether the goods were accompanied by export license. Upon investigations carried out by the Department of Customs it was verified that the Cypriot company was registered in the Customs Registry for customs clearance. However, there were no imports or export recorded in the name of the said company.

Case 1 (2017): The FIU disseminated a case related to transactions involving trade in cars conducted by a retired civil servant. The case was investigated, and a disciplinary inquiry was initiated in cooperation with the Attorney General's Office. The Attorney General's Office determined that there was insufficient evidence to institute criminal proceedings.

Case 2 (2017): The FIU received a report from a foreign FIU regarding the sale of counterfeit vehicle parts through the internet in which a Cypriot citizen was involved. Due to limited information available, the case is still under investigation.

Case 1 (2018): The FIU disseminated a case involving suspicious transactions of a Cypriot registered company. The aforementioned company conducted banking transactions for which the supporting documentation was suspected to be falsified. Following enquiries carried out in the databases of the Customs Department, no relevant information was found either in relation to the company or in relation to its beneficial owners. The Police and the Tax Department were informed accordingly in writing for possible actions.

### *3.2.2. STRs received and requested by competent authorities*

127. To a reasonable extent, competent authorities receive reports from the private sector which contain relevant and accurate information that assists them to perform their functions. In determining relevance and accuracy, the assessment team considered factors such as (1) volume and quality of STRs received; (2) the categories of reporting entities submitting STRs; (3) the number of STRs subject to further analysis by the FIU; (4) the number of STRs used in an investigations; (5) the circumstances (indicators) giving rise to the STRs; and (6) whether the STRs correspond to the main risks that Cyprus faces (in terms of volumes of funds, underlying predicate offences, resident and non-resident legal and natural persons involved, typologies, trends and patterns, etc).

128. The total number of STRs has followed a constant upward trajectory in the period 2013-2018, with a slight dip in 2014. In 2018, the FIU received 1818 STRs, more than twice the number of STRs received in 2013, which was 820. This is a positive trend which the authorities partly attribute to the implementation of an electronic reporting tool and ongoing updates to reporting guidance. According to the authorities, the overall quality of these reports has also reportedly improved as a result of closer scrutiny applied by private sector entities, particularly banks, targeted training by the FIU and supervisors and FIU guidance and feedback on reporting. It was also noted that defensive reporting has reduced significantly over the years. The authorities acknowledge that further improvement is needed within certain sectors.

129. As shown in table below, most STRs were submitted by the banking sector, which is the most material sector in Cyprus, followed by MSBs, and investment firms. The level of reporting by ASPs, which is another very material sector in Cyprus, has improved over time. However, given the risks faced by this sector and compared to the number of ASPs operating in Cyprus (over 2,000), the total number of reports from this sector (262 over a period of five years) raises concern. The same could be said of real estate agents, which have filed just one STR, considering that real estate is known to have been used to launder funds in some cases. Reporting by other FIs and DNFBPs in some cases is low or non-existent. The FIU is broadly satisfied with the overall increase in the number of STRs, though no detailed assessment has been conducted to determine whether the reporting level of the higher risk categories of reporting entities is adequate.

130. Reporting by MSBs sector experienced a sharp increase in 2016 (from 18 to 544). According to the explanations given by the country, these numbers have unusually increased because of stricter policies adopted by a large MSB with a worldwide presence. However, these mostly relate to predicate offences (e.g. customer being defrauded). Increased training of agents on detecting

suspicious transactions is also said to have had an impact on the larger volume of reports. The assessment team encourages the FIU to monitor the situation and take steps to reverse this trend, since the overload of these type of reports, which may contain very little valuable information, can adversely impact the resources of the FIU which are already stretched. It is positively noted that the FIU has adopted an expedited analysis procedure to deal with these cases.

**Table 11: STRs by reporting entity**

| | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|---|
| **Banks** | 629 | 547 | 695 | 797 | 701 | 553 |
| **Insurance sector** | 0 | 2 | - | - | - | 2 |
| **Securities sector** | 77 | 2 | 5 | - | - | - |
| **Investment firms** | 8 | 5 | 45 | 72 | 135 | 170 |
| **Cooperative Banks** | 34 | 22 | 40 | 39 | 36 | 36 |
| **Card Payments** | 12 | 3 | 4 | 7 | 4 | 3 |
| **MSBs** | 18 | 12 | 18 | 544 | 402 | 623 |
| **FOREX** | - | - | - | 5 | 21 | 5 |
| **Other (Paypal etc)** | - | - | 45 | 56 | 44 | 219 |
| **Casinos** | - | - | - | | 2 | 10 |
| **Real estate agents** | - | - | - | 1 | - | - |
| **Dealers in precious metals/stones** | - | - | - | - | - | - |
| **Lawyers** | 22 | 12 | 14 | 15 | 15 | 21 |
| **Accountants** | 4 | 11 | 19 | 21 | 40 | 36 |
| **Auditors** | - | - | - | - | - | |
| **ASPs** | 12 | 40 | 41 | 44 | 55 | 70 |
| **Supervisory Auth.** | 4 | 7 | 3 | 8 | 5 | 4 |
| **Other** | - | - | 7 | 8 | 5 | 7 |
| **Cross Border** | - | - | - | - | 25 | 59 |
| **TOTAL** | **820** | **663** | **936** | **1617** | **1490** | **1818** |

131. Given the materiality of the banking sector, the assessment team analysed the reporting patterns of each individual bank. Statistics were provided to the assessment team on STRs reported by each bank. It is positive that the two largest banks, which account for two thirds of the overall banking assets, regularly submit STRs and are the top reporters. However, when looking at the statistics, it was difficult to make any judgment on whether there has been a positive evolution across the entire banking sector in terms of reporting. The number of STRs has decreased within the sector collectively after 2016. The patterns at institutional level vary year on year, with some banks registering a progressive decrease. The assessment team is not in a position to reach a definite conclusion on whether the total number of STRs submitted by banks, other than the two largest ones, is sufficient. However, the case studies provided by the FIU do demonstrate that the banks have identified many suspicions which have resulted in either an investigation domestically or served as a catalyst for the FIU to disseminate spontaneous information to foreign FIUs (see Box 6.5 below).

**Box 6.5: Bank STRs involving Cyprus/foreign legal persons with foreign BOs and bank accounts in Cyprus**

Case 1: The FIU received an STR in 2018 from a local bank in Cyprus in relation to the account of Company X, registered in Cyprus. The beneficial owner of company X was a foreign national, individual A. An STR from a second Cypriot bank regarding Individual A was also received in 2018.

Individual A was UBO in another Cyprus registered company (Company Y) as described in the second STR. The Cyprus account of company X had a remaining balance of around USD 6.5 million which was frozen. The Unit had received a freezing order from the authorities of another country (Country A) with the aim to confiscate these funds. The banks filed the reports following negative press publications on Individual A which linked him to ML. Additionally, his property had been seized abroad and an MLA Request was received from the Competent Authorities of Country A requesting the freezing of the balance in the local bank accounts of Company X. Individual A was accused and imprisoned on charges of bribery, embezzlement, passive corruption, abuse of public office for private advantage and misappropriation of funds. The MLA Request was received subsequent to an exchange of information between FIU Cyprus and the FIU of Country A. Based on the STR and on the analysis of the financial information contained therein, it was determined that the account of Company X had been credited with amounts from other countries. It had received those funds from a number of foreign companies with accounts abroad and more specifically from accounts maintained in three foreign jurisdictions (Mauritius, Switzerland and Bahamas). The analysis performed also showed that the funds once received in the Cypriot account of Company X were transferred abroad and in particular to the accounts of foreign companies in 7 foreign jurisdictions (UAE, Switzerland, Spain, Italy, Liechtenstein, Mauritius and Portugal) related with company X and company Y, including the personal accounts of Individual A abroad.

Case 2: The FIU received a number of suspicious transactions reports from banks in Cyprus in relation to the accounts of a number of foreign companies that raised suspicions due to the nature and frequency of transactions. When the banks requested justification for these transactions the explanations provided by the clients did not satisfy the banks which filed the STRs. The FIU exchanged information with Country A and provided information on the foreign companies, with foreign beneficial owners, and transactions, unknown to them at that time. Based on information by Country A, it was determined that these companies were related with a company based in Country B which offered unlicensed money transmitting services. According to Country A, the owners of these companies knew that funds relating to a number of financial transactions that were processed by this company originated from illegal activities (such as identity theft, computer hacking, internet fraud, child pornography, trade in drugs) and knowingly processed such transactions. Following exchange of information between the two FIUs, Country A sent a MLA to the FIU in Cyprus, through the MJPO. The court in Country A issued an indictment against this company and against the individuals who were related with the company and who had been arrested in the meantime. The indictment, among others, requested the freezing of the funds in a number of accounts in Cyprus and abroad. The owner of this company pleaded guilty. Following an application by the FIU, the Nicosia District Court issued a freezing order (Order Against the Property of an Absent Suspect), in relation to 25 accounts maintained with three banks in Cyprus by a number of foreign companies. The total sum of the order was EUR 3,799,273.7 and USD 9,566,574.3. Country A sent a supplementary MLA to the FIU and requested the registration in Cyprus of the order which had been issued by the court in Country A. The abovementioned amounts are currently frozen for an indefinite period and will be confiscated once the confiscation order, which has already been issued in Country A, will be registered and enforced in Cyprus.

Case 3: A Cyprus-registered company maintained a business relationship with 2 banks in Cyprus. The company's declared business activities were *«Buy, restore and sell classic cars to private customers».* The declared UBO was a Romanian citizen residing in the UK. A suspicion was raised on 20/07/2018 when the bank received a swift message from a bank in France requesting the return of 8 SEPA transfers amounting to EUR 63,000 credited to the account of the Cyprus registered entity by order of their client XX, claiming that their client had been defrauded. According to information, the victim found an advertisement of a red jaguar belonging to the Cyprus registered company on carandclassic.co.uk website for the price of EUR 63,000 and transferred the aforementioned amount to the account of the said company. However, the victim did not receive the car upon the agreed date and had no information about the carrier. On 02/08/2018 the bank received two swift messages, from a bank in Spain. The subject of the messages concerned the return of two SEPA transfers dated 22/06/2018 and 13/07/2018 for the amounts of EUR 3,150

and EUR 29,000 respectively, by order of their client XXX in favour of the same Cyprus-registered company for the purchase of a car. The ordering client claimed she had been victim of fraud. On 06/08/2018 the bank received another swift message, this time from a bank in the UK requesting the return of EUR 5,607.96 credited to the account of the company under report by order of their client XXXX due to their client being a victim of scam. Based on the swift message, their client paid a deposit for the purchase of a car and arranged a meeting in Cyprus to see it. Nonetheless, nobody showed up at the arranged meeting with the excuse of an accident and since then the victim had no further contact with the beneficiary company. The analysis of the movement of the bank account of the Cyprus-registered company held with the bank in Cyprus showed several incoming payments where for most of them payment details related to the purchase of cars. The funds were further credited to: three natural persons, believed to be accomplices, at their accounts with a bank in Ireland; a bank account of the Cypriot company in the same bank in Ireland. Furthermore, the analysis revealed many cash withdrawals from ATMs in the Slovak Republic, the UK, Serbia and Ireland. As a result, FIU Requests were sent to France, Spain, UK, Ireland and Romania. There are suspicions that the accounts were opened using fake identification documents. The case is still ongoing as FIU Cyprus is still collecting intelligence.

132. The above cases are positive examples of banks reporting in line with the risk profile of the country. Equally, however, since most of the cases reported by banks involve legal persons/arrangements which are generally administered by ASPs, it is surprising that the reporting level of ASPs is not higher. It is of concern that, while banks have been able to identify suspicious activity on the basis of their ongoing monitoring procedures, ASPs have failed to do so in relation to clients common to both types of reporting entity. This would also suggest that, where legal persons/arrangements administered by an ASP do not have a bank account in Cyprus, the likelihood of a suspicious client or activity being identified in Cyprus is lower. The assessment team acknowledges that there has been some improvement in the volume of STRs submitted by ASPs which has increased from 12 STRs in 2013 to 70 STRs in 2018. Nevertheless, given the incidence of suspicious cases involving legal persons/arrangements and the number of ASPs registered in Cyprus (over 2,000), the assessment team considers that reporting by ASPs is still not up to a satisfactory level. This finding also has implications for the adequacy of CDD implemented by ASPs (IO 4) and the intensity of supervision by the ASP regulators (IO 3).

133. Notwithstanding the above, the FIU did provide some good case examples of reports submitted by ASPs. One case example is presented in the box below.

**Box 6.6: suspicious report by ASP**

The FIU received a STR from an ASP in relation to their client, a national from Country A ("Mrs A"), residing in Country A and is the BO of a company registered in Country B ("Company A"). She was also the authorised person for a company registered in Country C ("Company B"). The suspicions involved negative information identified from open sources for Mrs A, for her involvement in drugs trafficking, contract killing, arson, financial crimes etc. Furthermore, the ASP identified three more individuals with links to Mrs A ("Mr B", "Mr C", "Mr D"), all nationals of Country A, who were BOs of Company C (registered in Country C), Company D (registered in Country C) and Company E (registered in Country A), respectively.

From links identified in the FIU's database, the FIU identified that a STR had been received in the past from a bank for Company A. The bank accounts of Company A were analysed and transactions with other Cyprus bank accounts were identified. For these Cyprus bank accounts, using Article 55(2)(c) of the AML Law, were obtained information from the respective financial institution, about the holders of the accounts as well as their BO (who were also identified to be from Country A). It is noted that at the closing of the bank account of Company A, the balances were transferred to the Cyprus bank account held by another company ("Company H"). The FIU obtained information about the transactions of Company H and prepared a detailed summary. Furthermore, information was obtained from the financial institution about other companies that had common BOs and/or transactions with the counterparts of Company H and a detailed list was prepared.

Furthermore, the FIU identified another STR received from a Cypriot financial institution for another company (Company F), the director of which was Mrs A. The suspicions involved negative information identified from open sources for Mrs A and Company F and their involvement in money laundering. A detailed table was prepared with all incoming and outgoing transactions of Company F.

Moreover, the FIU identified another STR received from another Cypriot financial institution a company ("Company G"), registered in Country B, whose Bo was Mr B. Finally, the FIU identified another STR received from another Cypriot financial institution for a personal account held by Mr B.

All the aforementioned Cyprus bank accounts had been closed and almost all the aforementioned companies were registered abroad and that their BOs were from Country A.

Spontaneous Information was prepared and sent to FIU in Country A in 2018, which included a detailed description of the above, including detailed information about the companies and individuals involved, as well as details of the transactions.

134. Since 2015[19], the FIU received 5,899 STRs in total. The number of STRs which was subject to an in-depth analysis was 1,121 (19%), while the number of disseminations to the Police and investigations resulting from these STRs was even lower (see Table 13 above). Although there is no precise correlation between these various components within the chain, these figures would suggest that the degree to which some STRs are actionable may be limited. The FIU indicates that the surge in reports from MSBs would account, to some extent, for the discrepancy between the total number of STRs received and the number of disseminations and investigations based on these STRs. A more detailed analysis by the FIU of reporting patterns would assist the FIU in determining the cause of this imbalance. The FIU also provided the following figures in relation to the number of STRs that were related to a case being disseminated to the Police, which do not significantly alter the views formed by the assessment team.

**Table 12: STRs disseminated to the Police**

| Year | STRs received[20] | Cases disseminated to the Police | STRs related to the cases disseminated to the police[21] |
|---|---|---|---|
| **2016** | 1617 | 72 | 118 |
| **2017** | 1490 | 84 | 165 |
| **2018** | 1818 | 64 | 123 |

135. While certain exact figures in relation to STRs (e.g. the volume of funds involved; whether the STRs relate to resident vs non-resident customers; the top 5 predicate offences to which the STRs related to; etc) were not made available to the assessment team, the FIU provided many case examples (see Box 6.7, but also Box 6.9, Box 2.2 and Box 2.4) involving significant volumes of funds relating to legal persons registered in Cyprus with non-resident BOs or foreign-registered legal persons with non-resident BOs having bank accounts in Cyprus. Most relate to high-risk predicate offences such as fraud, corruption and tax evasion. The assessment team was also satisfied that the circumstances which generally give rise to reports being submitted to the FIU correspond to the type of business that is carried on from and through Cyprus, which include: insufficient documentation, customers not providing supportive documentation for executed/intended transactions, or provision of fake documents; transactions not in line with declared activity/customer profile; availability of negative information on the customer in open sources;

[19] The date of implementation of GoAML

[20] Total number of STRs and SARs

[21] Represents the number of analysed STRs/SARs which were the basis for the case files disseminated to the Cyprus Police in the given year (not including STRs categorised as 'Low')

unusual client behaviour, e.g. unclear business activities; absence of economic rationale of activity; and systematic and large cash deposits.

136. 11 STRs have been submitted in relation to the CIP; 8 from commercial banks, 2 from Supervisory Authorities and 1 from a fund administrator. All have been analysed by the FIU and disseminated to the Police. In some cases, the MoI has revoked citizenship. One such case is presented below. Other cases are presented under IO 1 and 7.

**Box 6.7: STR related to the CIP**

A number of STRs were received from local financial institutions in relation to an individual born in Country A, who obtained Cypriot nationality. The suspicions related to the submission of fake documentation in relation to the source of funds. Moreover, this person was declared to be a BO in a number of foreign entities and as he was relatively young in age and did not appear to have the necessary knowledge or professional background neither the expected financial standing that would have enabled him to get involved in such significant transactional activity, local financial institutions suspected that he might be used as a straw man in order to launder illegal funds.

An analysis of the movement of the accounts revealed that funds totalling EUR 6,934,940 were received in his bank account opened at a domestic bank, (reporting institution 1) originating from a bank in Country A. The client claimed that he wished to invest in real estate in Cyprus. Subsequently, part of these funds were transferred to another account in his name with a domestic bank (reporting bank 2) and thereafter, transferred to a bank in another EU country. Part of the funds was used to acquire property in Cyprus.

In parallel, a spontaneous report was received from an FIU of an EU member state (country X) in relation to the suspect indicating that two significant transactions had been executed in a personal account he maintained with a bank in the country X. During 2017, the amount of EUR 2,200,000 had been received in his account which was further transferred to an account at a Cypriot bank in order to buy shares in a company. According to the information received, the incoming funds had originated from an account in country Y. The foreign FIU also suspected that the person could have been a front person.

The FIU exchanged information with the FIUs of the involved countries and another country were the funds were transferred. The case was also disseminated to the Police for further investigation of predicate and money laundering offences. The Police contacted its counterparts via Interpol channels and the case is currently under investigation. The FIU also informed the MoI and as a result the suspect's Cyprus citizenship was cancelled.

137. A low number of STRs were filed relating to TF during the review period (38) and the FIU stated that the majority of these did not really relate to TF but were simply included as a tick-box exercise on the STR by the reporting entity. The low number of STRs may suggest a lack of awareness or pro-activeness regarding TF by reporting entities. Outreach and training is said to have been given to reporting entities, this issue having been identified in the NRA, yet there is no concrete evidence (such as an increase in SARs and in their quality) to suggest this outreach and/or additional training has yet yielded results. As noted under IO 4, FT risk understanding is less developed than that of ML risk within the private sector generally, which could also be a factor contributing to the low number of FT-related STRs.

138. The FIU has access to information on cash declarations maintained in the Customs Department database, including through the permanent posting of two Customs officers at the FIU. Customs information is used regularly in the course of the FIU's analysis (see core issue 6.3). In addition, the FIU receives reports on suspicious declarations from the Customs Department, as indicated in the table below. All reports received from Customs were analysed, subjects were checked against the FIU's database and the police database. Where deemed necessary, requests were sent to other FIUs or other local agencies such as the police, social insurance, tax authorities, Cyprus Intelligence Service etc. In some cases information has been forwarded to the police. It is not clear to the assessment team whether any of these cases have resulted in investigations,

prosecutions and convictions.

**Table 13: reports received by the FIU from the Customs Department**

| 2013 | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|
| 4 | 5 | 37 | 26 | 28 | 8 |

### *3.2.3. Operational needs supported by FIU analysis and dissemination*

139. Through its analysis and dissemination functions the FIU has the ability to support the operational needs of competent authorities to a large extent, albeit some further enhancements are needed. The staff at the FIU has long-standing experience and is highly qualified. The FIU is equipped with the necessary IT tools to generate actionable financial intelligence which is of value to law enforcement. The internal procedures in place are rigorous. FIU staff receives training on an ongoing basis.

Operational Analysis

140. The analysis procedure of the FIU is regulated by a written procedures manual which details the actions to be taken at every stage of the analysis. The analysis function falls under the responsibility of the Analysis Department, comprising a head and six analysts, who hold degrees in finance, economics, accountancy or similar academic qualifications.

141. Reports from the private sector (see core issue 6.2) are received electronically and subject to an integrity check to ensure that all the required fields are completed. This is followed by a comprehensive initial intelligence check, involving enquires to determine whether there any possible links or connections to persons or entities in the FIU database, the Police database, to which the FIU has direct access, commercial due diligence databases, Customs information. Critically, the Police database centralises a vast range of law enforcement information, including on criminal convictions, ongoing or previous investigations, investigations by the Drug Law Enforcement Unit, incoming and outgoing requests through Europol and Interpol, the Crime Intelligence Unit (see IO 7), Stop list/Alert list, arrivals/departures list for non EU residents. This permits the FIU to identify the existence of possible criminal elements at a very early stage of the analysis and facilitate prioritisation. Furthermore, the checks performed in the FIU database do not only focus on the involved persons and entities, but any other person mentioned in the narrative of the report to cast the net as widely as possible.

142. The analysis of STRs is prioritised based on the judgement of the principal officer in consultation with the secondary officer, both of whom are responsible for the case. Reports are categorised as 'high', 'medium', 'medium low' or 'low', depending on the seriousness of the suspicion, the results of the initial intelligence check, and a list of non-exhaustive risk indicators. The risk indicators are generally aligned with the risks identified in the NRA, such that the resources of the FIU are appropriately allocated to the highest risks facing the country. The prioritisation process is conducted manually. While the assessment team is of the view that human intervention cannot entirely be replaced by automated processes, there has been a steep rise in the number of reports submitted by the private sector and there is value in automating aspects of the prioritisation system to free up limited resources.

143. Reports that are categorised as low or medium low are accorded a lower degree of attention, though not entirely dismissed. They are recorded in the FIU database and analysed under a simplified procedure which may prompt a spontaneous disclosure to a foreign FIU, to the Police or other Government entity for information purposes (e.g. where there is match with the Police database or information sent to a supervisory authorities where there are indications that CDD had not been carried out adequately).

144. The focus of the analysis department is on high and medium category cases. In the past three years, on average, 315 reports (19% of the total number of reports received) have been classified annually under these two categories. Statistically, the proportion of reports classified as medium and high would appear low compared to the average number of reports received on an

annual basis (1,650), which arguably reflects negatively on the quality of reports received (see criterion 6.2). According to the FIU, there are various factors which contribute to the imbalance between STRs received and those classified as high or medium. Some STRs are prompted by a disclosure order issued by the court in the course of a criminal investigation by the Police; in such cases the investigation is already ongoing and the FIU simply informs the Police of the submission of the STR. Some STRs do not include justified suspicions that could lead to a thorough analysis and investigation. The FIU should look into the matter more closely to determine whether any other factors have an impact on a fuller exploitation of STRs.

145. Medium and high category reports are subject to a full and comprehensive analysis, which entails an extensive data and information gathering exercise. The power of the FIU to obtain information is wide and not subject to any unduly restrictive conditions. It is resorted to regularly to request additional information from the obliged entity filing the report, any other obliged entities, any public authority and foreign FIUs. Information is generally obtained in a timely manner. Although statistics are not maintained, no challenges were identified by the assessment team in this respect. The quality of the information received from the private sector is accurate and of the desired quality, even where it involves beneficial ownership information. Financial data (mainly in the form of bank statements) is collected in order to analyse incoming and outgoing financial flows and identify links with third parties. Financial data is submitted electronically in a secure manner and imported into the FIU's system. IT tools have been installed for data mining purposes. Banks and ASPs are regularly requested to provide information on beneficial ownership and bank account signatories since the large majority of cases involve legal persons. Banks are often contacted to identify the existence of bank accounts, which could be relevant for the analysis. Information is actively sought from foreign counterparts (see IO 2 analysis). The FIU's own database contains a wealth of available intelligence, data and information since it's been in operation for over twenty years. Administrative information, such as information from the company registry (on shareholders, directors, etc.), tax information, information from the Social Insurance Department and information from the Department of Lands are used to develop a financial profile of the suspect and identify any inconsistencies between the suspect's lifestyle and stated income. Law enforcement information is directly accessible, as noted earlier. The FIU also maintains close contact with the Police and the Customs Department through permanent secondments at the FIU from both authorities, which it fully exploits for analysis purposes.

146. The sanitised cases presented to the assessment team illustrate the FIU's ability to conduct multi-layered analysis of sophisticated ML cases involving the use of complex corporate structures spread over different jurisdictions, multiple bank accounts and extended ML networks. Examples are provided in Boxes 6.5 - 6.9.

**Box 6.8: FIU analysis based on STR**

The FIU received an STR from a bank in relation to the client of the bank's client, in relation to whom adverse information was identified. Subsequently, the FIU received 2 additional STRs from another bank in relation to the same group of companies. The suspicion was based on two factors: the declared BO was suspected to be a straw man and the companies' turnover was significant, considering that they were newly established. The analysis revealed that the companies within the group-maintained accounts with other banking institutions in Cyprus. The FIU obtained additional information from these other banks. It was determined that while the activities in some companies within the group appeared legitimate, others were being used to perform complex transactions with no economic rational. Each company was found to have several bank accounts with a number of banks. Funds were received from potentially fictitious investors either directly or through client accounts. Part of the funds were then channelled to the legitimate companies, while the rest through the other companies using all possible financial channels (internal transfers for inter-banking transactions, swift transfers, bankers' drafts, etc.), purportedly to conceal the source and trail of the funds. It was also established that, at least in one case, there was a false declaration of beneficial ownership. The case was disseminated to the Police.

147. The FIU has demonstrated the ability to analyse FT STRs as indicated under Box 9.2 in IO 9.

148. The length of the analysis varies depending on the nature and complexity of the case. On average, the analysis takes 2-3 days in case of low category and 2-3 weeks in the case of low medium category. In case of medium and high category of cases, the average length of analysis ranges from 2-10 months depending on the complexity of the case. The FIU states that a decisive factor for those cases that have an international element, which account for a sizeable portion of all cases under analysis, is the time taken to receive information from foreign FIUs. This can significantly delay the completion of the analysis. Besides this specific challenge, the upward trend in reporting and the absence of a more sophisticated case management system has inevitably put a strain on the existing human resources within the analysis department. On average every analyst deals with 125 case per year. A surge in reports may have diminished the analysts' ability to analyse all high priority cases with the required depth, potentially causing a negative knock-on effect on the dissemination process. The recruitment process, which was ongoing during the on-site visit, to bring in 5 additional staff within the analysis department is highly welcomed by the assessment team.

Strategic Analysis

149. The analysis procedures manual instructs analysts to conduct strategic analysis of private sector reports to identify any trends and patterns of ML and FT. Information on typologies on trends developed on the basis of analysis of private sector reports is presented in the FIU's Annual Reports. The FIU periodically issues more targeted typologies products, such as for instance on investment fraud; companies offering financial services without obtaining the relevant authorisation; attempts to use the services of professionals via e-mails for the purpose of depositing cheques and transfers of the money with the payment of specific remuneration; internet fraud using intermediaries known as "money mules"; typologies used by an organised criminal group of foreigners acting in Cyprus using the internet for fraud and forgeries. In 2018, the FIU issued a fuller strategic analysis report focussing on, *inter alia*, reports from MSBs, the main trends identified within the banking sector, and the investment sector. The assessment team had sight of this document and found it be very instructive for the private sector. The FIU is encouraged to produce similar products on a yearly basis.

Dissemination

150. The FIU may disseminate data and information to the Police for the purpose of conducting investigations where reasonable suspicions are identified that ML, predicate offences or FT has been committed. The decision to disseminate a case is taken by the Head of the FIU in consultation with the Head of Analysis upon the proposal of the case analyst. In practice, the FIU disseminates reports mainly to the Police. The FIU may also send disseminations to the Customs Department and the Inland Revenue Department for investigation purposes and supervisory and other government authorities for information purposes only. The table below contains ML/predicate offence dissemination-related statistics. Statistics on cases disseminated to authorities other than the Police were not kept before 2016.

**Table 14: Recipients of FIU Disseminations**

| | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|---|
| **Police** | 10 | 13 | 25 | 72 | 84 | 64 |
| **Customs Dept** | N/A | N/A | N/A | 1 | 2 | 1 |
| **Tax Dept** | N/A | N/A | N/A | 20 | 49 | 14 |
| **Supervisors** | N/A | N/A | N/A | 12 | 4 | 6 |
| **Other Gov. Auth.** | N/A | N/A | N/A | 4 | 4 | 7 |

151. The table below refers to FT-related dissemination statistics.

**Table 15: FT-related disseminations**

| | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|---|
| **Police** | 0 | 0 | 0 | 2 | 0 | 2 |

152. The statistics indicate that in the period 2016-2018 the number of disseminations increased significantly compared to previous years, although the figures dropped in 2018. The NRA identifies this component of the AML/CFT chain as one of the national vulnerabilities: the number of reports disseminated to the Police for investigation is low compared to the number of STRs received by the FIU, even though there has been an upward trend in recent years. This notwithstanding, there appears to be a reasonable analysis/dissemination ratio. As stated above, on average 315 STRs are classified as medium/high annually and are subject to in-depth analysis, whereas an average of 73 cases have been disseminated for further investigation. Furthermore, one dissemination may contain many STRs. In some cases, categorised as high or medium, where in-depth analysis is carried, the FIU, following a request to a foreign FIU, does not receive any negative information or information that would suggest that the transactions carried out through Cyprus were illegal and therefore the case is not further disseminated.

153. The FIU disseminated 4 FT cases to the Police. The number of FT disseminations would appear more or less consistent with the number of FT STRs received by the FIU. More information is provided under Immediate Outcome 9.

154. Reports disseminated to the Police include information on the facts of the case and the nature of suspicions, information on financial transactions, accompanied by the relevant supporting documentation (bank statements/swifts/copies of agreements/opening account documents and other). Information and intelligence obtained from other sources during the analysis process (e.g. from other FIU counterparts, from Government Departments) is also disseminated and clarified that it can be used for intelligence purposes only. When information/intelligence is received from foreign FIU, consent is obtained from the counterpart FIU prior to dissemination. The Police, as the main recipient of FIU disseminations, noted that dissemination packages are very comprehensive and actionable. However, as noted under core issue 6.1, the Police face some challenges in exploiting FIU dissemination products to their fullest extent. Information on the use of the FIU's products by Customs and Tax Department are also provided under core issue 6.1.

155. Since Cyprus is an IFC, in many instances STRs relate to foreign companies registered abroad and foreign beneficial owners with no physical or legal presence in Cyprus. The FIU noted that in these circumstances it is often challenging to take meaningful action domestically, including investigations and possible prosecutions. However, in these instances, the FIU, through its analysis function, has played a critical role in assisting foreign authorities in bringing to justice foreign perpetrators and seizing and confiscating proceeds of crime (see for instance case example in box 6.9 below). Feedback requested by the FIU on the use of these disseminations has generally been very encouraging. The assessment team positively notes that the number of spontaneous disseminations to foreign FIUs has increased significantly over the period under review.

**Table 16: Spontaneous sharing of information by the FIU**

| | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|---|
| **No of cases** | 50 | 98 | 93 | 126 | 242 | 135 |

156. As a best practice, the FIU has adopted a policy of providing complete analysis products to foreign FIUs, where following the analysis of an STR, grounds indicating the existence of criminal activity outside of Cyprus is identified. In these cases, the FIU will generally authorise the foreign FIU to disseminate information to LEAs for further investigation.

**Box 6.9: FIU analysis supporting the operational needs of foreign competent authorities**

The FIU received an STR from a bank in Cyprus regarding suspicions of ML regarding one of their clients, namely a company (Company X) holding accounts with the Cyprus bank. The BO of Company X was a national from Country A, who was also the signatory on the bank account. According to the STR, no documentation was provided to the bank as to the alleged licenced business activities of the company and no reference was found on the internet as to this company. Millions of euros were transferred to the bank accounts of Company X by another company abroad. The FIU of Country A was informed of the contents of the STR. In parallel, a number of other STRs were also received by other banks in Cyprus relating to Company X and involving other companies holdings accounts with Cyprus banks. In total 25 STRs were received by the FIU involving different accounts, banks and companies. Additional information was requested and obtained by the FIU from reporting entities. The FIU analysed all the STRs and exchanged information with the FIU of Country A. It also sent requests to a number of foreign FIUs. The analysis identified a complex scheme of transferring money through different companies using contracts or other invoices so as to justify the multimillion transactions. The analysis of the transactions and the information provided to the FIU in Country A were instrumental in revealing the entire ML scheme and the route the illegally obtained money followed through different accounts and the alleged justified documentation as well as the physical persons behind those companies. A number of these persons and the transactions through Cyprus were unknown to the investigators of Country A, who were investigating the facts of the predicate offence in Country A. The information provided assisted the authorities in Country A to proceed against a number of physical persons, who were arrested and prosecuted in Country A for ML. The case also resulted in millions of Euros in a number of bank accounts in Cyprus being frozen under court freezing orders. In addition, the authorities of Country A sent a number of MLA requests to the Cypriot authorities to obtain evidential material. The FIU applied for and obtained disclosure orders for vast volumes of evidential documentation which was transmitted to the authorities of Country A. The hearing of the case has been concluded and the accused persons were convicted at first instance of ML (currently under appeal) and a confiscation order was issued (pending appeal).

157. While the FIU is commended for taking a proactive approach in relation to these cases, the assessment team is of the view that certain cases should still be disseminated to the Police in Cyprus, especially where a Cyprus-registered company is involved (despite the fact that the BO is foreign) or there is the involvement of an ASP or other professional in Cyprus. This could lead to more third-party ML cases. The cases provided indicate that, as of late, the FIU has already started adopting this approach.

### *3.2.4. Cooperation and exchange of information/financial intelligence*

158. The FIU has an elevated standing within the domestic AML/CFT community owing partly to its placement at the Attorney General's Office but more significantly due to the commitment and dedication by its staff to improve not just the FIU's working methods but the AML/CFT system as a whole. Due to the respect that the FIU commands it receives full co-operation from all other domestic competent authorities.

159. There are no legislative or other barriers which serve as an obstacle to the proper cooperation or exchange of information between the FIU and other competent authorities. The Police is in a position to request any information held by the FIU which may assist their ongoing investigations of predicate and ML/TF offences as well as the tracing of criminal proceeds. The FIU, however, retains discretion as to whether information in its possession is communicated. The FIU has direct access to the Police database which is accessed invariably during the STRs analysis. Access is provided through secure channels. There are three police liaison officers permanently seconded to the FIU to facilitate cooperation between the two authorities. While the FIU does not have direct access to the Customs database, two Customs officers are also permanently seconded to the FIU who may directly access the database. In addition, the Customs Department regularly exports information on seizures and declarations into the FIU's system. The assessment team did

not identify any particular issues in relation to the protection of the confidentiality of information, neither in the context of exchanges between the FIU and LEAs or foreign partners, nor in the analytical work carried out by the FIU.

160. In general, it takes one to two weeks for public authorities to respond to the FIU's requests. Due to close contacts between the FIU and other competent authorities, the FIU often resorts to informal channels of co-operation to expedite the sharing of information. The FIU indicated that it has contact with the Police on a daily basis to strengthen the quality of disseminations. However, discussions at a more formal level do not appear to take place regularly on, for instance, enhancements to the operational framework between the FIU and the Police. The authorities excessively rely on interagency informal contacts, which may result in positive short-term results but not bring about systematic and long-lasting changes.

161. Cooperation and information exchange between the FIU and supervisors is underpinned by a legal provision in the AML/CFT Law[22]. In practice, there is very close co-operation. Apart from the participation of the FIU in the Advisory Authority (see core issue 1.5), where both policy and operational issues are discussed, the FIU communicates with supervisory authorities (see Table 15) where compliance matters are identified in the course of the analysis of STRs, in order for appropriate supervisory actions to be taken. The FIU also receives STRs from supervisory authorities where suspicions come to their attention. Strategic analysis and typology reports issued by the FIU are shared with supervisors who apply their contents to their supervisory policies.

*Overall conclusions on IO.6*

162. **Cyprus is rated as having a moderate level of effectiveness for IO.6.**

## *3.3. Immediate Outcome 7 (ML investigation and prosecution)*

### *3.3.1. ML identification and investigation*

*Identification of ML cases*

163. The Cyprus authorities state that the sources from which ML may be identified, and investigations initiated, are (i) the investigations of predicate offences; (ii) intelligence provided by the FIU based on analysis of STRs[23]; (iii) disclosures from the Customs Department; (iv) incoming mutual legal assistance requests or other information from foreign counterparts (e.g. through EUROPOL/INTERPOL); and (v) complaints by victims of predicate offences or public authorities.

164. The only available statistics are presented in Table 18. The figures provided demonstrate that the majority of ML investigations have been based on, and parallel to, predicate offence investigations and on STRs/FIU. From discussions with the authorities, it transpired that some investigations have been harvested from incoming MLA requests, on the back of referrals from Customs and/or from complaints by victims of predicate offences or public authorities.

**Table 17: Number of ML investigations initiated by the Police**

| Year | **Investigations based on FIU notifications** | **In parallel with the investigation of a proceeds-generating offence** |
|---|---|---|
| 2013 | NAV | 43 |
| 2014 | NAV | 82 |
| 2015 | NAV | 91 |
| 2016 | 15 | 38 |
| 2017 | 20 | 57 |
| 2018 | 56 | 43 |
| Total | 91 | 354 |

[22] Sec. 59(8)
[23] Up until 2016, the FIU investigated STRs in co-operation with the Police

165. The overall picture provided in the figures is consistent with Cyprus' prosecution record i.e. the vast majority of ML prosecutions and convictions relate to self-laundering ML parallel to a (domestic) predicate offence. Thus, the primary provenance of ML identification has been from parallel financial investigations (PFIs) of predicate offences, with ML being ancillary. PFIs, which are all encompassing and not necessarily a separate concept from an ML investigation, are undertaken in "serious cases" and are carried out, as rule, simultaneously to the substantive offence investigation. There is no need to wait for an indictment of the predicate offence before initiating a PFI.

166. PFIs are undertaken on the basis of instructions given by the Director of the CCD, the Head of the District Crime Investigation Department or the Commander of the Drug Law Enforcement Service. What "serious" means is a flexible concept although the police said that particular offences, such as drug/human trafficking, corruption, large scale frauds or if a case involves large amounts of proceeds, large quantities of drugs or other drug trafficking schemes, would usually trigger an enquiry into finances and potential ML, as would cases involving public persons. The assessment team recognises that there is desirability in having flexibility, but it is of the view that there could be a possibility of inconsistency when different constituent parts of the Police (district and national) have wide discretion whether or not to launch an investigation. Nonetheless, there is excellent co-operation between the different Police departments, which includes daily communication on cases and joint/investigative operations/investigations.

167. The assessment team has some reservations over whether all the police units which may be called upon to carry out PFIs have the adequate resource and capacity to do so, particularly whilst conducting in parallel the investigation of predicate offence. Therefore, the assessment team considers that the Police would benefit from having clear guidelines on when an ML investigation/PFI should usually be initiated or referred to the CCD for decision/direction on whether to initiate, to ensure that the authorities are fully exploiting the opportunities to pursue ML investigations.

168. The number of investigations arising out of STRs referred to the Police saw a healthy improvement in 2018, both in terms of its overall number (56) and the rate (87.5%). The Police have had the main responsibility to investigate ML since 2016 and their experience has been increasing. The need for increased usage of STR disseminated data for investigations was recognised by the NRA and Action Plan, and the Police have taken appropriate measures such as increasing resources, creating specialised units for financial crime, and issuing guidance (by the Chief of Police) in September 2018 to police to examine thoroughly all STRs received. The results of such measures are demonstrated by the improvement in investigations as a result of STRs. Various case examples presented under IO 6 and this IO involve STRs.

169. Cyprus recognises in its NRA, Action Plan and AML/CFT Strategy the need to be more proactive in identifying and investigating all types of ML, particularly where the predicate offence has been committed elsewhere and Cyprus' financial system has been targeted. This has resulted in the setting up of the Office for the Handling/Execution of MLA Requests and European Investigation Orders in 2018. One of the purposes of this office is to analyse incoming MLA/EIOs and identifying whether domestic investigations can be launched from them. This office is comprised of persons spread out amongst the police units (locally and centrally) which should enhance co-operation and ensure a holistic approach nationally.

170. It was said that at the time of the on-site there had been nine investigations on the back of incoming MLA[24] which could possibly involve ML. Some examples were provided of ongoing investigations relating to ML from foreign proceeds, including the one in Box 7.1 below.

[24] 2 additional investigations following the on-site

**Box 7.1: ML investigation harvested from MLAs**

The CCD (ECIO) is investigating connected suspicions of money laundering (both self-laundering and third party) regarding foreign proceeds of fraud and forgery, involving three natural persons and 22 legal persons.

This investigation was initially triggered when the CCD/ECIO of the Police received two STRs from the FIU. The reports related to a person from Malaysia who opened bank accounts in Cyprus for the purposes of purchasing real estate, through legal entities (both Cypriot and Foreign). The documents presented to the reporting entities were suspected to be forged, which created suspicions that the Malaysian person was a strawman.

In parallel to this, an MLA request in regard to the same persons was received from Iran concerning fraud, misappropriation of trust, forgery, OCG activity and ML. According to the MLA request, the Iranian nationals act as representatives of a Malaysian registered company (X), which encouraged another company, registered in the Labaun territory of Malaysia (Y) to enter into an agreement with a third company (Z) pursuant to which Z would receive funds from the customers of Y and remit them in accordance with Y's instructions.

Between October 2013 and June 2015, over USD 96 million was transferred on behalf of Y's customers to an account held by Z at a bank in Malaysia. Subsequently, Y instructed Z to transfer approximately USD 73 million of this to an account at a bank in Labaun. Instead of making this transfer, the Iranian national, who was the sole signatory of Z's account, misappropriated the relevant funds belonging to Y, with the aid of his father and other individuals, and they diverted and laundered those funds through the Malaysian and international banking system.

The MLA request is being executed by the MLA Office and the information generated by the request has been passed to the ECIO to support the domestic investigation.

The Iranian is now believed to be living in Cyprus under a false name with a Cypriot passport and ID. Based on information disclosed in the MLA request, he and his parents are suspected of transferring part of the funds deriving from the fraud to Cyprus.

171. As discussed under Immediate Outcome 8 (core issue 8.3) there have been some examples of referrals from the Customs Department leading to ML investigations and prosecutions.

*Investigation of ML cases*

172. Cyprus has taken measures to ensure that financial crime investigations, including ML, are prioritised by targeting resources accordingly, for example through the creation of the ECIO within the CCD and financial crime units within the districts of Limassol and Nicosia. Furthermore, the Cyprus authorities state that certain ML investigations involving PEPs, corruption cases, fraud or cases involving larger quantities of drugs or proceeds are prioritised by investigating officers. In particular, instructions given to investigators encourage imminent investigative measures such as applying for disclosure orders and production orders. There is also said to be constant monitoring of the investigation procedure by the head of the investigative department, and when deemed necessary the matter is submitted to the prosecutors for relevant instructions and guidance.

173. There is regular and good co-operation with the AG's Office/Public Prosecutor Office (all police units can liaise directly – no need to go through CCD). The AG/PPO is generally brought into the investigative process early on particularly when the matter is serious and/or complex. The assessment team encourages the continued and systematic involvement and assistance of the prosecutors earlier on in the life of ML investigations, to assist in building the case and evaluating the evidence, and the authorities agreed that consolidating and increasing this (already strong) co-operation would be beneficial.

174. In the life of an investigation, the Police can avail themselves of the assistance of qualified accountants. There are permanent personnel within the Police who are suitably qualified. Currently, there is one accountant and recruitment is under way for an additional five to be based within the Crime Combating Department. Accounting resources can be, and indeed have been,

seconded from other sources such as the Official Auditors Office for assistance in more serious and complex cases.

175. The police, as a whole, generally appear to be sufficiently resourced for identifying and investigating ML, although the ECIO with only 14 investigators could become relatively stretched dealing with more serious and complex financial crime investigations if Cyprus does indeed begin to pursue more complex third party and foreign predicate-based ML. This will be however be alleviated by the additional accountants referred to above and the creation within the ECIO of a "Team for Conducting Financial Investigations" to support all police units (four of the accountants referred to above shall be assigned to this team) The ECIO is not charged with all ML investigations as the district units have the capacity to deal with investigations which are localised to their district; where matters involve more than one district or are "complex" then the CCD/ECIO is likely to take on the lead for the investigation, but with the co-operation of the district units. This was the situation as explained on-site. The assessment team retain reservations on whether all the constituent parts of the Police have the sufficient resources and capacity to investigate ML, particularly the more complex cases.

176. Whilst there are economic crime units within the Limassol and Nicosia districts, there are no such units in other districts, and it is not clear whether the Drug Law Enforcement Service has independently sufficient resources to investigate ML as well as drug predicates. It is a matter for the Director of the CCD whether the investigation is carried out by the ECIO/other centralised units or the district units, but the assessment team recommends the introduction of some guidelines on when matters are taken over by the centralised and specialist units (indeed, the previous evaluation recommended guidance on which agency takes the lead). It should be stressed that the assessment team does not necessarily consider this to be a major issue at present. Subject to the reservations regarding the amount of ML investigations/prosecutions/convictions, the Police appear to be coping adequately at present but when more complex cases are pursued, clarity on when the specialised units take the lead would be advantageous.

177. There is a database which compiles and includes information for all investigations (including ML) throughout the Police. Access to investigations carried out by the Drugs Law Enforcement Service is restricted but investigating officers from the CCD can check the system to verify if there is an ongoing investigation by the Drug Service and the investigating officer can then make a request for the disclosure of information. The FIU also has access to this database. There is in any event strong co-operation within the Police and indeed between the Police and others such as the Customs Department, the FIU and the Tax Department. For example; the Police and Customs have a Memorandum of Understanding (based on an EU model) which sets out the co-operation and the operational arrangements between the two agencies; there are Police officers seconded to customs; and there are occasional instances of joint operations.

178. A new document management system, the Relativity system, was introduced in 2016 to increase the efficiency of investigations. This e-discovery platform enables the processing of evidence collected and allows further and detailed examination of the evidence which is mostly paper documents and digital data acquired from banking institutions. The former are scanned and converted to e-readable documents. A group of investigators can therefore search and view electronic data simultaneously from different locations. This provides instant and effective access to documentation in bulky cases, and original evidence is not moved around, with access restricted to authorised personnel. The assessment team was informed that the Police are also piloting a new system (Tovek) to act as a central repository system for the entire Police structure, to ensure the coordinated and effective analysis of information at both strategic and operational level. The initial version of Tovek purchased by Cyprus police is a closed system which will draw data only from closed sources and specifically from various police databases. In the future, the plan is to purchase the full version to ensure access to data from open sources too.

179. ML investigations are estimated to last between 3-18 months for domestic only investigations. There are no particular issues with this such as statutory limitations (which only apply in limited circumstances for minor offences attracting low sentences) and there are no

judicial limits on the length of investigation or requirements to open the file to the subject of the investigation which can be seen in some civil law jurisdictions.

180. Disclosure Orders are used frequently. All investigative tools are utilised for ML investigations, according to the authorities. However, the assessment team was unable to fully substantiate this because the only figures kept were for disclosure orders and requests by the police to FIU, and the figures below are not limited to ML but also associated predicate offences (see Tables 4 and 5).

181. The cases provided to the assessment team demonstrated that the main powers/tools for investigating ML used were surveillance, controlled delivery and disclosure/production orders. The Police would welcome expanded powers on communication interception (see Recommendation 31) but otherwise the scope of investigative powers is broad. The law enforcement authorities also have direct access to several databases or the power to expeditiously seek information from such databases, such as the land registry, tax, social security, shipping registry, motor vehicle registry, and companies' registry. The authorities provided examples of where they have used such searches effectively, and also demonstrated that they have not just focussed on the identified criminal but their wider network of associates, with the judiciary being receptive to applications for search warrants/disclosure orders regarding associates, where there are reasonable grounds for doing so.

### *3.3.2. Consistency of ML investigations and prosecutions with threats and risk profile, and national AML policies*

*ML risks arising from Cyprus's status as an IFC*

182. Cyprus has had one third-party ML conviction, which was one of only two convictions of a legal person during the review period (see Box 7.4) and no stand-alone ML convictions or ML convictions arising from foreign predicate criminality. Furthermore, the majority of ML investigations have been regarding natural persons despite the fact that Cyprus is a company formation and administration centre.

183. The authorities appear to be very conscious of the issues identified in their NRA regarding the lack of third-party ML and stand-alone ML being investigated, prosecuted and convicted, and also the lack of such action regarding foreign predicate crime. The jurisdiction accepts that there is a high threat of the proceeds of foreign crime being filtered into and/or through Cyprus, as it is an IFC, but the focus of prosecutions for most of the period under review has instead been on domestic crime proceeds. The low number of prosecutions for the laundering of proceeds of foreign criminality and the scarcity of outgoing MLA related to these types of cases demonstrates a lack of pro-activeness in addressing these foreign criminal threats. Therefore, it cannot be said that ML investigations and prosecutions have been fully consistent with the risk profile, particularly as there have been no prosecutions/convictions examples of ML identified to have been carried out through complex legal structures.

184. Although Cyprus has not demonstrated that it has, during the review period, been fully harvesting potential ML investigations (particularly as regards foreign predicate offending), the authorities have taken, and are continuing to take, steps to meet the aims of increasing ML investigations and prosecutions (qualitative as well as quantitative) by way of enhancing resources and training, and, as already mentioned, the creation of the Office for the Execution/Handling of MLA Requests. As such steps are relatively recent or are still ongoing, it is too early to fully assess the effectiveness. However, the jurisdiction has provided some examples of ongoing investigations and prosecutions which encouragingly suggests that things are going in the correct direction and the jurisdiction is moving towards the better application of an approach more consistent with its risk profile.

185. The authorities all appear to have a good awareness of the NRA and more importantly the substance of it, and are all on the same page as regards implementing the NRA and Action Plan and achieving more systematic targeting of stand-alone/third party/foreign ML. The Action Plan is a more substantive document (contrasted with the high-level National Strategy) and has been in the

process of implementation since early 2018. Specific measures have been implemented to meet such objectives, such as an increase in resources (e.g. 39 new prosecutors, 5 new accountants in the police, and the setting up of the new MLA office).

186. The National Strategy for AML/CFT is a high-level document and includes the aim of "*upgrading the structure, training and capacity of investigators and prosecutors, in order to enhance the effectiveness for prosecuting ML/TF and confiscating their illegal proceeds*." The Strategy goes on to envisage better resources (human and technological) and more emphasis on stand-alone and third-party ML, including where offences are committed in other jurisdictions. This Strategy was only adopted in January 2019, and endorsed by the Council of Ministers in March 2019, and is a policy document focussing on themes, and the Action Plan as discussed above is more important. A Police Strategy was also provided but not in translation and the assessment team was therefore unable to consider whether or not ML activities are in line with it or not.

187. In terms of legal persons, there were no independent investigations regarding legal persons between 2013-2015 and only 4 in 2016. However, some cases regarding Cyprus registered companies are still under analysis by the FIU, and where companies have been registered elsewhere, with no legal presence in Cyprus, the FIU has disseminated information spontaneously to counterparts in other jurisdictions such as the Republic of Moldova. Furthermore, there have been some good examples of Cyprus investigating complex ML involving legal persons. The FBME case is an example of investigating potential international ML involving natural and legal persons.

**Box 7.2: Investigation of foreign predicate ML**

FBME Bank's headquarters are in Tanzania and it has two service points in Cyprus. On 17/07/2014 the US Financial Crimes Enforcement Network (FinCEN) which is under the US Treasury Department, issued a Notice of Findings according to which FBME Bank was considered an establishment of primary concern for Money Laundering and Terrorist Financing. Also, on the same day, a notice on the proposed rule of law (Notice of Proposed Rulemaking) was issued by FinCen to impose special measures against FBME. The CBC acted swiftly to take supervisory measures and installed new management at the bank the very next day, and in 2015 revoked its Cypriot banking licence.

On 29/04/2015, a letter was sent from the Prosecutor General's Office to the Police Headquarters - Crime Prevention Division, with instructions to investigate the possible criminal offences in Cyprus by the directors, employees and shareholders of FBME, including money laundering.

The Police are currently investigating possible domestic and foreign offence generating money laundering, involving elements of self and third party laundering. The suspected persons involved (natural and legal) are as yet unquantifiable. The predicate offences range from conspiracy to defraud, misuse of devices, obtaining goods by false pretences, terrorism, corruption, and child pornography.

Up until now 13 EIO requests have been sent (to Germany, Italy, UK, Latvia, Croatia, Slovakia and Belgium) and 4 MLAs have been sent to USA and 2 MLA to Kazakhstan. Operational meetings took place in Cyprus with the representatives of USA and Kazakhstan. In addition, there has been incoming MLA from USA and Kazakhstan.

The Cypriot authorities are now in the process of reviewing the document and electronic data that was seized during the execution of a search warrant in the building of FBME BANK and through disclosure orders. The investigators are assisted by experts from the banking sector.

188. In another ongoing case, some 60 legal persons are currently under investigation for ML from a large investigation commencing in 2017. See case example below.

**Box 7.3: Ongoing ML investigation involving legal persons**

A ML investigation is ongoing in respect of two natural persons and an estimated 60 legal persons in connection with a large-scale tax fraud occurring in 2007 outside of Cyprus. The total amount of

the fraud is approximately USD 230 million. A complaint was reported to the Cyprus Police by the lawyers of the complainant in 2014 and following global media coverage of the tax fraud, this triggered around 20 STRs to the FIU. The misappropriated money was initially transferred to bank accounts in Lithuania, Moldova, Estonia and Latvia and from there to other countries including Cyprus. Part of the stolen money (approximately USD 27 million) was transferred to Cyprus through other countries and from Cyprus the money was transferred to the bank accounts of various companies abroad. Cyprus received MLA requests from Russia, USA, France, Switzerland and Germany. An MLA was sent from Cyprus to Russia and two Cypriot Police officers went to Russia and interrogated, with the assistance of the Russian Authorities, the two main suspects. Also, three operational meetings were organised between Cyprus, France and Switzerland. Other MLAs will be sent to the countries where the money was transferred, and all the persons involved will be interrogated. This case is considered as a complex money laundering case since many countries are involved and also there are open investigations in at least other five countries.

*ML risks arising from domestic criminality*

189. Cyprus does not have a negligible threat of ML from domestic criminality (arguably in contrast to many other IFCs) and, as a result, its activities regarding the same cannot be discounted. In terms of the domestic self-laundering cases, the ML investigations/prosecutions are generally in line with the identified high risk predicate offences, and indeed the banking system is the prevalent target for ML. Whilst statistical information was not available on the underlying predicate offences for ML investigations, the examples given by the authorities of ML investigations/prosecutions seem to indicate a prevalence of fraudulent offences, corruption and drug cases.

190. The case example in the box below is a good example of the authorities' efforts to curtail ML arising from serious domestic crime. It is also worth noting that the case involved third party ML and represents a ML conviction of a legal person.

**Box 7.4: 3rd Party ML Conviction example**

The case related to the investigation of criminal offences committed during the expropriation and purchase of Turkish Cypriot property in Dromolaxia, Larnaca, between a Turkish Cypriot Owner (Seller) and a state-owned Cypriot Legal entity (Buyer) and the subsequent investment of more than EUR 25,000,000 from the Cyta Employees' Pensions and Grants Fund, which was carried out during the period 2007 - 2013. The Police carried out a financial investigation, applied successfully for Disclosure Orders and interrogated owners and officials of the offender company. A large number of persons benefited from the fraud, including government officials and persons working for the company. Nine persons were prosecuted for fraud, theft by a public officer, misuse of power, money laundering, corruption, bribery, use of forged documents, circulation of forged document, theft, and extortion. Eight of the accused persons were found guilty and convicted with imprisonment sentences. Amongst them five natural persons were convicted for corruption related offences and money laundering (acquisition, possession, use of criminal property) and a legal person was found guilty for 3rd party money laundering. The legal person was sentenced to a fine of EUR 300,000 for the ML, and the natural persons were subject to imprisonment ranging from 4 ½ years to 8 years' imprisonment for the ML offences (with concurrent sentences for the predicate offences ranging from 4 ½ to 5 years' imprisonment). In addition, a confiscation court order was issued for the total amount of EUR 750,000, being equivalent value property of bribes received. EUR 300,000 which was frozen in the UK was repatriated to Cyprus to partly satisfy the confiscation orders.

191. Cyprus has recognised the threats associated with corruption and has successfully targeted corruption and ML in several instances. It has effectively tackled corruption in some cases by offering immunity to the bribe giving construction companies to turn evidence against the bribe receiving public officials.

**Box 7.5: Immunity example**

The authorities identified, through intelligence and through information provided by the Auditor General, corruption by the President and other executive members of the Sewerage Board of Paphos (CIPA), in the course of the management of the contracts related to the Paphos sewerage system. It was discovered that they were bribed by candidate contractors companies in order to award the tender to them. Two former mayors are implicated in the case.

Seven persons were prosecuted before the Assize Court for the offences of conspiracy to commit felony, bribery, abuse of power, corruption, illegal acquisition of property benefits by officials and public servants, and ML (acquisition, use or possession offence). All the accused persons were found guilty and convicted with imprisonment sentences (3 years imprisonment for the predicate offence and 6 years for the ML offence). In addition, a confiscation court order was issued for the total amount of EUR 750,000 for five of the accused persons and from the remaining two accused persons the amount EUR 371,500 was confiscated as well as immovable property. As a consequence of this criminal prosecution and conviction, the bribe giver companies where given immunity from prosecution but banned from public tenders.

192. Fraud generates considerable proceeds in Cyprus and the authorities have targeted related ML. One case example is presented below.

**Box 7.6: Fraud-related ML**

A matter is at the trial stage involving fraud and bribery in the private sector, and violation of the Law ratifying the Convention on the protection of the European Communities' financial interests. There are 6 natural and 1 legal persons on trial. The case was triggered by a report from the Auditor General to the Attorney General.

The offences are related to the Transnational Dissemination and Promotion Programme for Dairy Products in Third Countries and in particular to Russia and Ukraine. The Programme consists of three annual phases with defined implementation timetables and is co-funded for the total amount of EUR 4,988,000 from the European Union at 50%, from Cyprus and Bulgaria at 30% and from the Suggested Organizations Pancyprian Organization of Cattle Farmers Public Ltd and the Bulgarian Association of Dairy Processors (BADP) at a rate of 20%.

People who acted as a straw man opened bank accounts in the name of registered companies in Cyprus and other countries. Through these accounts the money from co-funding was received and then transferred to the final receiver (the suspect). The amount of money transferred and laundered is suspected to be EUR 1,313,000. Investigative measures such as Disclosure Orders and Search Warrants have been used and EUR 500,000 has been frozen in Belgium following an MLA request, with requests for assistance also being sent to the UK, Ukraine and Russia.

193. Many of the drug trafficking cases pursued by the Drug Law Enforcement Service involve a parallel financial investigation to trace criminal proceeds but also to identify the existence of ML offences.

**Box 7.7: Drug-related ML**

Three persons were convicted of drug trafficking and one of them was also convicted of ML (s.4(1)(a)(i) AML/CFT Law i.e. conversion/transfer of criminal property). The first accused arrived at Larnaca airport from abroad and according to information held by the Police he was considered suspicious and was put under surveillance. He was stopped together with his luggage at the customs point at the airport where he was found to be in possession of 5,786 grams of cannabis. He co-operated with the Police for the purposes of controlled delivery, according to the relevant legislation, in order to arrest the final recipients of the drugs. Subsequently, following many actions by the Police (among other things an undercover police officer was used), two more

offenders were arrested and charged. The one defendant convicted of ML was sentenced to six years for the ML and five years for the predicate offences.

*ML risks arising from specific events/issues*

194. Regarding specific events or issues which might give rise to ML investigations, the well-known Laundromat scheme has not triggered ML investigations in Cyprus despite estimations that a large volume funds connected to the scheme has been received in Cyprus. With respect to the CIP, there is an open investigation initiated following a case dissemination by the FIU (see Box 6.7); the police are investigating the use of forged documents, and ML. They are preparing MLAs to other countries, and have issued disclosure orders issued to all banks, to check if the suspect has used other banks to those mentioned in STRs. This is said to be at the final stages of investigation.

### *3.3.3. Types of ML cases pursued*

195. As fully explored under Recommendation 3, Cyprus has a strong framework for prosecuting ML, i.e. there is no requirement for a previous or simultaneous predicate conviction and the knowledge, intention or purpose which are required as elements of the ML offence may be inferred from objective and factual circumstances.

196. In the review period, Cyprus has had ML prosecutions and convictions as follows:

**Table 18: No. of ML investigations, prosecutions and convictions**

| Year | Investigations | Prosecutions | Convictions |
|---|---|---|---|
| 2013 | 43 | 29 | 9[25] |
| 2014 | 82 | 14 | 11[26] |
| 2015 | 91 | 15 | 24 |
| 2016 | 53 | 20 | 14 |
| 2017 | 77 | 19 | 17 |
| 2018 | 99 | 17 | 15 |
| Total | 445 | 114 | 90 |

197. As stated under core issue 7.2, Cyprus is not achieving the level of results in the type of ML cases which might be expected in an IFC. It does, however, have a reasonable record as regards pursuing ML in relation to domestic criminality, (albeit the overall numbers might arguably be said to be on the modest side if compared to the number of convictions for high-risk predicate offences). As demonstrated in Table 19 above, for a small jurisdiction, 90 ML convictions are indicative of a functioning system and the conversion rate from prosecutions, which is around 79%, is commendable[27]. The number of investigations which proceed to indictment is around 25% but given the strong conviction record, this perhaps demonstrates that the investigative process is adequately filtering out cases with no evidence or prospects of success.

198. Nevertheless, the vast majority of prosecutions and all but one conviction have been for self-laundering ML and for domestic criminal activity. There has been only one conviction for third party ML (Box 7.4). However, the authorities have provided the assessment team with information on ongoing prosecutions into 3rd party ML, which will hopefully be successful at trial. There was still only three such cases at this stage and the assessment team would expect to see more. One of them is presented in the box below.

[25] Including 1 legal person

[26] Including 1 legal person

[27] The table shows investigations and prosecutions commenced in particular years and convictions achieved: it will not necessarily be the case for example that a prosecution commenced in 2014 will be complete in that year, and it may show as a conviction in a later year

**Box 7.8: Example of an ongoing 3rd party ML, legal person prosecution**

Following an STR, the police investigated the offences of corruption, bribery of public servant, abuse of power, ML against three persons and a company. The case is against the ex-Governor of the Central Bank of Cyprus who is accused of receiving bribes in the course of his duties. In total there are 4 natural and 3 legal persons involved. An associated company of the ex-Governor is accused of ML (acquisition, use, possession offence and also conceal/transfer offence) since it, together with the accused natural persons, received the amount of EUR 1,000,000 knowing, or ought to have known, that it was proceeds deriving from the offences of bribery, corruption and other. The ex-Governor's daughter is a director of the company and is charged with 3rd party ML. The funds were transferred with payment details 'provision of consultancy payments' and were further transferred to the account of one of the accused. Restraint orders have been issued in respect of equivalent property (real estate totalling value of EUR 260,900), and including properties transferred to the mother of one of the accused as a gift (value EUR 665,800). Cyprus has sought MLA from, and used FIU co-operation channels with the UK and Greece in this case.

199. Issues arose in a separate stand-alone ML case where the accused was prosecuted on the basis of circumstantial evidence for stand-alone ML. He was acquitted because the circumstantial evidence was not deemed to be sufficient for his conviction for ML. The assessment team is satisfied that technically there was no issue (i.e. there was no requirement in the AML/CFT Law or by the judiciary for a predicate conviction) and this was instead more of an effectiveness issue relating to the reluctance of the judiciary to convict ML without the identification and proving of the underlying predicate offence. The authorities have taken actions to address this by amending the ML offence in the AML/CFT Law to seek to remove any doubt that ML can be convicted based on irresistible inferences. The authorities state that they took into account leading jurisprudence from other jurisdictions, the Warsaw Convention and a Moneyval report on typologies before reaching a conclusion on the appropriate new statutory wording.

200. When meeting some members of the judiciary on-site it was clear to the assessment team that their view is that the prosecution is required to prove the underlying predicate offence, although a stand-alone ML offence has not been brought before the courts since the change to the AML/CFT Law. Whilst it is therefore too early to fully assess the effectiveness of the newly untested legislation, the assessment team would encourage the authorities to monitor this issue very closely. Cyprus has ratified the Warsaw Convention and therefore the underlying predicate offence should not have to be identified/proven. The authorities plan to host seminars for the judiciary on the change in law (as per the Action Plan). Furthermore, prosecutors plan to continue to cite in court Article 9(6) of the Warsaw Convention, as well as jurisprudence from other jurisdictions such as England and Wales (which Cyprus courts are not bound by but may take into account as persuasive) which demonstrate that irresistible inferences may be drawn to prove ML even without the precise underlying predicate being established.

201. Guidance for the Police and prosecutors was developed by the Law Office of the Republic on the stand-alone ML offence, which includes reference to foreign jurisprudence on the subject. The guidance also specifies that there has been an amendment to the ML offence, which is intended to remove any ambiguity as to the need to provide evidence on the commission of the predicate offence. Furthermore, the Police stated that they are still willing to continue putting resources into time-consuming and resource-intensive stand-alone ML cases with a view to challenging the position of the courts. Two case examples, presented below, would suggest that this is the case.

**Box 7.9: Investigation/prosecution of stand-alone ML**

Case 1: In Limassol, a person of interest's property was searched under the authority of a search warrant (on suspicion of housing explosives and possession of narcotics) and over EUR 300,660 in cash was discovered. The explanations as to their provenance were not acceptable. Financial investigations were initiated against all his relatives, there have been transactions identified showing money going to and from Netherlands/Belgium, and there are suspicions that the

individual is involved in drug trafficking (the second suspect is resident in the Dutch Antilles). There have been meetings with EUROPOL and the Dutch and Belgian authorities. There are parallel financial investigations being conducted in those other jurisdictions. The Cyprus' investigation has been expanded to connected companies, with documents obtained from various sources such as the tax office and Companies Register, disclosure orders have also been ordered by the court, and two accountants have been hired from the private sector to assist.

Case 2: The Cyprus police are investigating potential ML originating from fraud committed abroad. In October 2018, correspondence was received from the FIU on suspicious transactions involving two natural persons. It was found that five remittances were received from French Banks in two different individuals' bank accounts at the former Achna Co-operative Savings Bank for a total amount of EUR 77,627 and analysis indicated that the fund transfers did not match the economic profile of the Cypriot national. Part of the amount in issue was refunded to the remitting banks while the amount of EUR 14,656 was withdrawn in cash by the account holder. The French authorities have submitted an MLA to Cyprus based on a complaint of fraud, and this has been executed and it is expected that an EIO request shall be sent in the other direction. The accounts were opened in 2011, 2012 and both were terminated in 2013. Both individuals have been questioned by the Famagusta Crime Investigation Department and made some allegations on the origin of the money while denying that the money is the proceeds of fraud. Examinations have been carried out through the Achna Co-operative Savings Bank but due to the fact that the accounts have been terminated it is not possible to consolidate any amount of money. The Police aim to indict the Cypriot national on stand-alone ML charges.

202. It is understood that there is no specialised unit for ML (or financial crime generally) within the PPO. Whilst it is recognised that Cyprus is a small jurisdiction, it is nonetheless an IFC and the creation of a specialised unit within the CCD of the Police demonstrates that the authorities are alive to the benefits of such specialisation. The prosecution authorities may benefit from further specialisation in financial crime (including ML and TF) and having dedicated units (e.g. Roskill model) as the police do. In the recent GRECO report, it was noted that there is no specific work allocation within the PPO as such, but cases are allocated randomly unless complex. GRECO recommended more specific criteria (for different reasons of course) and it is difficult for the assessment team to reach a conclusion on the appropriate allocation of resources without such criteria. However, the prosecutors noted that cases were generally allocated now depending on experience, so the Head of the Criminal Law Division ensures that financial crime cases are handled by those with sufficient expertise.

203. There are no statutory limitation issues in Cyprus (limitations only apply for minor offences (misdemeanours) attracting low sentences). There are also no extraordinary procedural issues affecting matters coming to trial in an as expeditious manner as possible, and the Courts appear to have sufficient resource in terms of personnel and physical court space to cope with the matters coming before them.

### *3.3.4. Effectiveness, proportionality and dissuasiveness of sanctions*

204. The framework in the AML/CFT Law provides for sufficiently effective, proportionate and dissuasive sanctions. The large majority of sentences imposed for conviction of ML in the review period are terms of imprisonment. Only one fine was imposed in the review period for ML.

**Table 19: Sanctions for ML**

| Year | Highest Prison sentence | Lowest Prison sentence | Average Prison sentence |
|---|---|---|---|
| 2013 | 5 years | 3 months | 27.6 months |
| 2014 | 8 years | 36 months | 44.6 months |
| 2015 | 6 years | 6 months | 27 months |

| | | | |
|---|---|---|---|
| 2016 | 3 years | 30 months | 33 months |
| 2017 | 6 years | 6 months | 33 months (maximum sentences ranging from 3-5 years) |
| 2018 | 6 years | - | Maximum sentences ranging from 2-6 years |

205. The average of sentences imposed might be said to appear moderate. However, the authorities provided several case examples where the imprisonment sentence imposed can be said to be dissuasive, as demonstrated in Table 21. The sentence will vary in each case according to the circumstances. The low level of monetary sanctions imposed further demonstrates the lack of prosecutions of legal persons.

206. The authorities confirmed that the sentences were usually imposed concurrently as opposed to consecutively. This is not in itself unusual but as most ML convictions have been parallel to predicate ones, and the ML penalty has in some cases been the same or lower than the predicate sentence, the assessment team considers that the protected value of ML is not always being recognised because it might not be adding anything of value to the predicate offence prosecution, where the ML penalty is subsumed within the predicate penalty. There have however been some examples of the ML penalty being higher than the predicate which is commendable. The comments already made regarding the need for Cyprus to target more stand alone and third party ML are re-emphasised under this core issue as it would protect the added value of ML convictions as opposed to it being only an ancillary offence (sometimes with a lesser and subsumed penalty).

**Box 7.10: Example of ML sanction being greater than predicate**

Two prosecuted persons were found guilty in 2017 following a long hearing of a case of conspiracy to commit a felony, conspiracy to defraud, forgery, circulation of forged documents, fraud, fraudulent transactions in relation to immovable property, obtaining goods by false pretences and money laundering, (case number 11193/14) by the Assize Court of Paphos. The complainant, an elderly person, wanted to buy immovable property and came in conduct with the two accused persons, one of which introduced himself as an estate agent. The accused, by false documents purported to sell parcels of land to the complainant, who paid the purchasing price. The real owners however never authorized the sale of the land. The purchasing price was EUR 15,000, EUR 7,000 and EUR 14,000 for the three parcels of land. Further to the above purchasing amounts the accused fraudulently requested and received a further amount of EUR 15,500 paid by the victim as alleged taxes. In addition, the accused offered also to the complainant to buy another piece of land, falsely representing to him that this was owned by a 3rd person. Again, the true owner never authorized or requested the sale of her land. The purchasing price was EUR 4,550,000. The first accused offered to the complainant to pay only EUR 130,000 in cash and in parallel to register the three parcels of land he previously bought. The complainant agreed and gave the sum of EUR 5,000 as a first instalment and later on he gave further EUR 10,000 as a second instalment. He gave also his consent to proceed to the exchange of the three pieces of land he had already bought. The complainant further paid amounts of EUR 6,000, EUR 20,000, EUR 30,000, and EUR 72,000. He was further defrauded and paid the amount of EUR 37,500 as alleged taxes. The complainant was asking for the title deed of the said land to be registered in his name. Due to the fact that no title deed was issued, the accused falsely presented to the complainant that the reasons that no title deeds were issued was because on the opposite side of the road there was another piece of land owned by the sister of the vendor and needed to buy that piece as well so as to enable the issue of the title deeds. The complainant agreed and paid further amounts of EUR 4,000, EUR 55,000, and EUR 5,000. Finally, the complainant, who was expecting the title deed of the land he bought was given a title deed for a different piece of land which he never agreed to buy. He thus returned this title deed to the accused. The accused said that it was a mistake and that he would arrange for the correct title deeds, which never happened. The matter came to the attention of the law Enforcement Authorities when the victim made a complaint, and the Police say they then conducted extended financial investigations in the case.

After conviction, the first accused was sentenced to 2-4 years imprisonment for the predicate offences and to 5 years imprisonment for the money laundering offence (s4(1)(iii)AML/CFT Law). The second accused was sentenced to 2 ½ years' imprisonment for the predicate offences and to 4 imprisonment for the money laundering offence (s4(1)(iii)AML/CFT Law). In parallel, civil actions were taken to resolve the property issues.

#### *3.3.5. Extent to which other criminal justice measures are applied where a ML conviction is not possible*

207. Cyprus has a Non-Conviction Based Forfeiture (NCBF) regime but it is limited to where the defendant is no longer alive or is outside the jurisdiction. As a regime, it seems to have been vastly underutilised and as discussed under IO8 there are practical restrictions on being able to utilise the regime. The Cyprus authorities point to issues with defendants outside the jurisdiction and in getting satisfactory MLA and that this explains the lack of prosecution of ML for foreign predicate offending. Such issues can to an extent be mitigated, where there are assets in Cyprus, by using NCBF powers to disrupt ML and dilute any attractiveness of Cyprus as a centre for laundering proceeds, although amendments may need to be considered to exploit further opportunities from the NCBF system.

208. Whilst not criminal justice measures as such, in the FBME case, Cyprus acted rapidly to remove the registration of the Bank, demonstrating the use of administrative/regulatory sanctions to punish legal persons (also noted under 9.5 re TF). Cyprus has also banned bribing companies from public tenders (under the Law Regulating Public Tenders) in addition to using the evidence and co-operation of the bribe givers to pursue the bribe accepting public officials. Where problems in pursuing ML prosecutions have arisen, the Tax Department has been informed in order to consider exercising their powers to recover unpaid tax.

209. Cyprus also assists other jurisdictions in pursuing matters when there are no natural or legal persons in Cyprus to prosecute. Relevant information and/or evidential material is provided to counterparts to pursue their own investigations or assist with ongoing court cases. In some instances, assets have been frozen in Cyprus in co-operation with the foreign countries, for the purposes of future confiscation.

*Overall conclusions on IO. 7*

210. **Cyprus has demonstrated a moderate level of effectiveness with Immediate Outcome 7.**

### *3.4. Immediate Outcome 8 (Confiscation)*

#### *3.4.1. Confiscation of proceeds, instrumentalities and property of equivalent value as a policy objective*

211. Cyprus has in place a comprehensive framework for confiscation and provisional measures, as detailed under Recommendation 4. Specifically, it has a value-based confiscation regime, extended confiscation, presumptions which reverse the burden onto the defendant, and also the provision for non-conviction based civil forfeiture in limited circumstances. Whilst the Assessment team was not provided with a breakdown between proceeds *per se* and equivalent assets frozen/confiscated, the authorities asserted that in most cases, equivalent assets were frozen/confiscated, and that there were no examples to provide of instrumentalities being frozen/confiscated. There was only one example provided of the non-conviction based civil forfeiture regime being used.

212. The Cyprus Authorities assert that confiscation has always been, as a matter of policy and practice, a priority and pursued as a policy objective. Following the money and freezing /confiscating criminal assets has been highlighted by the Attorney General in public statements and in meetings, training and seminars. Furthermore, the FIU has repeatedly issued guidance, through the AG, to the Police and prosecutors on the legal possibilities for freezing and confiscating based on the AML/CFT Law, and this guidance also emphasises the importance, in serious criminal cases,

of financial investigations being carried out at the initial stages of and parallel to the investigation of any offences.

213. The National AML/CFT Strategy, dated January 2019, is cited as underlining the policy objective of confiscation. The AML/CFT Strategy implementation is based on nine pillars, one of which is an upgrade in the structure, training and capacity of investigators and prosecutors in order to enhance the effectiveness for, *inter alia*, confiscating illegal proceeds. Additional training is envisaged as is increased focus on financial investigations. The Action Plan also targets increased training, and in the context of the FIU, additional resources, to enhance confiscation efforts.

### *3.4.2. Confiscations of proceeds from foreign and domestic predicates, and proceeds located abroad*

*Financial investigations with a view to confiscation*

214. Cyprus is developing and improving its approach to carrying out financial investigations yet as mentioned under Immediate Outcome 7, these are not carried out on a systematic basis. It is within the discretion of the investigating officer whether or not to launch a financial investigation. That in itself is not objectionable but it is not entirely clear on what basis FIs are ordered, for example there are no written guidelines on what indicators the police are to consider before initiating a financial investigation, other than that cases involving for example corruption, fraud, PEPs, persons of public interest, and large proceeds/drugs will usually trigger a financial investigation. This lack of clarity could also lead to inconsistencies given that some financial investigations are conducted by district units, and others by centralised units such as the Drugs Enforcement Service, or the Crime Combating Department and its sub-units such as the Criminal Operations Department, the Office for the Combating of Terrorism and the Economic Crime Investigation Office. It is accepted that there is strong co-operation between all the Police departments, with daily contact and joint investigative operations/investigations, but the assessment team raise the possibility that more concrete guidelines could be set to determine on what basis financial investigations should be initiated (whilst of course still affording the discretion currently enjoyed). The assessment team also has some reservations over whether all the police units which may be called upon to carry out financial investigations have the adequate resource and capacity to do so, particularly whilst conducting in parallel the investigation of predicate offences.

215. When the Police conduct financial investigations, they conduct them in a wide manner, following trails and looking at associates/connected persons, and are not narrowly just focussing on the identified criminal. In carrying out financial investigations, the police are reliant on utilising searches with central registries, such as the companies registry, land registry and registries on other property such as cars. The Police have relatively convenient access to some of these registers and even direct access to others. Otherwise, the Police may apply for production orders under the Criminal Procedure Law or disclosure orders under AML/CFT Law to seek the compulsory disclosure of information from banks and other institutions, or production orders to seek production of particular documents. The LEAs utilise a variety of avenues to identify and trace assets, particularly disclosure orders and the Police stated that 98% of banks responded within the 14-day period (the other 2% took longer due to paper-based systems). The Police would welcome the introduction of a banking register to further enhance effectiveness and the same will be achieved when the 5th AML/CFT EU Directive comes into force. The LEAs otherwise may send requests and/or have direct access to a number of sources/registers such as the Land Registry, Register of Companies, lawyers and accountants, records at the Tax Department and Social Insurance Department, and registries of motor vehicles and boats. The Assessment team was satisfied that the authorities were conducting thorough and effective investigations when they were initiated.

216. The authorities are conscious of the need to enhance the pursuit of confiscation generally with regular training given by the FIU lawyers to the police and prosecutors. Co-operation between law enforcement authorities in this area is also very strong, and this includes the FIU who have

some limited quasi-law enforcement competencies. It is stated by the authorities that Joint Investigative Teams are set up for more complex cases, comprising the Police, FIU and prosecutors. But in any event the co-operation on an informal basis is strong and is enhanced through the many secondment arrangements in place, and also the FIU's role in applying for freezing orders, and their assistance throughout confiscation proceedings, something which all law enforcement agencies and the judiciary agreed adds value to the process. Cyprus is encouraged to continue developing its co-operation and its training, and to give consideration to clearer guidelines on when financial investigations should be initiated in order to ensure that confiscation remains a strongly pursued policy objective. Thought should also be given to providing clearer guidelines on the mandates on the different organs of the police, and whether all units have the same resources and capacity to conduct complex financial investigations, and of course whether they are applying the same approach not just to the initiation decision but the parameters of the investigative process.

217. The FIU has a particularly successful record in achieving the confiscation of assets representing foreign proceeds of crime pursuant to requests from other jurisdictions (the majority of such cases relate to property held by legal entities in Cyprus). The FIU plays a significant role in executing the requests from other jurisdictions regarding the confiscation of foreign proceeds held in Cyprus. The FIU has the power to issue postponement orders under s.55 AML/CFT Law. These powers have been used on various occasions (2013;8, 2014;8, 2015;11, 2016;10, 2017;11, 2018;3) and the FIU has also sought freezing orders (even when not requested to do so by the requesting jurisdiction) to enable the effective prevention of assets being removed/dissipated prior to their confiscation and repatriation to the requesting jurisdiction. It is recognised that Cyprus is at an advantage having the use of such formal postponement powers.

*Frozen and confiscated assets*

218. In the review period, Cyprus froze assets worth in excess of EUR 115 million and confiscated assets worth some EUR 13 million in total. This overall figure is encouraging and not insignificant for a jurisdiction the size of Cyprus.

**Table 20: Amounts of funds and other assets frozen and confiscated**

| | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | Total |
|---|---|---|---|---|---|---|---|
| **Property Frozen at the initiative of the domestic competent authorities (EUR)** | 3,825,316 | 1,532,272 | 8,347,427 | 2,480,092 | 4,863,840 | 4,920,950 | 25,969,897 |
| **Freezing orders issued on the basis of a MLA (EUR)** | 23,771,999 | 5,821,271 | 8,870,347 | 28,931,505 2 real estate | 729,420 | 211,076 | 68,335,564 + 2 real estate |
| **Registration of a foreign freezing order (EUR)** | 4,530,383 1 real estate 1 motor vehicle | 15,795,640 | 372,259 | 90,776 | 521,466 1 real estate | 277,735 | 21,588,259 + 2 real estate properties |
| **Total** | 32,025,205 | 22,829,434 | 17,534,852 | 31,492,160 | 6,108,243 | 5,409,608 | 115,893,720 + 4 real |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | estate properties |
| **Confiscated property (domestic predicate offences and ML) (EUR)** | 1,739,275 | 30,507 | 2,110,954 | 7,500 | 1,103,596 | 100,000 | 5,091,832 |
| **Foreign confiscation orders (by consent of the account holder) (EUR)** | 9,160 | 0 | 223,843 | 0 | 124,738 | 76,782 | 434,523 |
| **Registration of foreign confiscation orders (EUR)** | 382,232 | 0 | 0 | 3,354,640 2 real estate | 3,393,192 | 696,605 | 7,826,669 + 2 real estate properties |
| **Total (EUR)** | 2,130,667 | 30,507 | 2,334,797 | 3,323,340 | 4,603,553 | 868,566 | 13,353,024 |

219. These figures relate to domestic predicates and also to the execution of requests from other jurisdictions. Considering Cyprus' profile as an IFC, the Assessment team placed a reasonable amount of weight on the freezing and confiscation of assets pursuant to MLA etc and Cyprus has provided examples demonstrating its positive activity in assisting other jurisdictions. There is still an expectation, given the jurisdiction's profile and its identified risks of proceeds generating offences from abroad, of more proactive freezing/confiscation of such proceeds, resulting from the initiative of Cyprus. The figures also include amounts returned to victims. Victims may pursue the offender through civil actions, and section 8 of the AML/CFT Law provides that confiscation orders do not prevent the same. However, after confiscation, proceeds are returned to any victims without the need for them to pursue matters personally.

220. Within the confiscation results that Cyprus has achieved, the success rate from property frozen has varied somewhat, and in some years (2014, 2016 and 2018) the domestic confiscation rates are not overly impressive when viewed in isolation (and even including the enforcement of foreign confiscation orders the figures in total for 2014 and 2018 are low). There are gaps between the amount of property frozen and that which has been ordered for confiscation (overall 13% of frozen assets confiscated). The assessment team recognises that property frozen in one year may remain so for a few years until proceedings are concluded, but the above shows a window of six years and an appreciable discrepancy between property frozen and property confiscated throughout the whole period. Notwithstanding, if cases are taking a long time to come to court, this could have a detrimental effect on the effective management of frozen assets, which is covered in more detail below. Whilst it is said that the majority of frozen assets are money in bank accounts and real estate, there may be such an effect on depreciating assets such as motor vehicles, and as Cyprus further improves its ML efforts and freezes more complex assets, this possibility for the need for enhanced asset management could become more relevant.

221. Regarding asset-sharing, Cyprus has scope to return foreign proceeds to the country from whence they came under certain multilateral treaties such as UNCAC and the Palermo Convention, and ss.39(3) and 43IA(4) AML/CFT Law provide the domestic *vires* for doing so. Examples of asset sharing have been provided under IO2.

222. The figures for the underlying domestic predicate crimes were not available for all the years

although the authorities did confirm that the majority of assets confiscated were proceeds or equivalent property from corruption, fraud and drug trafficking. The assets confiscated in domestic cases were mostly from natural persons, and the assets were mainly land, movables (such as cars) and monies in bank accounts.

**Box 8.1: Examples of confiscation**

Case 1: The Police investigated a case of a fraudulent sale of real estate to a state-owned company at a largely inflated price. A number of people benefited from the fraud, including government officials and persons working for the state-owned company. The Police carried out a financial analysis and co-operated with the FIU for freezing the traced assets. The money received as bribes was not found, therefore equivalent value property of the accused was frozen; money in bank accounts as well as real estate property. In the case of one of the accused the property frozen (EUR 300,000) was property identified to be owned by the accused in a foreign country i.e. money in a bank account in his name was traced in the UK, which was restrained by the UK following a mutual legal assistance request sent by the Cyprus Police to the UK Authorities. The other property frozen in this case was property held by a 3rd person to which the accused made a prohibited gift caught under the AML/CFT Law i.e. the accused transferred ½ of his house to his wife a few months before the criminal procedure started. This property was held to be realisable property and was also restrained with a Court order as a prohibited gift made by the accused to a 3rd party.

Five natural persons were convicted for corruption related offences and money laundering offences as well as a legal person, a company which was found guilty for money laundering offences. A confiscation order was issued against all the convicted persons natural and legal. All the accused were convicted both for the predicate offences (bribery offences) as well as for ML offences and a confiscation order was issued against them for the benefit they obtained from the commission of the offences.

Frozen – EUR 60,295, 12 real estates, 1 motor vehicle

Confiscation order for the total of – EUR 750,000

It is noted that for the satisfaction of the confiscation order the amount of EUR 300,000, which was frozen in UK, was subsequently, after consultation with the UK authorities, brought back to Cyprus and was used to partly satisfy the confiscation order with the consent of the accused person and the money was returned to the victim.

Regarding the property restrained in the hands of the 3rd party as a prohibited gift, the accused paid in cash the whole value of the said restraint property towards the confiscation order and thus the restraint of the property in the name of the third person was withdrawn.

Case 2: This was a case of drug trafficking through the dark-web and post office. During the search warrant executed by the Police at the house of the drug trafficker, laptops were seized. The Police carried out an analysis of the data in the laptops, and e-shop in the dark-web and e-wallets were traced. According to the analysis of his client list, he had managed to sell approximately 5 kilos of drugs in a year. In one of his e-wallets, among other e-wallets he had created, 48.8 bitcoins were traced. A Court Freezing Order was issued for the 48.8 bitcoins but by the time its execution, unknown persons removed the 48.8 bitcoins from the suspect's e-wallet, while he was in custody. In view of this event the freezing order could not be enforced against the bitcoins *per se*.

However, subsequently, financial investigations using disclosure orders revealed that the accused was the owner of real estate of significant value. The lawyers of the FIU applied to the Court for the freezing of equivalent value property i.e. immovable property of the accused. A restraint order was issued by the Court for the immovable property. The accused pleaded guilty to drugs offences and consented to the confiscation of EUR 100,000, as the equivalent amount to the bitcoin value.

On 15/11/2018 EUR 100,000 was confiscated, and the restraint order remained in force until the confiscated amount was paid by the accused, EUR 80,000 of which has been satisfied so far.

223. There have been no TF confiscations, albeit as discussed under IO9 there has been a confiscation relating to the proceeds of providing support to a terrorist group.

*Enforcement of orders and management of seized and confiscated assets*

224. Relative to the amounts ordered confiscated, the recovery rate of assets confiscated is strong as it is about 75-80%. Assets confiscated may be managed by the Official Receiver, who is usually appointed for realising real estate sales. Certain movable frozen property is managed by the Police; there is no specialised asset management unit, but each investigator is responsible for dealing with seized items. There is the possibility of appointing independent receivers to manage particularly complex property (this hasn't occurred yet: the *bitcoin* confiscated is in the process of being realised by the defendant paying the equivalent amount to the confiscation order) and there are powers to dispose of seized property although this has not been used in practice. Realised funds are transferred into the Confiscation Fund which is ring-fenced to be used for "social purposes" and not the general expenditure of the Republic.

225. As the jurisdiction matures in its approach to ML and asset seizure/confiscation, consideration could be given to creating a specific asset management unit with persons experienced in the same (the Asset Recovery Office within the FIU is merely a channel for international co-operation) or expanding the office of the Official Receiver. Such an office may create cost savings instead of having to appoint independent receivers when complex assets are under sequestration. It would also ensure consistency in the approaches taken as regards asset management.

*Non-Conviction based forfeiture*

226. As mentioned above, Cyprus has a non-conviction-based forfeiture regime, something which goes beyond the FATF standards and is a welcome addition to the Law Enforcement Authorities' arsenal in confiscating criminal property. The NCBF regime applies when the defendant is outside the jurisdiction or has died. The prosecutor must still present evidence and establish a *prima facie* case that the suspect committed the offence, and also satisfy the court that reasonable efforts have been made to locate the suspect. Therefore, the system is useful only to a certain extent which may explain the lack of its application so far. Cyprus may wish to consider adapting the system given the character of Cyprus' financial system. For example, there may be situations ripe for the use of this regime where the defendant is abroad and there is not enough evidence for the criminal standard to prosecute (and extradite). Cyprus is encouraged to explore the benefits of amending its legislation to enable the utilisation of this regime more regularly. So far there has only been one NCBF order:

**Box 8.2: Example of non-conviction based forfeiture**:

An MLA request led to identification of illegal proceeds in a Cyprus bank account. An NCBF order was made against the property of an absent suspect for €803,000. The offences were committed in the U.S.A. and the proceeds laundered in a Cyprus bank account held by a foreign company whose beneficial owner was also foreign. The monies were repatriated to the victim

227. According to the authorities, there are a number of freezing orders currently in force which might lead to more NCBF. Cyprus has recently enacted legislation to register non-conviction based civil forfeiture orders made in other jurisdictions, with the first order successfully registered in July 2019.

*Conclusion*

228. Cyprus has demonstrated to a reasonable extent that it is confiscating criminal property (primarily proceeds or property of an equivalent value) further to domestic criminality, or on the request of another jurisdiction as regards the proceeds of foreign criminality. The LEAs appear to be well resourced and equipped to carry out the investigations required to trace and seize property in relation to *domestic cases* and build those cases to successfully get confiscation orders. Whilst the overall figures are reasonable, there are variances between years, the divergence between frozen assets and those confiscated is appreciable, and there is not enough domestically initiated asset

freezing/confiscation regarding foreign predicate crimes. There is a desire to increase investigative activity regarding more complex money laundering and in respect of foreign predicate offending. Therefore, it could be said that the law enforcement authorities whilst able to manage at present, without too many issues, confiscation activities with regard to domestic centric and self-laundering matters and the execution of foreign requests, things could be more difficult as the jurisdiction begins to expand its activities in line with the risk profile and the findings under IO7.

### *3.4.3. Confiscation of falsely or undeclared cross-border transaction of currency/BNI*

229. As an Island, Cyprus does not have to contend with physical borders *per se* other than the so called "green line", operating since the cease fire since 1974, which separates the areas under the effective control of the Republic's government from the occupied areas.

230. Cyprus operates a cash declaration system at its port entry points (airport, harbour etc.) including for those entering from other EU jurisdictions. It also applies the declaration system to persons crossing from the occupied areas back into the part of the Island under the effective control of the Republic's Government (there are no customs controls carried out by the Cyprus authorities on persons leaving the areas controlled by the Government into the occupied areas[28]). Prominent signage is displayed at the entry/exit points in Greek, English and Russian.

231. The customs authorities are fully aware of the risks associated with their jurisdiction. There are threats associated with smuggling of tobacco and other goods from the occupied areas or Middle East jurisdictions. The high duties in Cyprus provide an incentive for smuggling such goods into Cyprus. However, in addition to the cash declaration system in place at the green line, Cyprus also carries out checks on goods entering from the occupied areas pursuant to EC Regulation 866/2004. Strict limits are placed on the amount of tobacco and alcohol which can be brought into the areas under the effective control of the Republic, and a maximum value of €260 applies for other goods. Counterfeit or other illicit goods are confiscated. Persons and cars are subject to searches at the crossing points, although it is acknowledged that constantly patrolling the entire green line/Buffer Zone poses inevitable challenges and difficulties.

232. Although, as identified under Recommendation 32, the declaration system does not apply to mail cargo, Cyprus does however exercise diligence regarding mail/cargo in general to detect illicit goods and large amounts of cash. Customs Officers are present at all times at entry points and utilise x-ray, random and targeted searches, and sniffer dogs (for drugs) to detect such items. There are, for example, ongoing proceedings for cases where large amounts of cash were discovered secreted in children's toys:

**Box 8.3: Mail/Cargo Cash seizure example**

In 3 separate cases[29], large quantities of cash (USD 50,000 USD 3,000 and USD15,600) were found during physical checks of mail of temporary storage boxes at Larnaca airport of mailed goods. The cash was thoroughly hidden; in one case in a teddy bear, in another an army shoe. The boxes were sent by females in USA/Canada and addressed to men of Nigerian nationality who reside in the occupied areas. Investigations are ongoing and the cash is seized.

233. The authorities acknowledge that the maximum penalty for false declarations or failure to declare (where there isn't a separate ML/TF offence) at €50,000 is a weakness which they intend to amend. For cases of false/failed declarations, the authorities separate out Category A cases (*bona fide* mistake), Category B (suspicion of ML/TF but co-operation and no evidence to proceed) and Category C cases (sufficient evidence to prove cash related to commission of ML/TF). The vast majority of cases have involved cash as opposed to BNI. In Category A cases, the authorities impose

[28] Protocol 10 to the Treaty of Accession only provides for controls on movements into the area under the effective control of the Republic of Cyprus

[29] After the on-site visit, the Assessment team was informed that there are now some 14 similar cases and confiscation proceedings were ongoing with EUR 200,000 already confiscated.

penalties between 8-10% of the amount of cash. In Category B cases, the authorities compound the criminal offence (at the discretion of the Director) by ordering the confiscation of the undeclared/falsely declared cash, where after thorough investigation the origin of the money can be justified and there is no evidence of ML/TF. The offender still has a criminal record and is forced to surrender all or a proportion of the cash. The authorities state that the penalty imposed is the "maximum possible" although this is not apparent from the figures below. The authorities explained that this referred to the amount falsely or not declared, not the maximum penalty of €50,000, yet the amounts confiscated are still not the full amount of those falsely/not declared. The penalties are said to range between 8-100% of the amount falsely/not declared. The decision of the Director on the amount by which to base the compounding is based on all the circumstances such as the evidence of ML/TF suspicion, and the explanations of origin of the cash. In category C cases, the authorities confiscate the whole amount under the Customs Code. Unless the offender submits a Notice of Claim within one month, the whole amount is summarily forfeited, otherwise court proceedings are instituted for the condemnation of the seized cash. Customs also refer the matter, in Category C cases, to the police/PPO for investigation/prosecution for the ML/TF offence. The following table provides the figures for the review period:

**Table 21: undeclared cash and related penalties**

| Year | Category | EU | | | | Non-EU | | | | Total | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Undeclared cash | Penalties | Per Cat. | Total | Undeclared cash | Penalties | Per Cat. | Total | Per Cat. | Total |
| 2014 | cat A | €1,006,414 | €87,574 | 36 | *40* | €498,426 | €42,451 | 26 | *34* | *62* | *74* |
| | cat B | €121,245 | €15,425 | 3 | | €298,248 | €57,580 | 7 | | *10* | |
| | cat C | €16,000 | €16,000 | 1 | | €26,965 | €26,965 | 1 | | *2* | |
| 2015 | cat A | €874,293 | €36,240 | 16 | *20* | €214,713 | €132,234 | 7 | *13* | *23* | *33* |
| | cat B | €181,500 | €22,000 | 4 | | €62,500 | €20,900 | 5 | | *9* | |
| | cat C | €0 | €0 | 0 | | €17,732 | €17,732 | 1 | | *1* | |
| 2016 | cat A | €273,345 | €24,620 | 8 | *18* | €263,924 | €144,074 | 8 | *12* | *16* | *30* |
| | cat B | €321,103 | €75,000 | 7 | | €24,164 | €21,900 | 4 | | *11* | |
| | cat C | €138,268 | €138,268 | 3 | | €0 | €0 | 0 | | *3* | |
| 2017 | cat A | €44,687 | €4,500 | 2 | *6* | €149,297 | €12,500 | 6 | *14* | *8* | *20* |
| | cat B | €254,079 | €58,000 | 3 | | €398,885 | €72800 | 8 | | *11* | |
| | cat C | €98,660 | €98,660 | 1 | | €0 | €0 | 0 | | *1* | |
| 2018 | cat A | €0 | €0 | 0 | *1* | €74,672 | €12,500 | 4 | *5* | *4* | *6* |
| | cat B | €0 | €0 | 0 | | €5,950 | €1,800 | 1 | | *1* | |
| | cat C | €113,600 | €113,600 | 1 | | €0 | €0 | 0 | | *1* | |

234. In deciding whether or not to compound the false/failure declaration offence, the Customs Authorities will take into account the evidence presented by the offender and that gathered during

the investigation. They will consider the following in determining whether there are ML/TF suspicions sufficient to continue with an investigation:

a) country of origin/destination/route of passengers;

b) unwillingness or avoidance to provide information about the scope of transfer or use;

c) insufficient documentation as to the origin of money

d) the amount of cash declared or found

e) method of concealment;

f) behaviour during controls; and

g) adversely known passengers.

The Customs Authorities will check their own database and the police one, which they have access to, in conducting these enquiries. They will also liaise with other partner agencies such as Ministry of Labour, Tax Office and immigration colleagues. It was said that in "serious" cases the matter would not be compounded but referred on for further investigation/prosecution for both the false/failure offence and also ML offence (whilst the cash would be potentially forfeit under the Customs Code). The authorities provided two examples of cases before the Court for ML prosecution based on undeclared cash, these cases are still ongoing.

235. It is recognised that there will be a range of offences and that a person falsely declaring might be considered to merit a higher sanction than someone who simply fails. However, Category B for example is said to involve those where there is a suspicion of ML/TF, and the penalties applied do not appear to be punitive particularly when they are less, by some way, than the amounts not declared/falsely declared:

**Table 22: Category B cases of undeclared cash and related penalties**

| Year | **Undeclared Cash (€)** | **Penalties (€)** | **%** |
|---|---|---|---|
| 2014 | 419,493 | 73,005 | 17.4 |
| 2015 | 313,734 | 42,900 | 13.6 |
| 2016 | 465,177 | 96,900 | 20.8 |
| 2017 | 652,964 | 130,800 | 20 |
| 2018 | 12,500 | 1,800 | 14.4 |

236. There is a danger of the penalties not being seen as sufficiently punitive and dissuasive in such circumstances. The compounding system is in itself not an issue and can be an efficient way of addressing the matter and confiscating criminal money without the burden of a formal prosecution (indeed the NRA recognises that compounding is often done as a way of saving administrative costs), but the penalties imposed should not be seen as light consequence. However, it is accepted that as the maximum fine is 50,000 EUR, formal criminal proceedings may at present not be seen to add much when similar amounts can be confiscated, and the offender is left with a criminal record in any event using the compounding system.

237. Customs officers have the powers to stop/restrain cash when there has been a false/failed declaration. In the absence of a false/failed declaration, the Police have this power. The strong co-operation between the authorities and the fact that Police are present at entry points for border control means that the system works relatively well in practice. However, the Customs authorities accepted that they would prefer to have this power themselves, and it would enhance effectiveness. Checks on passengers and their luggage are selected mostly on a random basis or the experience of the officers who recognise certain behaviours, appearances and travel patterns.

238. Certain high-risk flights may also be closely monitored and intelligence from other jurisdictions may be shared with the customs authorities which can also inform their targeting. A new Passenger Information Unit, due to be set up his year, should assist in processing information

from airlines, and a customs officer will be based within the Unit, to help enhance the systems on monitoring and searching certain passengers.

239. The statistics presented show that there is more cash detected at the ports leaving Cyprus which is not declared or falsely declared. These statistics include the occupied areas coming in the way but not outgoing. The figures therefore arguably demonstrate a heavier focus on cash leaving the jurisdiction. Whilst the authorities explained that all outgoing luggage (at the ports) is scanned whereas incoming passengers are targeted randomly, the assessment team would have expected, given that Cyprus is an IFC, more heightened focus on potential dirty money coming in to the jurisdiction, something which is also highlighted in the Action Plan. It is said that the introduction of a new PNR system (together with the new Passenger Info Unit) and the employment of new staff will enhance effectiveness by enabling the more targeted control of incoming passengers. Further, there are also provisions in the Customs Code which proscribe the giving of untrue statements on giving information for the purposes of the customs or other legislation, and this was the basis for the cases referred to in the example in Box 8.3.

240. Customs keep a database on declarations and also for false/failed declarations. They are alive to potential smurfing threats and monitor persons who have been detected to transport smaller amounts under the threshold on a regular basis, although it was acknowledged there is a reliance on such persons self-declaring even when below the threshold which is unlikely to lead to the detection of genuine criminals using smurfing techniques. If persons are identified to have suspicions, they may be referred to Customs HQ for possible onward dissemination to the FIU.

### *3.4.4. Consistency of confiscation results with ML/FT risks and national AML/CFT policies and priorities.*

241. Cyprus has achieved appreciable results as regards the confiscation of assets representing the proceeds of domestic criminality and, pursuant to requests for assistance, those representing the proceeds of foreign criminality. Where Cyprus is less effective is in freezing and confiscating the proceeds of foreign criminality, on the initiative of the domestic authorities (as opposed to be where it is triggered by requests from other jurisdictions).

242. The largest proceeds of domestic criminality correlate with the high-risk predicate offences. The table below shows the highest proceeds generating offences, drugs, fraud and corruption, between 2013-2018 and the total amounts confiscated in those years for all crimes (including predicate and ML):

**Table 23: Convictions for high risk predicate offences and total confiscation for all domestic predicate offences**

| Year | Fraud convictions | Drugs Convictions[30] | Corruption and Bribery Convictions | Total confiscation for all offences (€) |
|---|---|---|---|---|
| **2013** | 62 | 697 | 4 | 1,739,275 |
| **2014** | 32 | 749 | 6 | 30,507 |
| **2015** | 31 | 575 | 3 | 2,110,954 |
| **2016** | 14 | 438 | 4 | 7,500 |
| **2017** | 17 | 153 | 25 | 1,103,596 |
| **2018** | 8 | 44 | 2 | 100,000 |

243. The overall amount confiscated, particularly when one takes into account the figures confiscated pursuant to foreign requests, is not to be dismissed and demonstrates a system which is functioning effectively to some extent. The property confiscated is mostly real estate/land and money, and as mentioned above when the confiscation derives from a request from another jurisdiction, assets are usually held by legal entities. Cyprus has demonstrated an ability to go after

[30] These figures are inclusive of drug possession convictions which will not usually, if ever, have any potential to generate proceeds of crime, particularly compared to drug trafficking/distribution.

the proceeds of corruption, identified high-risk proceeds generating offence, as seen with the CBC ex-Governor case (see Box 7.8) and the example involving the Turkish-Cypriot property also detailed under IO7.

244. Given the risks identified in the National Risk Assessment regarding the international use of financial system and economy, the Assessment team does expect to see higher numbers overall and more specifically, an increase in proactive confiscations regarding foreign criminality proceeds, not just when it is in the execution of an MLA request. In some instances, the Cypriot authorities, on their own initiative, have however informed foreign counterparts of the existence of proceeds/equivalent property and have provisionally frozen such property pending the receipt and execution of an MLA request.

245. The National AML/CFT Strategy is relatively high level and focuses on further improving the jurisdiction's risk-based approach to freezing and confiscation. However, the steps taken by Cyprus, further to the Action Plan, to increase its resources within the FIU, police and PPO is welcome as is the utility of secondments between agencies. Such measures will no doubt enhance the efforts to prioritise confiscation commensurate to the jurisdiction's risk profile by taking a more proactive approach to pursue foreign proceeds.

*Overall conclusions on IO.8*

246. **Cyprus has demonstrated a moderate level of effectiveness with Immediate Outcome 8.**

## 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

### *4.1. Key Findings and Recommended Actions*

**Key Findings**

**Immediate Outcome 9**

1. Cyprus considers that its risk of TF is exacerbated by its proximity to conflict zones. The primary TF threats are not associated with domestic criminals/terrorism threat but with the jurisdiction's status as an IFC. However, there are very few cases and STRs and no incoming MLA regarding terrorism/TF, and no designated persons for TF have been identified to have assets in Cyprus. The NRA rates TF risk as Medium which conclusion appears to be based on caution given the status as an IFC.
2. There have been no TF prosecutions *per se*, but there have been two convictions for terrorism type offences, demonstrating that the jurisdiction is not complacent regarding potential terrorism threats. In these cases, the authorities carried out investigations (including in one case sending out MLA requests) to identify if there was any potential TF, and none was found.
3. The primary focus of the LEAs and intelligence authorities (including the Fusion Centre) is on terror threats and whilst this may encompass financial aspects, the bigger TF threats in Cyprus do not relate to domestic terrorism *per se*, but international terrorism
4. The authorities investigate the financial aspects where there is a terrorism investigation/prosecution and have carried out seven TF investigations in the review period. It is recognised that LEAs have not had much resource to harvest TF investigations from, given the low amount of SARs and no incoming MLA.
5. The jurisdiction has taken steps to increase training and awareness of TF risks, including training for the national authorities and discussions and conferences with other jurisdictions and NGOs, and there has also been outreach to the financial sector and NPOs.

**Immediate Outcome 10**

*Targeted Financial Sanctions*

1. TF-related targeted financial sanctions (TFS) are implemented without delay through a combination of supranational (at EU level) and national mechanisms.

2. Cyprus has not identified any targets for designation or proposed any designations to the 1267/1989 Committee or the 1988 Committee. It has never put forward a designation on its own motion, nor received a request from another country to give effect to freezing measures pursuant to UNSCR 1373. For both regimes, Cyprus relies on the EU supranational framework. However, an informal mechanism exists within the Cyprus government to develop materials capable of supporting proposals for the designation of specific targets of financial sanctions for terrorism-related activities through the EU autonomous sanctions regime.

3. The supervisors have effective channels to communicate new designations to obliged entities. They also communicate the seriousness of compliance with TFS through regulations, notifications, and examinations. Compliance with relevant requirements is verified during on-site inspections, with the exception of examinations by supervisory authorities of real estate agents and the casino. In general, checks on compliance with TFS form part of full scope AML/CFT audits. While the CBC has devised a detailed on-site checklist, other supervisory authorities do not have such manuals in place.

4. No funds or other assets have been frozen in Cyprus to date under TF-related TFS. However, in general, all obliged entities are aware of TF-related TFS screening obligations and the requirements to freeze funds/assets and have systems in place that allow them to implement TFS. There are

elements which are indicative of a functioning system e.g. identification of partial matches, matches with non-TF related sanctions regimes.

5. Obliged entities screen customers against sanction lists. However, the frequency and depth of screening varies widely: from real time screening of customers, incl. customer-related persons such BOs, all the shareholders in entire ownership chain and transaction counterparties, to screening checks of customers and BOs conducted on a periodic basis.

6. Banks articulated a sophisticated understanding of the sanctions evasion risk, expressing concerns about complex structures of legal persons and about activity on behalf of designated persons by associates of their customers. Consistent with this risk understanding, banks appear to apply adequate measures to mitigate sanctions evasion risk. Given the materiality of the banking sector, these findings would suggest that Cyprus is taking measures in line with the risks it faces.

7. Other obliged entities, especially ASPs, did not demonstrate the same level of understanding of the risks of TFS evasion as banks. The inability to identify individuals or entities who may seek to conceal their identity behind complex structures to evade sanctions constitutes a significant vulnerability in Cyprus given its status as an IFC and the role played by ASPs as gatekeepers.

*Non-profit Organisations*

8. At the time of the on-site, Cyprus started conducting a review of the NPO sector and, as such, has been in the process of identifying the subset of organisations which by virtue of their activities or characteristics are likely to be at risk of TF abuse.

9. None of the measures taken so far by Cyprus have been based on an in-depth understanding of the risk of TF faced by NPOs in Cyprus and no aspect of the oversight mechanism relates to ensuring that they are not abused for the purposes of TF.

10. A positive aspect of the system is the online Register of NPOs. Authorities are in the process of building a comprehensive database on NPOs that shall be used for the future assessment of the NPO sector and implementation of a more in-depth risk-based approach.

**Immediate Outcome 11**

1. Implementation and communication of PF-related TFS follow similar processes as with TF-related TFS (see related KFs under IO 10). No funds or other assets have been frozen in Cyprus to date under PF-related TFS.

2. There are domestic processes in place to issue export licences for dual-use goods and military equipment and exercise controls on the exportation of sensitive goods.

3. There has been one investigation by the competent authorities into a suspected case of PF related to a possible violation of sanctions on DPRK, which involved the importation of herbal medicine and cosmetics. The investigation revealed that no items were imported into Cyprus and no PF had taken place.

4. As with TF-related TFS, obliged entities are generally aware of the need to have protocols in place to freeze any assets without delay as part of the implementation of PF-related TFS. However, most obliged entities that were asked, including sophisticated banks, had difficulty in articulating differences between TF and PF, in terms of geographic risks, transaction typologies, or other types of distinctions. In the absence of a manifest geographical link, obliged entities might be less effective at identifying and taking action with respect to PF transactions and proliferator clients.

5. Limited initiatives to raise awareness of obliged entities in relation to PF issues have been taken by supervisory authorities.

6. The supervisory measures for monitoring compliance with PF-related TFS are similar to those described under IO 10. The on-site methodologies developed by the supervisory authorities do not specifically distinguish between PF-related TFS and other TFS regimes. Apart from the CBC, the

competent authorities do not appear to be prepared to monitor PF-related TFS requirements as such.

7. None of the supervisory authorities have detected any significant shortcomings in the area of PF-related TFS compliance, which is surprising given the findings of the assessment team that there does not appear to be widespread understanding of PF as distinct from TF requirements and there appears to be an absence of comprehensive internal control procedures directed at PF-related TFS.

**Recommended Actions**

**Immediate Outcome 9**

1. The jurisdiction should continue to try and harvest more TF investigations from SARs and increase its aggressiveness in doing so. Furthermore, it should also seek to explore, using the newly formed MLA Office, whether any TF investigations can be harvested from incoming MLA (bearing in mind that there has been no incoming TF MLA thus far).
2. Further training (including further bilateral/multilateral conferences with foreign jurisdictions such as those that Cyprus has already participated in) is strongly encouraged for investigators, prosecutors, and the judiciary to ensure all potential TF can be identified, investigated and pursued.
3. Consideration should be given to the FIU having a more permanent role/presence on the Fusion Centre.
4. The Police are also recommended to ensure that there are clear guidelines in place for when investigations are carried out and when they are done by the CCD/ECIO.
5. Further outreach to the financial sector and NPOs is also increasingly important to ensure they enhance and improve the understanding of TF risks to ensure that they can discharge their obligations as the first line of defence against TF.

**Immediate Outcome 10**

1. Cyprus should develop a formal procedure for domestic designations (addressing the requirements under c.6.1 and 6.2) and de-listing/unfreezing procedures (addressing the requirements under c.6.6).

2. The supervisors should intensify outreach to increase the risk understanding of the private sector, other than banks, in relation to TF-related TFS (with a specific focus on sanction evasion risks), and should ensure that all obliged entities have detailed internal written procedures in place and implement those procedures.

3. Supervisory authorities should take further steps to enhance the supervision of obliged entities in relation to TF-related TFS, including the development of offsite and onsite supervisory tools (off-site monitoring, on-site methodologies and checklists) and maintain comprehensive records of the supervisory findings, etc.).

4. Supervisory authorities, particularly of non-bank FIs and DNFBPs, should apply sanctions for non-compliance with TF-related TFS requirements, such as the requirement to screen all customer transactions against applicable sanction lists, and to maintain adequate internal controls in this regard.

5. Cyprus should conclude the risk assessment of NPO sector to identify those NPOs that are vulnerable to TF abuse and implement a risk-based approach to monitor the NPO sector consistently with TF risks.

6. Cyprus should raise the awareness of NPOs regarding the FT risk within the sector and provide advice to NPOs on best practises to protect themselves from TF abuse.

7. Measures should be taken to ensure that the banking sector assess the risks posed by NPOs on a client-by-client basis.

**Immediate Outcome 11**

1. Cyprus authorities should provide targeted outreach, training and guidance on PF-related TFS to the obliged entities, prioritising sectors deemed at highest risk.

2. Supervisory authorities should take further steps to enhance the supervision of obliged entities in relation to PF-related TFS, including the development of offsite and onsite supervisory tools and practices (on-site methodologies, comprehensive records on the supervisory findings, etc.).

3. Supervisory authorities should apply sanctions for non-compliance with PF-related TFS requirements.

4. Supervisors should develop sufficient expertise in relation to PF-related TFS to ensure adequate monitoring of compliance by the private sector.

247. The relevant Immediate Outcomes considered and assessed in this chapter are IO.9-11. The Recommendations relevant for the assessment of effectiveness under this section are R. 1, 4, 5–8, 30, 31 and 39.

## *4.2. Immediate Outcome 9 (FT investigation and prosecution)*

### *4.2.1. Prosecution/conviction of types of FT activity consistent with the country's risk-profile*

248. Cyprus considers that its terrorism risk is exacerbated primarily by its proximity to conflict zones. The authorities recognise that despite Cyprus historically being considered to be at low risk of facing terrorist incidents, the threat (of terrorism) is regarded as medium. This is due, they say, to the proximity issue, the instability and lack of basic security in the Middle East, the trend of terrorist attacks in Europe, the presence of British armed force bases and other Western interests in the Island, and illegal immigration from Turkey through the occupied areas.

249. The TF risk is also rated as medium in the NRA, although the primary TF threats are not associated with domestic criminals and/or the above terrorism threat as such, but because of its status as an IFC and the risks of funds being transited through Cyprus or being managed within Cyprus. During the review period, there were no TF prosecutions, very few TF investigations (7), a negligible amount of TF STRs (38) and non-existent incoming MLA regarding terrorism/TF. Furthermore, there are no persons or entities on designated EU/UN lists who have been identified to have assets in Cyprus. No designated persons have been reported to have attempted to conduct transactions in or through Cyprus.

250. Cyprus has had no TF prosecutions but has had one conviction under section 8 of the Combating of Terrorism Law 2010 for the providing of support to a terrorist group:

**Box 9.2: Abdallah Case (2015)**

In 2015, a Lebanese national, who was a holder of a Canadian passport, was arrested by Cyprus Police at a house in Larnaca, having been identified as a possible Hezbollah operative in relation to a planned terrorist attack. Intelligence had detected that the house was used by Hezbollah to store thousands of kilograms of Ammonium Nitrate, which Police suspected would be used to conduct a terrorist attack against a target in Cyprus or abroad. During the investigation, approximately 8.5 metric tons of Ammonium Nitrate, was found to have been stored in the basement of the said house and the authorities also discovered EUR 9,400 which represented the defendant's payment of fees and personal expenses. The defendant was convicted of several charges including the provision of support to a terrorist group, under section 8(1)(a) of the 2010 Law, and also for money laundering in respect of the money (s4(1)(a)(iii) AML/CFT Law; acquisition, possession or use of criminal proceeds), and this money was also confiscated. He was sentenced to 6 years' imprisonment.

The authorities confirm that a financial investigation was conducted but no further financing, in either direction, was discovered.

The Cyprus Police took all investigative measures to pursue any TF aspect of the case. A TF investigation was undertaken but no funds were traced in Cyprus since, following inquiries, it was established that the accused had no accounts held with local banking institutions and no other assets were traced in Cyprus. Additionally, Interpol messages were sent to all involved jurisdictions and FIU channels were also used. The respective information acquired was utilized for the purposes of pursuing the investigation of the case, including the preparation and submission of three outgoing MLA requests to three foreign jurisdictions and the issuing of a European Arrest Warrant.
Given the fact that this was a lone wolf case with unsophisticated methods and small amounts of money involved, it is not necessarily surprising that no TF was detected in either direction.

251. Whilst this was not a TF conviction, he was convicted of providing support to a terror group in return for payment, and he was also convicted of ML. The intelligence and law enforcement authorities are of course to be commended for the success of this case, which is a demonstration of their vigilance and their proactive efforts to disrupt terrorist activities, but as IO9 is concerned with terrorist financing, only so much weight can be placed on it. Furthermore, as stated above, the primary risks associated with the jurisdiction are not with individuals planning terror attacks at home or abroad (albeit that like most jurisdictions there is always a need to be alert against such possibilities), but with the international business taking place in the jurisdiction. As the National Risk Assessment puts it:

"*In Cyprus there are no native groups designated as terrorists.*
*It is assumed that TF threat emerging from external funding is higher than the threat emerging from domestic funding. Although, there is little evidence of TF, and despite the low number of operations relating to terrorism activities up to date, the risk of terrorist funding cannot be excluded.*
*Cyprus, being a financial centre, offering international business facilities, can be abused for TF. Therefore, the threat level is assessed as medium*."

252. Cyprus thus recognises that being an IFC may heighten the potential threat of the financial system being abused for TF. This conclusion was primarily made out of an abundance of caution and to avoid complacency (which as discussed further below is reflected in the actions taken by Cyprus), given that Cyprus is an IFC and is proximate to conflict zones. As mentioned under Immediate Outcome 1 (see Para 68 and Key Finding 1) TF risk has clearly been considered and assessed and Cyprus has a good understanding of the risk. Some authorities (e.g. the FIU and Cyprus Intelligence Service ("CIS" or "KYP") which are key authorities as regards this matter) appear to have a more sophisticated understanding of TF risks and as discussed further below (Para 262), the Fusion Centre (which is comprised of *inter alia* the CIS) carries out quarterly counter terrorism risk assessments. In order to gain a more complete understanding of TF risk, all potential avenues explored may need to be explored to a greater depth.

253. In terms of prosecutions/convictions which are consistent with the risk profile, there have been no TF prosecutions/convictions. Regarding substantive terrorism offences, there has been the Abdallah case (above) and there has also been a conviction for participation in an organised crime group (discussed further under core issue 9.5 below). There have however been no prosecutions/convictions of terrorist financiers, or third-party abusers of the financial system or identified vulnerable areas such as NPOs and MSBs. So whilst it is not possible to conclude that the terrorism cases prosecuted were necessarily wholly consistent with the country's TF risk profile, or at least the higher risks, because they were not TF cases nor did they involve abuse of the financial system, the authorities have demonstrated that they are not complacent and therefore that if a TF case presented itself, they would react accordingly and aggressively investigate and prosecute it..

254. No TF cases have come before the PPO to prosecute. There is no specialised unit for financial crime within the PPO but as discussed under IO7, cases are generally allocated to those with more experience of financial crime. As also mentioned under IO7, thought could be given to considering more specialism within the PPO for financial crime.

### *4.2.2. FT identification and investigation*

255. As stated above, there were seven TF investigations during the review period. Two of these were carried out as a result of the terrorism/participation in OCG cases. One is the FBME case (see below). The remaining four were as a result of SARs disseminated to the Police by the FIU. Within the Police Crime Combating Department, there is a dedicated Office for Combating Terrorism ("**OCT**"), which *inter alia*, co-ordinates the actions and policies that Cyprus Police should adopt regarding terrorism in accordance with international obligations; it collects, evaluates and analyses information related to terrorism; it provides expertise to operations and investigations; it prepares and delivers training programmes and seminars to other police officers and other LEAs on terrorism; and it maintains a national database concerning terrorist attacks, terrorist organisations and individuals related to terrorism. The OCT is therefore a welcome step and it can investigate TF albeit when there is a financial element, the Economic Crime Investigation Office will also usually be involved in the investigation given its specialist financial crime knowledge and experience which has been, and continues to be, developed through the TF investigations carried out so far, which have included tracing financial transnational links for possible TF. It is not automatic that these specialised units would lead on/be involved in, all TF investigations as the authorities state that Police Standing order 3/39 provides that the OCT may provide support to local investigations concerning such offences. Similar to the issues raised under IO7, there may be difficulties in expecting the district offices to have the resources and capacity to investigate TF (particularly those districts without an economic crime unit). Passing such investigations to the centralised specialist units may be more desirable, as would the development of clearer guidelines to provide on what basis that takes place. The Assessment team welcomed the steps the Police and other authorities have taken, in accordance with the Action Plan, to increase their understanding of TF through, for example, attending conferences, bilateral meetings, and regular training with external experts from other jurisdictions with more experience of dealing with TF, which is to be commended.

256. The FIU stated that the vast majority of the 38 TF SARs submitted during the review period did not really relate to TF. Some SARs by MSBs were done as a tick-box exercise, however this was not necessarily the usual pattern across other SARs (by banks, investment companies and ASPs), and although there might not have been substantial suspicions of TF, the reporting entities elected to submit a TF SAR to provide the information to the FIU to consider for further analysis and action. The overall number is low (average of six per annum), which may suggest a lack of awareness or pro-activeness regarding TF by reporting entities (see Paragraph 119 under IO6). Outreach and training has been given to reporting entities, this issue having been identified in the NRA. The FIU has a good knowledge of TF, and regularly provides training to industry (and issues guidance to the Police and Prosecutors) and it is therefore envisaged that such outreach will lead to an increase in the quality of TF SARs.

257. 34 SARs did not result in investigations by the Police. The FIU analysed them, checked relevant databases of local authorities and commercial and international websites/databases, contacted the CIS to establish if it held any intelligence which substantiated the TF suspicions, and sent requests to foreign FIUs. Replies received did not show any information or intelligence which connected the relevant persons with TF. In some cases, spontaneous disseminations were made to foreign FIUs in case they wished to investigate themselves, particularly when there was no presence (natural or legal) in Cyprus. Four of the 38 SARs were passed to the Police for further investigation, two in 2016 and two in 2018. Two of these cases are still under investigation, as discussed below, whilst the other two were closed with no further action because the Police said there was no evidence of TF identified. In the course of the investigation of those two cases, the Police issued Disclosure Orders and used its powers based on the Criminal Procedure Law to obtain information, and also contacted the Cyprus Intelligence Service for possible intelligence, and no further links were found to continue TF investigations.

Below are four ongoing TF investigations:

**Box 9.3: TF investigations**

**Case 1:** In 2017, the Police initiated an investigation following a disclosure by the FIU, based on SAR analysis, regarding suspicious transactions involving the director and financial controller of a co-operative organisation. They had used the accounts of the said organisation using false documents to carry out suspicious transactions, some of which may possibly be indirectly related to TF. In particular, two Cyprus registered companies conducted transactions with the above organisation using false documents and invoices regarding fictitious purchase of goods and materials.

The owner of one of the above Cypriot companies was also owner of a company in another country which supported a terrorist organization.

Court disclosure orders were issued, and the banking information and other financial evidence is under evaluation by the Police for further investigation. Outgoing MLA requests are due to be sent in the near future. The suspected amount involved is approximately €550,000.

**Case 2:** In 2015, the Attorney General instructed the Police to investigate possible criminal offences (including ML and TF) committed by directors, employees, shareholders of a large bank, FBME Ltd, or other persons who held accounts with that bank.

This followed the issuing of a Notice of Findings in 2014 by the US Financial Crimes Enforcement Network (FinCEN) which is under the US Treasury Department. The Notice to FBME notified the bank that FinCEN considered it to be an establishment of major concern for Money Laundering and Terrorist Financing.

With this announcement FinCEN restricted FBME BANK LTD from accessing the US financial system and indirectly informed the international financial community of the risks involved in trading with FBME BANK LTD.

With the above announcement, the correspondent banks suspended or blocked transactions in the accounts of FBME BANK LTD.

The very next day, the Central Bank of Cyprus, in view of the above developments, took the supervisory measure of managing the operations of the FBME BANK LTD branch and in 2015, the Central Bank of Cyprus revoked the license of the FBME BANK LTD branch in Cyprus.

This is said to be a very complex financial investigation which requires the gathering of huge volume of evidential material. In the course of the investigation MLA Requests were sent to the authorities of other countries and the Police are in the process of drafting a number of other MLA Requests to different jurisdictions. Thirteen have been sent out so far as mentioned under IO2 (Paragraph 662).

In parallel, the Police duly executed two MLA Requests regarding FBME Bank submitted by a foreign country.

**Case 3**

A SAR was received from a local banking institution in 2017 in relation to a Cyprus registered entity which was noted to import and export cereals. One of the UBOs of the entity is a non-EU national for whom negative information was identified from open sources identifying him as having links to terrorist organizations.

Meanwhile an SAR for the same Cyprus registered entity was also received from a different local banking institution in 2017, the UBO of which is the same aforementioned non-EU national. Similar negative findings for the UBO were also identified in open sources by the second reporting institution.

The entity under report tried to send an amount of EUR 250,000 to a foreign company abroad,

however the local bank declined to perform the transaction in view of the open source negative information.

Another SAR from a third banking institution was also submitted in relation to the same Cyprus registered entity in the year 2018, since the same negative information was identified from open sources in relation to the UBO of the entity.

All three banks terminated the business relationship with the client at their own initiative.

The FIU sent a case file to the Police in relation to all three SARs, including information on the transactions analysed. The case is still under investigation. The FIU also disseminated information both to the Attorney General and to the Auditor General, as the company under report had transactions in the year 2016 with a former state-owned enterprise which created concerns as to possible commission of other criminal offences.

**Case 4**

A SAR was received in 2018 from a banking institution in relation to a request for a new personal account of a person, who has arranged to buy property in Cyprus.

According to the information she provided at that stage, her source of funds is derived from funds deposited in a joint account with her husband. After requesting copies of her passport and that of her husband, since he was part of her source of funds, the searches in the internet revealed negative information regarding an individual whose name and age match that of her husband (possible match with detained person for terrorism).

In the light of the above, the bank rejected the request to open an account.

The information was disseminated to the Cyprus Police Authorities and to the Ministry of Interior.

Enquiries are currently being made to identify possible bank accounts at any other local banking institution and the results will also be disseminated to the Cyprus Police Authorities.

258. The FBME investigation is ongoing and it is not clear at this stage whether there is any TF. Whilst this investigation was prompted by the work of FinCEN and was not necessarily identified by Cyprus on the basis of a SAR, Cyprus is recognised for quickly introducing supervisory measures, by revoking the bank's licence and initiating investigations for ML and TF. It will remain interesting to see how this case develops as it is more consistent with the risks one might associate with an international finance centre such as Cyprus.

259. In terms of addressing particular vulnerabilities and raising awareness, the Cyprus authorities acknowledged that the abuse of the NPO sector is a risk. Action has been taken in amending the governing legislation so that all such entities are now in the process of being registered and supervised and must submit audited financial statements. There is also further outreach planned to this industry. The Cyprus Authorities also note that areas of concern for abuse for TF are money transfer businesses. The Assessment team notes that Cyprus has a large number of migrants from high risk jurisdictions, and many transmit money back to these jurisdictions, which may be a particular TF risk. The CBC routinely receives information on wire transfers from banks and MSBs and has carried out analyses (including wire transfers to and from high risk jurisdictions) in view of such risks. The analyses and wider supervisory engagement such as onsite inspections (which cover TF) have not established any patterns which might necessitate a SAR to be filed with the FIU for TF suspicion. Also, the directive to credit institutions similarly makes references to TF indicators. The appropriateness of procedures are examined and reviewed during on-site examinations by means of an audit programme dedicated to TF. No major weaknesses have been identified by the CBC. In September 2016, all supervised institutions were informed about key risk indicators relevant to TF from the FATF and were required to proceed with the necessary actions for mitigating the risks. CBC supervisory programs include questions on how entities have taken such indicators into account. Furthermore, the Cyprus authorities have disseminated a document arising out of an IFC Conference on TF risk ("Guidance on Identifying, Assessing and

Understanding the Risk of Terrorist Financing in Financial Centres") to reporting entities to increase awareness of TF risks. A directive was issued to MSBs in 2009 providing some examples of suspicions transactions/activities relating to TF and the CBC organised a training seminar on TF for all reporting entities in 2017, with international experts.

260. Regarding cash couriers, indicators for addressing the risks are discussed under Core Issue 8.3. The Assessment team also welcome the development that there will be two EUROPOL officers seconded to Cyprus to assist in the training and development of the police officers at the air and seaports, in identifying those presenting terrorism threats. It was reported that in the investigation of cases of tobacco smuggling by customs/police that there were no indicators or suspicions connected to the commission of TF. Most cases involved persons coming from the Middle East or the occupied areas, trying to smuggle tobacco in to avoid Cyprus' higher customs duties, and the collective view of the authorities was that persons were doing this for personal gain. The issue raised under 8.3 regarding the Customs' lacking the power to stop/restrain cash where there is TF suspicion (but no false/failed declaration) is something which could impact on the effectiveness of detecting TF, albeit the presence of Police at the borders would in reality alleviate any real concern over this.

261. No domestic TF investigations have resulted from incoming MLA requests since there have not been any relating to TF. Cyprus has set up an office within the Crime Combating Department for handling MLA requests, its primary purpose [as mentioned in IO2 and IO7] is to alleviate backlog issues with MLA. However, it is also charged with analysing MLA and if there are indicators for ML/TF, sending the file onto colleagues to consider initiating a domestic investigation. This office was set up only in late 2018 and so it is too early to assess the effectiveness of it. Of course, Cyprus has had no MLA requests relating to TF in the review period, and so it is not expected that the creation of this office will suddenly harvest dozens of TF investigations from incoming MLA. Yet, the authorities are encouraged to carefully analyse all MLA, not just those marked as TF, which may have TF indicators and initiate investigations where appropriate. The establishment of this office (as well as the ECIO) is a welcome step. It demonstrates a proactive approach by Cyprus. Moreover, it shows that Cyprus is taking steps to increase and apply resources in a risk-based approach by seeking to harvest more TF investigations where possible. In other words, Cyprus is not simply resting on its laurels and dismissing its risk rating as merely cautionary (and simply assuming there is no, or little threat given the lack of SARs and no incoming MLA regarding TF) but actually taking positive action to address that risk.

262. The FIU has received requests from counterpart FIUs during the period, (ten between 2016 and 2018) but akin to many of the SARs, the majority of such requests did not actually concern TF. Furthermore, in some case, there were requests sent out not just to Cyprus but to all EGMONT countries to seek assistance with ongoing enquiries. The FIU states that it replied to all requests, having carried out searches on its databases, and that no information was identified by the FIU to show links to TF in Cyprus, and no further feedback or requests for additional co-operation were received. In addition to the formal channels of cooperation with respect to TF, there are additional avenues of cooperation, such as the National Europol Unit, Interpol channels, and through the OCT. The OCT, for example, exchanges information with other EU counterparts through encrypted/specialised information systems but also with third countries by way of liaison officers who are posted to Cyprus. Members of the OCT participate/attend the meetings of the Working Group on Terrorism of the Council of the European Union, as well as Europol's European Counter Terrorism Centre and First Response Network.

263. In the two terrorism cases discussed under Core Issues 9.1/9.5, the terrorist financier was not identified. The authorities stated however that they would always conduct a financial investigation when terrorism is identified, even in lone wolf scenarios where the planned attacks may be unsophisticated and the funds minimal (which was the case in both examples provided).

264. Intelligence plays a big part in identifying terrorism threats. The CIS is the Republic's security service. It searches for, collects, evaluates, analyses, processes and discloses information to competent authorities on a case by case basis. This may include information on the prevention and

combating of financial and organised crime. It co-operates with other foreign counterparts or international bodies. The CIS monitors potential terrorists and sits on the Fusion Centre as discussed further below. It is not known whether the CIS has identified any potential TF threats. It confirmed on-site that it is cognisant of TF threats and that it considers it to be part of the bigger counter terrorism picture. The Assessment team queried whether the influx of migrants into Cyprus from the Middle East coupled with the defeat of ISIS in Syria and Iraq could increase threats of returning FTFs. The authorities stated they had found no evidence of residents travelling to conflict zones and were alive to the potential of some individuals posing a threat, but that measures were in place to monitor and detect any risks.

265. Cyprus has had few TF investigations. This is not surprising given the limited amount of sources from which to identify TF. It is hoped that the further developments discussed above, such as further outreach and training for NPOs and other reporting entities, and the creation of the new MLA office, will help to enable the authorities to mine TF investigations, more consistent with the risk profile, from such sources.

### *4.2.3. FT investigation integrated with -and supportive of- national strategies*

266. The Cyprus' Council of Ministers adopted, in 2014, a National Counterterrorism Strategy ("**the CT Strategy**"). This is a confidential document which has not been shared with the Assessment team, but it is said to be based on the EU's Counter-Terrorism strategy. The CT Strategy is based on a four-pillar approach of Prevent, Protect, Pursue and Respond. As part of the Protect pillar, the goals include enhancing measures to prevent abuse of the financial system for, *inter alia,* TF, and combating the exploitation of non-governmental organisations for TF. As part of the Protect pillar there is the goal on reporting and investigating suspicious transactions for TF. Whilst these are the type of goals the Assessment team would expect to see in national strategies against counter terrorism, little specific information was provided about the substance of this and its effective implementation, other than the details on further outreach and training. Therefore, it is difficult to fully assess whether TF investigations are integrated with and supportive of this strategy.

267. There is an inter-governmental strategy body known as the Fusion Centre (comprising representatives of the CIS, Police, National Guard and officials of the Ministries of Foreign Affairs and the Interior) which analyses trends and provides quarterly threat assessments on terrorism threats. The Fusion Centre does not have operational powers but provides strategic guidance on matters identified in its discussions and analyses terrorist threats faced in Cyprus. It can meet outside its three-monthly programme if circumstances require it. The threat assessment is provided to the National Counter-Terrorism Co-ordinator who is the Permanent Secretary of the Ministry of Justice and Public Order and who co-ordinates the jurisdiction's CT Strategy at the policy level.

268. The Fusion Centre and the Co-ordinator's primary focus is terrorism threats. Whilst this may encompass TF, these bodies are not focussed on TF from the perspective of abuse of the financial system, which is more likely to be the remit of the FIU. It is noted that the FIU is not a member of the Fusion Centre but can be invited to meetings if any participant considers information is required from the FIU, although this has not yet happened. The FIU has a designated contact person responsible for TF, as a means of enhancing the co-operation between the FIU on the one hand and the police/CIS on the other. It may be beneficial for the FIU to have a more permanent presence on the Fusion Centre so as to enhance co-operation further and underline the commitment to fighting TF.

269. There is also of course the National AML/CFT Strategy, adopted in 2019. As part of its goals, there is the aim to enhance CFT measures through specialised training for all relevant parties, broadening information and data collection and promoting an outreach to the NPO sector.

270. The information provided to the Assessment team shows that there have been TF investigations relating to suspicious transactions and which involve the financial system. There have also been prosecutions for supporting a terror group and for participation in a terrorist OCG.

The investigations could be said to generally be consistent with the CT Strategy (to the extent the Assessment team can conclude this without seeing the CT Strategy). The National AML/CFT Strategy is more high level and focussed on outreach and training as opposed to particular investigative strategies.

271. As mentioned above, the overall number of TF investigations is not significant considering Cyprus' status as an IFC. Given the commendable efforts to recognise terrorism threats and strategize on how to mitigate against them, the Cyprus authorities are encouraged to continue their efforts and explore more potential sources for possible TF.

#### *4.2.4. Effectiveness, proportionality and dissuasiveness of sanctions*

272. There have been no TF convictions and therefore no sanctions. The sanctions handed down for the one terrorism conviction and the participation in OCG (discussed below) appear in themselves to be reasonably effective, proportionate and dissuasive.

#### *4.2.5. Alternative measures used where FT conviction is not possible (e.g. disruption)*

273. The authorities provided a case where the person was convicted for participation in an organised crime group as opposed to participation in a terrorist group, because of a gap existing at the time on the EU list which meant that Hezbollah was not a proscribed organisation by the EU.

**Box 9.4: Yacoub (2012)**

A Swedish national of Lebanese origin was prosecuted for belonging to Hezbollah conducting surveillance activities on Israeli targets in Cyprus. He was convicted for participation in a criminal organization and sentenced to imprisonment of 4 years and was deported to Sweden by the end of 2014 after he had served his sentence. His re-entry to Cyprus is prohibited for the next five years and his personal particulars were placed on the Cyprus Police Stop-List.

Cyprus took investigative measures to ascertain whether or not there was any TF. No funds were found to be in Cyprus and the person had no bank accounts in the jurisdiction. In the course of the investigation of this case, respective information was also sought from foreign jurisdictions, through Interpol and Europol channels but also through liaison officers posted to Cyprus. Cooperation between the Police and the FIU was also conducted.

274. This case was not one of TF but demonstrates an alternative criminal justice measure used to disrupt terrorism. Whilst Cyprus was unable to prosecute under section 8 of the 2010 Law, the authorities nonetheless found a way to pursue this matter and prosecute the offender. Hezbollah has since been proscribed and the above case (Abdallah) has demonstrated a successful prosecution under section 8 based on the revised lists. This case can be said to be a demonstration of disrupting terrorism activities (albeit not TF activities).

275. Cyprus has had no outgoing MLA on TF (and has had no incoming related to TF). However, examples have been provided of FIU-FIU co-operation. In terms of incoming requests, as stated above, the FIU notes that most requests were ones sent to all EGMONT jurisdictions. The FIU has also disseminated to counterpart FIUs on some occasions yet no examples are known of where this has led to a TF investigation/prosecution elsewhere.

276. There has also been some other LEA co-operation through EUROPOL, but no information was provided on the outcome elsewhere.

277. Although not a criminal justice measure, the FBME case demonstrated the authorities resolve to act swiftly in imposing administrative sanctions when TF is suspected.

*Overall conclusions on IO.9*

278. In conclusion, Cyprus has shown that it is vigilant regarding terrorism, with a strong counter terrorism infrastructure in place, and the Police have carried out TF investigations where possible. The number of investigations and lack of prosecutions is understandable given the low

number of SARs and the non-existent incoming MLA specifically related to TF. Further efforts to enhance TF understanding in the finance industry is welcomed and encouraged as are the exercises taken to monitor activity (including wire transfers) with high risk jurisdictions. Cyprus has also taken steps to increase its national authorities' understanding and experience of TF by attending bilateral and multilateral conferences and training with other jurisdictions more experienced in TF. Finally, Cyprus has set up specialised units such as the MLA Office and the ECIO to target financial crime and harvest investigations where possible, including of TF, and this is a strong example of increasing and applying resources in a risk based approach instead of simply resting on its laurels and assuming there is no TF threat given the low number of SARs and no MLA. Therefore, it can be said that Cyprus is achieving the Immediate Outcome to a large extent and the Recommended Actions can be said to constitute only moderate improvements.

279. **Cyprus has demonstrated a substantial level of effectiveness with Immediate Outcome 9**.

## *4.3. Immediate Outcome 10 (TF preventive measures and financial sanctions)*

### *4.3.1. Implementation of targeted financial sanctions for TF without delay*

280. Cyprus uses a combination of supranational (at EU level) and national mechanisms to implement TF-related TFS. UNSCRs are incorporated into EU Law, and thus into the national legislation of EU Member States, through Decisions and Regulations adopted by the Council of the EU. Cyprus implements the binding provisions of the UNSCRs through the relevant Decisions and Regulations of the Council of the EU. In addition, Cyprus has in place domestic legislation which ensures that TFS are implemented without delay.

281. As an EU MS, Cyprus is able to rely on the EU's mechanism for proposing persons or entities to the 1267/1989 and 1988 UN Committees and for designating persons under UNSCR 1373. Access to the EU mechanism does not completely substitute for an autonomous domestic TFS authority, particularly where a request for designation is put forward by another country. However, there is an informal domestic mechanism for proposing listings at UN and EU level, which provides some of the benefits of an autonomous system. The domestic mechanism is rooted in the MFA's role, as conferred by the Constitution of the Republic of Cyprus, as the natural representative and negotiator of the Republic of Cyprus on issues pertaining to the imposition of international and EU sanctions. Competent authorities, such as the Police, the Intelligence Service, the FIU, other Public Departments, the supervisory authorities of the financial sector, can submit to the MFA relevant proposals they have identified in the course of exercising their functions and carrying out their activities. The MFA may also act in its own capacity when it receives intelligence for potential listings from a third country. To date, Cyprus has not proposed any persons or entities for a TF-related listing, nor has Cyprus been requested to give effect to TF-related freezing measures taken by another country. However, Cyprus has used this informal procedure in relation to a TFS regime not related to TF: the MFA received intelligence from another country on two persons that potentially matched the criteria for listing under an EU autonomous sanctions regime against Syria. This information was shared with the European External Action Service (EEAS) which after careful examination determined that there was not sufficient evidence to support the listing.

282. The country developed a domestic communication mechanism to notify relevant competent authorities and all obliged entities of new designations. The MFA plays a coordinating role with regard to UN and EU sanctions regimes. The website of the MFA provides, inter alia, information on the role of the MFA, as well all the relevant links to UN and EU websites. The MFA continuously monitors relevant UN and EU bodies in order to keep apprised of developments with respect to decisions to impose sanctions on specific jurisdictions, natural or legal persons, or vessels. The MFA circulates any updates to the UN and EU lists received from the Permanent Representations of the Republic of Cyprus to the UN and EU to the competent authorities, in particular the Police, the MJPO, the MoF, the MoI, the Ministry of Defence, the Ministry of Communications and Works, the Ministry of Industry Commerce and Tourism, the CIS, the Cyprus Ports Authority, the FIU and all the supervisory authorities.

283. The supervisors maintain up-to-date contact lists that allow them to send notice of such actions to obliged entities by email; in addition, the supervisors post such notices on their websites. Supervisors generally send and post such notices the same business day they receive notice from the MFA, and certainly do so by the next business day. This generally means that decisions announced after Nicosia business hours on a Friday will be communicated to obliged entities no earlier than the following Monday. FIs and DNFBPs are required to immediately inform their supervisor of any freezing measures under the TFS regime (which would include reporting attempted transactions). The supervisory authorities are required, in turn, to inform the MFA.

284. Most supervisors not only communicate new designations to obliged entities, but also promote the understanding of TFS obligations through regulations (binding directives), notifications/circulars, consultations, trainings and on-site examinations. This communication encompasses information highlighting differences between sanction regimes, practical guidance on compliance with freezing requirements, country risks (countries subject to restrictive measures, FATF listed countries, etc.) and information about general ML/TF related internal controls applied by the reporting entities.

285. In general, all obliged entities are aware of TF-related TFS obligations and the requirements to freeze funds/assets of designated individuals/entities. They have systems in place that allow them to implement TFS and screen the entire customer database as soon as they become aware of new designations (e.g. by checking updates on relevant UN sources or upon receipt of a notification from the supervisory authorities). Terrorism-related sanction hits have never been identified in Cyprus and, as a result, no funds or other assets of TF-related designated persons or entities have been frozen. The obliged entities interviewed on-site confirmed that regular screening against sanction lists often results in partial matches, which are usually examined in more detail and determined to be false positives. Furthermore, the few obliged entities that had concrete experience of freezing assets (under other sanctions regimes) appear to have been able to act and to coordinate with other relevant financial institutions promptly and efficiently, and to have immediately notified the competent authorities. These examples are indicative of a functioning system.

286. Interviewed banks and large ASPs screen customers and BOs on an automated basis against TFS sanction lists before entering into business relationships and as part of their ongoing monitoring (i.e. real time screening at the time of the execution of each transaction and periodic, scheduled screening of the entire customer database). The majority of other FIs and DNFBPs interviewed have less comprehensive TFS controls: while all of them are aware of the obligation to screen customers at the on-boarding stage, the frequency of TFS checks in the course of a business relationship varies. The variations generally correlate with the size and financial resources of obliged entities. The frequency of checks is usually determined on the basis of customer risk level (i.e. high-risk customers are screened more frequently than medium or low risk customers, irrespective of the transactional activity) and changes in customer profile (e.g. changes in shareholding structure) that trigger additional screening. Since customer screening is carried out on a periodic basis, unlike real time screening of transactions, obliged entities may not immediately identify the designation of their customers but may only become aware of such designation sometime after the fact.

287. The banking sector, due to its materiality, arguably faces the highest risk of being misused in connection with TFS. Banks articulated a sophisticated understanding of the sanctions evasion risk, expressing concerns about complex structures of legal persons and about activity on behalf of designated persons by associates of their customers. The banks showed that they understand the need to identify and screen not only customers and BOs, representatives/signatories of the legal person, but also all shareholders and directors of legal persons within all the layers of the ownership structure, as well as all parties to a transaction. The CBC reported that banks' understanding of TFS obligations and overall level of compliance have improved significantly in recent years due to the CBC's awareness raising efforts. This claim is supported by supervisory findings. The internal AML/CFT procedures of banks examined by the assessment team contain

instructions on the implementation of TFS.

288. Other obliged entities did not demonstrate the same level of understanding of the risks of TFS evasion as banks, and their internal AML/CFT procedures are not as comprehensive. Consequently, they may not always be in a position to identify individuals or entities who may seek to conceal their identity behind complex structures to evade sanctions. This constitutes a vulnerability in Cyprus given its status as an IFC and the role played by ASPs as gatekeepers, especially where Cypriot banks are not involved. There are known cases where potential underlying customers of ASPs were found to have direct or indirect links (through a group structure) with persons and entities on sanctions lists (not related to TF or PF), indicating how immediate these risks are. These customers were not on-boarded.

289. Banks are aware of the requirement to report any frozen funds or other assets, including attempted transactions, to the CBC. While the other obliged entities were all aware of the requirement to report an exact match, some could not consistently identify the authority which is competent to receive such reports i.e. their supervisory authority. This is perhaps not surprising given that most have never had to report any matches.

290. Monitoring of banks for compliance with TFS obligations appears to be adequate. Checks on compliance with TFS form part of AML/CFT audits. The CBC has devised a detailed on-site checklist, which covers various aspects of the internal controls that are expected to be implemented. Some form of off-site monitoring is also carried out; banks must report when they freeze customer assets pursuant to TFS, must submit reports on frozen assets when requested, and must also submit annual reports on frozen assets, with all reports being submitted to the CBC. Submission of reports can trigger follow-up questions from the CBC; in one example provided by the CBC, a bank that reported a decline in frozen account balances was required to provide evidence of having received permission for the withdrawals from the Advisory Committee.

291. Given the limited documentation made available, the assessment team did not have the opportunity to examine the supervisory practices of the other supervisors in detail. During the on-site visit, the ICPAC, CBA, and CySEC reported that they verify compliance with relevant requirements during on-site inspections. Checks on compliance with TFS obligations form part of AML/CFT audits. They reported that they test the screening mechanisms of obliged entities, verify whether obliged entities maintain any business relationships with the sanctioned persons, look at whether partial matches with lists which are classified as false positives are satisfactorily resolved. The Real Estate Registry Board acknowledges that it does not examine for real estate agents' screening of their customers for TF or other targeted sanctions. This creates the risk that compliance with TFS by real estate agents may not be effective; however, the risk is somewhat mitigated as the Land Registry independently screens real estate property transfers against targeted sanctions lists. Given that casino has started operating just recently no on-site inspections (except a desk-based review) have been carried out so far.

292. None of the supervisory authorities have detected any significant shortcomings in the area of TF-related TFS compliance. Consequently, no remedial actions have been applied in relation to breaches of TF TFS-related requirements to date. This raises some concern considering the findings of the assessment team in relation to ASPs' limited understanding of TFS risks, issues with periodic monitoring and absence of comprehensive internal control procedures. It also calls into question the comprehensiveness of supervisory practices in this area.

### *4.3.2. Targeted approach, outreach and oversight of at-risk non-profit organisations*

293. There are five types of entities in Cyprus which may carry out not-for-profit activities:

a) Charities – entities set up for educational, literary, scientific or public purposes (regulated by the Charities Law – CAP. 41)

b) Societies – organised associations of at least twenty persons, other than political parties or trade unions, set up for the attainment of a certain non-profitable object (regulated by the Law on Societies and Institutions and other related matters – 104(I)/2017 – 'LSI')

c) Institutions (foundations) – assets of a value of more than EUR 1,000 appropriated to serve a certain non-profitable object (regulated by the LSI)

d) Federations/associations – a cooperation of three or more societies, institutions, non-profit companies/legal entities with common objects (regulated by the LSI)

e) Non-profit companies – companies/other legal entities registered under the Companies Act which conduct non-profit activities to promote one of the following causes: commerce, art, science, religion, charity or any other similar cause/objective. Non-profit companies apply their profits and income for the promotion of their activities and may not distribute dividends. (regulated by the Companies Law)

294. Under the LSI a non-profit society, institution or federation/association is defined as an entity which does not distribute profits arising from its activities to its members, founders, administration or officers, but rather invests or uses those profits to carry on and achieve its objectives.

295. The large majority of NPOs in Cyprus are societies as indicated in the table below:

**Table 24: types of NPOs**

| Type of NPO | Number (as of year) | Competent authority |
|---|---|---|
| Charities | 58[31] | MoI |
| Societies | 4929 | MoI |
| Institutions | 406 | MoI |
| Federations/associations | 0 | MoI |
| Non-profit companies | 382 | MCIE |

296. Cyprus has not yet identified the sub-set of NPOs which may be vulnerable to TF abuse and, as a result, is not in a position to apply a risk-based approach to the sector. The absence of a targeted approach may have the effect of disrupting or discouraging legitimate NPO activities. In fact, banks consistently describe NPOs as uniformly high-risk. One bank has mentioned that it does not provide services to any foreign NPOs. The CBC reported cases of some (smaller) banks refusing to open accounts for NPOs on the indiscriminate assumption that the NPO sector poses a higher risk. This was confirmed during the interviews with the representatives of the NPO sector.

297. The risk associated with NPOs in Cyprus is rated as medium-low in the NRA. This conclusion does not appear to be based on a comprehensive review of the entire sector, but, rather, on international typologies relating to the sector. This is, to some extent, expected since Cyprus has not had any TF cases involving NPOs.

298. The authorities are, however, credited for having taken some measures to strengthen the oversight framework of NPOs. The authorities state that the framework of the NPO sector was completely overhauled with the coming into force of the Societies and Institutions and other related matters Law (LSI) in 2017. The law was adopted with a view to streamlining the legal and institutional framework governing the sector and is seen by the authorities as the first step to establish a risk-based approach. The law includes measures which are envisaged under Rec. 8, such as registration requirements for NPOs, public availability of information, etc. At the time of the on-

[31] At the time of the on-site visit, Cyprus was in the process of phasing out the application of the Charities Law. Charities were in the process of re-registering as an institution under the LSI. In order to expedite the process, specific measures were taken including: banning the creation of new charities, introducing tax exemptions for institutions operating under the LSI, etc.

site visit, the NPO sector was still in the process of implementing these new requirements. The assessment team could, therefore, not fully assess the degree to which these requirements are complied with.

299. Cyprus maintains a register of NPOs, which is managed by the General Registrar, who is the Permanent Secretary of the Ministry of Interior, in cooperation with the District Officers/Registrars. They are jointly responsible for collecting and updating information on Societies, Institutions and Federations/Associations. The transitional period for the collection of information, which started after the adoption of the LSI, was due to come to an end in July 2019 (after the on-site visit). Therefore, the register had not yet been populated with all the information.

300. In order to expedite the implementation of a full-fledged risk-based approach, the authorities initiated an information-gathering exercise in the Districts of Larnaca and Paphos. This exercise will serve as a basis for assessing the activities and characteristics of NPOs that have already gone through the registration procedure and award a risk rating to each entity. The assessment team retains some concerns that the General Registrar (including District Officers/Registrars) does not yet have sufficient human and technical resources to carry out the risk assessment.

301. The General Registrar is empowered to take supervisory actions and/or corrective measures against non-compliant NPOs. It is assumed that more activity will be taken once the transitional period is over. The General Registrar and the District Officers/Registrars is currently focusing on ensuring that the documentation submitted by the entities is compliant with the LSI. Also, as fundraising is regulated by the "Fundraising Law of 2014" NPOs that are not complying with the LSI are not granted a license for fundraising.

302. After the adoption of the LSI, the Cypriot authorities have carried out awareness raising activities in order to inform the NPOs of the new legal requirements. The representatives of the NPO sector met by the assessment team held contradictory views on the adequacy of these awareness-raising initiatives. The overall understanding by the NPOs of the TF risks is not extensive and is generally based on individual experience in the sector. No actions have been taken to encourage NPOs to conduct transactions using formal financial channels.

303. Cyprus reported that there has been only 1 TF-related STR regarding NPOs filed to the FIU by obliged entities; and to date, there have not been any TF investigations involving NPOs.

### *4.3.3. Deprivation of TF assets and instrumentalities*

304. Cyprus has never identified terrorism-related sanction hits and, as a result, has not frozen funds or other assets under TF-related TFS. Nevertheless, obliged entities demonstrate a general awareness of the need to have operational protocols in place to freeze any assets without delay as part of the implementation of targeted TF sanctions. Most obliged entities have not had to act on those protocols, but the few obliged entities that the assessors interviewed that had concrete experience of freezing assets appear to have been able to act and to coordinate with other relevant financial institutions promptly and efficiently, and to have immediately notified the relevant authorities.

305. The obliged entities interviewed confirmed that regular screening against sanction lists often results in partial matches, which are usually examined in more detail and determined to be false positives. Obliged entities seem to be aware of their obligations under the TFS regime, all implementing screening solutions against sanctions list (either automated or manual). Frequency of screening varies among obliged entities, but obliged entities were aware of the obligation to identify and freeze funds or other assets related to TF activities.

306. Cyprus has mechanisms in place to deal with the examination of financial sector requests related to UN or EU restrictive measures, in particular with respect to freezing and unfreezing of

assets, and providing access to frozen funds.[32] Cyprus has presented some case examples which, however, were not related to TF-related TFS regimes. Competent authorities for dealing with these requests have consulted with the European Commission and the European Bank for Reconstruction and Development when appropriate. They also take into account the guidelines, recommendations, and opinions issued by relevant UNSC sanctions committees and their Panels of Experts, by the Council of the European Union, and by the European Commission.

307. There were no criminal freezing or confiscation orders in relation to terrorists, terrorist organisations and terrorist financiers. The authorities are currently conducting financial investigations in the context of ongoing TF investigations (see IO 9), which may lead to the issue of court freezing orders.

#### *4.3.4. Consistency of measures with overall TF risk profile*

308. The TF risk is rated as medium in the NRA. The primary risks are associated with Cyprus's status as an IFC in connection to funds being transited through Cyprus or being managed within Cyprus. As mentioned, banks, which constitute the most material sector, have articulated a sophisticated understanding of the sanctions evasion risk, expressing concerns about complex structures of legal persons and about activity on behalf of designated persons by associates of their customers. Consistent with this risk understanding, banks appear to apply adequate measures to mitigate sanctions evasion risk. ASPs, the second most material sector, were not found to have a comparably sophisticated understanding. Consequently, it is not clear whether they are in a position to identify individuals or entities who may seek to conceal their identity behind complex structures to evade sanctions. This constitutes a vulnerability in Cyprus given its status as an IFC and the role played by ASPs as gatekeepers.

309. Cyprus has not applied supervision and monitoring of NPOs consistent with the risks of TF abuse. The NRA on TF threats to NPOs makes clear that more measures are considered necessary in order to identify potential vulnerabilities of the sector aiming in identifying which subsets of NPOs pose higher risk for possible abuse for TF purposes. Due to a lack of comprehensive understanding of the risks of NPO abuse for TF, Cyprus does not appropriately apply focused and proportionate measures to specific NPOs. However, a new legal and regulatory framework for NPOs has been put in place and is currently being implemented with a view to establishing a fully-fledged risk-based approach.

*Overall conclusions on IO.10*

**Cyprus is rated as having a moderate level of effectiveness for IO.10.**

### *4.4. Immediate Outcome 11 (PF financial sanctions)*

310. Cyprus is exposed to potential PF activities due to its status as an IFC and a company formation and administration centre. Authorities have a basic understanding of Cyprus's exposure to PF activities. They have expressed the view that the geographical position of Cyprus is inevitably a long-standing challenging factor. However, some measures taken during the period under review, such as stronger controls by the banking sector with respect to shell companies and introduced customers and improvements in supervisory practices, albeit only indirectly related to PF, are positive steps in managing the country's exposure.

311. The authorities state that trade volumes between Cyprus and Iran and DPRK are limited. Nationals from DPRK hold no bank accounts in Cyprus, and DPRK has no diplomatic presence in the

[32] The Advisory Committee on Financial Sanctions (Advisory Committee) established since 2012 is responsible for examination of requests for the release of frozen funds maintained in accounts of credit institutions; its decisions are binding. Unit for the Implementation of Sanctions in the Financial Sector deals with the examination of requests that fall within the financial sector affected by UN sanctions and/or EU restrictive measures; it submits relevant recommendations for approval or rejection to a Ministerial Committee comprising the Ministers of Finance, Foreign Affairs, and Justice.

country. No Iranian- or DPRK-owned vessels are registered in Cyprus.

312. Cyprus ratified all international treaties related to non-proliferation and is a member of almost all export control regimes (except for the MTCR and the Wassenaar Arrangement– but in practice Cyprus applies the provisions of both these regimes).

### *4.4.1. Implementation of targeted financial sanctions related to proliferation financing without delay*

313. Cyprus uses a combination of supranational (at EU level) and national mechanisms to implement TF-related TFS. UNSCRs are incorporated into EU Law, and thus into the national legislation of EU Member States, through Decisions and Regulations adopted by the Council of the EU. Cyprus implements the binding provisions of the UNSCRs through the relevant Decisions and Regulations of the Council of the EU. In addition, Cyprus has in place domestic legislation which ensures the implementation of TFS without delay.

314. The country developed a domestic communication mechanism to notify relevant competent authorities and all obliged entities of new designations. The MFA plays a coordinating role with regard to UN and EU sanctions regimes. The website of the MFA provides, inter alia, information on the role of the MFA, as well all the relevant links to UN and EU websites. The MFA continuously monitors relevant UN and EU bodies in order to keep apprised of developments with respect to decisions to impose sanctions on specific jurisdictions, natural or legal persons, or vessels. The MFA circulates any updates to the UN and EU lists received from the Permanent Representations of the Republic of Cyprus to the UN and EU to the competent authorities, in particular the Police, the MJPO, the MoF, the MoI, the Ministry of Defence, the Ministry of Communications and Works, the Ministry of Industry Commerce and Tourism, the CIS, the Cyprus Ports Authority, the FIU and all the supervisory authorities.

315. The supervisors maintain up-to-date contact lists that allow them to send notice of such actions to obliged entities by email; in addition, the supervisors post such notices on their websites. Supervisors generally send and post such notices the same business day they receive notice from the MFA, and certainly do so by the next business day. This generally means that decisions announced after Nicosia business hours on a Friday will be communicated to obliged entities no earlier than the following Monday. FIs and DNFBPs are required to immediately inform their supervisor of any freezing measures under the TFS regime (which would include reporting attempted transactions). The supervisory authorities are required, in turn, to inform the MFA.

### *4.4.2. Identification of assets and funds held by designated persons/entities and prohibitions*

316. As with TF, obliged entities are generally aware of the need to have protocols in place to freeze any assets without delay as part of the implementation of PF TFS. Several obliged entities reported taking action to close (or refuse to open) client accounts because of suspicions of ties to proliferators such as DPRK. While no obliged entities reported having to freeze assets or funds held by persons or entities designated under PF sanctions programmes, there is no reason to doubt that obliged entities can take such steps effectively, at least as regards specifically named jurisdictions and persons. Whether this generalizes to a broader understanding of how to identify proliferation financing, however, is an open question (see 4.4.3 below).

317. The Ministry of Energy, Commerce, Industry and Tourism issues export licences for dual use goods and military equipment. In making its determination, the Ministry consults with the CIS, with other EU Member States, and, as necessary, with other domestic authorities, in addition to the MFA. In the period 2013-2018, there were no licences issued or any applications rejected concerning exports of these products to Iran or DPRK. Exporters are informed about control requirements through publications in the press and through the official website of the Ministry of Energy, Commerce, Industry and Tourism. Announcements are also sent to the Cypriot Chamber of Commerce and to the Employers and the Industrialist Federations.

318. The control and checks on the exportation of sensitive goods is the responsibility of the Department of Customs. Customs officers are empowered by Customs legislation to check whether

the goods to be exported are subjected to an export license and to verify that it corresponds to the goods that are to be exported. It is empowered with, inter alia, conducting a physical examination of goods, requesting the procurement of the necessary documents, carrying out searches of persons, premises, customs controlled areas, vehicles, vessels or aircraft in accordance with existing legislation, taking samples, having access, detaining or seizing goods or documents, conducting audit controls, instituting legal proceedings before the appropriate court and fostering international collaboration on customs issues with other customs departments There are various units within Customs overseeing the transportation of sensitive goods and commodities: the National Intelligence Unit, the Special Anti-smuggling Team and the Mobile Units.

319. Cyprus has mechanisms in place to coordinate national efforts in combatting the proliferation of weapons of mass destruction and some aspects of PF; the National Committee for the Implementation of the Convention on the Prohibition of Chemical Weapons and the Committee on Export Control of the Ministry of Trade and Industry. More specifically, action is coordinated through the Coordinating Unit to Combat International Terrorism, which was set up for the purpose of coordinating the activities of the relevant Ministries and Departments in the fight against terrorism and in the suppression of illegal activities, but also co-ordinates the combating of trafficking of harmful chemical substances and dual-use goods. There are also two bodies dealing specifically with aspects of PF-related TFS. The first is the Advisory Body on Financial Sanctions[33], set up by the Council of Ministers and chaired by the MoF dealing with (1) requests for the release of funds and financial resources falling within the exceptions/derogations provided for in the relevant resolutions and decisions of the UNSC and the EU and (2) the notification via the MFA of the release of funds and financial resources to the relevant UNSC Sanctions Committees, as well as the European Commission and EU Member States as necessary. The other body is the Unit for the Implementation of Sanctions in the Financial Sector[34], which is chaired by the MoF and deals with the examination of requests pertaining to UN and EU restrictive measures that fall within the financial sector.

320. There has been one investigation by the competent authorities into a suspected case of PF. Confidential information was forwarded to the MFA on suspicions of a possible violation of UN/EU Sanctions in relation to DPRK by a Cypriot natural person and a Cypriot company. According to the information furnished to the authorities, there were suspicions that the Cypriot company and its director entered into an agreement with a company in DPRK for the importation of herbal medicine and cosmetics. The MFA forwarded this information to the Police for investigation based on Law 58(I)/2016 (section 4). The investigation, until now, has not revealed that any items have been imported.

321. In the past two years, the relevant competent authorities have attended seminars in Brussels on the implementation of UN sanctions against DPRK under the initiative of EU Member States in their capacity as non-permanent UNSC members and chairs of the 1718 Committee. Speakers include members of the Panel of Experts on DPRK and experts from the European Commission and the EEAS. The purpose of these seminars is to increase awareness on the risks of circumvention of DPRK sanctions by presenting real life complex scenarios. Cyprus actively participates in these seminars and the information is shared on a confidential basis with the competent authorities in Cyprus through the MFA.

### *4.4.3. FIs and DNFBPs' understanding of and compliance with obligations*

322. Obliged entities generally understand their obligations with respect to PF sanctions to be roughly the same as their obligations with respect to TF sanctions, only substituting countries of proliferation concern for individuals and institutions of terrorism concern. This finding is

[33] Membership includes representatives of the MoF, the FIU, the MFA, the CBC, CySEC, the MJPO and the Ministry of Energy, Commerce, Industry and Tourism, which includes both the Company Registry and the Trade Services (Imports/Exports Licensing Section).

[34] Membership includes representatives of the Ministries of Finance, Foreign Affairs and Energy, Commerce, Industry and Tourism, the AG's Office, the CBC and CySEC.

supported by an examination of the internal procedures of obliged entities provided to the assessment team, which lack detailed controls on the identification of PF-related TFS. The issues identified in relation to the private sector's application of measures also apply here.

323. Most obliged entities that were interviewed, including sophisticated banks, had difficulty in articulating differences between TF and PF, in terms of geographic risks, transaction typologies, or most other types of distinctions. The only concrete step that obliged entities typically take that demonstrates awareness that there may be different risks associated with PF is the categorical refusal of most obliged entities to provide services to persons engaged in the weapons trade. Lumping together TF and PF may not significantly impair compliance with jurisdictionally related PF sanctions, given that obliged entities clearly understand the need to take appropriate steps with respect to FATF and EU country lists. But it suggests that, in the absence of a manifest geographic link, obliged entities may be less effective at identifying and taking appropriate action with respect to proliferation financing transactions and proliferator clients whose activities are not clearly tied to sanctioned countries, than they appear to be with respect to TF and terrorist financiers.

324. This is not for lack of trying by competent authorities to explain the risks associated with PF. The CBC acknowledges that financial institutions involved in trade finance services are at risk of being abused for PF with financial services and products such as letter of credit, documentary credits, loans and electronic funds' transfers and, for example, has organized specialized training on TFS that included sessions on trade-based finance and its risks. However, very limited awareness raising initiatives, if any, have been taken by other supervisory authorities in relation to PF issues.

#### *4.4.4. Competent authorities ensuring and monitoring compliance*

325. Obliged entities did not appear to distinguish between TF and PF as distinct subjects of competent authorities' concern: none volunteered that they received communications on the subject of PF *per se*, and those that were asked reported no communications dedicated to the subject. At the same time, it is clear that competent authorities both understand the distinctions between TFS related to TF and PF and attempt to articulate an understanding of PF concerns to obliged entities. The CBC in particular has paid special attention to bank involvement in trade finance activities as a PF risk factor, and it monitors institutional risk assessment reports with PF risks in mind.

326. The supervisory measures for monitoring compliance with PF-related TFS are similar to those described under IO 10. Similarly, to TF-related TFS, there are no offsite supervisory tools to monitor compliance with PF-related TFS (except in the case of the CBC). In general, checks on compliance with TFS form part of full scope AML/CFT audits, with the exception of the supervisory authorities of real estate agents and casino. However, it is not clear whether supervisors draw a distinction between TFS related to PF and TF when conducting on-site inspections. On-site inspection checklists that have been reviewed by the assessment team do not suggest that there are methodologies in place to specifically check compliance with TFS related to PF. Although the assessment team was provided with statistics related to TFS compliance checks, statistics do not distinguish between TF and PF.

327. Supervisory findings suggest that no significant shortcomings have been identified in the area of compliance with PF-related TFS by the reporting entities, which is surprising given the findings of the assessment team that there does not appear to be widespread understanding of PF risks. Moreover, the same deficiencies in relation to TFS, as discussed in IO 10, apply here: limited understanding of sanctions evasion risk (except by the banking sector), shortcomings in TFS implementation (in relation to frequency and depth of checks) and an absence of comprehensive internal control procedures directed at PF-related TFS.

328. As discussed in IO 3, lack of supervisory resources hamper the effectiveness of the supervisory regime. This equally affects the supervision of compliance with PF-related TFS. The competent authorities do not appear to be sufficiently equipped to monitor PF-related TFS requirements.

*Overall conclusions on IO.11*

329. **Cyprus is rated as having a moderate level of effectiveness for IO.11.**

# 5. PREVENTIVE MEASURES

## *5.1. Key Findings and Recommended Actions*

**Key Findings**

*Financial Institutions*

1. Banks' understanding of ML/TF risk is generally sophisticated. Larger banks in particular can articulate their own sectoral and institutional risks and appropriately identify the different ML/TF risks of different types of products, lines of business, and types and identities of customers (including customers brought to banks by professional introducers).

2. Non-bank FIs all have an understanding of ML risk comparable to that of the banks. They demonstrated a general understanding of TF risk but are less consistently able to articulate how their business can be misused for TF purposes. The majority indicate that more guidance is needed.

3. Among FIs, particularly banks, understanding of AML/CFT legal obligations is very high, and in addition banks are aware of international best practices and prudential considerations that go beyond legal obligations.

4. FIs consistently refuse to engage in business with clients and customers that do not provide requested information for CDD purposes, but there is a widespread perception that banks are particularly intense in their collection and evaluation of CDD information. Other FIs and DNFBPs believe that banks are applying CDD measures without real regard to risk distinctions. Most non-bank financial institutions consider bank CDD, perceived to be more rigid, as a supplement to their own risk-based compliance measures. This places undue risk-mitigation expectations on the banking sector and weakens the overall compliance effectiveness of the Cyprus financial system.

5. FIs generally apply specific and enhanced measures appropriately to correspondent accounts, new technologies, wire transfers, higher risk countries and targeted financial sanctions. With regard to PEPs, FIs generally screen aggressively for PEP status or associations but are still in the process of developing a reliable understanding of PEPs' source of wealth.

6. Banks file STRs far more frequently than other types of financial institutions (including the MSBs met on-site). However, within the banking sector, both the frequency with which internal investigations of suspicious activity are instituted and the frequency with which internal investigations lead to STR filings vary greatly.

*DNFBPs*

7. Among DNFBPs, the larger ASPs, which have significant international risk exposure, have a sophisticated understanding of risk. Smaller ASPs, real estate agents, and the casino are less sophisticated in their assessments and less articulate in describing the AML/CFT risks they face.

8. For DNFBPs, awareness of AML/CFT obligations appears to be a function of size and international exposure. Most of the larger institutions and those with foreign clients, such as ASPs, have a detailed, sophisticated understanding of their legal obligations. The casino operator understands its own legal obligations and has limited direct interaction with most other obliged entities. Real estate agents know that they have legal obligations but are not always clear about what those obligations are.

9. DNFBPs consistently refuse to engage in business with clients and customers that do not provide information requested for CDD purposes. However, only a few sophisticated non-bank institutions with significant international business, including a few large ASPs regulated by CySEC and ICPAC and a money and value transfer service with a multinational location network, appear to have compliance practices that are designed to establish a completely free-standing structure to protect against ML/TF risk, without consideration of bank practices. Reliance on bank diligence

with respect to some transactions such as large real estate transactions is explicit.

10. Large and/or sophisticated ASPs do a good job of collecting and verifying BO information. Although the obligation to collect BO information has been in place for a number of years, ASPs that have acquired customers through acquisition of other ASPs report that it can take several years to harmonize knowledge of newly acquired customers with knowledge of pre-existing customers. This, together with the wide variation in size and sophistication of the remaining participants in the highly fragmented ASP sector, suggests that compliance with BO collection and verification obligations within the ASP sector has been uneven.

11. The casino is currently operating at or beyond the limits of its ML/TF compliance and risk management system. An action plan prepared by an outside consultant, which is nearing completion, will identify mitigating steps that are needed to address current deficiencies, but it is unclear whether the plan is intended to identify steps that will need to be taken to accommodate anticipated growth.

12. Among DNFBPs, real estate agents have not demonstrated that they apply enhanced measures appropriately.

13. The low level of reporting by ASPs and the real estate sector raises concern.

**Recommended Actions**

1. Supervisory authorities of non-bank obliged entities, including DNFPBs, should enhance their efforts to highlight obliged entities' independent obligations under the law to undertake effective CDD and other preventive measures with respect to their clients, irrespective of the systemic role played by other obliged entities, in particular Cyprus banks. The Advisory Authority should oversee the monitoring of this work and recommend relevant policy actions.

2. Obliged entity regulators should issue guidance identifying and addressing the specific ML/TF risks associated with each sector or type of obliged entity.

3. Cyprus should take steps to ensure that its legal and regulatory framework adequately addresses the ML/TF risks associated with transactions involving real estate, and that AML/CFT regulation of real estate brokers is effective. This could involve requiring the use of a real estate broker to conclude a transaction in high value or otherwise high-risk real estate, extending formal AML/CFT obligations to persons engaged in the business of real estate development, and/or extending formal AML/CFT obligations to the Department of Land and Surveys with respect to the operation of the Land Register. Additionally, Land Register information should be made available to all persons with a need to know that information, even without permission of the owner of the real property involved, to the extent consistent with data protection requirements.

4. Cyprus should consider whether the casino can responsibly manage the ML/TF risk associated with its current configuration, and if not then whether the current configuration should be changed in ways that provide more certainty about AML/CFT effectiveness, such as to a membership model. In any event, until the casino can demonstrate an effective AML/CFT program at its current level of activity, Cyprus should consider not permitting it to expand that activity.

330. The relevant Immediate Outcome considered and assessed in this chapter is IO.4. The Recommendations relevant for the assessment of effectiveness under this section are R.9-23.

### *5.2. Immediate Outcome 4 (Preventive Measures)*

331. Because of Cyprus's role as an IFC, where financial flows in and out of Cyprus are to a large extent channelled through bank accounts held by legal persons and arrangements managed by licenced intermediaries, implementation issues were weighted most heavily for banks, followed by ASPs. Although the risks associated with the domestic economy of Cyprus are secondary to those

associated with its international financial business, they are not insignificant. Therefore, the real estate sector, which faces risks both international (because of the CIP) and domestic, is weighted third on implementation issues. During the on-site visit, it became clear to the assessment team that AML/CFT compliance by the casino had weaknesses. Given that the casino is planning aggressive expansion, the assessment team weighted the casino fourth on implementation of AML/CFT requirements. The other sector that the assessment team focussed on, albeit ranked fifth in terms of materiality, was the MSB sector as it was determined that Cyprus hosts a significant number of temporary resident workers from South East Asia who remit funds through MSBs to their country of origin. Other types of financial institutions and DNFBPs are of less weight with respect to implementation given their more limited materiality to ML/TF issues.

332. Reflecting this understanding, during the on-site visit, the assessment team devoted a considerable amount of time to meetings with banks, ASPs, real estate agents, the casino and MSBs; individual meetings were held with 10 banks, 12 ASPs, 2 of the largest payments institutions (acting as MSBs) and one agent of an EU established payment institution (MSB), three real estate agents and property developers and the only licenced casino. Other private sector entities that were interviewed included: four securities firms (CIFs, AIFM and self-managed AIF), two life insurance firms, two e-money institutions, and one currency exchange office.

333. The selection of private sector entities was based on an analysis of data and information provided by the supervisory authorities. For instance, the assessment team had detailed knowledge of the activities of each bank as it requested and received from the CBC extensive data on 1. customers and operations (number of customers and volume of transferred funds, private banking clients, PEPs (incl. BOs), high risk customers, turnover through high risk customers' accounts, non-resident customers (split by natural and legal persons, incl. non-residents BOs) and turnover through non-resident customers' accounts, cash transactions, etc.; 2.geographical location of customer (offshore companies, countries of residence of the customers (split by natural, legal persons and BOs), customers residing in high risk countries, transactions with high risk countries (number and volume of incoming and outgoing funds); 3. correspondent banking data (countries of respondent banks and volume of funds transferred); 4. delivery channels (business relationships initiated non face to face, number of introduced customers); 5. size of the bank (in terms of assets); 6. other data (number of refused and terminated business relationships due to ML/TF related considerations, of which cases followed by an STR, number of STRs submitted by each bank), etc. The assessment team also evaluated trends related to the above-mentioned figures.

334. Banks were selected in the following manner: the assessment team prioritised the 7 banks which have the highest share of non-resident and other higher-risk customers; have a higher exposure to international risks (e.g. flows of funds from and to high risk areas); provide correspondent services, etc. The assessment team also met three branches of foreign banks (one based in an EU member state and two outside the EU). There are three types of ASPs in Cyprus; those supervised by the CySEC, ICPAC and CBA. A sample from each category was selected.

335. The on-site interviews served as a basis for assessing IO 4. However, the findings were further supported by numerous other sources of information including: 1. the Policies and Procedures (incl. customer intake forms) of obliged entities; 2. responses to a questionnaire sent to all the supervisors prior to the on-site visit that included data on onsite inspections (e.g. on-site inspection methodologies and procedures), sanctions for AML/CFT breaches and sanctions' application procedures, inspections covering implementation of TFS, commonly identified breaches/supervisory findings, risk assessment data (incl. data being gathered for offsite supervision purposes and risk assessment procedures); 3. The NRA findings; 4. summary of the institutional risk assessment carried out by the CBC of each interviewed bank.

336. The assessment team also held detailed discussions with the CBC on the implementation of the recommendations of the Special Assessment. Where relevant, the findings of the assessment team are presented in a separate section under each core issue.

### *5.2.1. Understanding of ML/TF risks and AML/CFT obligations*

Understanding of ML/TF risk

*Banks*

337. Banks interviewed by the assessors gave evidence of a sophisticated understanding of both ML and TF risks. As the assessors interviewed banks that collectively hold a majority of the assets held by all Cyprus banks, it is reasonable to characterize this understanding as widespread throughout the banking sector. Banks can articulate their own institutional risks and identify differences from the more generic risks articulated in the NRA that derive from banks' own specific mix of business and customers. Banks re-evaluate their overall institutional risks on a regular basis, often more than once per year (including on an ad hoc basis, if required). Banks develop business risk assessments (BRA), based on these institutional risk evaluations and customer risk assessments (CRA). Bank BRAs are approved at a managerial level and ultimately by the Board of Directors, together with an action plan to mitigate higher risks.

Banks typically express their understanding of risk in terms of tripartite risk matrices (high/medium/low) for evaluating prospective and existing customers with respect to aspects such as the customer's businesses, the nature of the customer's ties to Cyprus, and the specific foreign jurisdictions with which the customer may be associated by citizenship, residency, source of funds, or source of wealth. These variables – nature of business, nature and depth of ties to Cyprus, and geographical focus of the customer's life, business, and wealth – are what banks overwhelmingly identify as the key determinants of customer risk. The variables may be evaluated individually on a simple scale of high/medium/low, or they may be given numerical weights, but there is little evidence that banks themselves have determined that certain factors are comparatively more significant than others, or that banks differ as to the factors that they consider significant – there is broad consensus among banks about the sources of customer risk. A few banks use more finely calibrated risk scoring models that incorporate quantitative and qualitative factors and weight those factors to produce more deliberative, transparent numerical thresholds for three- or four-part risk matrices. Banks re-evaluate the risk weights assigned to different businesses, jurisdictions and other factors feeding into risk matrices on a regular basis.

338. CBC examinations have shown that banks can misclassify customers even under superficially impressive risk rating systems, which can lead to AML/CFT lapses with respect to specific customers (for example, failure to conduct EDD when a customer is wrongly classified as medium rather than high risk). CBC has occasionally fined banks for failures in this respect, and CBC considers that these fines have caused banks in general to pay attention to customer risk assessment.

339. All interviewed banks identified acceptance of new customers introduced to the banks by professional introducers (often ASPs) as an institutional risk, as any deference to the judgment of the introducers as to the appropriateness of customers dilutes the effectiveness of banks' own risk evaluation and risk management practices. They stated that they have adopted or been required to adopt certain practices to mitigate those risks. In particular, banks meet the underlying customers within three months of the commencement of the business relationship[35] and in any case before a transaction is executed within the business relationship[36], they assess introducers, and they regularly re-evaluate these relationships on the basis of the number of customers recommended by the introducers, the number of customers with whom the customer relationship was terminated for non-compliance reasons, and the number of internal suspicious activity reports and STRs to the FIU that the introduced customers generate. Banks' reliance on introducers has declined from 1,880 business relationships in 2014 to 1,015 in 2018 (a decline of 46%). According to CBC data, only 13 banks (out of 34) still rely on business introducers for CDD purposes, and those banks rely less on introducers than formerly. However, this continues to be a material issue in Cyprus since it is

[35] Requirement introduced in 2016
[36] Requirement introduced in 2019

estimated that 5.6% of the entire customer base of these 13 banks is still introduced customers.

340. Banks also appear to understand that weaknesses in systematic AML/CFT processes can be a source of ML/TF risk by creating false confidence in the reliability of essential systems. This risk can be mitigated by investment in infrastructure and technology. For example, assessors noted that a number of banks received negative examination results in 2014-2016 with respect to their compliance with AML/CFT obligations; without exception, these banks reported that they subsequently made significant investments in upgrading their compliance infrastructure, including hiring additional personnel and upgrading automated customer and transaction review software, in order to improve their management of ML/TF risk.

341. Several banks reported that they have modified their business models – particularly by trying to focus their business more on customers residing or active in Cyprus and decreasing the number of their non-resident natural person and legal person customers – for the specific purpose of reducing their overall institutional ML/TF risk by shedding high-risk customer categories. CBC is of the opinion that this reflects pressures imposed by foreign correspondents to mitigate AML/CFT risk, combined with banks' conscious adoption of strategies to comply with CBC guidance not to take on risk that cannot be managed. Clearly, it reflects these banks' understanding of the sources of institutional risk and their increasingly conservative risk appetite.

342. Banks reported that a monthly roundtable meeting with the CBC is a useful forum for obtaining and exchanging general information about ML/TF risks and specific information about emerging ML/TF issues that have arisen in the banks' actual business activities.

343. Comprehensive supervisory findings presented by CBC support the conclusions that the intensity of effort by the banking sector to assess risks has increased in recent years. This is likely the result of the full scope CBC examination cycle conducted between 2014 and 2016, the introduction of stricter legal requirements and the provision of significant guidance by the CBC). Banks generally assess the sources of ML/TF risks in a manner consistent with the National Risk Assessment – they identify the primary sources of risk as arising from the position of Cyprus as an IFC, particularly the activities of foreign customers managing businesses with non-Cypriot activities or assets. Although this may somewhat underestimate risks with domestic origins, the assessment team considers this understanding of ML/TF risks to be basically sound.

*Special Assessment-related issues:*

**Business Risk Assessments**: The CBC reported a significant increase in the quality of BRAs in recent years. Banks were required to submit their BRAs for CBC review. The first BRAs were not up to the desired standards since they followed operational risk assessment models. The quality of BRAs, however, increased after CBC imposed fines for low quality BRAs; and delivered a specialised training seminar for compliance officers (seeking the help of international experts) aiming to increase the knowledge and expertise of banking personnel in conducting BRAs. The CBC reported that banks have appropriate methodologies in place to conduct BRAs (analysis takes into account a broad range of criteria: client base, products, services, etc.), develop more sophisticated tools to conduct BRAs, and seek the help of external experts, when needed. In addition, BRAs are approved by the board of directors and action plans are being followed up to monitor the progress and prevent residual risk from occurring.

*Non-bank FIs*

344. Non-bank financial institutions, such as insurance companies, investment advisors, broker/dealers, AIFs, and MSBs, all have an understanding of ML risk comparable to that of the banks in terms of identifying sources of risk, including being able to identify the primary risk-related attributes of customers or clients, evaluate them in terms of high/medium/low risk matrices, and determine overall client risk on the basis of cumulative attribute scores. They demonstrate a general understanding of TF risk but are less consistently able to articulate how their business can be misused for TF purposes. They consistently report that Cyprus bank diligence measures are excessively strict, but they do not identify, and assessors saw no evidence of, any

specific ways in which other financial institutions disagree with banks' understanding of the main factors influencing ML/TF risk.

*DNFBPs*

345. Among DNFBPs, large ASPs with significant international risk exposure evaluated by the assessors expressed an understanding of overall ML/TF risk and an ability to evaluate the specific risks posed by specific clients comparable to that of the banks. Smaller ASPs, real estate agents, and the casino tended to be less formal in their assessments and less articulate in describing the ML/TF risks they face, but they expressed a practical understanding of risks that appears to be appropriate to their lines of business. Even real estate brokers, who had the least sophisticated modes of expression with respect to ML/TF issues of the obliged entities that were interviewed, were clearly capable of explaining how real estate transactions and their own services could be exploited for ML/TF purposes.

346. The casino's employees appear to understand the qualitative ML/TF risks associated with the casino's services – in particular the risks associated with a highly cash-intensive business involving patrons with little desire or incentive to disclose information about their identities, business, or other facts that allow for more nuanced evaluation of risk. However, the casino's employees appear to not fully appreciate the quantitative magnitude of those risks when attached to operations of the casino's current size – much less its anticipated future size. They discount, for example, the possibility that they may need significantly greater institutional resources to establish and manage the AML/CFT processes that they will have to put in place when the casino expands in the next few years.

347. Some DNFBPs have expressed a desire to improve their understanding of ML/TF risks. ASPs regulated by the CBA and ICPAC in particular expressed a desire to receive from regulators, in addition to the voluminous general and topical guidance already issued, more information about emerging ML/TF risks and regulators' risk-related concerns, and typologies. This may reflect a desire for education, training, and guidance that is more narrowly focused on the professional obligation of ASPs. Particularly with respect to ASPs that are Cyprus branches or affiliates of larger, multinational organizations, it may also reflect a desire for guidance that integrates and applies international standards in the framework of specific Cypriot ML/TF circumstances and legal requirements. CySEC-regulated ASPs generally demonstrated to the assessors a more sophisticated understanding and evaluation of ML/TF risk than did ASPs regulated by CBA and ICPAC and did not express a similar desire for additional guidance.

348. The ASP regulators regularly discuss matters of common regulatory concern but do not formally coordinate the issuance, or harmonize the content, of guidance they issue and training they give. This may be in part a natural consequence of the different professional audiences to which the training and guidance are addressed, but it may also contribute to some ASPs' perception that the regulatory playing field is uneven. Those that expressed this perception tended to be the same ASPs that offered the unsolicited opinion that overall ASP understanding of ML/TF risk, AML/CFT duties, and strategies for effective compliance would improve if there were a single regulator for all ASPs (of those ASPs interviewed, none articulated unsolicited support for the current regulatory framework). The ASPs that advocated for a single regulator appear to have been motivated at least in part by the perception that a government agency is a stricter supervisor than a self-regulatory body, and that being subject to unified government agency regulation would enhance ASPs' international reputation. These ASPs uniformly expressed the opinion that CySEC should be that single regulator. While this would be one mechanism for achieving a level regulatory playing field, an alternative would be to enhance coordination efforts among the three regulators, all of which have committed themselves to maintaining common regulatory standards to the extent that differences among their communities of regulated ASPs make it possible.

349. Assessors were able to interview only a small fraction of ASPs and of real estate agents active in Cyprus, as both sectors are very numerous. Moreover, as the collective business of both sectors is widely distributed among those numerous entities, the assessors did not consider it

appropriate to assign the interviews that were conducted the same weight that they could give to interviews of (for example) key banks. Finally, supervisors on an annual basis have conducted on-site examinations of a percentage of regulated entities. In the case of CySEC, for example, in the years 2013 through 2018 it has conducted examinations of ASPs (selected on a risk basis) that collectively maintain customer relationships with 65% of the customers of all CySEC-regulated ASPs. The total number of ASPs that CySEC has examined over this five-year period still amounts to only 20% of the ASPs it supervises. Some regulators' examination coverage is better as a percentage of regulated entities: over the last three years, ICPAC has examined virtually all of its regulated ASPs. Some are worse: the RE Council conducts a couple of onsite inspections per year on a population of 340 real estate agents. Overall, DNFBPs' supervisory examinations, therefore, provide a better basis for conclusions that the trend in risk awareness is upwards than for conclusions that overall risk awareness among regulated entities is high. In the absence of more definitive proof, assessors are therefore inclined to discount somewhat DNFBPs' self-reported understanding of ML/TF risk, and to believe that their understanding of ML/TF risk, overall, is of average quality.

Understanding of AML/CFT Obligations

*Financial institutions*

350. Banks' understanding of AML/CFT legal obligations is high – generally higher than that of other financial institutions. In addition, both banks and most other financial institutions with international exposure are aware of international best practices and prudential considerations that go beyond legal obligations. For example, several banks expressed awareness that excessive reliance on an automated screening service to screen names of potential customers and transaction counterparties was risky because all screening services have deficiencies of one kind or another, and the optimal solution is use of several automated services supplemented by the institution's own thematic searches. Among non-banks, CBC on-site examinations have indicated that electronic money institutions and payment institutions, manifest compliance weaknesses (particularly customer profiling, KYC and STR reporting) that arise from inadequate staff understanding of ML/TF obligations.

*DNFBPs*

351. For DNFBPs, awareness of AML/CFT obligations appears to be a function of size. Larger institutions such as ASPs, and even large non-financial businesses such as real estate developers that interact intensively with DNFBPs, have a detailed, sophisticated understanding of obliged entities' legal obligations – including those of the banks with which they interact. Among smaller DNFBPs, real estate agents know that they have legal obligations but are not always clear about what those obligations are.

### *5.2.2. Application of risk mitigating measures*

*Banks*

352. Banks have adopted a wide range of routine practices to mitigate ML/TF risk. Banks report that they collect and verify BO information (personal meeting or a meeting conducted through controlled video streaming tools (such as Skype call)) before conducting transactions for legal persons, collect copious tax return and other information to satisfy themselves as to the legitimacy of customer wealth and funds, and develop detailed customer business profiles (and update them both at regular intervals and when called for by events). Regulators of other obliged entities also report that banks obtain information from them about prospective and current customers that are obliged entities – for example, banks obtain certificates of supervision from the CBA as part of CDD on ASP customers regulated by the CBA.

353. To the extent that the banks have been able to apply these practices successfully, all of this gives banks a good understanding of the expected business activities of their legal person customers and allows them to effectively mitigate ML risk associated with that business, identify transactions and activities that are out of the ordinary, and mitigate risks associated with those activities as well. Risk assessment drives the selection of risk mitigation practices to be applied to a

particular customer – where on the risk matrix a customer fits generally determines the level of customer scrutiny and the frequency of customer review, for example. Thus, weakness in risk assessment undermines the effectiveness of risk mitigation irrespective of the range of techniques available. The CBC has found that banks have made significant strides in integrating the AML-related information obtained into comprehensive, well-analysed business and customer risk assessments, skills that they were weak at even a few years ago, when they focused primarily on specific tasks, such as identifying BOs of legal person customers.

354. Banks do not rely exclusively on risk matrices to determine risk mitigating measures to take. They also have categorical prohibitions on specific types of new business that are intended to address risks outside banks' risk appetite – one bank, for example, accepts no new foreign NGOs as customers, another accepts no new foreign PEPs and extends no new credit to existing foreign PEP customers, and a third claims to have accepted no new customers since 2016 from countries it has deemed to be high-risk. It appears to be more the rule than the exception that banks do not accept customers engaged in the gaming industry, the manufacture or sale of weapons, and dealings involving virtual assets (which several banks opined posed an unacceptable risk on the basis of its novelty, as well as its ML/TF risks, and about which CBC has warned Cyprus banks).

355. Banks also mitigate the risks associated with reliance on introducers for new business by typically working with far fewer introducers than they used to work with, by requiring that the introducers satisfy the bank that they have appropriate policies and procedures to control risk in their acquisition of customers (including the introducers' own AML/CFT practices), and by regularly re-evaluating introducer relationships on the basis of the number of customers recommended by the introducers, the number of customers with whom the customer relationship was terminated for non-compliance reasons, and the number of internal suspicious activity reports and STRs to the FIU that the introduced customers generate.

356. Banks that have acquired customers *en masse* from other banks in mergers and acquisitions, generally in the aftermath of the crisis of 2013, have undertaken large-scale exercises to apply their risk mitigation strategies to these new customers. These transitional initiatives have absorbed considerable resources for the banks obliged to undertake them, but all banks involved report that they have completed or will by the end of this year complete the integration of new customers into their systems, eliminating risks that could arise from maintenance of customers evaluated under different risk management standards.

357. Overall, this ML/TF risk mitigation activity appears to represent a conscious, strenuous effort by Cyprus banks to clearly improve their compliance with the established regulatory framework, and the public perception of such compliance. While still a work in progress and not uniformly successful, overall this effort has had remarkable results. Examination results tend to confirm that banks are taking more, and more effective ML/TF risk mitigation steps than they did in the 2013-2016 examination cycle. The CBC also reports that overall bank spending on ML/TF compliance has increased fourfold in the last several years, and that hiring has increased 40%. Non-bank obliged entities uniformly complain that banks have ramped up their application of CDD measures and have become extremely risk-averse, to the point that there is a widespread perception that banks essentially look for excuses to refrain from taking on new customers, particularly customers that operate in businesses with which banks are not familiar, rather than calibrating their client monitoring according to risk evaluation. Some non-bank obliged entities opine that banks' uncompromising AML/CFT commitment discourages new banking business and may drive business in general away from Cyprus. It should be pointed out, however, that non-bank obliged entities are not subject to the same pressure as banks to respond to the AML/CFT demands of foreign correspondent banks. In addition, some of this behaviour may well be attributable to banks' autonomous decisions, on the basis of institutional risk assessments, that the risk associated with specific customer categories cannot be efficiently managed and should not be accepted under banks' acceptance policies.

358. While non-bank obliged entities complain about the difficulty of doing business with the banks, they also tend to use the banks' AML/CFT activities to their own advantage. Cyprus-based

insurance companies, whose business is predominantly domestic, can afford to take a relatively formulaic approach to risk mitigation with respect to non-cash premium payments, because those transactions are overwhelmingly being conducted by customers of Cyprus banks. ICCS as the insurance sector supervisor emphasizes the obligations of insurance companies to undertake appropriate CDD at the time of pay out, and do not need to focus obliged entities on their duties with respect to receipt of customer premium payments. ASPs facilitating the set-up of new legal entities for clients find it easier to obtain BO information because they are asking for no more information than Cyprus banks would ask, and in many cases have already asked, of the same clients. Real estate brokers can perform rudimentary due diligence on a foreign customer expressing an interest in living in Cyprus and still obtain some assurances by handing the customer a list of the documents that a Cyprus bank will require to open a local bank account. To the extent that the banks' gatekeeper function cannot be circumvented, non-bank obliged entities' use of the banks as a regulatory reassurance for their own compliance efforts is an effective systemic risk-mitigation dynamic, albeit one that magnifies the systemic consequences of the failure to maintain high AML/CFT standards by any bank in Cyprus.

359. One area that banks acknowledge to be high-risk but do not categorically refrain from doing business in is the CIP programme, which requires that financial transactions required for the conclusion of an investment need to go through the Cypriot banking system. Banks perform due diligence with respect to CIP transactions in the same way that they do with respect to other transactions. However, because purchasers of property through the CIP programme are not required to have a Cyprus bank account – and most appear not to – banks' due diligence on these transactions is part of their overall monitoring of the account activities of the sellers of that real estate (typically large real estate developers) – rather than being focused on the purchasers. Bank risk mitigation in connection with the CIP therefore cannot be relied upon to police the CIP.

360. Another type of business that banks claim not to categorically refrain from involves NPOs. However, from their own reports it is clear that banks regard all NPOs as presumptively high-risk, and that they are extremely reluctant to take on new NPO customers.

*Special Assessment-related issues:*

**Higher risk customers:** Customer acceptance policies are prepared by the AML compliance officer (AMLCO). They are submitted to the Board of Directors for approval. The AMLCO bears the responsibility for submitting necessary proposals to amend the said policies on the basis of risks faced by a bank. Banks consult the AMLCO before on-boarding high-risk customers. High-risk customer files go through compliance department's checks – this applies to both new and existing customers – the AMLCO exercises an advisory role before the final decision is taken. Changes to customers' risk category from high risk to lower require the approval (not mere consultation) of the AMLCO. The CBC reported that compliance departments tend to provide good quality advice on customer risk scoring/profiling. In cases of disagreement between the business line and AMLCO's opinion, these are usually escalated to the Senior Management or the Board of Directors who take a final decision. Banks produce special CDD reports on high-risk customers (that contain an overview of the customer base, risk profiling, reports commissioned specifically for this purpose from international consultants, etc.), which are submitted for Senior Management approval on a yearly basis.

**Tax crimes**: In 2014-2015, supervisory authorities, in cooperation with the FIU, delivered seminars to the supervised entities on tax crimes. Banks were expected to properly manage risks with respect to this offence, including, where necessary by obtaining audited financial statements and tax declarations from the customers to support source of wealth and source of funds; obtaining such documentation immediately upon the establishment of a customer relationship, or before the execution of the first transaction on a revived dormant account; and taking into account a customer's relationships with non-cooperative tax jurisdictions (e.g. FATF- and EU-listed countries, offshore financial centres) when assessing customer risk. Based on its monitoring, the CBC reported that banks consider ML in relation to tax crimes adequately. This has been confirmed by the FIU, which receives tax evasion related STRs.

*Non-bank FIs*

361. Other financial institutions, particularly CIFs, AIFs, and investment advisers, take steps comparable to those that banks take, while asserting that they are essentially duplicating the steps taken by the banks. Insurance companies apply ordinary or simplified CDD measures according to their assessment of the risks associated with their lines of business and specific customers. CySEC examinations in particular tend to support this impression of widespread CDD compliance.

362. MSBs mitigate risk associated with remittances to foreign countries (the great majority of their business) by refusing to remit funds to legal persons, by doing diligence on offices in foreign countries that handle transfer to beneficiaries (if offices are not affiliates), and by limiting transaction size (per transaction, per month, per year). These measures are reasonable with respect to a line of business perceived as being of moderate risk – additional measures may need to be taken if Cyprus analysis of risks associated with domestic financial activities, including generation of remittances, results in identification of heightened risk.

*DNFBPs*

363. Among DNFBPs interviewed by the assessors, it is the ASPs that demonstrated the most varied and sophisticated risk mitigation strategies – not surprisingly, as those interviewed were among the larger ASPs, which according to their supervisors are the most sophisticated and effective representatives of the sector. When considering a potential new client, these ASPs generally collect significant amounts of information, sometimes essentially duplicating banks' information collection measures; smaller ASPs apparently sometimes supplement their execution of the formal CDD process with personal on-site review of client business and assets by their principals. This formal and informal CDD information can provide a basis for refusing to take on the client, but more often helps in determining the intensity of monitoring procedures for clients taken on. ASPs in general also reported collecting significant amounts of information for regular and episodic updates of client profiles, terminating existing clients that were unwilling to provide such information on the theory that such clients posed higher risks. One ASP reported that it will recommend a bank to its client and will review the client's choice of bank if not recommended for risk-related issues such as the quality of jurisdiction of the client's chosen bank, and the client's rationale for its choice of bank. With respect to existing clients, all ASPs that were interviewed reported that the number of their clients has declined dramatically (whether measured by number of BOs or number of legal persons), through a combination of client self-selection because of unwillingness to provide requested information promptly and on a regular basis, increased ASP fees to cover compliance costs, and a more conservative risk appetite. ASPs almost uniformly report that they will not accept new clients who engage in arms trading, adult entertainment, gaming, and virtual asset activity (which ASPs regard as posing risks on account of novelty as well as ML/TF potential – and which ICPAC in particular among their regulators has warned them to be vigilant about), and that they will sever relationships with clients that become involved in these activities.

364. The larger ASPs have maintained their size despite a perceived decline in the market for ASP services by merging with and acquiring other ASPs.[37] Appreciating the risks arising from maintaining clients initially brought onboard under different risk evaluation practices, ASPs in this position have taken extraordinary steps to evaluate newly acquired clients under firm-wide common standards, and report having severed client relationships with numerous newly acquired clients whose backgrounds were discovered to pose unacceptable risks under the acquiring ASPs' standards. These acquiring ASPs tend to be the ASPs that started out relatively large, and with mergers and acquisitions they have grown larger. Their efforts to establish firm-wide standards tends to confirm supervisors' opinions that it is the larger ASPs that have the most sophisticated risk mitigation strategies.

[37] Reports of the decline in ASP services is in tension with statistics showing a continuing rise in the number of legal entities organized and registered in Cyprus. This may in part be attributable to a rise in the number of companies operating in Cyprus, which have traditionally not sought the services of ASPs.

365. Assessors were unable to determine how much and in what respects the ML/TF risk mitigation activities of these few large ASPs differed from those of the large number of small ASPs. Because of the fragmentation of the sector, assessors were also unable to reach independent conclusions about characteristic differences on this score that might or might not exist between ASPs regulated by CySEC, CBA, and ICPAC. That regulators such as CySEC were prepared to distinguish sharply between large and small ASPs on the subject of risk mitigation, however, and that ASPs themselves were prepared to offer unsolicited opinions drawing distinctions among the ASP regulators in terms of their apparently "toughness" suggest that there may be variability in risk mitigation efforts and in AML/CFT effectiveness in the ASP sector.

366. Real estate agents at most collect basic identifying information themselves, while informing their customers – particularly foreign customers – that Cyprus banks will require significant documentation before being willing to handle funds to be used in a real estate transaction.

367. The casino attempts to mitigate the risks associated with gaming by encouraging customers to enrol in its loyalty program, which allows the casino to do a basic customer background check. The casino also imposes diligence requirements on cage and table transactions over certain euro limits. However, the casino acknowledges that these strategies do not address risks associated with a large number of small and medium-sized transactions, representing the wagers of a large minority – possibly a majority – of the casino's patrons. Such transactions are essentially anonymous, except to the extent that review of security tapes (possibly to be assisted by facial recognition software at some point) allows positive identification. The casino reportedly considered a membership model for its gaming activities, which would have addressed these risks, and rejected it on business grounds. An outside consultant is preparing an action plan for the casino, but the plan had not been finalized at the time of the onsite visit. The Gaming Commission demonstrates awareness of the issues associated with the casino's relatively casual attitude towards risk mitigation but having been constituted only in 2018 it has found building the capacity to effectively mandate the necessary changes to the casino's AML/CFT approach to be challenging.

368. The casino is also planning aggressive expansion, to include significantly increasing the size of the gaming operations, attracting foreign junket operators, and attracting foreign VIP customers. The casino is conducting due diligence on prospective junket operators, including requiring proof of their AML/CFT practices. This expansion of activity and of ML/TF risk strains both the casino's and its regulator's AML/CFT resources. It is unclear what risk mitigation strategies the casino is planning on implementing as part of any of its other plans. It is also unclear whether the action plan being prepared for the casino will address any of the casino's expansion plans or propose concrete steps to take on these matters.

### *5.2.3. Application of CDD and record-keeping requirements*

*Banks*

369. Banks rigorously apply basic CDD and keep records of information obtained, a claim that is generally supported by examination results and by anecdotal reports from other obliged entities. Banks report, and CBC confirms, that this includes, preparation and retention of notes of face-to-face meetings with BOs of new legal person customers (or recordings of Skype conversations where BOs could not be physically present in Cyprus), with direct contact typically being made within a short period after opening new customer accounts, and in any event before executing any transactions for these new customers, in compliance with CBC's 2019 directive on the subject. Banks' stringent standards for deeming CDD information satisfactory has reportedly had the effect of discouraging foreigners in particular from establishing business relationships in Cyprus. Several banks, along with ASPs, and real estate developers, characterise meticulous compliance with CDD requirements as perhaps the most significant change in bank practices in Cyprus since the financial crisis of 2013. Banks collect BO information with respect to any prospective customer that is a legal person. Banks can easily explain in impressive detail the BO information that they regard as necessary, and they report that they routinely demand such information, sometimes being forced to delay account opening for weeks or months pending receipt of satisfactory BO information from

prospective customers. In addition, and in particular since the CBC's circular requiring banks to refrain from offering services to shell companies, banks have become aggressive in collecting and updating information about the purpose of formation of legal entity customers that are not clearly operating companies with a physical presence in Cyprus. Minimally detailed *pro forma* explanations of purpose of formation appear to be largely unacceptable as a basis for a legal person to obtain banking services in Cyprus.

370. Banks also report, and CBC confirms, that banks engage in risk-based ongoing monitoring, including of changes (if any) in BO information.

371. Banks increasingly refuse or terminate business based on ML/TF risk. The basis for such refusals is usually that CDD is incomplete or that a customer falls outside the risk appetite of the bank (e.g. banks tend not to enter into business relationships with businesses of questionable reputation or that engage in activities unfamiliar to the institution such as virtual currency related business).

*Special Assessment-related issues:*

372. **Use of complex structures**: Banks take into account the accumulation of risks of complex businesses. Although there is no precise definition of a complex structure, the CBC reports that it is assumed that legal structures with three or more layers of ownership are deemed complex and should be treated as high risk. Banks obtain information about a customer's group structure (which has to be signed by the director or the BO) and a shareholder certificate by each company in the group. In addition to identifying the BO, directors at each layer are also identified. When creating the business profile of the customer, broader risk is assessed by obtaining information on the activities of the companies belonging to the group, associate companies, source of wealth of each of those companies, etc. Detailed and transparent information on mitigating measures for complex risks are set out in internal policies and procedures (e.g. specifying the EDD measures, monitoring scenarios and listing concrete documents that have to be obtained for CDD and monitoring purposes).

373. **Resources for monitoring of high-risk international businesses**: The CBC reported that, since the Special Assessment, compliance personnel in the banking sector has doubled: a very sharp increase in human resources in banks' compliance departments has been noted in bigger banks (in one case amounting to 35 FTEs). Banks have also made significant investments in technical equipment to assist with ongoing monitoring, CDD databases, customer screening tools, etc. The CBC reported that during onsite inspections it performs checks in relation to specialised monitoring scenarios that have been developed for higher risk customers (and where needed – developed for individual customers). For example, electronic funds transfer transactions are filtered on a real-time basis against sanctions list and in case of possible positive match the transaction is not executed until further investigation is performed. In addition, different limits are set for particular type of accounts (high risk customers) or transactions (e.g. cash transactions) on the basis of customer's economic profile. Banks evaluate their monitoring system at least once every 2 years. The CBC acknowledges that banks are expected, in addition to relying on the ready-made IT scenarios for monitoring, offered by well-known brands, to develop specific scenarios that would fit the risk profile of the institution.

374. **Introduced business**: Banks implement stricter controls in relation to business introducers: they satisfy themselves that the business introducer is a regulated person for AML/CFT purposes; and they assess business introducers by reviewing their policies and procedures and gathering additional information to assist in assessing the reputation of, and the risks posed by, specific introducers. Some banks use a scorecard to risk rate the introducers. The assessment is reviewed on an on-going basis. On the basis of this assessment, the compliance department makes a decision whether to enter into or maintain the business relationship with the introducer. Thus the risk of entering into the business relationship with unreliable introducers is minimised. Since 2016, banks meet the introduced customers (personal meeting or a meeting conducted through controlled video streaming tools (such as Skype call)). When on-boarding

higher risk customers, banks tend to organise face to face meetings or even visit the customers' premises. CBC expects banks to record minutes of the meetings, maintain records of video calls and supporting documentation, such as photos). These meetings serve as a risk management tool and result in a better understanding of the business activities of the customer. With the increasing efforts of banks to perform their own research on introduced customers, the CBC reports that the role of business introducers has changed, with their non-introducing roles diminishing.

375. **Outstanding CDD**: After the completion of the Special Assessment, banks initiated CDD review projects. The full scope onsite examination cycle, that covered all banks, was finalised by the CBC in 3 years period. Based on onsite examination findings, the CBC reported that it has identified cases in the past when customer CDD reviews were delayed, however, at the time of the on-site visit all banks had made significant progress. Some of the larger banks have also employed IT systems to monitor CDD renewal and updates. Frequency and prioritization of CDD review checks CDD is determined according to customer risk.

*Non-bank FIs*

376. MSBs face a challenge in enforcing compliance with CDD requirements across networks that include offices owned by the principal, agents, and sub-agents. MSBs' compliance with CDD obligations varies according to access to technology: those MSBs that process transactions through fully automated systems have a significant compliance advantage, in that their systems prevent any transaction processing without accomplishing specific compliance tasks. This allows MSBs with access to this technology to control compliance by agent offices, as well as those owned and operated by the principal, reasonably effectively.

377. Other non-bank financial institutions of all types routinely assert that their collection of CDD information essentially duplicates the CDD collection efforts of Cyprus banks, but it is difficult to substantiate this claim. In interviews, some investment managers discussed their model as being based on obtaining clients primarily through the personal connections of one or two firm principals. While these firms asserted that they conducted all required CDD appropriately, they also acknowledged that they used the principals' personal knowledge of clients to supplement CDD. So long as such personal knowledge is supplemental, it is at worst neutral and may make CDD more effective. Supervisors such as CySEC strongly assert that such reliance is not reflected in examination results but acknowledge the risk posed and the need for regulatory vigilance to guard against such reliance.

*DNFBPs*

378. Larger ASPs consistently report that they conduct CDD scrupulously, and most report that they do not hesitate to terminate (or refuse to establish) a client relationship if CDD information is not forthcoming. This, together with the larger ASPs' reports of declining volumes of business[38] and expressed concerns about the viability of the ASP business model in an atmosphere of stringent CDD compliance, lends support to the conclusion that the larger ASPs are making serious efforts to perform CDD. Supervisors' examination findings also tend to corroborate self-generated evaluations of compliance, notwithstanding the possible conflict between the need to maintain personal relationships with clients and the need to obtain, verify and act on CDD information.

379. Personal relationships still drive a significant share of the ASP business, however, and personal assurances can function as a supplement to more formal CDD. One ASP, for example, reported that its principal will physically inspect all real estate assets of prospective new clients wanting to set up real estate holding companies in Cyprus with real estate assets in another country, as the principal travels to that other country regularly to acquire business. This same ASP will also obtain independent third-party information about reasonable rents, reasonable purchase

[38] This in tension with statistics showing that numbers of legal persons have continued to rise. This may be explicable by an increase in the number of companies organized in Cyprus and operating in Cyprus, which do not traditionally use the services of ASPs.

price and valuation of real estate, supplementing the principal's own information as part of the process of determining the reasonableness of the client's reported assets and income. So long as the CDD process remains intact and effective, informal investigation by a principal may be a useful supplement. However, the fact that it is the principal undertaking these efforts can contribute to the impression that the firm is merely an extension of the principal and that it is the firm's CDD compliance efforts, not the principal's personal efforts, that are supplemental. This impression, in turn, raises the question of how diligently the principal will supplement the firm's CDD compliance, and how effective overall that compliance will be, when conflicts of interest arise between the principal's desire for new business and the AML/CFT obligations of the ASP as a regulated entity. These impressions arise most urgently in evaluations of ASPs controlled by a single dominant individual or a small group. This suggests that the AML/CFT practices of the larger ASPs are not just more complex and rule-driven than those of the smaller ASPs, as is to be expected with larger institutions, but may be more effective as well.

380. Other DNFBPs do not appear to undertake the same CDD efforts, nor are they as diligent in their collection of CDD information, as the large ASPs. Real estate agents collect minimal CDD information about any of their customers. The casino collects CDD information about customers who voluntarily join the casino's loyalty program, or whose gaming transactions cross specific euro thresholds. There is no evidence that, when customers of these types of DNFBPs are legal persons (a circumstance that is likely to arise regularly if infrequently for real estate agents, though unlikely with the casino), BO information is collected or verified. To the extent that these DNFBPs have ongoing customer relationships, there is also no evidence that the DNFBPs conduct meaningful ongoing due diligence.

### *5.2.4. Application of specific and EDD measures*

*Politically exposed Persons*

381. Banks perform automated screening for PEP status, supplemented by open-source research and in some cases private investigatory agencies. Banks update PEP screening both at regular intervals and as a result of events like domestic elections and widely publicised scandals such as the publication of the Panama Papers; this is more effective at identifying PEPs rather than their family members or close associates. For the purposes of identifying family members and close associates, banks obtain self-declarations from the customer although this practice is not applied uniformly across the banking sector. Direct or indirect business relationships or links with family members or close associates of PEPs are followed up through ongoing monitoring. PEPs are subject to enhanced CDD measures, such as enhanced monitoring, additional information on the source of wealth and funds, and approval of senior management.

382. Some other FIs and DNFBPs, which are generally less sophisticated than banks, still have an insufficiently effective understanding of the source of PEPs' wealth, enhanced monitoring and identification of close associates and family members of PEPs (although there was a uniform understanding of the need to obtain senior management approval before entering/continuing the business relationship with a PEP. FIs assert that they perform PEP screening, with those having a more international customer profile performing screening along the same lines as the banks. ASPs perform comparable screening to banks with comparable results. Real estate agents perform no such screening and do not collect information on source of wealth/funds, leaving compliance to other obliged entities (particularly banks) and lawyers.

383. Based on supervisory findings, the CBC considers that beyond identification of PEPs, banks previously have been less effective than they should be in understanding the source of PEPs' wealth, although current supervisory data suggest that they have improved recently.

*Correspondent Banking*

384. Most banks provide limited if any *vostro* services. Some banks do not provide *vostro* accounts at all. Despite the fact that no enhanced measures are legally required to be applied with respect to respondent banks established in EEA countries (see Rec. 13), banks apply a risk based

approach, i.e. assess the risk of correspondent relationships on a case by case basis and may decide to apply the full set of EDD measures in relation to high-risk banks within the EEA. Respondent banks established in third countries are subject to EDD measures (including an assessment of geographical risks, evaluation of the internal AML/CFT controls of the respondent, enhanced monitoring, etc.), which appear effective at limiting risks arising from those correspondent relationships. Those that maintain *vostro* accounts do so only for a few financial institutions in low risk, effectively regulated jurisdictions, or for their own parent institutions if they are part of a financial group. Two banks provide correspondent services to banks established in higher-risk jurisdictions and appear to apply satisfactory EDD.

*New Technologies*

385. Consistent with the CBC's directive on the subject, banks require risk evaluations of new products, services, delivery channels and technologies before implementation, asserting that the AMLCO has to perform a risk assessment prior to the launch of new products, initiation of new business practices, or use of new or developing technologies. For example, banks have notified CBC of plans to install customized ATMs at the premises of cash intensive bank business customers, which appears to be an example of a new technology in which business advantages in minimizing cash handling costs and security must be balanced against increased AML risk. Some banks have made firm decisions not to expose themselves to specific new technologies – for example, a number of banks categorically reject prospective customers that do business involving virtual assets. IT tools used for monitoring purposes are assessed before being launched to identify any potential gaps which may have an impact on compliance.

386. Other types of FIs understand their obligations in relation to the assessment of new technologies, new business products or practices. However, it is not clear whether and/or to what extent these risk assessments include an AML/CFT element.

387. DNFBPs expressed a general understanding of these requirements, stating that such risk assessments are very uncommon in practice, as they very rarely, if ever, launch new products or services or develop new delivery channels. Some obliged entities (such as ASPs) have practices comparable to those applied by banks and others (such as real estate agents) mitigate new technology risk by resisting the implementation of new technologies in general.

*Wire Transfers*

388. Banks and payment sector firms, including e-money institutions and MSBs, assert that they follow wire transfer information collection and record retention procedures scrupulously. CBC on-site examinations using dedicated audit programs have identified no major systemic weaknesses in compliance, though examination results suggest that compliance with requirements is not completely uniform. Assessors saw no basis for disagreeing with CBC's conclusions.

*Targeted Financial Sanctions*

389. Obliged entities in general rely heavily on subscription services, public notices from FATF, and bulletins from Cyprus regulators to establish screening protocols for objects of targeted financial sanctions; they understand the risks associated with relying too heavily on a single list and typically have separate, redundant screening services. No interviewed banks, and of other obliged entities only a few small ones, rely on manual screening for objects of targeted financial sanctions. Obliged entities freeze[39] customer/client assets promptly to comply with sanctions when required. More detailed information on the application of TFS-related requirements is provided under IOs 10 and 11.

*Higher-risk countries*

390. Most banks report developing their own risk ratings of jurisdictions to supplement use of FATF lists to identify appropriate subjects for EDD. As a result, banks appear to be discharging

[39] These freezing measures do not relate to UN/EU TF or PF TFS.

their EDD obligations effectively. These obligations include obtaining additional information to understand the intended purpose and nature of business relationships of the customers residing in higher risk jurisdictions, enhanced identification and verification of UBOs, etc. However, application of enhanced monitoring to transfers from and to high risk jurisdictions (irrespective of the country of residence of the payer or the payee) is uneven.

391. All other FIs and DNFBPs seem to be familiar with the concept of high risk third countries and apply the required EDD measures. However, risks related to the transfers executed from and to high risk countries are significantly less well understood. There is lack of evidence to justify that enhanced monitoring scenarios are applied to flag up such transactions in all cases.

### *5.2.5. Reporting obligations and tipping off*

*Banks*

392. Banks assert that they have well-established policies and procedures for initiating investigations of suspicious activity, preparing internal reports of suspicion, making determinations as to the appropriateness of filing STRs, and making such filings. While examination reports do not specifically challenge these assertions, significant variations in filing frequency that bear little relationship to obvious sources of bank risk such as PEP customers, foreign customers, and high net worth customers suggest that filing triggers could vary significantly from bank to bank. The CBC has observed that discrepancies in filing frequency have declined over time, however, suggesting a gradual convergence within the banking sector concerning filing triggers. Regardless of the frequency of STR filings, banks have considered the problem of tipping off and put in place procedures, often involving carefully worded account agreement language, written statements to customers, and scripts for conversations, to avoid tipping off customers when adverse action is associated with STR filing.

393. In addition to issues specifically with filing reports, the CBC has noted that obliged entities under its authority have not monitored transactions subsequent to STR filings but involving the same accounts as closely as they should. This suggests that obliged entities may not have fully appreciated the value of ongoing monitoring to corroborate conclusions reached in individual STRs or to produce fuller pictures of more complex undertakings. CBC considers that banks have largely rectified this weakness.

*Non-bank FIs and DNFBPs*

394. Most other types of obliged entities report their STR filing to be rare – most report filings in the single digits per year, and it appears not to be unusual for obliged entities to go several years without filing any STRs. For ASPs, the assessors found this to be of concern because it seemed inconsistent with the ASPs' accounts of increased due diligence, a more conservative risk appetite, and heightened standards for client behaviour. It is also inconsistent with the ASP regulators' assertions about the number and clarity of their communications to and training events for ASPs, suggesting a failure of communication about reporting standards and triggers. For MSBs, the assessors found individual filing numbers to be strikingly at variance with statistics showing total MSB filings to be in the hundreds per year. This variance strongly suggests that MSBs have starkly different standards for filing STRs – differences so stark that it calls into question whether conclusions about the MSB sector as a whole can be drawn from the STRs that have been filed.

395. For further information on STR reporting see core issue 6.2.

### *5.2.6. Internal controls and legal/regulatory requirements impeding implementation*

396. The internal AML/CFT controls of FIs and larger DNFBPs generally comprise three lines of defence. All obliged entities have written policies and procedures in place for the implementation of AML/CFT requirements; however, some AML/CFT procedures lack detailed instructions on TFS implementation.

397. Banks have established clear internal control frameworks, involving unambiguous policies and procedures, to implement CDD, EDD, and STR reporting. These frameworks typically give the

AMLCO a large degree of control over ultimate decisions, with regular and episodic reporting to responsible members of the bank's Board of Directors. Internal quality control and audit functions are typically documented as well. All banks appoint a member of the Board who is responsible for ML/TF risk management and oversight. As mentioned under core issue 4.2, BRAs are typically documented and submitted for Board approval. Internal quality control and audit functions are typically documented as well. The branches of foreign banks implement group-wide policies and procedures and are often subject to group internal audit.

398. The CBC's supervisory findings support above conclusions based on onsite interviews. Internal audit departments of banks have seen a noticeable improvement in recent years, with units being specifically dedicated to AML/CFT. AML audit is carried out on a yearly basis, and findings have to be reported to the CBC. The CBC reported that no issues have been ever encountered in relation to the requirements of R. 18 (neither in relation to the banks established in EU nor in third countries). There is only one bank established in Cyprus that has a branch in another EU member state.

399. Larger ASPs' internal control frameworks are similar to those of banks, albeit less stringent. Other types of obliged entities, particularly smaller ones, do not uniformly have well-established, formalised controls and procedures as banks and larger ASPs, some of them relying on external providers to perform an AML/CFT audit function and/or hire external compliance consultants.

400. The CySEC's supervisory data demonstrates that all supervised entities, irrespective of their size and the nature of their activities, have an independent audit function which comprises AML/CFT matters, as annual AML/CFT reports are approved by the Board of directors and submitted for CySEC review. The latest supervisory data maintained by ICPAC shows that 30 percent of active ASPs have undergone an external AML audit; increasingly external compliance consultants are engaged by ASPs supervised by ICPAC. There is limited supervisory data CBA-supervised ASPs to demonstrate whether appropriate internal controls (in particular, audit function) have been established by its supervised ASPs.

401. The frequency of internal AML/CFT training programmes depends on the size of the entity: larger obliged entities organise ongoing internal AML/CFT training for their employees and encourage employees to attend external training and/or obtain international certificate. Smaller entities generally attend training events organised by external consultants or supervisory authorities.

402. Secrecy laws do not impede the implementation of AML/CFT requirements.

*Special Assessment-related issues:*

**Staff training**: In addition to general AML/CFT training (CDD, EDD, construction of customers' risk profile, ongoing monitoring), banks have developed specialised training programmes (e.g. TF, trade finance). The said training programs are developed in-house or delivered by external experts. This information has to be reported to the CBC on an annual basis; the CBC sample checks the attendance sheets and material used for the training in the course of on-site inspections. Many banks' employees have international certificates, such as CAMS or similar. Overall, compliance culture in banks has significantly improved since 2013 - CBC reported a significant increase of expenditures for compliance. It is estimated that compliance costs in the banking sector increased from EUR 0.7 million in 2014 to EUR 2.7 million in 2018.

*Overall conclusions on IO.4*

403. **Cyprus is rated as having a moderate level of effectiveness for IO 4.**

# 6. SUPERVISION

## *6.1. Key Findings and Recommended Actions*

**Key Findings**

*FI Supervisors*

1. The supervisory authorities apply comprehensive controls in relation to preventing criminals from owning or controlling licensees;

2. There is a good understanding of ML risks; in some cases, there is very good understanding, for example, where specific risk exercises have been undertaken by the CBC. Overall, there is good understanding of FT risks although this is less developed than for ML;

3. The supervisory authorities use risk-based approaches to focus AML/CFT programmes. The approaches used by the CBC for banks and CySEC for securities market participants are the most robust and sophisticated although there is scope for these to be refined (ie for minor changes to be made).

4. The CBC's approach to non-banks is not as comprehensive as for banks. These sectors are still at the development stage;

5. Inspections by the CBC and CySEC are very good quality and they always require breaches to be remediated. There is scope for both authorities to increase the number of inspections.

6. Sanctions have been imposed by the CBC and CySEC. Each of the two authorities has stonrg elements of effectiveness and dissuasiveness although, overall, the frameworks are not wholly effective for either authority. In addition, the CBC process is not streamlined. Sanctions have not been imposed by the ICCS;

7. For the CBC and CySEC shortfalls in staff resources are limiting the efficiency of the licensing process (but not its quality beyond this) and for all three authorities, shortfalls in staff resources are limiting the volume of supervision, linked work on risk assessment, and sanctioning that can be undertaken;

8. The authorities have demonstrated that they have made a positive difference to the level of compliance by FIs;

9. The authorities have promoted a clear understanding by FIs of their AML/CFT obligations and risks, with a greater emphasis on AML.

*DNFBP Supervisors*

10. All DNFBP supervisors apply market entry measures albeit with varying degrees of intensity.

11. The ASP supervisors have a good understanding of the ML risks of the sector, while the understanding of TF risks is less developed. Although a similar risk assessment approach exists between the three ASP supervisors, there are differences in risk assessment methodologies and all of them require further enhancement or at least some refinement (e.g. extension of the set of AML/CFT risk data to be collected). The Estate Agents Registration Council underestimates the ML/TF risks of the supervised sector. The Casino Commission has a comprehensive understanding of ML risks to which casinos are exposed and has a general understanding of TF risks.

12. The resources allocated to AML/CFT supervision within all supervisory bodies (except for ICPAC's onsite inspections) are not sufficient to ensure the implementation of a fully effective risk-based supervision.

13. The risk assessment systems utilised by the DNFBP supervisors are adequate and, in general, supervision is taking place on a risk-sensitive basis (except for the Estate Agents Registration

Council). However, a fully comprehensive and more harmonised application of a risk-based supervisory approach for the ASP sector is missing.

14. The number of on-site inspections conducted so far by all DNFBP supervisors (except for the ICPAC) is low. Very few sanctions for AML/CFT infringements have been imposed by DNFBP supervisors. There is a tendency to adopt a consensual approach which calls into question the effectiveness, proportionality and dissuasiveness of the sanctioning regime.

15. All DNFBP supervisors (except the Estate Agents Registration Council) were able to demonstrate improvements in AML/CFT compliance as a result of their interventions.

16. Guidance has been issued and training on the application of the provisions of the AML/CFT Law is provided by most DNFBP supervisors to promote a clear understanding by DNFBPs of their AML/CFT obligations. However, the focus on CFT is still limited.

17. Supervision of the ICPAC by the CyPAOB and the CBA by the Attorney-General with regards to their function as SRBs has very limited focus, if any, on AML/CFT matters. The Estate Agents Registration Council as SRB is not supervised by a competent authority.

**Recommended Actions**

*FI Supervisors*

1. All three supervisory authorities should increase staff resources and provide relevant training for the new staff. This will also mean an increase in budgets.

2. The CBC and CySEC should refine their risk models in line with their planned timetable, including taking account of both the NRA and current risks and refining the focus on FT. The ICCS should formalise its approach to risk categorisation.

3. The CBC and CySEC should use the increased staff resources and the refined risk assessment models (and risk assessment process overall) to enhance their onsite inspection programmes so as to ensure risk-based supervision is comprehensive. In addition, the ICCS should formalise its risk-based approach to supervision.

4. The CBC should amend its internal processes so that decision-making and the imposition of sanctions will be timelier; both the CBC and CySEC should refine their approaches to sanctions so that they are demonstrably proportionate and dissuasive; the ICCS should develop a written process for the imposition of sanctions.

5. As the updating of the NRA unfolds, all three authorities should provide more detailed outreach on TF.

*DNFBP Supervisors*

6. DNFBP supervisors should strengthen their licencing procedures:

a) The CBA should implement measures to check the criminal background of individual licensees and persons controlling or managing ASPs or LLCs and to verify that no persons other than advocates are the BOs or acting as directors of such companies. The CBA should implement measures to prevent close associates of criminals from being licence holders or BOs or holding a management function in a licence holder. The CBA should implement measures to ensure active and comprehensive on-going monitoring of licence holders (including BOs and management) with the licencing requirements.

b) The Estate Agents Registration Council should ensure that measures are applied to prevent criminals and their close associates from being license holders or BOs or holding a management function in licence holders. The licensing requirements should be underpinned by adequate regulatory provisions.

c) The ASP supervisors should ensure that information is exchanged systematically on rejected applications and withdrawn licences to prevent persons who are not deemed fit and proper by one supervisor from seeking a licence elsewhere.

7. The risk-based supervision processes should be strengthened by the ASPs supervisors:

a) CBA and ICPAC should expand the set of AML/CFT risk data that is collected through the AML Questionnaires; risk data collected by CySEC needs refinement.

b) The CBA should collect AML/CFT risk data annually and take more active control over the ML/TF risk assessment process of its regulated entities.

c) The CBA and the CySEC should reconsider the selection criteria for the review of AMLCO Reports and ensure an effective use of risk-related information for risk assessment purposes.

d) The CySEC should subject at least a certain amount of low risk ASPs, chosen randomly and on the basis of off-site risk data, to an on-site inspection. The aim should be that every ASP, irrespective of its risk category, is subject to an on-site inspection within a certain period of time.

e) Overall, all ASP supervisors should ensure that a harmonised and consistent approach is applied for off-site and on-site monitoring, sanctioning of ASPs and that harmonised industry standards are communicated to the market participants.

8. The Estate Agents Registration Council should immediately introduce a risk-based approach to supervision starting with a risk assessment based on regular collection of ML/TF risk data from its supervised entities.

9. The Casino Commission should expand the set of AML/CFT risk data that is collected through the Casino Regulatory Return and should develop a methodology to determine the scope, frequency and intensity of on-site inspections taking into account the specific individual risks.

10. All DNFBP supervisors should increase their resources (except for ICPAC) to ensure fully effective risk-based supervision.

11. The number of on-site inspections should be increased by all DNFBP supervisors (except for ICPAC) to ensure that they are in line with Cyprus' risk profile. Additionally, the Estate Agents Registration Council and the Casino Commission should build up specific knowledge required for conducting risk based onsite inspections.

12. All DNFBP supervisors should make use of their sanctioning powers and impose effective, proportionate, dissuasive sanctions for AML/CFT breaches. All DNFBP supervisors should adopt a sanctions application policy with clear criteria to be used when determining the type and level of administrative sanctions.

13. All DNFBP supervisors should provide more detailed outreach on TF.

14. Supervision of the ICPAC by the CyPAOB and the CBA by the Attorney-General with regards to their function as SRBs should be more focussed on AML/CFT matters. The Estate Agents Registration Council as SRB should be under the supervision of a competent authority.

404. The relevant Immediate Outcome considered and assessed in this chapter is IO.3. The Recommendations relevant for the assessment of effectiveness under this section are R.14, R.26-28, R.34, and R.35.

### *6.2. Immediate Outcome 3 (Supervision)*

405. The most material sectors in Cyprus, in descending order, are banking, ASPs, real estate, the casino and MSBs (see Chapter 1 and paragraph 320 for underlying factors). When assessing this Immediate Outcome, the supervision of these sectors was weighted more heavily.

### *6.2.1. Licensing, registration and controls preventing criminals and associates from entering the market*

*FI Supervisors*

406. FI supervisory authorities apply comprehensive controls in relation to licensing so as to prevent criminals from holding, or being the beneficial owner (BO) of, a significant or controlling interest or holding a management function in FIs. While the number of new entrants into the finance sector in recent years has been limited, the new entrants comprise a relatively substantial increase in the number of e-money businesses; the CBC and CySEC ensure they understand the varying business models of these entrants and seek to ensure that only good quality businesses enter the market. There have been no new entrants to the insurance sector in recent years, but it is apparent that ICCS also has processes in place to ensure the same standards. More generally, a depth of sources of information from within and outside Cyprus has been used by the authorities in licensing and vetting changes of controller. The table below indicates the number of licences issued, withdrawn and refused applications and withdrawn licences by type of regulated entity.

**Table 25: Licence applications/withdrawals by the type of regulated entity (2013-2018)**

| Type of Regulated Entity | Licencing Authority | Number of licences issued | Number of licence applications withdrawn | Number of licence applications refused | Number of licences withdrawn |
|---|---|---|---|---|---|
| **Banks** | CBC[40] | 19[41] | 1 | 0 | 0 |
| | ECB [42] | 0 | 0 | 0 | 19[43] |
| **PSPs** | CBC | 13[44] | 2 | 0 | 2 |
| **EMIs** | CBC | 15[45] | 1 | 0 | 2 |
| **Bureaux de change** | CBC | 4[46] | 0 | 0 | 1 |
| **Life Insurance companies** | ICCS | 0 | 0 | 0 | 0 |
| **Cyprus Investment Firms** | CySEC | 182 | 36 | 21 | 62 |
| **UCITS Management Companies** | CySEC | 5 | 0 | 0 | 0 |
| **Self-Managed UCITS** | CySEC | 0 | 0 | 0 | 0 |
| **Alternative Investment Fund Managers** | CySEC | 25 | 3 | 2 | 3 |
| **Self-Managed Alternative Investment Funds** | CySEC | 2 | 1 | 0 | 0 |
| **Self-Managed Alternative Investment Funds with a Limited Number of Person** | CySEC | 67 | 0 | 2 | 0 |
| **Companies with sole purpose the management of AIFLNPs** | CySEC | 9 | 0 | 0 | 1 |

CBC

407. The licensing team of the CBC has eight staff. It is experienced and receives training in AML/CFT and related matters. This includes FinTech and on electronic money institutions and

[40] up to the 4th of November 2014
[41] includes, inter alia, the 18 cooperative credit institutions formerly operating under a licence issued by a different authority, after the transfer of the competence for their supervision to the CBC.
[42] after the 4th of November 2014 when the Single Supervisory Mechanism became operational.
[43] includes, inter alia, the withdrawal of the authorisations of the 18 cooperative credit institutions that were affiliated to the Cyprus Cooperative Bank Ltd, in view of their merger with the latter, which stopped acting as their central body.
[44] 10 operational.
[45] 10 operational.
[46] 4 operational, 1 licence revoked in 2017.

payment institutions as well as legislation. Some increase in resources is required, not only to replace resource lost due to a retirement last summer; to allow a more consistent approach to maintaining awareness of, and more readily addressing, developments led by the ECB, to more proactively engage with the ECB on recommending or engaging with developments; and to allow for more systematic training, including on e-business models and ML/FT risk, and so as to remove any possibility that the shortfall in resource might have an effect on the quality of approaches to licensing. Applications for e-businesses take about a year to resolve. Consideration of the reputation of BOs, shareholders and directors/senior management and source of funds has been, and is, fundamental to the CBC's approach.

408. The ECB has responsibility for licensing Cypriot banks and therefore would make the final decision on whether to issue a licence. No new credit institution has been licensed since 2013.

409. A 10% "qualifying holding" threshold is used to evaluate BOs of banks. Individuals must complete a detailed questionnaire. Consideration of BOs extends to whether persons under the threshold are operating in association with each other; association would trigger the 10% threshold. Each individual must complete a detailed questionnaire, allowing judgements to be made on their experience and reputation, and provide a CV. Where individuals have been resident abroad during the last ten years, confirmation of whether or not they have a criminal record in the foreign jurisdiction is required by means of an original "criminal certificate"; this is also required from Cypriot residents. In addition, information is sought on whether individuals have been subject to investigation or administrative sanction and whether they have been bankrupt. Tax returns for the last five years are obtained from individuals, together with their source of funding, a personal statement of assets and liabilities, and a diagram showing the flow of funds indicating, inter alia, originating banks.

410. BOs must declare an ownership interest of more than 10% in a company (and provide information on when this was obtained), voting rights, what directorships they hold and whether any of the entities in which the BO has a relationship has a link with a credit institution in Cyprus. Where the BO has a majority holding in an entity further documentation must be submitted to the CBC, such as information on the structure and financial statements, including at the group level if applicable. There have been no examples of individuals listing holdings in seemingly unrelated companies, but the CBC confirmed that the potential for links would be explored should such a case arise.

411. Internet checks are conducted, and searches made of commercial databases. Firms providing such databases are requested to provide a report on BOs and shareholders where they trigger the threshold. Professional and university qualifications are checked by means of receipt of certificates certified by an appropriate person and, on a risk basis, liaison with the certifier or the qualification awarding body. Where there is a link with a foreign supervisor, that supervisor is always requested to provide an opinion; there are no cases of the CBC proceeding without a response. There is also liaison with CySEC and the ICCS; information has also been sought from the Police. References from two third parties are also taken. Interviews are held on the basis of risk.

412. There are close links between the licensing department and the CBC's AML/CFT and supervisory departments so that information relevant to licensing is shared.

413. With regard to ascertaining whether a person is an associate of criminals, specific checks are not undertaken but the quality and range of checks undertaken in practice form a reasonable approach to ascertaining such association.

414. Consideration of governance and the qualities of the board and senior management is an important component of the licensing; as part of this, AML/CFT procedures manuals are required as part of the application, together with a three-year business plan.

415. Shareholders, directors and senior managers who are individuals are required to complete the same questionnaire as BOs and are subject to the same checks (except for source of funding for the acquisition as this is not applicable to them). The judgments made by the CBC are informed by

the individual's particular role and responsibilities.

416. Ten applications have been withdrawn in relation to directors and senior management since the beginning of 2015 as a result of the quality of the CBC's checks. The majority of these are to do with the experience of the individuals but, while not directly relevant to AML/CFT, are indicative of robust approaches by the CBC.

417. With regard to payment and e-money institutions, the CBC is mindful that the ECB is not involved in the licensing process. Some 20 applications for e-money businesses were being processed at the time of the assessment team's visit to Cyprus. In general, the same process as for banks is applied. At the level of detail, the CBC recognises that the technical nature of business plans for such institutions requires a different focus so as to understand the business. In addition, IT systems are tested, and e-money institutions have a mandatory test period before they can accept customers. As with banks, the CBC requires external third parties to test systems. With regard to source of funding, the applicant must provide information, including a statement of assets and liabilities and the latest tax returns; a residency certificate; a personal statement of assets and liabilities and a tax return for each beneficial owner is also required. The legitimacy of the source of funding is assessed and funds for the applicant must be transferred to Cyprus through an EU credit institution. Questions on source of funds have led a few institutions to withdraw their application.

418. The same approach as for banks would be taken for other entities subject to the CBC's supervision; there are no licensed leasing companies.

419. For non-bank FIs, the CBC uses external auditors to assess systems and controls (including those relevant to AML/CFT) after a licence has been issued prior to providing consent for the commencement of operations; for banks, the CBC requires the assignment of an independent external auditor, at least once every three years, to assess the adequacy and effectiveness of the internal control framework, including for AML/CFT purposes. These checks provide an opportunity for detecting potential control by criminals. Notification of prospective changes of BO, shareholder and director/manager are made on time by FIs. The CBC periodically checks whether its records on ownership and control are consistent with those of the institution. As part of this, at least annually the CBC reconciles its records with those of the Registrar of Companies.

420. Searches of the internet and of the databases of commercial information providers are undertaken by use of key words to ascertain if unlicensed business is being carried out. In addition, there have been rare cases where the CBC has received information from other EU national authorities, local authorities and regulated entities about unlicensed activity from outside Cyprus. The first step in dealing with these latter cases is to issue a letter to the entity to seek information. Where there is a lack of cooperation, the case is referred to the Attorney General. The CBC has advised that, to date, cases have not been sufficiently serious to result in a criminal charge being made.

<u>CySEC</u>

421. The application department has 28 full time equivalent staff (23 officers and 5 support staff). Products as well as service provider are authorised. The combination of delays in licensing and the amount of overtime worked means that resources are over-stretched and additional staff are required. It takes approximately a year to complete the process. CySEC's approach to dealing with FIs is also informed by its approach to, in some cases, complex ownership structures for ASPs.

422. With regard to BOs, the same approach is taken as for the CBC with minor differences. Checks include: obtaining a clean criminal record and non-bankruptcy certificate for BOs, legal owners and directors/senior management who are individuals, as well as tax returns for the last three years, bank statements/confirmation of funds, a bank reference and evidence of source of funds; requiring audited accounts; evidence of financial soundness of BOs; applying EDD where shareholders are individuals with shareholdings in the applicant of greater than 50%. The information is assessed, including the consistency of the information provided. Where this relates to a foreign bank CySEC contacts the bank to ascertain that the information is not fraudulent. The

relevant stock exchange is approached for input where BOs are listed. Where foreign supervisors are approached for input the view has been taken that a reminder will be issued in the absence of a response and the correspondence makes it clear that an absence of a formal response will lead CySEC to conclude that there is no negative input to be provided on the person in question. There have been cases where, on risk grounds, BOs have been interviewed.

423. As with the CBC, there is great emphasis on reputation and source of funds. Particular attention is paid to applications which have a sole shareholder to assess, for example, whether that person might be a strawman.

424. With regard to officers of the applicant, the financial status is not checked as the focus is on reputation and professional experience; AMLCOs are always interviewed.

425. In connection with ascertaining whether a person is an associate of a criminal, the overall checks are a reasonable approach. CySEC is investigating a number of cases for licensees where potential association with criminals is a feature.

426. There is a convincing number of examples of applications both withdrawn and refused to demonstrate the robustness of CySEC's approach to applications.

427. Changes of BO, shareholder, director or senior manager must be notified to CySEC before they take effect. These are checked; there has been no cause to reject any change. Notifications have been made within the statutory period.

428. CySEC has taken action against unauthorised business when such business has come to its attention through internet searches, whistle blowing and media monitoring. There are examples of cases where individuals have carried out such business prior to applying for a licence; the applications have not been progressed by CySEC. Notifications about unauthorised business are placed on CySEC's website, although it does not communicate the possibility of commission of potential criminal offences to the Police. The assessment team considers that notifications and other relevant information should be transmitted to the Police.

ICCS

429. The same approach is taken as for the CBC by the ICCS for insurers and insurance intermediaries with relatively minor differences. There is focus on the EU's solvency II framework, which means that particular attention would be paid to corporate governance and internal controls as part of the application process. The background of BOs who are individuals is checked, inter alia, to ascertain if they have worked for firms which have run into problems for negative reasons. Independent accountants would be asked to verify the initial balance sheet of the applicant; audited financial statements are required for the last financial year. The FIU has on one occasion been requested to provide input on a shareholder. Shareholders, directors and internal auditors are interviewed.

430. Changes of BO, shareholder, director or senior manager must be notified to the ICCS before they take effect. There has been no cause to reject any change. Notifications have been made within the statutory period.

431. Steps are taken in connection with unlicensed business (in practice this is intermediary business). During onsite inspections the ICCS has noted to whom commission has been paid and on occasion this has included members of staff of an insurer. This is *de minimis* and action has been taken to prevent recurrence. The FIU has also provided the ICCS with a notification of potential unlicensed insurance intermediation in one case; the ICCS investigated and found that, in practice, unlicensed business was not being undertaken. In addition, following three complaints, which related to intermediaries operating outside the scope of their licences, the licences withdrawn by the ICCS and the complainants urged to forward their complaints to the Police. There is scope for the ICCS to liaise with the Police to ascertain outcomes.

432. During licensing no cases have arisen where individuals have been found to be associates of criminals. No licences have been issued since 2013. In one case an applicant withdrew its licence as

the ICCS considered the company had an insufficient system of governance. On one occasion an application by an internal auditor was rejected due to a lack of sufficient experience.

*DNFBP Supervisors*

433. All DNFBP supervisors apply market entry measures albeit with varying degrees of intensity. The licensing of ASPs falls under the competence of three separate supervisors, namely the CBA, ICPAC and CySEC, depending on whether the ownership and management of the ASP comprises advocates, accountants or other professionals. CySEC and ICPAC apply comprehensive controls in relation to licensing so as to prevent criminals from holding, or being a beneficial owner of, a significant or controlling interest or holding a management function in ASP. However, the CBA does not apply appropriate market entry controls. Certain registration or licence renewal requirements for real estate agents could not be substantiated due to the lack of supporting documentation. The Casino Commission has applied appropriate market entry measures for the sole casino operating in Cyprus.

CBA

434. The CBA's verification checks at the initial authorisation stage to prevent criminals acting as advocates or partners, shareholders or directors of LLCs and ASPs have limited effectiveness. Practising advocates are required to be enrolled in the Register of Practising Advocates kept by the CBA. The applicant (natural person) must be of good character and not an unsuitable person. To confirm this, the CBA relies on a document of self-confirmation signed by the applicant[47]. Further measures, such as the submission of a criminal record certificate to the CBA are not required.

435. Upon application, the CBA approves the incorporation of a LLC if all of the partners, shareholders, BO are advocates enrolled in the Register of Practising Advocates. The suitability of these persons is not further verified by the CBA at the stage of the licensing of the LLC, as it is accepted that suitability was established in the initial authorisation of each natural person. Moreover, verification measures in order to ensure that solely enrolled advocates act as shareholders, BOs, partners and directors of LLCs are not applied. In order to determine who of those advocates and LLCs provide administrative services, the AML Questionnaire (see chapter 6.1.2) that is sent annually to all members of the CBA contains a specific question as to whether or not administrative services are offered. In addition, the request of a member to the CBA to issue a certificate of supervision is considered as a trigger that a member has started offering administrative services and is seeking to enter into a business relationship with a bank. The CBA estimates that by the end of 2017 around 60 % of all practising advocates provided administrative services in addition to litigation services; the remaining part provided litigation services only.

436. A firm that belongs exclusively to advocates and/or LLCs may apply for a license as an ASP issued by the CBA on the basis of the Administrative Service Providers Directive.[48] The suitability of the partners or shareholders, BOs is not further verified by the CBA at the stage of licensing of the ASP, as it is accepted that suitability was established in the initial authorisation of each natural person (practising advocate). There is no requirement that directors of an ASP have to be licensed advocates. Accordingly, a director of an ASP who is not a licensed advocate is not subject to any fit and proper measures. In such cases, the CBA performs background checks on those directors using a well-known international database and, prior to approval, requires a service provision agreement containing a clause that the licensed advocate ultimately owning the ASP takes full responsibility for any breaches. However, it is the view of the CBA that the issue is not of material significance, as the majority of persons acting as directors of ASPs are licensed advocates.

437. The assessment team is of the view that there are insufficient measures to prevent close associates of criminals acting as advocates or partners, shareholders, BOs or directors of LLCs and

[47] When registering as a trainee advocate, a criminal record certificate has to be obtained by the applicant in order to issue the self-confirmation. However, there is no requirement to submit the criminal record certificate to the CBA.

[48] According to the CBA, advocates would usually set up separate companies providing administrative services to segregate their business activities from common advocates' activities and to take advantage of tax benefits.

ASPs except where the database referred to above might disclose such relationships for directors.

438. In terms of on-going monitoring, there are neither specific obligations for advocates, LLCs or ASPs to notify the CBA of any changes in their compliance with licensing requirements, nor any regular on-going monitoring measures. Advocates are required to submit a "Declaration of Advocate" to the CBA on an annual basis; however, this declaration primarily serves as an assurance for the CBA that advocates are still practising and reside in Cyprus.

439. The following table shows the number of licence applications withdrawn by applicants, the number of licence applications refused by the CBA and the number of licences withdrawn by the CBA in the period from 2013 to 2018:

**Table 26: Licence applications/withdrawals by the type of regulated entity (2013-2018)**

| Type of regulated entities | Number of licences issued | Number of licence applications withdrawn | Number of licence applications refused | Number of licences withdrawn |
|---|---|---|---|---|
| **Advocates** | 1248 [49] | 0 | 0 | 3 |
| **LLCs** | 689 | 0 | 0 | 0 |
| **ASPs** | 1555 | 0 | 0 | 3 |

440. In total, six licences were withdrawn of which three were withdrawn due to breaches of AML/CFT requirements, and further three licenses due to the provision of false or misleading BO information (breaches of the licensing requirements).

ICPAC

441. At the time of the assessment team's visit, all persons in receipt of a licence by ICPAC had been subject to comprehensive checks confirming their suitability. ICPAC issues four types of licences: General Practising Licence; Audit Practising Licence; Administrative Service Provider Licence; Insolvency Practitioners Licence. Before a person is permitted to provide any professional activities, they are required to file an application to become a member of ICPAC.

442. In order to be, and remain, registered, applicants must comply with comprehensive requirements; inter alia, applicants must declare that they have not been convicted of any criminal offence and, as of 1 January 2019, must provide a copy of a valid, recent criminal record certificate. In addition, ICPAC performs background checks on all applicants during the application phase and annually upon renewal, using a well-known international database. References from two existing ICPAC members are required in which they confirm the suitability of the applicant. A confirmation is also required from the professional accounting body of which the applicant is a member.

443. An application for a General Practising Licence may be filed by a member of ICPAC. A declaration is required that the applicant has not committed any criminal offence and will comply with the provisions of the AML/CFT-Law and the relevant directives issued by ICPAC. To be licensed as an accounting firm, ASP or auditing firm, separate licence applications are required, and comprehensive verification measures are applied to non-ICPAC members who want to act as partners, shareholders, BOs or directors.

444. All practising licences issued by ICPAC have to be renewed on an annual basis. In the course of renewal, declarations confirming compliance with the licensing requirements must be made by the licence holders. Declarations are required that, inter alia, licence holders have not committed a criminal offence and that neither shares nor a position as a director are held on behalf of other individuals. All licensed practitioners are obliged to notify ICPAC on an on-going basis of any matters affecting their suitability that may occur in between the renewal of each licence.

445. The Admissions and Licensing Department undertakes comprehensive on-going monitoring of compliance with the licensing requirements through evaluation of the annual declarations

[49] The number does not include renewed licences.

received in the renewal stage and through regular media screening. All license renewal applications are carefully reviewed, along with supporting documents, before being approved. Media screening is undertaken on ICPAC's behalf by an independent media company. Furthermore, during the AML, Rules & Regulation on-site visit, the inspectors review the continued suitability of licence holders, and information received from third parties (e.g. complaints from clients, media screening) is taken into account. These measures are satisfactory for preventing close associates of criminals being licence holders or acting as BOs or directors of licence holders.

446. The following table shows the number of licence applications withdrawn by applicants, the number of licence applications refused by ICPAC and the number of licences withdrawn by ICPAC in the period from 2013 to 2018:

**Table 27: Licence applications/withdrawals by the type of regulated entity (2013-2018)**

| Type of Regulated Entity | Number of licences issued | Number of licence applications withdrawn | Number of licence applications refused | Number of licences withdrawn |
|---|---|---|---|---|
| **Accountants** | 960 | 0 | 6 | 2 |
| **Auditors** | 750 | 0 | 5 | 0 |
| **ASPs** | 453 | 0 | 2 | 0 |

447. The reasons for withdrawal of licences were criminal convictions (identified from publications in the media) and falsification of documents submitted for the renewal of a licence (identified during the review of the documents at the renewal stage of the licence).

CySEC

448. ASPs have to fulfil comprehensive requirements when they apply for a licence from CySEC. The persons who effectively manage the business (i.e. members of the Board of Directors, its senior management and the AMLCO) must be of sufficiently good repute and sufficiently experienced and hold sufficient academic or professional qualifications to ensure the sound and prudent management of the licensed person. CySEC does not authorise the provision of administrative services until it has been informed of the identity of all shareholders and all BOs and has confirmed their suitability. Natural persons must submit a valid, recent criminal record certificate. CySEC's use of interviews with the intended AMLCO is a very positive element of their process.

449. In cases of relationships with an entity regulated in the financial sector of another jurisdiction, CySEC requests information from the relevant jurisdiction's supervisor. In addition, CySEC requests information on whether licence applications were rejected, or licences were withdrawn by other domestic authorities. If the applicant states that an application was rejected or a licence was withdrawn, CySEC will contact the respective domestic authority.

450. ASPs are required to assess and review the suitability of their shareholders, BOs and persons managing the business and the AMLCO, and have to notify CySEC of any changes in compliance with licensing requirements. In addition, CySEC undertakes frequent media screening and analyses information received from third parties (e.g. complaints from clients of ASPs). These measures are satisfactory for preventing close associates of criminals being licence holders or acting as BOs or directors of licence holders.

451. With respect to ASPs, the table below shows the number of licence applications withdrawn by applicants, the number of licence applications refused by CySEC and the number of licences withdrawn by CySEC in the period from 2013 to 2018:

**Table 28: Licence applications/withdrawals by the type of regulated entity (2013-2018)**

| Type of Regulated Entities | Number of licences issued | Number of licence applications withdrawn | Number of licence applications refused | Number of licences withdrawn |
|---|---|---|---|---|
| **ASPs** | 159 | 28 | 6 | 37 |

452. 36 licences have been withdrawn for the following reasons: (i) licence withdrawals after

mergers with other ASPs; (ii) decisions to be licensed and supervised by other ASPs supervisors (namely ICPAC or CBA); (iii) disproportionate costs of compliance when compared to the volume of business made. Only one ASP licence has been withdrawn by the CySEC for breaches of the Administrative Services Law and the AML Directive (non-compliance with the internal obligations, non-submission of compliance officer's annual report and non-submission of monthly prevention statement). 6 licence applications have been refused due to the following reasons: (i) submission of incomplete information at the authorisation stage; (ii) non-suitability of members of the Board of Directors / Compliance Officer; (iii) non-suitability of shareholders – submission of incomplete information; (iv) provision of unauthorised services. 28 license applications were withdrawn due to the change of circumstances following the implementation of the Administrative Services Law. The CySEC reported that the main reasons for those withdrawals were increased compliance cost, mergers to form more viable entities and the ownership nature implying that supervision by either the CBA or ICPAC would have been more appropriate.

Estate Agents Registration Council

453. The Estate Agents Registration Council (RE Council) replaced the FIU as the competent supervisor for registration and supervision of real estate agents. The Council took over supervisory responsibility from the FIU as of May 2018.

454. In order to be registered, natural persons have to comply with the qualifications for registration outlined in the Real Estate Agents Law. Besides educational and training qualifications, natural persons must provide a valid, recent criminal record certificate to the Council and to prove that they are not under bankruptcy.

455. The registration of a legal person is a separate and independent registration and is carried out in parallel with the registration of any natural person related to a legal entity. The RE Council reported that shareholders, partners and BOs must provide clean criminal record certificates. However, this could not be verified by the assessment team due to the lack of supporting documentation. There is no requirement for directors to undergo a licensing/verification process.

456. Licences have to be renewed annually under the same terms and conditions applying upon issuance. The RE Council reported that licensees are required to submit current documentation concerning directors, partners and shareholders, BOs as well as criminal record certificates. However, this could not be verified by the assessment team due to lack of supporting documentation. All above measures are of limited efficiency in preventing close associates of criminals from acting as licence holders or partners, shareholders, BOs or directors of licence holders.

457. The RE Council does not employ measures for detecting unlicensed activities, despite it being aware that a large number of unlicensed estate agents act as intermediaries in real estate transactions. While banks were urged in 2013 by the FIU not to open bank accounts for real estate agents who do not present a certificate of their registration, the assessment team considers that this measure is not sufficient to prevent unlicensed activities, particularly since real estate transactions are not commonly conducted through bank accounts maintained by real estate agents.

458. In the period from 2013 to 2018, 1880 licences have been issued; no licence applications were withdrawn by applicants; 40 licence applications were refused, and 60 licences were withdrawn due to failure to request a renewal by the agents. Most of the refusals were due to non-compliance with professional experience requirements. These refusals indicate that some form of checks are being undertaken by the RE Council.

Casino Commission

459. The National Gaming and Casino Supervision Commission (Casino Commission) was established in 2017 and became operational in January 2018 as the competent authority for licensing of casinos. The first licence for operation of the temporary casino in Limassol was issued in June 2018 and licences for operation of two satellite casinos in Nicosia and Larnaca were issued in December 2018. An integrated casino resort is currently in the construction phase and is

intended to be completed by the end of 2021. The resort facilities will be of a far greater scale than those of the temporary casino and the operator will have to migrate its internal control systems to accommodate this increased level of complexity. The Casino Commission recognises this within its strategic planning.

460. The Casino Commission has applied appropriate market entry measures for the casinos operating in Cyprus. A Steering Committee approved the licensee for the integrated casino resort licence, being satisfied that the selected candidate, each shareholder, BO, and every associate of the candidate and the owner of the land on which the casino is located, were suitable persons for the management or operation of the casino resort or ownership of the land. The applicable thresholds for the determination of the BO of a casino are lower than the general thresholds in case of corporate entities pursuant to Section 2 (1) of the AML/CFT-Law. If the casino applicant is owned by other companies or entities, it is required to submit the ownership structure of the entire group and to disclose details of all the shareholders in the group up to the ultimate beneficial owners. Any changes to shareholders above the set thresholds (10 %/5 %)[50] or in the landowner must be approved by the Casino Commission, following the Commission's due diligence of the proposed transferee. Changes in management and directors also have to be approved. Furthermore, all employees of a casino are required to have a valid casino employee licence and those identified as key employees are required to have a casino key employee licence. The Commission has measures in place to establish the suitability of each employee before granting a licence. These measures include, inter alia, a requirement for applicants to provide valid and recent criminal record certificates from all jurisdictions in which the applicant has lived over the past ten years.

461. The one-to-one nature of the relationship between the casino operator and the Commission ensures on-going monitoring of compliance with licensing requirements.

In general

462. In order to detect unauthorised businesses operating in Cyprus, ASP supervisors mainly rely on whistleblowing and media checks. There is no routine exchange of information between the three ASP supervisors on rejected applications and withdrawn licences to ensure that persons deemed unsuitable by one supervisor are precluded from seeking a licence elsewhere.

463. All ASP supervisors keep a publicly accessible register of ASPs on their websites. The registers kept by CySEC and ICPAC contain information on the licensed entity, the administrative services provided, the names of its fully owned subsidiaries which offer administrative services, the names of its employees, the name and communication information of the AMLCO, and any other information deemed necessary. The ASP register kept by the CBA does not contain full information on supervised ASPs, as is required by the Administrative Services Law (e.g. name of the compliance officer and names of fully owned subsidiaries are missing).

464. There are no additional safeguards serving as a second line of regular on-going monitoring to ensure suitability of the licence holders, e.g. regular information exchange channels with the DRCOR[51] and the competent courts[52], where relevant.

465. According to the definition of FATF, the CBA, ICPAC and the RE Council qualify as SRBs. They are required to be supervised by a competent authority in relation to the functions they perform. ICPAC is monitored by the Cyprus Public Oversight Audit Body (CyPAOB) and the CBA by the Attorney-General with a very little focus (if any) to AML/CFT supervisory matters. The RE Council as SRB is not subject to any supervision/oversight by a competent authority.

[50] In detail, the Steering Committee shall not approve a person to hold a casino resort license unless it is satisfied that the selected candidate, each shareholder holding 10 % or more of the shares and/or voting rights of the candidate for public listed companies and each shareholder holding 5 %or more of the shares and/or voting rights of the candidate for all other shareholders, and every associate of the candidate, are suitable persons for the management or operation of the casino resort (Section 22 of the Casino Law).

51 where changes made to the ownership structure and the organisation of a legal person are available

52 the website www.cylaw.org, where all court decisions are published

### *6.2.2. Supervisors' understanding and identification of ML/TF risks*

*FI Supervisors*

466. The FI authorities understand the traditional markets which they supervise and licensees' business models, although there might be relatively less understanding overall of e-money businesses depending on the extent of supervisory engagement with individual businesses; there is good understanding of ML risks (in some aspects there is very good understanding) and, overall, good understanding of FT risks, although understanding of FT risk is less developed than that for ML. The CBC has noted that it has required supervised entities to fully understand their risks; this assists understanding by the CBC.

CBC

467. Following the special assessment, the CBC has taken assertive steps to understand the risks to the banking system of legal persons, legal arrangements, introduced business and complex linked risks. For example, the CBC has conducted a specific analysis of complex structures and identified a number of risks relating to legal persons (see IO.5). The CBC also requires banks to apply, mitigating measures to address the recommendations in the assessment report and these measures also aid understanding. Additional measures have been put in place since the special assessment (for example, in relation to introduced business and the meeting of customers (beneficial owners in relation to legal persons) which have increased understanding by banks. For example, there has been a significant increase in the quality of business risk assessments by banks in recent years and this has informed understanding by the CBC. In addition, the CBC has undertaken initiatives in response to international issues which have arisen (Panama Papers, the Laundromat case and an issue with a Danish bank). Quite significant offsite information is also routinely received.

468. A risk tool was developed in 2013 to inform risk-based supervision of banks by, for example, enabling ML/FT risk rating of individual banks. The tool takes into consideration structural factors, business risks and control functions (including information on risk management within institutions from its offsite returns)[53]. In light of experience, it has been recalibrated. The tool has had a significant, positive effect on understanding and supervision. While important elements relevant to CFT are included in the tool (in particular, deposits from high risk countries, cash transactions and wire transfers), it is weighted towards ML and the assessment team has concluded that understanding of FT is not as developed as for ML. The AML/CFT department has been assisted by a modelling expert from the CBC's Economic Research Department of the CBC to enhance understanding and assist a prospective recalibration of the tool to also include information in relation to CFT (including NPOs), trade finance, e-money and the control environment. The addition of qualitative information and human judgment is also proposed. The assessment team would also suggest the incorporation of bank-specific events such as group restructuring into the risk tool, together with potential refinement of what appears to be an over weighting towards the size of the bank. In addition, the elements could usefully be refined to add further focus on the risks pertinent to Cyprus. The totality of these comments amount to a refinement of the tool rather than significant changes.

469. Information is gathered from returns by banks every six months to repopulate the tool; as a result, the risk rating is also refreshed. In addition, the risk rating is refreshed as part of the onsite inspection process and any changes to the bank's ownership structure or business model. This data includes the number and value of non-face to face customers, non-residents, foreign and local PEPs, customers vulnerable to tax evasion, client accounts, private banking, correspondent accounts, cash transactions, information on natural persons and their risk classification, geographical risk, introduced customers, the twenty largest depositors and borrowers for each of natural persons and legal persons, client accounts and closed accounts.

[53] This information is used in risk assessment and is checked as part of onsite inspections.

470. Information is gathered and considered by the AML/CFT team from the risk tool and other parts of the CBC. It also receives and assesses a range of types of information from the bank, including monthly reports on loans, deposits, cash transactions and money transfers; annual reports by AMCLOs; reports from the internal auditor; board minutes and other aspects of corporate governance. The annual reports from AMLCOs include information in relation to potential suspicion and STRs made by the bank. The CBC also assesses information from the media and foreign authorities.

471. Furthermore, banks themselves have considerably improved their understanding of risk and their AML/CFT countermeasures since 2013, and these factors have also informed and improved the CBC's understanding of risk. Understanding in both regards has been increased by the closure by banks of a significant number of business relationships, including relationships with shell companies, and better understanding of complex risks. Banks must meet their customers (the beneficial owners in the case of legal persons), including before any transaction with a customer who has been introduced by a third party , and this and other positive developments described in IO.4 benefit understanding of risk by the CBC of the banking sector, its subsectors and individual banks.

472. With regard to CFT, TF indicators have been issued to banks. The AML/CFT department considers sanctions and wire transfer risks in particular. It also considers other matters relevant to CFT. Inspections include discussions on TFS, use of cash, wire transfers, and banks' monitoring of IP addresses, use of cards, customer behaviour and approach to geographic risk (higher risk countries and proximity of customers to conflict zones). Significant cash transactions and fund transfers are reported to the CBC on a monthly basis. The CBC has also participated in dedicated training on TFS and FT (which it has sponsored).

473. Non-banks are not currently risk rated; a risk tool is being developed for such institutions supervised by the CBC. Until recently the sector has been very small. Offsite information is provided from prudential returns on wire transfers and balances relating to e-money instruments, together with annual reports and risk reports from AMLCOs. There is routine contact between the designated CBC liaison officer for each licensee and the entity, and bilateral meetings are held with internal auditors and management annually. There is also very good liaison between the AML and licensing teams. Non-banks other than those recently licensed have been subject to onsite supervision. These factors have a positive effect on understanding.

474. With reference to e-money institutions in particular, differences with banks include geographic risk, increased risks of onboarding and the anonymity associated with prepaid cards. The CBC seeks specialised training on the business models of e-money institutions, liaises with the prudential supervisors and includes the sector in its onsite inspection programme. The CBC makes strong efforts to understand the sector and individual entities and its understanding is developing towards that for banks.

475. With regard to payment[54] and e-money institutions, information on incoming and outgoing money transfers is collected in the same way as for banks on a monthly basis and analysed. The data received includes cash deposits and withdrawals, large transactions and the number and value of incoming and outgoing transactions split by jurisdiction. This information enables the CBC to assess transaction and geographical risks. Institutions are mostly used by migrant workers. Volumes of inward transactions are lower than outbound; this pattern is linked to migrant workers in Cyprus largely accounting for outward flows by remitting funds to families in their home jurisdictions. Transaction sizes are not large and businesses, which are agents of global firms, monitor transactions using the firms' software. The CBC routinely participates in supervisory college meetings for one of the providers. New entrants have altered the pattern of the market. As the payment sector is becoming more material the CBC plans to develop more comprehensive offsite monitoring and adopt a risk assessment tool similar to the one used for the banking sector.

[54] 6 payment institutions are authorised to provide money remittance services.

476. Currency exchange was traditionally the preserve of the banking sector, which still accounts for the very large majority of the market. Only two, relatively recently established, non-bank licensees are in operation. Information on volumes bought and sold is provided to the CBC, with most transactions being in GBP and USD. The average transaction is 350 EUR. The highest turnover is at the airport. The CBC also receives information on governance and meets with compliance officers. Most customers are tourists. Onsite inspections are not undertaken although offsite monitoring allows some understanding of the sector and individual institutions.

CySEC

477. Authorised businesses include a combination of traditional investment firms providing services in relation to collective investment schemes, shares, debt instruments and linked instruments and Fintech businesses.

478. CySEC is aware of and understands the varying simple and complex models used by traditional firms.

479. There are some one hundred online CIFs. CySEC was confident in talking about the uncertainties, risks and the existing and prospective EU standards for these businesses and how these differ from traditional businesses. The majority of online businesses are online brokers which offer their services through an electronic trading platform. Models typically involve a narrow range of services to a broad spectrum of clients, which mainly comprise small investors around the globe. The main risk derives from the delivery channel as the majority of business relationships are non-face to face. Online firms mostly receive small deposits from each client and most of the funds are transferred via banks or payment service providers. CySEC is proactive in considering the risks of *blockchain*, crypto currencies, ICOs, securitised tokens and e-wallets and the boundaries of what is known internationally and at the EU level about those risks. CySEC closely follows international developments.

480. CySEC focuses attention on the source of funds and wealth, country of residence and, more generally, the information in the customer's profile maintained by the institution compared with transaction activity. It is cautious about developing its risk model in line with EU standards as they evolve. As part of this caution, it has limited trading of crypto currencies to five businesses so as to ensure risks are better understood. There is limited trading in crypto currencies.

481. During 2014 CySEC developed a risk based supervisory framework (RBSF), which was established in 2015. A risk assessment, based on impact and probability measures, was undertaken for each entity which was used to define the entity's overall risk. The assessment was calculated based on four categories (AML/CFT, prudential, governance and conduct) with the assessment comprising quantitative and qualitative measures. Therefore, since 2015, for FIs it has been possible to separate AML/CFT from other categories and to create a separate thematic risk score, and this has been done. The AML element also includes factors relevant to CFT although the CFT element would benefit from enhancement. The ML/FT risk rating is scored annually. There is a validation process for information received with significant assessment undertaken by officers looking at trends between years, comparisons between firms, and checking information held by the various departments of CySEC such as licensing information. Where necessary officers liaise with businesses to check information. The results of the risk model are communicated to the AML/CFT department in order to provide a basis for the formulation of the annual supervisory programme. The system can be used to re-assess the risk where trigger events might warrant this but it is not clear to the assessment team whether this has been done in practice. Following a project in 2018, CySEC intends to enhance the risk model so that the AML/CFT risk rating for FIs sits not only separately but in parallel with a prudential, governance and conduct rating. The NRA report will also inform the enhancement.

482. The range of quantitative and qualitative measures informing the risk model includes customer, geographical, and product/service risks and vulnerabilities. Negative intelligence about a firm is also included. This is positive. The factors used are good quality. Nevertheless, the assessment team would suggest adding further depth to them. With regard to FT, in its ratings

CySEC pays attention to jurisdictions which have a high FT risk and NPOs. Nevertheless, the assessment team concluded that understanding of FT is not quite as developed as that of ML both in relation to the authorised sectors and in relation to individual businesses. The assessment team notes that the enhancements to the model discussed above would be refinements rather than significant changes. The risk department has numerous functions but only three officers and an acting head of department, whose role encompasses much more than AML/CFT (in practice the full-time equivalent time devoted to AML/CFT is considerably less than one FTE). In addition, the department purchases the services of two contractors and support from external consultants. In order to devote sufficient time for AML/CFT, maintain the model and also deal with the increasing wider demand for more statistics and better statistics, more engagement with other parts of CySEC and more routine monitoring of risk (and to retain knowledge and experience within CySEC), additional staff resource is needed.

ICCS

483. While there are no formal, written processes, in practice, the ICCS risk rates insurers and brokers annually for AML/CFT purposes and articulates its conclusions. This approach is made possible by the small number of insurers, the level of understanding by the ICCS of each entity as a result of its supervision, and the understanding of the market and ML/FT risks it presents (see the paragraph below). The approach appears to be based on factors relevant to AML/CFT, including customer, geographical, and product/service/delivery channel risk, together with controls. The ICCS takes into consideration the specificities of each entity separately, including the scale of premiums written, products sold, number of policies, geographical area covered and significant changes to the entity (for example, shareholder structure or management). While not possessing IT tools like those of its counterpart FI supervisory authorities, the ICCS is committed to understanding the business and ML/FT risk of each institution, including the corporate governance and internal controls of each firm. It seems to the assessment team that, overall, the process is directed at ML (with an over emphasis on Solvency II requirements for AML/CFT purposes) with TF underrepresented at least to some extent.

484. The market is understood by the ICCS. It is stable and the reasons for the purchase of insurance policies by non-residents are understood. Products offered are simple and cash activity is low. ML is seen as more of a risk than TF with TF being associated with country risk. Customers do not originate from countries with high TF risk. Nevertheless, an enhanced understanding of TF would enhance understanding of the insurance sector and firms.

*DNFBP Supervisors*

485. ICPAC, CBA and CySEC actively contributed to the first NRA Report. The assessment established the ML risk level of the ASP sector as medium-high. The sector is the second most risky after the banking sector. The other sectors (i.e. accountants, auditors, and advocates and LLCs providing only litigation services) were rated as low risk. While, the risk understanding developed and maintained by ICPAC, the CBA and CySEC was considered in relation to all of their supervised entities, the main focus of the assessment is on the ASP sector.

486. The three ASP supervisors have a good understanding of the ML risks that are associated with the ASP sector as a whole, in particular, due to their services and international clientele. All ASP supervisors have off-site systems in place to assess the risk of individual supervised entities. However, the risk assessment methodologies for the assessment of ML/TF risks in individual ASPs vary to some extent. The Casino Commission has a comprehensive understanding of the ML risks that casinos are commonly exposed to. The RE Council demonstrated low awareness and understanding of risks in real estate sector. Understanding of TF risks is less developed by all DNFBP supervisors.

ICPAC

487. ICPAC introduced offsite supervisory tools for the purpose of assessing the ML/TF risks of regulated entities in 2014. Off-site monitoring is conducted by ICPAC using an annual AML

Questionnaire. The data requested covers the following ML/TF risk factors: countries and geographical areas, customers and delivery channels, products and services, and some elements of governance and internal control relevant to AML/CFT. This enables ICPAC to undertake a risk assessment based upon specific AML risk data. However, the extent and the level of detail of risk data that is collected could be more comprehensive and is not aligned with that of the other ASP supervisors. For instance, ICPAC does not request data on complex structures and unusual transactions, customers considered as high-net worth individuals, customers transactional activities including cash transactions, TF specific indicators.

488. In addition, regulated entities are required to submit an AMLCO Report on an annual basis that includes information on significant risks and weaknesses, corrective and risk mitigating measures taken, changes in policies and procedures, and training and information on STRs. Review of AMLCO reports complements the risk assessment process; AMLCO reports chosen for review are those from entities identified as high risk, where deficiencies have been identified previously and/or intelligence was provided by other departments of ICPAC.[55] Analysis of the AMLCO reports complements the process of risk calculation to a great extent.

489. ICPAC's risk assessment based on data from 2017, categorised regulated entities (excluding non-active and unclassified entities) as follows:

**Table 29: Risk classification of ICPAC-regulated entities**

| | High risk | Medium-high risk | Medium-low risk | Low risk |
|---|---|---|---|---|
| **All ICPAC-regulated entities[56]** | 20 % | 25 % | 34 % | 21 % |
| **ASPs** | 28 % | 32 % | 27 % | 13 % |

490. Following the publication of the NRA Report, ICPAC has amended its risk assessment system by allocating higher elements of risk to those entities offering ASP services, relying on third parties and having a significant percentage of international clients.

CBA

491. Since 2014, the CBA has been collecting specific AML risk data using an AML Questionnaire. The data requested covers the following ML/TF risk factors: countries and geographical areas, customers and delivery channels, products and services, and some elements of governance and internal control relevant to AML/CFT. This enables CBA to undertake a risk assessment based upon specific AML risk data. However, the extent and the level of detail of collected risk data could be more comprehensive and is not aligned with that of the other ASP supervisors. For instance, CBA does not request data on complex structures and unusual transactions, customers considered as high-net worth individuals, customers transactional activities including cash transactions, TF specific indicators.

492. While ICPAC and CySEC issue their AML Questionnaires annually, the CBA does so every two years. This somewhat delays the updating of the individual risk profiles.

493. Similarly, to ICPAC and CySEC, the CBA requests an annual submission of AMLCO Reports, the content of which is comparable to those used by ICPAC. Although the AMLCO reports contain information on controls, significant risks and weaknesses etc., this data, however, is used only to a limited extent for determination of the residual risk of individual entities, i.e. only the reports of entities subject to an on-site inspection in a given year are reviewed and used for risk assessment purposes. The assessment team is of the view that such limited use of AMLCO reports does not allow the CBA to form a comprehensive risk picture ahead of future on-site inspection cycles. The criteria applied for the selection of ALMCO reports should be reviewed and extended, and cover, at least, all the supervised entities that, on the basis of the individual risk assessment, have been assigned a higher inherent risk rating.

[55] In 2017, the sample used comprised 37 % of all submitted AMLCO Reports.

[56] These figures cover ASPs, accountants and auditors licensed by ICPAC.

494. The CBA has outsourced the assessment of risk data to an external adviser. Although the risk assessment calibration tool seems to be adequate, the assessment team is concerned that the involvement of the CBA in this risk assessment exercise is limited, in particular, in co-ordinating the entire process, reviewing the appropriateness of the results (individual risk ratings calculated by the external adviser) and reviewing the adequacy of the risk model.

495. The CBA's risk assessment based on data from 2017, categorised regulated entities as follows:

**Table 30: Risk classification of CBA-regulated entities[57]**

| High risk | Medium-high risk | Medium-low risk | Low risk |
|---|---|---|---|
| 15 % | 35 % | 39 % | 11 % |

CySEC

496. CySEC developed its Risk-Based Supervisory Framework (RBS-F) in 2014. The Framework assesses the ML/TF risk of ASPs based upon risk factors identified using an AML Questionnaire. The set of risk data collected includes information on customers and delivery channels, products and services, (cash) transactions, countries and geographical areas, and some elements on governance/internal control relevant to AML/CFT. However, the level of detail of collected risk data could be more refined and is not aligned with the other ASP supervisors. Additionally, CySEC requests all of its regulated entities to submit a Monthly Prevention Statement to CySEC stating whether cash of more than EUR 10,000 was received from a client and/or whether any STRs were submitted to the AMLCO (internal STRs) and/or to the FIU (external STRs). These monthly statements are assessed by CySEC and used in the risk assessment of regulated entities.

497. Like ICPAC and the CBA, CySEC requests all of its regulated entities to submit an AMLCO Report on an annual basis which is used for risk assessment purposes. The selection of those AMLCO Reports used for analysis is based upon the risk categorisation of ASPs: for high risk ASPs CySEC conducts annual analysis of AMLCO Reports; for all other ASPs, a minimum of 20 % of ASPs AMLCO Reports are analysed each year. In the latter case, the selection is based upon various criteria (e.g. the general view of the responsible officer formed on the basis of the overall relationship and contact with the ASP). In addition to the AMLCO Report, CySEC requires all ASPs to submit their Internal Auditors' Report and the documents outlining the implementation of corrective measures following an internal audit. The review is based upon the same criteria as those applied to AMLCO Reports. CySEC's approach, as described above, is adequate and risk driven. However, in the view of the fact that only 3 % ASPs have been assigned to the high-risk category, there is a merit to extend the above-mentioned selection criteria to include medium-high risk ASPs.

498. CySEC's risk assessment based on data from 2017, categorised ASPs as follows:

**Table 31: Risk classification of CySEC ASPs**

| High risk | Medium-high risk | Medium-low risk | Low risk |
|---|---|---|---|
| 3 % | 15 % | 38 % | 44 % |

499. During the first quarter of 2018 and as part of the RBS-F annual cycle's risk identification phase, CySEC performed a gap analysis in order to identify potential shortcomings arising from regulatory developments. Following an analysis of the NRA Report of Cyprus and relevant EU Directives and Guidelines, the gap analysis has led to the incorporation of sectorial risk elements and a more targeted use of risk elements based on countries and geographical areas. Accordingly, the above figures on risk categorisation may change with a tendency to shift some regulated entities from lower risk categories to the risk categories "high risk" and "medium-high risk".

[57] The figures are based on the numbers of regulated entities comprising of ASPs, advocates and LLCs. In this context, it should be taken into account that around 60 % of all advocates provide administrative services.

Estate Agents Registration Council

500. The overall ML risk for real estate agents was assessed as medium in the NRA.[58] Since then, the risk of the sector has increased significantly as it has become the preferred choice of investment vehicle for the acquisition of Cypriot citizenship. The RE Council demonstrated low awareness and understanding of ML and TF risks. It considers the real estate sector to be low risk as licensed agents are involved in real estate deals of comparable low monetary value, whereas large real estate transactions (incl. CIP-related) are performed by advocates, property developers or ASPs. This view is mainly based on hypothetical considerations rather than any evidentiary data, as RE Council does not collect any data or information from its regulated entities for the purpose of assessing the ML/TF risk of individual real estate agents and of the real estate sector as a whole. The absence of an appropriate risk understanding is further intensified by the lack of exact information on all market participants (including large number of unlicensed agents) and insufficient expertise in AML/CFT matters by the RE Council.

Casino Commission

501. The Commission has a comprehensive understanding of the ML risks that casinos are commonly exposed to while TF risks are understood to a lesser extent. The sole casino has been categorised as high risk.

502. The casino is required to submit a Casino Regulatory Return to the Casino Commission on a monthly basis. This monthly return includes a set of AML data such as number of PEPs, number of STRs received by the AMLCO and submitted to the FIU and numbers of customers assigned to different thresholds of financial transactions starting from EUR 2,000 and going up to EUR 100,000, etc. In addition, the Casino Commission uses available information such as the casino operator's size and business model, the quality of internal policies as well as distribution channels to assess the risk of the casino. Although offsite monitoring tools (in terms of data collection frequency and scope of collected information) are considered strong supervisory measures, the extent and the level of detail of the risk data collected could be more comprehensive and should specifically cover ML/TF risks that are relevant to the industry.

503. The Casino Commission has recently launched a project with the aim of improving the quality and content of information submitted by the operator. Furthermore, the operator shall be obliged to submit the annual AMLCO Report to the Commission.

General information

504. CySEC, ICPAC and the CBA collect information on the countries of residence of BOs, countries of incorporation of legal persons who are customers, customers' business activities and total flows in and out of customers' bank accounts (the latter information is only collected by CySEC) for the 10 largest customers, whereby the "size" of customers is calculated on the basis of the total fees invoiced during the reporting period. However, this information is not used in the risk assessment of individual entities. It is collected for supervisory purposes in order to decide as to whether ad hoc on-site inspections should be carried out. In the view of the assessment team, the risk assessment systems of all ASP supervisors would benefit significantly from the use of this valuable information, particularly the countries of residence of BOs. Moreover, all three ASP supervisors should consider extending the collection of the above data to the entire, or at least or a significantly larger proportion, of the customer base.

Conclusion

505. ASPs: The three ASP supervisors have a good understanding of the ML risks that are associated with the ASP sector as a whole. When it comes to the individual risk of each regulated entity, the risk assessment methodologies for the assessment of ASPs' ML/TF risks vary between

[58] The Estate Agents Registration Council did not participate in the elaboration of the NRA Report as it took over responsibility from the FIU only in May 2018. Accordingly, the FIU was responsible for the assessment of ML/TF risks in the NRA exercise.

the ASP supervisors. Despite some differences, a common approach between the risk assessment methodologies could be identified by the assessment team and the risk assessment systems utilised by the ASP supervisors for the calculation of individual risk ratings are good. However, the scope of AML risk data collected by ICPAC and CBA via the AML Questionnaires should be enhanced, although for CySEC refinement would be needed. Moreover, the selection criteria for AMLCO Reports that are reviewed, analysed and integrated in the risk assessment should be reconsidered by the CBA and CySEC and there should be a broader use of the information collected via the AML Questionnaires by all supervisors (e.g. 10 largest customers, as discussed above) in the risk assessment process. TF risks are usually understood to a lesser extent which is confirmed by the absence of TF specific questions in the data collection.

506. Other DNFBPs: The Casino Commission has a comprehensive understanding of the ML risks that casinos are commonly exposed to while TF risks are understood to a lesser extent. Monthly returns of the casino seem to be a good offsite supervisory tool that is planned to be further expanded to fully address all the elements of ML/TF risks and get information on controls applied by casino. The RE Council demonstrated low awareness and understanding of ML and TF risks in the real estate sector, it does not collect any off-site data from its regulated entities for the purpose of assessing the ML/TF risk of individual real estate agents and of the real estate sector as a whole. The overall ML risks of accountants, auditors and advocates who are not providing services as ASPs have been assessed as low in the NRA. In the view of the assessment team, the identified risks by the supervisors correspond with the results of the NRA, the business performed and limited international exposure.

507. CIP: With respect to the provision of services relating to the CIP, the CBA and CySEC do not collect any specific information through their AML Questionnaires.[59] Nevertheless, following the publication of the official registry of CIP service providers on the website of the Ministry of Finance,[60] service providers are identified by the authorities when they schedule their on-site inspections. This information is taken into account when selecting the files for review during on-site inspections. However, the provision of CIP services does not form part of the individual risk assessments of ASPs and therefore, has no impact on the final risk rating.

[59] After the onsite visit, ICPAC has revised its AML Questionnaire that is used for the collection of data referring to 2018 and integrated a specific question in relation to the CIP. Although this is seen as a positive step, it is, however, questionable, whether and how requested data on the number of rejected clients under the CIP can be used to identify potential ML/TF risks as these clients are not administered by the regulated entity.

[60] http://cipregistry.mof.gov.cy/en/

### *6.2.3. Risk-based supervision of compliance with AML/CFT requirements*

FI Supervisors

**Table 32: Number of onsite inspections and sanctions for AML/CFT breaches**

| Year | Total number of entities | Total number of AML/CFT on-site inspections, of which: | (a) Full scope AML/CFT requirements checked | (b) Specific AML/CFT requirements checked | Number of inspections, that identified AML/CFT breaches | Number of warning letters issued[61] | Number of entities sanctioned | Number of fines issued | Total amount of fines (Eur) | Restriction/ withdrawal of the licence | Number of sanctions for senior managers and directors |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **BANKS and foreign bank branches** | | | | | | | | | | | |
| 2014 | 58 | 17 | 11 | 6 | 1 | 4 | 1 | 1 | 89.000 | | |
| 2015 | 56 | 10 | 10 | | 1 | | 1 | 1 | 1.200.000 | | |
| 2016 | 55 | 15 | 11 | 4 | 5 | 1 | 4 | 4 | 3.885.000 | | |
| 2017 | 36 | 2 | 1 | 1 | 4 | 3 | 1 | 1 | 800.000 | | |
| 2018 | 34 | 6 | 2 | 4 | 5 | 1 | 4 | 4 | 2.401.000 | | |
| **E-money institutions** | | | | | | | | | | | |
| 2013 | 1 | | | | | | | | | | |
| 2014 | 4 | | | | | | | | | | |
| 2015 | 6 | 1 | 1 | | | | | | | | |
| 2016 | 9 | | | | | | | | | | |
| 2017 | 12 | 1 | 1 | | | | | | | | |
| 2018 | 13 | 3 | 3 | | | | | | | | |
| **Payment institutions** | | | | | | | | | | | |
| 2013 | 13 | | | | | | | | | | |
| 2014 | 13 | | | | | | | | | | |
| 2015 | 13 | 3 | 3 | | | | | | | | |
| 2016 | 13 | 3 | 3 | | | | | | | | |
| 2017 | 13 | | | | | | | | | | |
| 2018 | 13 | | | | | | | | | | |
| **Currency exchange offices** [62] | | | | | | | | | | | |
| 2015 | 4 | | | | | | | | | | |
| 2016 | 5 | | | | | | | | | | |
| 2017 | 5 | | | | | | | | | | |
| 2018 | 4 | | | | | | | | | | |
| **Credit acquiring companies**[63] | | | | | | | | | | | |
| 2018 | 5 | | | | | | | | | | |
| **Life insurance companies and foreign branches** | | | | | | | | | | | |
| 2013 | 10 | | 2 | | | 2 | | | | | |
| 2014 | 10 | | 3 | | | 3 | | | | | |
| 2015 | 10 | | 0 | | | 0 | | | | | |
| 2016 | 10 | | 4 | | | 4 | | | | | |

[61] A warning letter is not considered as a sanction but rather as a mandatory requirement to remedy the deficiencies found.

[62] Started operating in 2015

[63] Started operating in 2018

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 2017 | 10 | | 0 | | | 0 | | | | | |
| 2018 | 10 | | 6 | | | 6 | | | | | |
| **Cyprus investment firms** | | | | | | | | | | | |
| 2013 | 148 | 14 | 9 | 5 | 5 | 4 | 5 | 1 | 5000 | | |
| 2014 | 161 | 5 | 2 | 3 | 8 | 4 | 8 | 5 | 59000 | | |
| 2015 | 172 | 10 | 0 | 10 | 8 | 2 | 8 | 8 | 408000 | 1 | 2 |
| 2016 | 191 | 7 | 4 | 3 | 5 | 4 | 5 | 1 | 12000 | | |
| 2017 | 219 | 19 | 13 | 6 | 1 | 28 | 1 | 0 | | | |
| 2018 | 229 | 19 | 17 | 2 | 0 | 30 | 0 | 0 | | | |
| **AIFM** [64] | | | | | | | | | | | |
| 2015[65] | 6 | | | | | | | | | | |
| 2016 | 11 | | | | | | | | | | |
| 2017 | 13 | | | | | | | | | | |
| 2018 | 23 | 4 | 4 | | | | | | | | |

508. All the FI supervisory authorities use risk-based approaches to focus ML/FT programmes; these are of varying robustness and completeness (see the section above on risk understanding). The models used by the CBC (for banks) and CySEC are the most sophisticated and robust. The CBC is developing a model for other entities it supervises. The ICCS's approach is the simplest of the FI supervisors, but it seems to focus attention on ML where needed. The table below provides information on the number of onsite inspections undertaken and sanctions imposed by the three supervisory authorities.

CBC

509. The CBC has significantly enhanced its supervisory approach since the special assessment. Onsite inspections to banks are of very good quality, being undertaken by experienced officers with diverse backgrounds and relevant expertise, and the process and findings being subject to a quality and consistency review within the CBC. Inspections are guided by a checklist. Coverage includes policies and procedures; governance and internal control elements relevant to AML/CFT, incl. compliance and internal audit arrangements, AMLCO role, employees' training; AML/CFT risk assessment and risk management; customer due diligence, customer risk profiling and monitoring, IT systems (used for monitoring, sanction/PEP screening, record keeping); products and services (e.g. correspondent banking, private banking wire transfers); customers in accordance with the risk exposure of the bank (e.g. PEPs, private banking clients, complex legal structures including trusts and other types of legal arrangements, customers having links with high risk jurisdictions, other high risk clients); transactions (cash transactions, large complex and unusual transactions, cash intensive business, transactions to/from higher risk countries); delivery channels (e.g. introducers, third parties) STR reporting; and TFS. In addition, significant offsite information for banks is provided to the CBC and informs its approach to inspections. During the period to the end of 2016 the onsite inspection programme was abnormally overloaded as it was dictated by the special assessment and the Troika's AML action plan. It met this challenge and, since then, there has been a reduction in the onsite programme; while noting that the offsite programme has continued as usual, a shortfall in resources has led to some reduction in the amount of supervision which can be undertaken and the speed at which the CBC can undertake its overall supervisory programmes. The reduction in the onsite programme was the result of the significant effort devoted to the FBME case and other risk prioritised efforts such as the introduction of a questionnaire to introducers and a score card for the assessment of the quality of introducers. In addition, the team was significantly involved with the NRA in 2016 and 2017, and the development of directives and the transposition of the fourth EU AML directive.

[64] UCITS Management Companies, Self-Managed UCITS, Self-Managed Alternative Investment Funds, Self-Managed Alternative Investment Funds with a Limited Number of Persons, Companies with sole purpose the management of AIFLNPs have not been inspected to date.
[65] Started operating in 2015

510. The AML/CFT department is responsible for onsite and offsite supervision as well as the issue of sanctions. Following an uplift after the banking crisis, the team comprises 8 FTE staff and a Head of Department. There is an emphasis on training (both ML and TF). Team members receive specialised training, including on e-money business and other Fintech-related products. The team is very committed, and its work is high quality, perhaps in part forged by the banking crisis, addressing the recommendations in the Special Assessment report, addressing EU requirements and of making significant revisions to the supervisory process since 2013. Nevertheless, the team is under resourced. The department was complemented by the use of accountants for onsite inspections in 2014 and from 2016 to 2018.

511. The risk tool has identified 11 banks as high risk and 16 as medium risk. The assessment team has a minor concern that a low number of low risk banks (3) might suggest that, to a partial extent, banks are not sufficiently differentiated by risk. The CBC has advised that the spread of risk ratings reflects the NRA's overall medium high-risk rating for banks.

512. Offsite supervision comprises assessment of a range of routine reports (see below). Offsite information received and analysis of it is integral to the CBC's supervisory approach and informs onsite supervision.

513. A statement of large cash transactions and fund transfers is received on a monthly basis. The report includes information on the total amount of cash deposits and withdrawals, the total amount of inward and outward transfers, the payments systems used and information on country of origin and destination. This enables identification of customers executing large transactions and large numbers of transactions. The information is assessed and leads to follow up queries with banks so as to ensure information and risks are understood. In one case, an ad hoc inspection was conducted, and the CBC filed a STR and imposed a sanction. Wire transfer information was available at the time of the NRA, but this was increased after the NRA and also collected on a retrospective basis. In addition, information on deposits and loans based on the country of residence of the beneficial owners of legal persons and legal arrangements is provided monthly to the AML/CFT department, together with relevant prudential or market conduct reports received such as compliance reports.

Banks are also required to provide data used to populate the risk assessment tool on a six-monthly basis.

514. On an annual basis the CBC receives AMLCO and risk reports. This information is followed up where necessary and informs the content of onsite inspections. In addition, the CBC holds meetings with internal and external auditors at least on an annual basis. Meetings are held more frequently when the need arises (for example, in relation to the finalisation of an internal or external audit).

515. In addition to the foregoing, there is routine communication between the CBC AML team and AMLCOs and with other departments of the CBC, including the licensing and supervision departments.

516. Following the three-year cycle of full scope inspections to all banks required by the Troika programme, which ended in late 2016, the CBC now formulates its onsite inspection programme based on its risk tool. As the basic elements which are fed into the risk tool, such as business model and customer risk profile, do not change from year to year, risk assessment changes are inevitably unaltered in the short term. In 2017 and 2018, due to the demands of other projects, the onsite programme was reduced. Full-scope inspections (with complementary resources from auditing firms secured via a tendering process) are carried out; in addition, short duration special (i.e. ad hoc) inspections are undertaken as a response to trigger events. The majority of inspections since 2016 have been the result of trigger events well publicised internationally such as the Panama Papers, the Laundromat case and a Danish bank, and information obtained from foreign authorities. In another case, the CBC responded to a concern about a bank's internal audit function by way of an inspection. It is positive that the CBC is using its limited resources in this way so that it can be responsive to, and address, emerging risks. Nevertheless, the volume of inspections is lower

than should be the case in comprehensive risk-based supervision although the CBC is of the view (and the assessment team agrees) that offsite supervision mitigates the gap to some extent. In addition, there are some delays in being able to complete the whole of the inspection process for banks inspected.

517. Prior to 2014 banks were subject to both full and themed inspections. During 2014 to 2016 all banks were subject to a full scope inspection. These covered corporate governance, policies and procedures, risk assessment, CDD, internal controls, IT systems, introducers, correspondent banking, the AML unit, PEPs, private banking, STR reporting, training, trusts/legal arrangements and UN/EU sanctions. Since that time, inspections have continued to be full scope; the intention is to move to a thematic approach in the future.

518. With regard to the intensity of supervision, overall, while risk is a factor, there is some bias towards the size of a bank. There are three systemic banks; each is inspected more frequently than other banks. They offer more sophisticated products and services to their customers and have a larger percentage of international business compared with the other banks. The number of officers in an inspection team is dictated by the number of the customers of the bank and its size. More files are sampled at larger banks (some 250) compared with smaller banks (perhaps 10, bearing in mind that the customer base can be very small). The volume of international business is also a factor in file selection. Some smaller banks have received deeper inspections than would be warranted by their size alone. The intensity of inspection is dictated by the number of customers, volume of fund transfers, type of products and services offered, distribution channels and the geographical areas where the bank operates. Nevertheless, there would appear to be scope to refine the approach further.

519. Inspections are detailed, covering both ML and TF. The main focus of separate TF supervision is on sanctions programmes with focus on the transfer of cash, wire transfers and high risk countries being more generic. They also focus on the adequacy of TF related scenarios in monitoring systems. Nevertheless, the assessment team considers that they would benefit from refining the degree of focus on FT.

CySEC

520. CySEC's dedicated AML/CFT and risk units also allow for good quality supervision, although a shortage of resources has had an effect with the volume of supervision being lower than suggested by individual risk assessment results. There are eight officers devoted to supervision.

521. To aid offsite supervision, CySEC receives monthly reports on cash deposits over EUR 10,000 and on internal suspicion reports and STRs filed.

522. Onsite inspections are planned on an annual basis. Provision for ad hoc inspections is included as part of the programme. For example, in 2016 inspections were carried out as a result of the Panama Papers, intelligence about cash reporting and an investigation. In 2017 five inspections were held as a result of complaints or whistle blowing. A checklist is used to guide the inspection.

523. CySEC's inspections have focussed on high and medium-high risk CIFs (high risk dominating), with a few CIFs in the two lower risk categories also being inspected. All entities rated as high risk were inspected during the period 2015 to 2018 except for one institution rated as high risk in 2018. Inspections of collective investment fund management companies were introduced in 2018 although the whole process for the four management companies had not been completed at the time of the assessment team's visit to Cyprus. Management companies had not previously been inspected as their risk ratings were medium low or low; the four were selected on the basis of risk from within the cohort of such licensees and each inspection has raised issues which could potentially lead to the imposition of a sanction. The assessment team considers that additional inspections would need to be undertaken to CIFs for risk based supervision to be comprehensive.

524. Inspections appear to be very good quality. With regard to intensity of supervision, there are differences of approach to inspections between firms based on the number of customer files sampled and the concentration on source of funds. Some 20 customer files are sampled, in relation

to which the assessment team would suggest a greater sampling range subject to risk. The sample is based on risk factors such as STRs, the Panama Papers, the CIP and ensuring coverage of customers in all risk categories. Inspections devote greater focus on areas which have led to a higher risk score within the overall AML/CFT risk rating. The higher the risk of the entity inspected, the more CySEC will increase its focus, for example, on the number of transactions considered, the examination of source of funds and counterparties, and governance (including the audit programme). The information received as part of the offsite supervisory programme also has a bearing on the intensity of the inspection (for example, a high proportion of PEPs might lead to attention on controls for such persons).

525. Onsite inspections cover TF to some extent by looking at some types of company that might be used for TF; jurisdictions of clients; prepaid cards; NPOs. These factors are considered when customer files are selected for review. More training on TF would be beneficial.

ICCS

526. The ICCS is also undertaking positive supervision but a shortfall in staff resources has had an effect.

527. Two of the ICCS' staff specialise in AML/CFT matters and cover licensing as well as all aspects of AML/CFT. They are not devoted full time to AML/CFT as ICCS staff generally cover all supervisory matters. From time to time, another member of staff assists the specialist team to review customer files during onsite inspections. It is planned to merge the ICCS with the pension authority; one of the outcomes of this merger is expected to be that junior staff will be involved on a systematic basis with the specialists so as to address the resource gap. It was also clear to the assessment team that the addition of further IT tools would benefit supervision and alleviate some of the resource gap; this too is anticipated after the merger.

528. With regard to offsite supervision, the ICCS receives a range of information from insurers. This includes an annual report by the AMLCO, a confirmation from the board that the insurer has been in compliance with the ICCS' AML/CFT Order and an annual statistical return. This return includes information on the size of the insurer, the number of PEPs, non-face to face business and cash transactions In addition, under the solvency II framework insurers must provide risk assessment and supervisory reports and publish information on their corporate governance. While not focussed on AML/CFT, this information on corporate governance is relevant to AML/CFT.

529. There are onsite inspections dedicated to AML/CFT. If an inspection covering, for example, other matters such as solvency II were to raise a matter of AML/CFT concern that matter would be investigated. Whilst the ICCS uses a checklist to guide onsite inspections, it would require modification in order to provide for comprehensive inspections; it proposes to revise this document to take account of the issue of new Orders. The programme is driven by a combination of the size of the insurer and risk. There is a focus on the three systemic insurers as result of solvency II but, in practice, there appears to be a direct link between risk and the market share/size of the three systemic insurers. The highest risk rating is medium low for AML/CFT. Customer files are sampled on a random basis, but coverage includes customers with a spread of risk (particularly high risk) and including unit linked and single premium products, PEPs and non-residents (including from high risk countries). Remediation of problems found at previous inspections is checked.

530. There is some change in the intensity of supervision based on risk. For example, for higher risk more information is required and there are more meetings with management.

531. The frequency of onsite inspections is subject to a policy (high risk: annually; medium to high risk; annually; medium to low risk; every two years; low risk: every four years) unless ad hoc issues arise. While the triggers are not articulated in writing, the ICCS is conscious of what factors would increase risk and justify an inspection. The pattern of inspections in some years and not others is not ideal. Three systemic insurers comprise more than 70% of the market and these are the focus of the inspection programme. Supervision is aimed more at ML than FT; this is consistent

with the difference in ML and TF risk of the insurance sector. Highest risk insurers are rated as medium low risk.

*DNFBP Supervisors*

532. The overall number of onsite inspections conducted by the DNFBPs supervisors to cover the most material DNFBP sectors (ASP and real estate sector) is generally low (with the exception of ICPAC), see table 33. Although the ASP sector faces similar risks, supervisory approaches used for on-site monitoring by the three different supervisors are not fully consistent to ensure a common level playing field (on-site inspections cycles vary in frequency and scope, different criteria are used to determine the intensity of individual on-site inspections). In general, the ASPs supervisors determine their inspection plans on the basis of risks. However, it is questionable whether individual on-site inspections are fully risk-based. The RE Council does not use a risk-based approach to determine the scope and frequency of supervisory actions. The Casino Commission is actively engaged in monitoring casino operations.

**Table 33: Number of AML/CFT on-site inspections by DNFBP supervisors compared to the total number of regulated entities[66]**

| Type of DNFBP | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|---|
| Casinos[67] | - | - | - | - | - | 1 (1) |
| Real estate agents | 3 (291) | 1 (290) | 2 (279) | 3 (316) | 2 (361) | 2 (353) |
| Advocates[68] | 23 (2767) | 27 (2994) | 180 (3208) | 199 (3452) | 91 (3741) | 80 (3808) |
| Lawyers' Companies | - [69] | 27 (512) | 180 (556) | 199 (576) | 91 (630) | 80 (689) |
| Accountants / Auditors | 185 (471)[70] | 195 (506) | 90 (542) | 91 (597) | 99 (613) | 123 (671) |
| ASPs (licensed by ICPAC) | 0 (263) | 14 (295) | 45 (277) | 79 (322) | 52 (315) | 43 (326) |
| ASPs (licensed by CySEC) | 2 (19) | 2 (107) | 19 (132) | 8 (143) | 7 (151) | 9 (159) |
| ASPs (licensed by CBA) | 0 (0) | 27 (906) | 180 (1011) | 199 (1172) | 91 (1449) | 80 (1555) |

CBA

533. Since 2013, the AML Department of the CBA has been conducting on-site inspections of advocates, LLCs and ASPs. LLCs were only introduced in 2014 and ASPs were licensed by the CBA in 2014 for the first time. The CBA's onsite inspection plan is determined on the basis of risks. With regard to off-site monitoring, the CBA categorises its supervised entities under four risk categories. The risk category is used to determine the frequency of on-site inspections as follows: high risk (6 months to 1 year); medium-high risk (2 years); medium-low risk (3 to 4 years); low risk (litigation services; 5 years).

534. Prior to the on-site inspection, the CBA requires from the obliged entity a copy of its internal AML manual. During the on-site visit, the Supervisory Control Officer interviews the AMLCO in

[66] X (Y), where X is the number of onsite inspections and Y (in brackets) is the total number of licensed/registered entities as of the end of the year.

[67] The first license for operation of a temporary casino was issued in June 2018. Before that time, no casinos were operating in Cyprus.

[68] The numbers of on-site inspections provided by the CBA do not represent the regulated entities that were subject to an on-site inspection, but rather have to be understood as consolidated numbers. According to the CBA, on-site inspections would regularly cover a larger number of LLCs, advocates and ASPs that are connected with each other (e.g. through employment) and therefore, would be subject to one on-site inspection. For instance, the on-site inspections by the CBA in 2017 and 2018 covered 322 and 357 entities.

[69] The option of incorporating Lawyers' Companies was introduced in 2014; before that, the legal institution of Lawyers' Companies did not exist.

[70] Up to and including 2014, these inspections included a review of AML awareness where only some elements of the AML/CFT-Law and ICPAC's Regulations were monitored. As of 2015, self-contained AML on-site inspections called "AML, Rules and Regulations reviews" covering all aspects of the AML/CFT regime were implemented.

accordance with the CBA Audit Checklist. For the inspection of the entity's files, the CBA has drafted various checklists (e.g. Trust Checklist; Client Accounts Checklist; Third Persons Checklist). On-site inspections are usually conducted as full-scope inspections, i.e. compliance checks with respect to all CDD obligations (including internal controls and manuals) and other preventive measures.

535. The CBA has reported that on-site inspections differ in intensity depending on the size, extent of services, and risk level of the inspected entity. In the case of larger and riskier firms, more officers (up to four instead of one or two officers) are usually assigned to an on-site visit. The number of client files inspected also depends upon the size and risk level of the entity and the type of services it offers, and the CBA has stated that various criteria are applied when selecting the types of client files for review (e.g. PEPs, HNWI, trusts, high risk countries, etc.). However, almost the same sample size (at least 5 to 10 % of the total client files) is applied to all risk categories.

536. Although the CBA's onsite inspection plans are determined on the basis of risks of individual entities, it is not clear whether individual on-site inspections are fully risk driven, i.e. whether they fully focus on the specific risks of the individual entities (which result in determination of the scope and depth of the inspection, e.g. how many client files have to be chosen for the review, focusing on the specific types of clients, particular services, transactions, etc.). Moreover, it is not clear to what extent the information from the AMLCO Reports is used to determine focus areas for on-site inspections. For instance, if the review of an AMLCO Report leads to the conclusion that the quality of the internal risk management system is not satisfactory, it is not clear that emphasis is placed on this issue during the on-site inspection.

537. Given the relatively low number of resources of the CBA (i.e. four officers) and the high number of regulated entities, there are doubts as to whether on-site inspections are carried out effectively and according to the required frequency (see table 34). It should be noted that the four officers of the CBA are not only responsible for on-site visits but also other responsibilities (inter alia, licensing, on-going off-site monitoring and preparation of risk assessments).

538. Despite its significant lack of resources, CBA has been proactive in conducting thematic reviews on an ad hoc basis, e.g. *Panama Papers* (72 regulated entities were subjected to specific on-site reviews in the years 2015 and 2016); *Laundromat* cases. Even though this exercise is noted as a positive example, it required a substantial amount of resources leading to a lower volume of scheduled on-site inspections of those entities that were not involved in these publicised cases.

ICPAC

539. Since 2005, ICPAC has been conducting on-site inspections (i.e. audit monitoring visits and quality check monitoring visits). Up to and including 2014, these inspections included a review of AML awareness where only some elements of the AML/CFT-Law and ICPAC's Regulations were monitored. As of 2015, self-contained AML on-site inspections called "AML, Rules and Regulations reviews" covering all aspects of the AML/CFT regime were implemented. This followed a pilot review strictly for ASPS in 2014.

540. The on-site inspection plan is determined on the basis of risks. On the basis of its off-site monitoring, ICPAC classifies supervised entities under four risk categories. The risk category is used to determine the frequency of on-site inspections as follows: high risk (1 to 2 years); medium-high risk (2 to 4 years); medium-low risk (3 to 5 years); low risk (6 years). Holding and non-active entities have to submit an annual declaration notifying ICPAC of their status.

541. An inspection schedule for determining those entities to be inspected is drafted by ICPAC's Monitoring and Compliance Department every three months. It may happen that entities listed on the schedule are thereafter replaced by other entities due to circumstances that indicate a higher risk (e.g. adverse media information, complaints, requests from the management of ICPAC or from the Admissions and Licensing Department, intelligence received from the FIU or other supervisors, unexpected events such as the *Panama Papers* or the *Laundromat* cases). The on-site inspections are carried out by the Senior Reviewers from the ACCA with the possible support of ICPAC (e.g. for on-site inspections of larger and high-risk ASPs). For inspection purposes, the ACCA has developed

a methodology and checklists that are used for reviewing client files. On-site inspections are usually conducted as full-scope inspections, i.e. compliance checks with respect to all CDD obligations (including internal policies and manuals) and other preventive measures.

542. Although ICPAC's onsite inspection plans are determined on the basis of risks of individual entities, it is not clear whether individual on-site inspections are fully risk driven. As regards intensity of on-site inspections, ICPAC has established (written) guidelines that the ACCA Reviewers must follow when they are on-site. Although guidelines include criteria for selecting client files and set minimum standards for the checks (e.g. at least three business relationships with directorship services have to be chosen, if applicable), more detailed references are missing to the specific risks to which the regulated entity is exposed and a more comprehensive set of criteria for selection of client files and clearer standards for the determination of the number of client files to be inspected (sample size) are required. The ICPAC reported that in practice differences are made between the different risk categories of supervised entities when deciding on the scope/intensity of onsite inspections. Moreover, the sample sizes of the client files are dependent on the size of an entity and the services it provides (i.e. a larger number of client files are selected in the case of a larger entity and when a variety of services is offered).

543. The number of on-site inspections (including of ASPs) conducted in the period from 2013 to 2018 (see table 33) is adequate. In addition to scheduled on-site inspections, ad hoc thematic reviews were also carried out in relation to *Panama Papers* allegations, *Laundromat*, etc.

544. Although additional resources may be requested from ACCA at any time[71] for conducting on-site inspections, ICPAC has confirmed that it lacks internal resources in the Monitoring and Compliance Department, which is responsible for AML/CFT oversight and supervision. As a consequence, some of the tasks are currently outsourced to external advisors, e.g. to provide ICPAC with assistance in the risk assessment process and in off-site monitoring. This is in addition to the long-standing agreement with ACCA and the use of their Reviewers for on-site inspections.

CySEC

545. Since 2014, CySEC has been utilising its RBS-F to assess the ML/TF risk of ASPs and to implement a risk-based approach to supervision; including the on-site inspection planning which is determined on the basis of risks. The supervisory system provides for four risk categories determining the frequency of on-site inspections as follows: high risk (annually); medium-high risk (2 to 5 years); medium-low risk (5 to 8 years); low risk (ad hoc). Accordingly, on-site inspections are carried out for entities in all risk categories except low risk (unless there are certain trigger events indicating the need for immediate inspection).[72] The general approach of excluding low risk entities from on-site inspections to some extent limits the effective supervision of ASPs.

546. An annual inspection schedule to identify those ASPs to be inspected is developed by CySEC's AML/CFT Department at the beginning of each inspection period. As is the case with ICPAC's schedule, it may happen that ASPs listed on the schedule are replaced by other entities due to significant events indicating the need for an earlier inspection. Certain documents are requested prior to the onsite inspection, e.g. AML procedures manual, a comprehensive list of clients (including information on countries of residence of BOs, business activities of clients), transactions (cash, banking account turnovers), etc. This information, together with the offsite returns' data is used to determine the sample of client files chosen for the review. During the on-site inspection

[71] ICPAC has outsourced the performance of on-site inspections to the ACCA UK in order to benefit from their long-standing expertise. 3 full-time Senior Reviewers of the ACCA permanently reside in Cyprus and are available for on-site inspections. In case further assistance is required, for instance due to a large number of planned on-site inspections, additional resources may be requested from the head offices of ACCA in London. Such additional resources are requested three to four times a year.

[72] In the period from 2015 to 2018, three ASPs categorised as low risk were subject to an on-site inspection undertaken by CySEC. The trigger events for inspection of low risk ASPs were the Panama Papers, involvement of shareholders/directors in an investigation of financial crime abroad, customers included in sanctions lists, customers involved in high risk business activities (i.e. arms dealing). A formalised list of "main" trigger events for on-site inspections of low risk ASPs does not exist.

officers may amend the sample size depending on the circumstances. The methods used by CySEC to determine the sample size are relatively sophisticated as they are based on a comprehensive set of risk data.

547. Generally, on-site inspections are carried out as full-scope inspections, i.e. compliance checks are carried out in relation to all CDD obligations (including internal controls and manuals) and other preventive measures. The higher the risk of the ASP, the more CySEC will increase its focus, for example, on the number of transactions considered, the examination of source of funds and counterparties, and governance. The information received as part of the offsite monitoring also has a bearing on the intensity of the inspection (for example, a high proportion of PEPs might lead to attention on controls for such persons).

548. The number of on-site inspections of ASPs (see table 34) is relatively low. Lack of resources hampers the effectiveness of on-site supervision. Given that the high and medium-high risk ASPs account for 18 % of all ASPs, it is doubtful that the current resources are sufficient to carry out an on-site inspection of the remaining 82 % of ASPs (medium-low risk ASPs (38 %) within the next 5 to 8 years (as scheduled) and low risk ASPs (44 %) within a reasonable timeframe)..

549. Despite lack of resources, CySEC was proactive in carrying out thematic reviews: e.g. following *Panama Papers* allegations, CySEC has collected information from approximately 410 regulated entities, out of which 60 reported that their customers had a business relationship with *Mossack Fonseca* or other links with *Panama Papers*. As a result, CySEC has carried out additional thematic on-site inspections of five ASPs in 2016.

Estate Agents Registration Council

550. The RE Council does not use a risk-based approach to determine the frequency and intensity of its supervisory actions. The RE Council does not collect any risk data from its supervised entities on a regular basis for the purpose of generating individual risk profiles. Also, the FIU, as a former supervisor, did not apply a risk-sensitive approach to supervision. So far, the selection of real estate agents for on-site inspections has been conducted on a random basis; the individual inspections are also not risk based.

551. Significant lack of resources hampers effectiveness of supervision – currently RE Council employs only 2 inspectors. The number of on-site inspections compared to the total number of real estate agents (see table 34) is very low.[73] Given the vulnerability of the real estate sector in Cyprus, the absence of risk based supervision to real estate agents, including low number of onsite inspections, is a major concern.

Casino Commission

552. The Casino Commission only became operational in 2018 with the casino commencing operations in July 2018. An AML compliance specialist was appointed to the Commission in October 2018 and an inspection was conducted in the last quarter of 2018 (see table 34), the focus of which was on compliance with the AML/CFT-Law and the structure of the licensee's AML control system. This resulted in a licence condition being applied that required the licensee to submit to a special AML review by a professional and independent third party.

553. The Commission collects risk data on a regular basis and is in the process of establishing a comprehensive risk-based approach to supervision. Even though the extent of the collected data needs to be enhanced, the Commission is already in a position to develop an understanding of the specific ML risks posed by the casino and the satellite casinos. The Commission does not yet have a methodology in place that determines the frequency and intensity (scope) of future on-site inspections taking into account specific and individual risks.

554. The Commission is currently enhancing the resources and technical knowledge required for comprehensive and consistent supervision of existing casinos and for the much larger integrated

[73] For instance, in 2018 only 0.6 % of all regulated entities were subject to an on-site inspection.

casino resort. Taking into account the on-going work towards enhancement of supervision of casinos and the fact that there is a pending licence application for a further satellite casino, with the possibility of a fourth at the end of 2019, a substantial increase in resources is likely to be needed should these licences be issued. The integrated casino resort is expected to have operations four times the size of those of the current casino.

### *6.2.4. Remedial actions and effective, proportionate, and dissuasive sanctions*

*FI Supervisors*

555. All three financial supervisory authorities require breaches to be remedied and verify this during onsite inspections. Notifications by all of the authorities of the requirement to undertake remediation are issued by means of a warning letter. Table 33 above provides information on the sanctions imposed by FI supervisory authorities.

CBC

556. Sanctions have been imposed by the CBC for AML/CFT breaches by banks, namely fines against institutions. No sanctions have been applied in relation to senior managers/directors although in one case the CBC worked with the institution to have an officer removed on the ground that he was not adhering to his duties. Fines have been applied for poor quality BRAs, customer risk misclassifications; poor recording of information on the nature and purpose of relationships; and a poor-quality internal audit function. The total fines levied from 2015 to 2018 amounted to just over EUR 8.3 million (an average of over EUR 830,000); for each of the fined institutions. All but one fine is over EUR 350,000 and four fines were more than EUR 1 million. Cypriot banks are still suffering from the global economic and financial crisis and in that context the level of fines has had an increased effect. Importantly, with two exceptions all fines have been published. In the two cases, breaches were found at two small bank branches, which were closed. The number of banks fined is quite a significant part of the sector. The CBC has noted from market intelligence, complaints received from banks, and enquiries from correspondent banks which have relationships with fined banks, that the fines and publication of them has a strong impact. The assessment team notes that the internal process (based on legislation) leading to a sanction has more steps than would seem necessary and, partly because of this and partly because of resourcing (including the time needed to complete the inspection process), it takes one to two years to make a decision on a sanction. This means the application of sanctions is not timely. The assessment team also notes the absence of sanctions in relation to individuals and that sanctions other than fines have not been used. Linked with this, the reduced number of onsite inspections since 2016 has removed some possibility of further sanctions. Overall, the assessment team accepts that the sanctions framework operated by the CBC has strong elements of effectiveness and dissuasiveness while leaving scope for enhancement,

557. Sanctions have not been imposed by the CBC in connection with other types of entity subject to its supervision. Non-banks have not been subject to the same level of supervision as banks and, while accepting that non-banks had limited materiality at the time of the assessment team's visit to Cyprus, this will have removed some possibility of sanctions. The increase in resources proposed above and a more intrusive supervisory regime based on risk, combined with a streamlined internal process should enable the CBC to demonstrate it has an effective sanctions regime.

CySEC

558. In 2015 CySEC withdrew a CIF licence due to a combination of AML and other supervisory breaches. CySEC has issued fines, all of which have been published. Most fines have been imposed on firms but, in 2015, fines of EUR 300,000 were imposed on directors/senior managers. The deficiencies leading to the fines have included unsatisfactory customer economic profiles and risk assessments and monitoring. Two fines, one of EUR 300,000 and one of EUR 450,000 (the latter in May 2019) for firms, albeit combined with non-AML/CFT matters are of a sufficient size to demonstrate an appetite to apply larger fines in the context of Cyprus even if no large fine has been applied solely for AML/CCT failures. The overall average level of fine is not wholly dissuasive and

overall the sanctions framework is also not wholly effective and dissuasive. CYSEC's conclusions from its onsite inspections as to whether or not there have been breaches are credible and it therefore appears that the imposition of a sanction is consistent with the breaches identified. In light of this, the range and number of penalties applied, combined with feedback received by CySEC from licensees that its administration of the sanctions framework is effective, the assessment team has concluded that there are very good elements of effectiveness and dissuasiveness. There is scope to increase the number of onsite inspections and, therefore, potentially, the number of sanctions.

ICCS

559. To date the ICCS has not considered any breach to be sufficiently serious to warrant the imposition of a sanction. Breaches found have been minor or relatively minor. It appeared to have the appetite to impose sanctions if the severity of a breach warranted this. The ICCS does not have a procedure for the imposition of penalties but has advised that the legislation under which it operates contains relevant provisions.

*DNFBP Supervisors*

560. The number of sanctions imposed by the DNFBP supervisors is very low. While remedial actions imposed by the supervisory authorities in the form of a warning letter serve as a precautionary measure (followed by the requirement to remedy AML/CFT breaches and verify this during follow up on-site examinations), only few administrative sanctions (fines) have been imposed to date. Table 34 provides an overview of remedial actions and sanctions imposed by the DNFBP supervisors. Sanctioning for AML/CFT breaches imposed by DNFBP supervisors is not considered proportionate and dissuasive. There is a tendency to classify breaches as not being serious or repeated, and therefore granting entities the opportunity to remedy them on the basis of an action plan. There are no sanctions or other remedial measures issued by the RE Council (or the FIU as former supervisor of the real estate sector). Casino Commission has imposed specific licence conditions on casino as a result of its desk-based review that revealed AML compliance gaps.

**Table 34: Overview of remedial actions and sanctions of DNFBP supervisors**

| **Type of DNFBP** | **2013** | **2014** | **2015** | **2016** | **2017** | **2018** |
|---|---|---|---|---|---|---|
| **Casinos[74]** | **-** | **-** | **-** | **-** | **-** | **1[75]** |
| Warning | - | - | - | - | - | 0 |
| Fines (number) | - | - | - | - | - | 0 |
| Fines (total amount | - | - | - | - | - | 0 |
| **Real estate agents** | **0** | **0** | **0** | **0** | **0** | **0** |
| Warning | 0 | 0 | 0 | 0 | 0 | 0 |
| Fines (number) | 0 | 0 | 0 | 0 | 0 | 0 |
| Fines (total amount | 0 | 0 | 0 | 0 | 0 | 0 |
| **Advocates / LLCs / ASPs (CBA)[76]** | **3** | **17** | **58** | **28** | **24** | **9** |
| Warning | 3 | 17 | 58 | 28 | 24 | 7 |
| Fines (number) | 0 | 0 | 0 | 0 | 0 | 2 |

[74] The first license for operation of a temporary casino was issued in June 2018. Before that time, no casinos were operating in Cyprus.

[75] The first on-site inspection conducted with the casino resulted in specific AML related license conditions that were imposed in December 2018 and which includes the obligation to perform a special AML review by a third party.

[76] According to the CBA, on-site inspections regularly cover a large number of LLCs, advocates and ASPs that are connected with each other (e.g. through employment). Consequently, sanctions refer to different license holders who were subject to the same on-site inspection. This is the reason why the above figures are not split into the different types of license holder (i.e. advocates, LLCs and ASPs).

| | | | | | | |
|---|---|---|---|---|---|---|
| Fines (total amount | 0 | 0 | 0 | 0 | 0 | 18,000 |
| **Accountants /** | **0** | **0** | **11** | **13** | **16** | **21** |
| Warning | 0 | 0 | 11 | 13 | 16 | 21 |
| Fines (number) | 0 | 0 | 0 | 0 | 0 | 0 |
| Fines (total amount | 0 | 0 | 0 | 0 | 0 | 0 |
| **ASPs (ICPAC)** | **0** | **0** | **10** | **13** | **11** | **11** |
| Warning | 0 | 0 | 10 | 13 | 11 | 11 |
| Fines (number) | 0 | 0 | 0 | 0 | 0 | 0 |
| Fines (total amount | 0 | 0 | 0 | 0 | 0 | 0 |
| **ASPs (CySEC)** | **0** | **7** | **3** | **15** | **37** | **67** |
| Warning | 0 | 7 | 3 | 15 | 35 | 67 |
| Fines (number) | 0 | 0 | 0 | 0 | 2 | 0 |
| Fines (total amount | 0 | 0 | 0 | 0 | 36,000 | 0 |

CBA

561. After an on-site inspection, an inspection report is drawn up containing any identified deficiencies and corresponding recommendations. The entity must provide the CBA with an action plan to remedy deficiencies. When agreement on the remedial actions is achieved, the CBA sets a time frame for the implementation of the action plan.

562. When deciding whether a review of the remedial actions should be carried out before the next on-site inspection, the type of breaches and their severity are taken into account by CBA. If a follow-up inspection is considered necessary, it usually takes place within a maximum period of six months after the initial on-site inspection.[77] If the CBA then ascertains that the entity did not comply with the action plan, a warning letter making clear the obligation to establish a further action plan is issued, or if the deficiencies are severe, the case is referred to the Board of the CBA. The Board is responsible for the imposition of administrative sanctions. If no (earlier) follow-up inspection takes place, remedial actions are followed up at the next on-site inspection. Until the following on-site or follow-up inspection takes place, entities are not required to notify the CBA about on-going progress to rectify deficiencies or to confirm full implementation of the action plan.

563. The CBA has issued a sanction directive but has no sanctions application policy[78] containing a list of criteria for determining what constitutes "serious", "repeated" or "systematic" AML/CFT breaches and what type and level of administrative sanctions should be imposed accordingly. If a deficiency is deemed serious or repeated[79], the case is forwarded to the Board of the CBA. In all other cases, sanctions will not be imposed, and remediation is required on the basis of an action plan. The assessment team considers this approach insufficiently dissuasive. While entities that comply with the action plan are generally deemed compliant with AML/CFT requirements, it is unclear whether sanctions can be imposed where the same types of breaches reoccur at a later stage.

564. As indicated in Table 34, administrative fines have only been imposed on advocates twice in

[77] Number of follow-up inspections that have previously been carried out: 3 (2013); 17 (2014); 58 (2015); 28 (2016); 24 (2017); 7 (2018). Typical examples that have led to a follow-up inspection were: (a) background screening of the client was carried out only when first taking them on and no subsequent screenings have occurred; (b) no measures were applied in order to verify transactions.

[78] The CBA has issued a Directive to the members of the CBA for imposing sanctions/fines (lastly amended in July 2017). However, this Directive does not serve as a sanctioning policy as it does not include any criteria for determination of sanctions nor any definition of deficiencies that are considered, e.g. "serious", "repeated". Apart from that, this Directive is outdated as it does refer to the fines of the previous AML/CFT-Law.

[79] However, it is unclear what precise threshold needs to be overstepped for a deficiency to be considered "serious" or "repeated".

2018, and these fines only amounted to roughly 1 % of the possible maximum fine. Moreover, the CBA did not make its actions public, considering this to be disproportionate due to the small size of Cyprus.

565. In the period of 2015 to 2018, the CBA requested the removal of AMLCOs in three cases and withdrew the licences of three regulated entities due to breaches of the AML/CFT-Law. These administrative measures are positively recognised by the assessment team. However, it is noted that no monetary fines for breaches of the AML/CFT-Law were imposed by the CBA in the years before 2018. Given the large numbers of entities, it is concerning that almost no serious, repeated or systemic breaches of the AML/CFT requirements have been identified. The adequacy of the decision-making process regarding the application of sanctions is questionable, in particular, the willingness to impose effective, appropriate and dissuasive sanctions.

ICPAC

566. Like CBA, ICPAC requires remediation of breaches detected during an on-site inspection in the form of an action plan to be developed by the inspected entity.

567. Remedial actions are usually followed up at the following scheduled on-site inspection. Follow-up inspections are carried out within 3 years of the initial inspection, except in the case of low risk entities which are inspected within 6 years. Until the follow-up inspection takes place, most entities are not required to notify ICPAC of their on-going remediation work, other than in their routine annual AMLCO Report. However, if serious deficiencies are detected, the entity may have to provide ICPAC with certain documents demonstrating that breaches have been remedied (e.g. a contract with an external IT firm in order to prove the use of an electronic monitoring system),[80] and a follow-up inspection may be carried out earlier than scheduled. The monitoring of action plans is led by ICPAC in cooperation with the ACCA Reviewers.

568. So far, no sanctions for AML infringements have been imposed on regulated entities by the Regulatory Committee or the Disciplinary Committee. As indicated in Table 34, warning letters were issued in those cases were the entities did not comply with the action plan. In addition, ICPAC has imposed sanctions for failure to comply with the obligation to submit the AMLCO Report. Those sanctions have been made public on the website of ICPAC and in the quarterly magazine that is circulated to all members.

569. Like the CBA, ICPAC has not adopted a sanctions application policy. The Members Handbook includes some elements in this regard, but it is not sufficiently comprehensive. There are no clear criteria for determining the type and level of administrative sanctions or a definition of serious, systemic or repeated breaches of the AML/CFT regime. Furthermore, on the basis of the case examples provided, it appears that there is a tendency to classify breaches as not being serious or repeated, and therefore granting entities the opportunity to remedy them on the basis of an action plan. As with the CBA, the adequacy of the ICPAC's decision making process regarding the application of sanctions is questionable, in particular, the willingness to impose effective, appropriate and dissuasive sanctions.

CySEC

570. Like the CBA and ICPAC, CySEC requires remediation of breaches detected during an on-site inspection in the form of compliance with an action plan.

571. If the findings of the on-site inspection are deemed "serious" or "repeated", the case is presented to the Board, which reviews the case and decides whether or not to call the entity for a written and if necessary oral representation. Depending on the information provided by the entity, the Board may impose any administrative sanctions.

[80] Number of follow-up inspections that were carried out: 0 (2013); 0 (2014); 0 (2015); 1 (2016); 1 (2017); 35 (2018). Typical examples of serious deficiencies leading to earlier follow-up inspections: (a) no documented background screening of clients; (b) inadequate documentation of source of wealth of PEPs; (c) repetitive findings in the follow-up inspections without any improvement; (d) systematic weaknesses.

572. If the findings are not deemed "serious" or "repeated", all identified deficiencies are included in a warning letter sent to the entity with the requirement to take specific minimum corrective measures within a predefined maximum time frame. Within two weeks of receipt of the warning letter, the entity shall inform CySEC of the corrective measures it intends to take and the time frame within which the said measures shall be concluded. This is done by submission of a "Declaration of Intention to Comply" that has to be signed by the Board of Directors and is accompanied by a table of rectifying measures. If the AML/CFT Department of CySEC confirms their adequacy, a signed "Compliance Confirmation" by the Board of Directors must be submitted to CySEC.

573. In case of non-compliance with the corrective measures with the time frame specified, the matter is brought before the Board of CySEC. The corrective measures are usually followed up at the next ordinary on-site inspection. Follow-up inspections where the implementation of the corrective measures is specifically reviewed and at an earlier stage are undertaken if CySEC finds that this is necessary due to the seriousness, systemic nature or possible impact of deficiencies.

574. As indicated in the table 34, CySEC has issued warning letters in several cases. Additionally, CySEC has withdrawn one licence of an ASP due to breaches of the Administrative Services Law and the AML/CFT-Law (violation of reporting obligations). So far, administrative fines have been imposed in only 2 cases, with a total amount of EUR 36,000. While warning letters are a call for mandatory correction, CySEC should ensure that they are an effective sanctioning instrument, i.e. entities not complying with the action plan must be appropriately sanctioned (e.g. by imposing monetary fines) when the same deficiencies occur on another occasion.

575. Moreover, CySEC does not have a formal sanctions application policy in place containing a clear list of criteria to determine what constitutes "serious", "repeated" or "systematic" AML/CFT breaches and what type and level of administrative sanctions can be imposed accordingly. On the basis of the case examples, it appears that there is a tendency to classify breaches as not being serious or repeated and accordingly, granting regulated entities the opportunity to remedy them on the basis of an action plan. It is unclear what precise threshold needs to be exceeded for a deficiency to be considered "serious" or "repeated.

576. The current consensual approach applied by CySEC to AML/CFT supervision is not sufficiently adequate, and it is not clear that CySEC is willing to impose effective, proportionate and dissuasive sanctions.

Estate Agents Registration Council

577. No sanctions have ever been imposed against real estate agents for AML/CFT breaches. The FIU, as a former supervisor, and the Estate Agents Registration Council, as the current supervisor, have not made use of the available range of administrative sanctions nor have issued any warnings to supervised entities.

578. This might be due to the very low number of on-site inspections, but the assessment team also has concerns about the quality of on-site inspections. Supervisory findings show that no AML/CFT deficiencies have been identified during the onsite inspections. The FIU (former supervisor) reported that during inspections conducted by the FIU it was determined that the real estate agents keep transactional records for accountancy purposes only. Thus, the FIU recommended that they keep a second copy for AML/CFT files.

Casino Commission

579. So far, the Commission has conducted 1 specific desk-based review focusing on the checks of AML policies of the casino operator. This review revealed certain deficiencies that resulted in specific licence conditions being imposed in December 2018 and which required a special AML review by a professional third party, covering not only technical framework of AML/CFT controls but also practical implementation of controls.

580. The special AML review was completed in May 2019 and identified certain deficiencies.

Despite the fact that some of those deficiencies were the same as identified during the initial review process carried out by the Commission, no sanctions were imposed on the casino operator. The Casino Commission will now request an action plan including corrective measures and only in case of non-compliance with the action plan, sanctions (e.g. monetary fines) may be imposed by the Commission.

581. According to the Commission, it will not proceed with the applications for further satellite casinos until the deficiencies are remedied. While this might be seen as a type of sanction, it is not clear why the Commission has not imposed administrative sanctions such as a monetary fine. The Commission has not yet adopted a sanctions application policy.

### *6.2.5. Impact of supervisory actions on compliance*

582. As indicated in IO.1, the risks in the banking sector have reduced significantly since the global and economic crisis. This is due in very large part to strategic decisions taken by the CBC to take strong counter measures to mitigate the risks in the sector, these risks being identified during the crisis, the NRA process and day to day supervision. This strategic approach and supervision, and the linked reduction in risks in relation to both market participants and their customer bases, have taken place since before the beginning of the period under review in this report.

583. The risks in the ASP sector have also reduced and are mitigated in a better way since the global economic and financial crisis. This is due to the introduction of the Administrative Services Law, the imposition for all ASPs to comply with AML/CFT obligations, the establishment of ASP and trust registers, the evaluation of the results of the Troika Special Assessment and the NRA process. However, the risk reduction and mitigation cannot be compared with the extent as in the banking sector. The business of ASPs appears to have recovered after the economic crisis and is corroborated by an increase of new registrations of legal persons and arrangements up until 2018 and increasing numbers of ASP licence holders.

*FI Supervisors*

584. All three FI authorities have been able to demonstrate they have made a positive difference to the level of compliance by the sectors they supervise.

CBC

585. The CBC's responses since the special assessment have had a significant positive effect on banks. Business relationships have been reviewed; risks have reduced significantly (with some relationships being terminated); the quality of introducers has been reassessed, the number has reduced markedly and the quality of introducers has improved; risks are better understood; business risk assessments have improved; anti-money laundering compliance officers are in a stronger position and now prepare customer acceptance policies; these officers are consulted before high risk customers are accepted or when there is a change in risk rating; compliance departments are providing good quality advice; banks are routinely seeking reports from private sector companies on high risk customers; CDD, monitoring and other measures have improved; complex risks and accumulation of risks are much better understood and addressed; training programmes have improved with specialised training now being provided; training budgets have increased significantly; internal audit has improved; and governance has improved. Compliance cultures have altered and there has been significant investment in compliance; compliance and internal audit departments have grown in size, importance and ability. STRs have increased in number and improved in quality. In addition, banks' interactions with the CBC are more sophisticated. Correspondent banks have also advised the CBC that they have noted significant improvements in compliance culture and better information flows.

CySEC

586. CySEC has found during its onsite inspection programme that there has been significant improvement in licensees' procedures, countermeasures and corporate governance, with significant good practice developed by firms across the range of procedures and countermeasures.

In addition, compliance teams have grown in size and become stronger as a result of CySEC's supervision. Training programmes have improved, including participation at training by compliance staff. Internal audits have also improved.

ICCS

587. The quality of STRs has improved, as has the quality of internal treatment and record keeping within insurers of whether an unusual situation might be suspicious. In addition, insurers have better quality statistics and internal reports and more robust corporate governance, level of compliance and procedures. Moreover, insurers have enhanced IT systems and monitoring as a result of proactivity by the ICCS.

*DNFBP Supervisors*

588. Most of the DNFBP supervisors were able to demonstrate that they have made some form of impact on the level of compliance as a result of their supervisory practices. This is supported by statistics of supervisory findings, consolidated information on the basis AML/CFT off-site returns and several case studies.

589. The CBA provided statistics on the level and quality of compliance by regulated entities with AML/CFT requirements for the years 2015 to 2018. These statistics show a substantial improvement e.g. in terms of AMLCOs' training (which is mandatory for this position) and training of other staff involved in AML matters, a substantial decrease in reliance on third parties (from 42 % in 2015 to 17 % in 2018), a slight improvement in the implementation of a proper risk-based approach, a better application of identification and verification obligations and improvements with regards to transaction monitoring.

590. Despite the improvements that have been observed by the CBA, the statistics show that there are still some significant weaknesses and deficiencies that need to be remedied. In 2018, results of on-site inspections show that there are still regulated entities which, for instance, do not monitor any transactions and cases where the source of wealth is not verified with appropriate supporting documentation.

591. ICPAC identified significant weaknesses in the proper documentation of KYC and the quality of compliance with AML/CFT obligations in the initial on-site visits of 2015. Regulated entities demonstrated varying levels of compliance in relation to internal procedures and policies, the application of a risk-based approach and KYC obligations. Following the publication of various guidance notes and circulars, a number of seminars delivered to supervised entities, and the offer to use online screening tools for a reduced price, ICPAC has observed an improvement in regulated entities' level and quality of compliance. In 2018, negative findings regarding KYC obligations and monitoring reduced by half, and fewer instances of insufficient documentation were found. Furthermore, there has been a significant improvement in the screening of customers against PEP and TFS lists, with an increase from 28 % of entities using online screening tools (as opposed to manual checks) in 2015 to 70 % in 2017. Additionally, ICPAC has observed a decrease in reliance on third parties; such reliance has dropped from 44 % in 2015 to 17 % in 2018. However, weaknesses still remain in some areas, such as the obligation to keep proper CDD documentation. In addition, ICPAC has noted that the overall compliance with the obligation to submit an AMLCO Report and an AML Questionnaire is very high with only 3 to 4 % of non-compliance. In cases of non-compliance, monetary fines were imposed, and reprimand letters were sent.

592. CySEC regularly publishes material on common weaknesses and deficiencies identified in on-site inspections which are brought to the attention of all regulated entities by using circulars published on the CySEC website. The most recent circular on common weaknesses/deficiencies and good practices is circular no. C314, published on 7 May 2019. This circular, referring to the results of the on-site inspections of 2017 and 2018, indicates an overall improvement in the internal systems, controls and procedures applied by the regulated entities. However, in addition to the good practices identified, CySEC identified common weaknesses and deficiencies (e.g. in some instances there was insufficient documentation of source of funds and source of wealth in the

economic profile, lack of accurate information on the customers' main business activities, inadequate application of the risk-based approach).

593. Based on the assessment of the annual AMLCO Reports and the Internal Auditors' Reports, CySEC observed that the said publications were duly taken into account by regulated entities and that the level of compliance increased. In addition, CySEC publishes its findings of the assessment of AMLCO Reports and the Internal Audit Reports through a circular. Circular no. C307, published on 28 March 2019, identified an overall improvement in the content of the reports. However, CySEC also identified some common and recurring weaknesses (e.g. in some instances there was insufficient analysis of the specific method of conduct of inspections and reviews performed by the AMLCO, no or limited information provided by ASPs in relation to the country of origin and type of high-risk customers).

594. The Estate Agents Registration Council (and the FIU as former supervisor of real estate agents) could not demonstrate that supervisory efforts so far have had an effect on the level and quality of compliance by estate agents.

595. The Casino Commission pointed to the one-to-one relationship between the casino operator and the first on-site inspection as well as the special AML review that have been conducted recently. The Commission will further engage strongly with the operator in order to enhance the level and quality of compliance to a satisfactory extent.

596. Apart from the positive impact that most of the DNFBP supervisors have noted, the overall low numbers of on-site inspections of DNFBPs and the very low number of sanctions issued so far remain a concern. Moreover, the fragmentation of ASP supervision has resulted in some differences regarding supervisory approaches and practices that require harmonisation to ensure an equal level playing field of ASP supervision.

#### *6.2.6. Promoting a clear understanding of AML/CFT obligations and ML/TF risks*

*FI Supervisors*

597. All three FI supervisory authorities have promoted a clear understanding by FIs of their obligations. They have pointed to the value of directives, circulars and guidelines issued and of the onsite inspection process. Offsite information requested also promotes understanding as do websites and responses to bilateral queries made by firms. The supervisory authorities have also engaged the private sector with the NRA process. There is some scope to enhance the TF elements of outreach programmes (see R.34 and IO 4).

CBC

598. The CBC places particular importance on the training of staff. It has organised seminars on legal and regulatory obligations, sanctions, TF, emerging risks and good and bad examples noted at onsite inspections. It also meets monthly with AMLCOs of banks which, inter alia, allow information on typologies and trends to be disseminated. The CBC has devoted significant effort to assisting AML/CFT units to improve their role and status within banks.

CySEC

599. CySEC also focuses to a great degree on training of staff. There are compulsory educational requirements for senior staff in specified positions such as money laundering compliance officers and senior managers. CySEC has held seminars (7 in 2017 and 10 in 2018) for authorised entities, albeit focussed to some extent on those staff subject to educational requirements.

ICCS

600. The ICCS has participated in training events held by the CBC, the World Bank, ICPAC and private sector firms. It considers the small size of the sector and its positive relationship with the ICCS as facilitating the sector's contact with it where there are issues.

*DNFBP Supervisors*

601. Most of the DNFBP supervisors promote the understanding of ML/TF risks and AML/CFT obligations to the private sector through feedback and guidance as well as training seminars.

602. CBA presents common deficiencies and weaknesses as well as best practices during training seminars that are offered on an annual basis. Moreover, the CBA has issued and circulated various Directives and Guidelines. However, the AML Directive as the most fundamental publication for the private sector was not updated at the time of the on-site visit[81] and therefore, did not take into account the amendments to the AML/CFT-Law. In addition to the annual training seminars on common deficiencies and weaknesses, the CBA has conducted training seminars together with the FIU (8 seminars in the period from 2014 to the beginning of 2019) to enhance understanding of reporting requirements thereby increasing the quality of STRs. In this regard, the CBA requires AMLCOs to receive at least 6 hours of AML-related training a year. Additionally, the CBA has notified the regulated entities of the results of the NRA by forwarding the concise version of the NRA Report. The CBA stated that it also participates in meetings with other supervisors in order to achieve consistency regarding licensing, monitoring and supervision. According to the CBA, so far, it has participated in 3 meetings with ICPAC and CySEC and a further 3 meetings with ICPAC.

603. ICPAC has issued a number of circulars and guidance notes on amendments to laws and regulations, best practices and AML/CFT obligations on its website. A very positive example is the Practice Guide for ASPs that ICPAC has issued in order to provide an overview of best practice procedures when providing administrative services. ICPAC's AML Directive has been revised to reflect the amendments of the AML/CFT-Law. According to ICPAC, a meeting was held with the CBA and CySEC in July 2018 and another meeting with only the CBA in April 2019, where elements of the AML Directive were discussed and views on interpretation of certain provisions were exchanged. Additionally, common deficiencies and weaknesses as well as best practices identified in the AML, Rules and Regulations monitoring visits are presented on an annual basis and the presentations are available on ICPAC's website. The results of the NRA were circulated by ICPAC to its members to ensure a common understanding of ML/TF threats and vulnerabilities. ICPAC offers a number of training sessions on an annual on-going basis. These training sessions are available for all members. ICPAC requires the AMLCOs to receive a minimum of 10 hours of AML-related training a year. ICPAC also intends to introduce an obligation for AMLCOs to pass a written examination as foreseen in the NRA Action Plan.

604. CySEC has developed and established various communication channels with the private sector. In particular, it publishes a variety of circulars on an on-going basis to communicate amendments to the relevant legislation and further developments in the AML/CFT area. In addition, CySEC issues circulars on common and recurring deficiencies and weaknesses as well as best practices identified during on-site and off-site monitoring. The AML Directive has been updated recently in order to reflect the amendments of the AML/CFT-Law of 2018. Moreover, the outcome of the NRA has been communicated to the regulated entities through publication of a circular. This circular refers to the AML/CFT-Law and the Risk Factors Guidelines according to which regulated entities must take into account the NRA results when assessing ML/TF risks. In addition, CySEC provides targeted AML/CFT training seminars on a regular basis (7 seminars in 2017 and 9 seminars in 2018). The AMLCOs of ASPs are required to achieve at least 10 hours of AML-related training a year. Furthermore, CySEC has launched a project which will introduce the obligation for AMLCOs to pass a written examination shortly.

605. Despite individual actions taken by the three supervisors, there is a need to communicate harmonised industry standards to market participants.

606. The RE Council has recently published a Directive on the prevention and suppression of ML activities and the financing of terrorism laws. A training session for estate agents was organised in 2014 and another training seminar was conducted in 2015. Apart from those 2 seminars that were organised by the FIU, no further outreach activities were carried out such as the publication of

[81] The AML Directive has only been updated in September 2019.

circulars, for example, on common deficiencies and weaknesses or the results of the NRA, training seminars or regular meetings with the private sector, etc.

607. The Casino Commission has established a one-to-one relationship with the casino operator and communication of relevant AML/CFT matters is done on a bilateral and regular basis.

608. The DNFBP supervisors have been proactive in promoting a better understanding of AML/CFT obligations by conducting trainings, issuing directives and other types of guidance notes. However, supervisory directives contain little guidance on how to identify TF (see Rec. 34). Also, as noted in IO 4, some DNFBPs expressed a need for more supervisory guidance.

*Overall conclusions on IO.3*

609. **Cyprus is rated as having a moderate level of effectiveness for IO.3.**

## 7. LEGAL PERSONS AND ARRANGEMENTS

**Key Findings**

1. The authorities understand that Cyprus, as a company formation and administration centre, is exposed to ML/TF risks associated with legal persons created in the country. However, given that the country has not formally identified and assessed those risks, the precise nature and extent of the risks are not yet fully understood. This reduces the authorities' ability to implement mitigating measures which specifically target identified risks.

2. As a result of a campaign undertaken by the DRCOR, the quality of basic information contained in the registry has increased significantly. Nevertheless, since the second part of the campaign has not yet been finalised, basic information for around 63,000 companies (out of 215,346) remains inaccurate and out-dated. This has an impact on the availability of accurate and current basic information to competent authorities.

3. As a way of ensuring transparency of non-resident owned/controlled legal persons and legal arrangements, which pose the highest ML/TF risk, Cyprus uses a combined approach: (1) implementing a regulatory and supervisory framework for ASPs for both prudential and AML/CFT requirements; (2) imposing a requirement for non-resident owned/controlled legal persons or legal arrangements to engage the services of an ASP licensed and resident in Cyprus; and (3) placing an obligation on the ASP to obtain and hold adequate, accurate and current BO information on such legal persons/arrangements.

4. Significant efforts were made by the supervisors to establish a comprehensive ASP regulatory and supervisory framework, which have resulted in an increased level of compliance by the ASP sector and improved the quality of BO information maintained by them. However, as discussed under IOs 3 and 4, further progress is required, with certain areas requiring major improvement.

5. In addition, there is no comprehensive mechanism in place to verify that the requirement to engage the services of a Cyprus-licensed ASP is applied for all non-resident owned/controlled legal persons/arrangements.

6. A positive measure taken by Cyprus in relation to trusts is the establishment of a trust register, which contains details of all trusts governed by Cyprus law and is available to competent authorities.

7. As an additional safeguard, a requirement was introduced for banks to meet the BO in person where the customer is a legal person with nominee shareholders, a trust or the customer relationship is introduced. This requirement has been implemented effectively by banks.

8. In order to obtain BO information, competent authorities mainly rely on information maintained by ASPs and banks in accordance with Recs. 10 and 22. The authorities have adequate powers, described under R. 29 (for the FIU) and R. 31 (for the Police), which ensure timely access to information.

9. Reliance by competent authorities on BO information maintained by ASPs, which are seen as the primary repository of BO information, may be problematic for two reasons: (1) the application of BO-related requirements by ASPs was not uniformly convincing; and (2) there are some concerns about the effectiveness of supervision of ASPs. This constitutes a gap in transparency of BO information of legal persons/arrangements.

10. This gap is to some extent mitigated where the legal person/arrangement holds a bank account with a bank in Cyprus. Banks were found to apply BO-related requirements soundly.

11. Adequate sanctions have been imposed for the late or non-submission of annual returns. No dissuasive or effective sanctions have been issued under the AML/CFT Law for violations of BO

information requirements or other related requirements under the Administrative Services Law.

**Recommended Actions**

1. Cyprus should conduct a formal and comprehensive risk assessment of legal persons created in Cyprus to determine the risks associated with the various types of legal persons, taking into account all relevant information available within the country. On the basis of the risks identified, more targeted mitigating measures should be undertaken.

2. Cyprus should enhance existing measures to ensure that BO information on legal persons/arrangements created in Cyprus is obtained consistently by all ASPs so that the information held is adequate, accurate and current.

3. Cyprus should implement a mechanism to verify that the requirement to engage the services of a Cyprus-licensed ASP is applied for all non-resident owned/controlled legal persons and legal arrangements.

4. Cyprus should ensure that effective, proportionate and dissuasive sanctions are imposed for failure to comply with BO requirements and other relevant requirements under the Administrative Services Law.

5. The DRCOR should expeditiously complete the striking-off process of the remaining 63,000 companies.

610. The relevant Immediate Outcome considered and assessed in this chapter is IO.5. The Recommendations relevant for the assessment of effectiveness under this section are R.24-25.[82]

## *7.1. Immediate outcome 5 (legal persons and arrangements)*

611. An overview of the type and number of legal persons and arrangements that are registered in Cyprus is provided under Chapter 1. For the purposes of this Immediate Outcome, societies, federations and associations (see Rec. 8) are considered as other types of legal persons (see footnote 69 item 3 of the FATF Methodology), while institutions and charities (see Rec. 8) are considered as legal arrangements.

612. Cyprus is a trust and company formation and administration centre – a sizeable portion of its legal persons and arrangements are managed by ASPs on behalf of non-residents and feature in international corporate structures. The authorities estimate that between 20 to 30% of all Cypriot-registered legal persons are beneficially owned/controlled by non-residents mainly from Greece, the Russian Federation, Switzerland, Ukraine and the United Kingdom. However, this estimation relies on data held by the CBC in relation to the share of non-resident BOs of total deposits and does not take into account those Cypriot legal persons which have bank accounts outside of Cyprus. The percentage is therefore likely to be higher.

613. As noted under Chapter 1, the number of new Cypriot companies reduced dramatically between 2012 and 2013 as a result of the financial crisis. The business increased slightly during 2014 and 2015, exhibiting some further growth thereafter up until 2018 with a downturn from 2019 onwards.

614. While trust business is also offered in Cyprus, it is less developed than the business of company formation and administration. The sector is therefore considered less material in terms of ML/FT risks.

[82] The availability of accurate and up-to-date basic and beneficial ownership information is also assessed by the OECD Global Forum on Transparency and Exchange of Information for Tax Purposes. In some cases, the findings may differ due to differences in the FATF and Global Forum's respective methodologies, objectives and scope of the standards.

*Legal persons*

615. The most material type of legal person in Cyprus is the private company limited by shares, both in terms of volume and risks – private companies limited by shares constitute 94 % of all legal persons and are the preferred choice of corporate vehicle chosen by non-residents to structure and manage their assets. The focus of this immediate outcome is on these types of legal persons and reference to legal persons in this chapter is mainly intended to capture this category.

616. When assessing mitigating measures to ensure availability of BO information in Cyprus, the assessment team distinguished between (a) legal persons administered by an ASP; and (b) legal persons which are not administered by an ASP.

617. The first category captures those legal persons whose legal owner and the BO is not the same person. These are the riskiest types of legal persons. In most cases, they are beneficially owned and/or controlled by non-residents. They generally form part of international corporate structures or are stand-alone asset management vehicles e.g. for tax planning. Availability of BO information of this type of legal person in Cyprus relies on the ASPs administering the legal person and, where the legal person maintains an account in Cyprus, from banks. The exact percentage of legal persons which are under ASP management is not known. It is also not known how many of these legal persons do not have a bank account in Cyprus.

618. The second category comprises those legal persons that conduct commercial, trading or entrepreneurial activities in Cyprus. In these legal persons, the director/secretary of the legal person owns at least 25% of the legal person and the share capital is not held on behalf of third persons[83]. Since they do not feature nominee shareholders, the legal owner and the BO are the same. ASPs do not act as directors or secretaries in these legal persons. Information on the legal owner/BO would be available from the legal person itself or at the registry maintained by the DRCOR. BO information could also be obtained from banks, where the legal person holds a bank account in Cyprus.

619. In 2018, Cyprus introduced provisions in the AML/CFT Law which provide the legal basis for the setting up of a BO registry. These provisions, which are found under Sec. 61A, require legal persons to obtain and hold adequate, accurate and current BO information and for that information to be held in a registry. At the time of the on-site visit, arrangements had been initiated to set the registry up. This mechanism was, therefore, not taken into consideration for the purpose of this analysis. The authorities aim to have the register in place by 10 January 2020.

*Legal arrangements*

620. The most material type of legal arrangement is the trust. There are 3,996 trusts governed by Cypriot law. Of these, 3,877 are likely to have an international element, e.g. non-resident settlor, beneficiary, etc. and are required by the Administrative Services Law and the International Trusts Law to have at least one licenced trustee who is a Cyprus resident. The other 119 trusts are family trusts i.e. the trustee or family members are the settlor or beneficiaries of the trust. These trusts do not require the services of a licenced trustee. For all trusts, trustees must obtain and hold BO information on the trust pursuant to the AML/CFT Law. Reference to legal arrangements in this chapter is primarily intended to capture trusts.

### *7.1.1. Public availability of information on the creation and types of legal persons and arrangements*

621. Information on the creation of the various types of legal persons in Cyprus is publicly available. Details on the different types of legal persons (i.e. companies, overseas companies, partnerships[84] and SEs) and how each can be incorporated are described on a website[85] of the

[83] The ASP Law lists the situations where a legal person need not be administered by an ASP (Article 4(3) of the ASP Law).

[84] According to the Partnerships and Business Names Law, general and limited partnerships are not considered as legal entities. However, for the purposes of this assessment partnerships are subsumed under

Cyprus government. The website also contains all the necessary forms that are required for the creation of a legal person and any changes thereafter (e.g. change in directors, shareholders, registered address, etc).

622. No information on the creation of trusts has been made available by the authorities to the public. The authorities argue that this type of information would usually be obtained directly from the trust provider. Furthermore, a significant amount of information on the characteristics of Cyprus trusts can be obtained from open source searches on the internet.

623. Societies, institutions, federations and associations are registered by one of four District Officers of the Republic of Cyprus depending on where the registered office of the entity is located. Information (in Greek) on how these arrangements can be established and the legal basis for registration is provided on the website of the MoI[86]. Information (in Greek) on registered entities is publicly available on a website of the MoI[87]. A list of approved charities in Cyprus is maintained (in Greek) on a website of the MoF[88].

624. In addition, a publicly-accessible general database containing the entire legislation of Cyprus can be found on www.cylaw.org (free of charge and in Greek). Furthermore, access to official translations in English of various pieces of legislation, including laws for incorporation/registration of legal persons and arrangements, can be found on the website of the Office of the Law Commissioner[89].

### *7.1.2. Identification, assessment and understanding of ML/TF risks and vulnerabilities of legal persons*

625. While Cyprus has not formally identified and assessed the risks posed by legal persons created in the country, the authorities understand that, as an international company formation and administration centre, Cyprus faces a heightened risk of legal persons being misused for ML/TF.

626. The competent authorities understand that Cypriot legal persons whose BOs are non-resident, and which do not conduct any underlying business in Cyprus are inherently vulnerable to misuse. This understanding derives from supervisory practices, cases investigated by the FIU and the Police and information gathered through the implementation of the action plan agreed with the Troika Institutions based on the 2013 Special Assessment. Knowledge of risks is also evident from corresponding risk mitigation measures (see section 7.1.3 of this Chapter) that have been undertaken by the authorities.

627. The authorities are aware that the majority of financial flows in and out of Cyprus are conducted through stand-alone asset-management vehicles or legal persons forming part of an international corporate structure. An analysis[90] of complex structures found that these are generally characterised by the presence of nominee shareholders with an average of three levels or layers of intermediary BOs, four or more individuals involved in the ownership structure and an average of three countries of residence or incorporation.

628. The most common types of activities of non-resident owned legal persons are known to be holding companies, shipping and investments. Higher-risk features such as nominee shareholder arrangements and professionals acting as directors are available and widely used[91]. The authorities

---

the definition of "legal persons" (cf. FATF Guidance on Transparency and Beneficial Ownership, October 2014, page 12).

[85] http://www.businessincyprus.gov.cy/mcit/psc/psc.nsf/All/A2E29870C32D7F17C2257857002E18C9?OpenDocument

[86] http://www.moi.gov.cy/moi/moi.nsf/page61_gr/page61_gr?OpenDocument

[87] http://www.moi.gov.cy/moi/moi.nsf/All/EB27634CFA8868DAC2257B5D002CAF58?OpenDocument

[88] https://www.mof.gov.cy/mof/tax/taxdep.nsf/charity_gr/charity_gr?openform

[89] http://www.olc.gov.cy/olc/olc.nsf/dmllegislation_en/dmllegislation_en?OpenDocument

[90] Conducted as part of the 2013 Special Assessment

[91] According to figures provided by the CySEC, the CBA and the ICPAC, a majority of clients of ASPs receives directorship services provided by ASPs.

understand that, while legal persons with nominee shareholder arrangements are generally set up for tax purposes, they are inherently risky. Certain trends in the corporate sector have been observed, such as, for example, a decrease in company registrations following the 2013 economic crisis in Cyprus (see the section on 'Legal Persons' under Chapter 1).

629. Following the 2013 Special Assessment, a number of risks relating to legal persons using the banking system were identified. It was determined that economic profiles of legal persons maintained by banks were not detailed enough. Excessive reliance was placed by banks on third parties to provide information on companies with complex ownership structures and legal arrangements. The complexity of legal persons added to the ML/TF risks taken by banks.

630. Risks were identified by the Troika Institutions and the Cypriot Authorities as part of the Economic Adjustment Programme, which included a review of the system regulating legal persons. It was found that details of a number of companies were not up-to-date as annual return forms were not being promptly submitted and, to a lesser extent, due to a backlog in the processing of documents. This gave rise to some transparency issues for legal persons. Risks were also identified in relation to some legal persons and arrangements which were managed by persons not subject to licensing and supervision.

631. In the wake of the Panama Papers revelations, the ASP supervisors issued circulars[92] requesting obliged entities to report any connection with the Panamanian law firm in question with a view to, *inter alia,* understanding the related risks and taking supervisory and investigatory measures. A number of connections to obliged entities or their customers were identified and reported to the supervisors and the FIU. This prompted supervisory actions to ensure that legal persons and arrangements were not misused for criminal activity. A similar examination of risks relating to the involvement of Cypriot legal persons in the Laundromat cases has not been conducted by all ASP supervisors.

632. Despite these various strands of risk understanding, in the absence of an in-depth and more comprehensive risk assessment, Cyprus does not yet have a complete picture of the corporate landscape and the manner in which legal persons created in the country can be misused. For instance, the following factors, which are likely to increase the ML/TF vulnerability of legal persons, are not known to a precise extent: (1) the number and proportion of legal persons beneficially owned or controlled by non-residents and countries in which those non-residents are based; (2) the percentage of Cypriot legal entities forming part of a corporate chain and the types or nationalities of companies or legal arrangements that Cypriot legal entities are most frequently associated with; (3) the extent to which nominee shareholder arrangements have been subject to abuse; (4) the number of legal persons owned or controlled by non-residents which do not hold bank accounts in Cyprus; (5) the use of bearer shares or bearer share warrants issued by foreign companies forming part of corporate chains with the involvement of Cypriot companies; and (6) the types of legal persons that are most frequently used in criminal schemes. The absence of such a risk assessment is deemed by the assessment team as a significant shortcoming given the materiality of legal persons in the context of Cyprus and diminishes the ability of the competent authorities to undertake mitigating measures which specifically target identified risks.

### *7.1.3. Mitigating measures to prevent the misuse of legal persons and arrangements*

*Measures relating to basic information*

633. The database of the DRCOR includes current and historical information on legal persons. Information on current directors and registered address can be retrieved online and free of charge on the website of the DRCOR. Access to full information (e.g. names of shareholders, historical information) is available for a flat fee of EUR 10 per legal person. The Police, the FIU, the CBC and the Tax Department have full free access. Any pending amendments to company information of

[92] ICPAC:https://www.icpac.org.cy/selk/newsandeventsdetails.aspx?id=1399&catid=1001;
CySEC:https://www.cysec.gov.cy/CMSPages/GetFile.aspx?guid=71e6fa79-c410-4204-8a8f-156824f56984 ;
https://www.cysec.gov.cy/CMSPages/GetFile.aspx?guid=99f45bf8-2460-45f7-a24d-819fe24e5029

which the DRCOR has been notified but have not yet been registered are indicated on the online platform, free of charge, to ensure that the public is aware of any pending issues.

634. Part of the action plan under the Economic Adjustment Programme of the Troika Institutions involved the complete reform of the DRCOR. Aside from an internal re-organisation, the action plan required the DRCOR to ensure that basic information on companies was made available and up-to-date. This involved identifying all the companies that had not filed annual returns and whose basic information was, therefore, out-dated. The DRCOR contacted non-compliant companies by means of a formal letter obliging them to file updated annual returns within a specified deadline. Upon the expiry of the deadline, a list of non-compliant companies was published in the Official Gazette of the Republic for a three month period for the purpose of alerting creditors of imminent strike off. Absent any claim by creditors, these companies were struck off the register and a notice was published in the official gazette.

635. By 2018, more than 68,000 companies had been struck off the register for failure to submit an annual return (by the end of 2018 there were 215,346 companies on the register). There remain around 63,000 companies whose strike off was suspended due to claims made by creditors, including public authorities such as the Tax Department and the Social Insurance Services. These will be subject to a renewed effort by the DRCOR to proceed with their strike-off. However, it does raise the issue of having a sizeable number of companies whose basic information is not up-to-date, albeit they are publicly identified as being under a strike-off procedure.

636. In addition to the cleansing of the register, the reform of the DRCOR also included a review of the legal, policy and operational framework and the setting up of a new IT structure for the registry. For instance, the powers of the Registrar have been enhanced and the sanctions for the late or non-submission of annual returns will be increased in the near future.

637. An electronic database was created by scanning the physical files of all active, registered legal persons. The process included the scanning of all documents/applications submitted to the DRCOR by the legal persons during the course of their existence. It did not include data extraction as the relevant data already existed in the database of the Register of Companies and consequently there was no need for data verification. The end result was the creation of an electronic file for every company. The physical files of 295,000 (companies, partnerships, overseas and business names) were scanned (more than 16m pages). The register is accessible to the public via the DRCOR's website by payment of a fee of EUR10 per legal person/entity. The process of creating and maintaining the electronic database is a continuous process.

638. In relation to other types of legal persons, as noted under core issue 5.1, societies, institutions, federations and associations are registered by one of four District Officers of the Republic of Cyprus depending on where the registered office of the entity is located. These entities are registered. On a yearly basis, they are required to submit audited financial statements and notify the Registrar of Societies and Institutions of certain changes (e.g. information of expulsion/registration of new members of societies, change in the address and contact details, whether minimum number of meetings stipulated in the Articles of Association was held, etc).

639. The Registrar is required to keep the information in the register up-to-date. The name and registration number of the legal person are published in the Official Gazette. The board of directors of a society is required to keep a fully updated register of its members, which shall be updated at least once a year and shall be available for inspection by the Registrar of Societies and Institutions and any other third party with a legitimate interest. Further information on these types of entities is provided under Rec. 8 and core issue 10.2.

*Measures relating to beneficial ownership information of legal persons*

640. The ASP regulatory and supervisory framework for both prudential and AML/CFT matters is seen by Cyprus as the main mechanism to ensure the transparency of non-resident owned/controlled legal persons, which as noted earlier pose the highest ML/FT risk. The framework was designed specifically for that purpose in consultation with and with the assistance

of the Troika Institutions as part of the Economic Adjustment Programme. The implementation of the programme was under close scrutiny by the Troika Institutions from its inception in 2012 to its completion in March 2016.

641. The framework was introduced through the enactment of the Administrative Services Law (ASL) in 2012. Pursuant to the ASL, any person intending to provide administrative services to a legal person, including acting as a director, nominee shareholder, company secretary or providing a registered address, is required to obtain a licence. Licensing and supervision are allocated to three different supervisors, the CBA, the ICPAC and the CySEC, depending on whether administrative services are provided by advocates, accountants or other professionals.

642. Crucially, the ASL requires all non-resident owned/controlled legal persons to engage the services of a Cyprus-licensed ASP – as a minimum the ASP must act as the company secretary of the legal person and must be a natural person resident in Cyprus[93]. Since ASPs are subject to AML/CFT requirements they are obliged to gather information on the BO of a legal person receiving administrative services. The three ASP supervisors monitor ASPs' compliance with both the requirements under the ASL and the AML/CFT Law.

643. The three ASP supervisors maintain an updated publicly-available register of all licensed ASPs, including their employees. This enables competent authorities, obliged entities and the public to identify in a timely manner the ASP acting as a shareholder/director of a company in a nominee capacity/trustee of a trust. ASPs are required to furnish updated information to the supervisors on an ongoing basis under pain of dissuasive sanctions[94].

644. The effectiveness of this mechanism relies heavily on a robust implementation of AML/CFT measures by ASPs and a well-functioning supervisory framework. Significant efforts have been made by the supervisors to establish a comprehensive supervisory framework, which efforts were under ongoing monitoring by the Troika Institutions until March 2016. This has resulted in an increased level of compliance by the ASP sector. However, as discussed under IOs 3 and 4, further progress is required, with certain areas requiring major improvement. In addition, there is no comprehensive mechanism in place yet to verify that the requirement to engage the services of a Cyprus-licensed ASP is applied for all non-resident owned/controlled legal persons. Some form of verification takes place as part of on-site visits by supervisors to ASPs but this process only affords limited coverage as only (a sample of) those legal persons under ASP administration will be subject to review.

*Measures relating to beneficial ownership information of legal arrangements*

645. The ASL and the International Trusts Law require that a trust governed by Cyprus law must have at least one trustee who is licenced and resident in Cyprus[95]. While it is positive that this requirement has been introduced, there is no mechanism to ensure that it is implemented in practice. This shortcoming is perhaps less material in the case of trusts than in the case of companies since trust business in Cyprus is less developed than the business of company formation and administration. The shortcoming is also to some extent mitigated since trustees wishing to maintain a bank account in Cyprus for a Cyprus trust are required to produce evidence of registration to the bank[96]. Registration can only occur if one of the trustees is licenced and resident in Cyprus.

646. The ASL also introduced the obligation for ASP supervisors to set up trust registers with respect to each trust governed by Cyprus law and where one of its trustees is a licenced entity resident in Cyprus and supervised by one of the said supervisors[97]. In addition, the CySEC keeps a

[93] The requirement to engage a licenced ASP does not apply if the director/company secretary of the legal person owns at least 25 % of the legal person and the share capital is not held on behalf of third persons.
[94] Section 26 of the Administrative Services Law
[95] Section 5 (2) of the Administrative Services Law and Section 2 of the International Trusts Law.
[96] Pursuant to the CBC Directive
[97] Section 25A of the Administrative Services Law.

register of those Cyprus trusts in which the trustee or family members are the settlor or beneficiaries (family trusts). The trust register contains the name of the trust, details of the trustees, the date of establishment of the trust, the date of any change in the law governing the trust; and the date of termination of the trust. Information in the register is available to competent authorities only. Cyprus is credited for undertaking this measure which is a step beyond standard international practice.

647. ASPs who manage and administer trusts are required to keep information on BO of the trust in Cyprus pursuant to both the ASL[98] and the AML/CFT Law. This information must be made available for disclosure to and inspection by the relevant authority at all times[99]. This obligation applies to all kinds of trusts, irrespective of the law they are governed by. In addition, it applies to family trusts where trustees are exempt from the licensing requirement. As in the case of legal persons, the availability of BO information on trusts depends on the adequacy of CDD carried out by ASPs. The same issues which reduce the level of effectiveness with respect to the transparency of legal persons also apply to trusts.

*Other measures*

648. In addition to the ASP framework as a main mechanism for risk mitigation, banks also have an important role in ensuring the transparency of Cyprus-registered legal persons/arrangements. As part of their CDD requirements, banks are obliged to determine who the BOs of a legal person/arrangement are, identify them and verify their identify. It should be underlined that this mechanism is only capable of mitigating risks insofar as the legal person/arrangement maintains a bank account with a bank in Cyprus. There is no requirement for all such legal persons/arrangements to do so and it is not known how many maintain bank accounts outside of Cyprus. There are indications that non-resident owned/controlled legal persons are increasingly seeking to open bank accounts outside of Cyprus.

649. In addition to the BO requirements under the AML/CFT Law, in 2016, the CBC introduced an important requirement for banks to personally meet the BO of customers that are administered by an ASP (or foreign equivalent third party). The measure was implemented in response to the findings of the NRA, which concluded that banks are particularly vulnerable to customers that are legal persons with nominee shareholders or trusts and customer relationships introduced by third parties. Although this measure was not intended to serve as a universal mechanism for the purpose of ensuring availability of BO information of all Cyprus-registered companies, it has had the indirect effect of providing additional safeguards.

650. The CBC requirement stipulates that banks must establish direct contact with the BO within a reasonable period of time, but not later than three months after the date of the account opening and before the execution of any transaction. The same applies when there is a change in beneficial ownership. A meeting with the third party introducing the customer to the bank or with persons directly or indirectly associated with the said third party or registered shareholders acting as nominees of the BO is not sufficient. The meeting may be held using online means provided that adequate safeguards such as sound and video recording of the meeting are in place.

651. In practice, this requirement has been applied consistently by the banking sector. As noted under IO 4, banks report that CDD includes preparation and retention of notes of face-to-face meetings with BOs of new customers that are legal persons/arrangements (or recordings of Skype conversations where BOs could not be physically present in Cyprus), with direct contact typically being made within a short period after opening new customer accounts, and in any event before executing any transactions for these new customers. The CBC confirmed that this requirement is applied stringently. Its application is being verified during on-site inspections.

[98] Section 3 (7) of the Administrative Services Law.
[99] Section 61B (1) of the AML/CFT-Law.

652. Another mitigating measure put in place by Cyprus is found under the AML/CFT Law, which contains an overarching provision criminalising the act of providing false or misleading BO information. Section 68(c) of the AML/CFT Law provides that in the event that the customer, or a person who is authorised to act on behalf of the customer, or a third person on whom the obliged entity relies for CDD purposes, knowingly provides false or misleading evidence or information for the identity of the customer or of the ultimate BO or provides false or forged identification documents, is guilty of an offence and, in case of conviction, is subject to imprisonment not exceeding two years or to a pecuniary penalty of up to EUR 100,000 or to both of these penalties.

While no person has yet been convicted of this offence, some cases have been identified by banks and reported to the FIU. The FIU, after having analysed these cases, disseminated them to the Police for investigation. One example is presented in the Box below.

**Box 5.1: investigation of false information on BOs**

An STR was submitted by a bank in Cyprus in relation to a company registered in Cyprus administered by an ASP in Cyprus. According to the information provided by the bank, the signatory of the account was a national from Country A and the declared UBO a national from Country B. A declaration of trust showing the UBO was provided to the bank. In April 2018, the bank was informed by the ASP that the UBO had changed and the new UBO was a national from Cyprus. The bank requested sale purchase agreements and proof showing the payment from previous to current BOs. The customers refused to provide the requested information. The financial analysis conducted by the FIU determined that the actual UBO of the company was a foreign national who had not been revealed to the bank. Further analysis indicated that the national from Cyprus, who had been indicated as the UBO, did not have sufficient means to purchase the company. It was also revealed that she had received income from the ASP administering the company. It was therefore determined that the ASP had intentionally provided false information in relation to the UBO in an attempt to conceal the identity of the real UBO. The case was disseminated to the Police for further investigation.

653. On bearer shares, it is noted that public companies limited by shares and listed on a regulated market may, if so authorised by their articles of association, issue share warrants to a bearer. These share warrants have characteristics that are similar to bearer shares. Before December 2012, this possibility also existed for other public companies. The Cypriot authorities indicated that a manual check of the files at the DRCOR was performed to check whether any of the existing public companies were, or had ever been, authorised to issue bearer share warrants. It was found that four companies were so authorised. These companies were visited by the Cypriot authorities, and it was confirmed that none of them had (ever) issued bearer share warrants. Considering that no bearer share warrants currently exist, and the possibility to issue them is limited to public companies limited by shares that are listed on a regulated market, the assessment team considers that potential risks arising from the use of bearer share warrants issued by Cypriot companies are effectively mitigated.

### *7.1.4. Timely access to adequate, accurate and current basic and beneficial ownership information on legal persons and legal arrangements*

*Access to basic information*

654. The competent authorities have direct and full access to all basic information kept by the DRCOR[100]. In practice, information is retrieved through a commercial company which supplements basic information on legal persons with additional information, such as whether the legal person is part of a corporate structure, the activities and financial health of the legal person, etc. It is clarified that the commercial company does not maintain a database on legal persons registered with the DRCOR. It accesses the DRCOR register and collects information directly from the DRCOR register upon each request.

[100] With respect to the information kept by the DRCOR and the access to that information for authorities, additionally, please see the remarks under 7.1.1.

655. As noted under core issue 5.2, there are currently 63,000 companies pending strike-off in relation to which basic information is not up to date. This has an impact on the competent authorities' access to accurate and current basic information. The assessment team acknowledges that the authorities are in the process of addressing this matter.

*Access to beneficial ownership information*

656. At the time of the on-site visit, competent authorities mainly relied on BO information obtained by ASPs and banks in accordance with R. 10 and R. 22 and acquired timely access by utilising the powers described under R. 29 (for the FIU) and R. 31 (for the Police). There are serious repercussions for ASPs and banks should they refuse to make information available upon request or should they disclose the fact that a request for information had been made by a competent authority. To the authorities' knowledge this has never happened. They emphasised that ASPs and banks are acutely aware of their obligation to co-operate with the authorities.

657. Both the Police and the FIU have presented numerous examples of requests to ASPs for BO information in the course of an investigation/analysis of STRs or in response to a request from a foreign counterpart. The assessment team had sight of sanitised versions of requests sent by the FIU and the responses by ASPs. This notwithstanding, the assessment team retains reservations about the availability of BO information maintained by ASPs for the reasons already mentioned under core issue 5.2 which are repeated here: (1) the application of BO requirements by ASPs was not uniformly convincing; and (2) there are concerns about the effectiveness of certain aspects of the licensing and supervision of ASPs.

658. Where a Cypriot legal person or arrangement holds a bank account in Cyprus, information is generally requested from both the ASP and the bank. Banks have adequate procedures in place to comply with their BO requirements. They also have systems in place which enable them to search their databases and furnish the requested information promptly. The information maintained by banks is broadly adequate, accurate and current (see CDD measures applied by banks under IO 4). This was confirmed by the FIU and the Police, who expressed satisfaction with the availability and quality of the information maintained, and by the CBC, which has not identified any major deficiencies when conducting on-site inspections. A case example is presented below.

**Box 5.2: Timely access to BO information by FIU**

The FIU received a request from foreign authorities in relation to proceeds of a predicate offence committed in Country A which were transferred to a bank account in Cyprus of a Cypriot company through a number of complex transactions. The BO of the company (residing in Country A) was unknown to the investigators of Country A since he was not among the primary suspects of the case. The FIU gathered BO information of the company from the bank in Cyprus and basic company information from the DCROC. This information, together with financial information, was provided to the foreign authorities initially via FIU to FIU co-operation and later on via an MLA Request. This led to the arrest and prosecution of the BO in Country A.

659. It is recalled that no precise data or estimates exist on the number of Cypriot legal persons/arrangements that are administered by ASPs, nor any data on the number of legal persons/arrangements that do not hold a bank account in Cyprus and in relation to whom access to BO information relies entirely on ASPs. The assessment team was, therefore, not in a position to quantify the extent to which accurate and current BO information on Cypriot legal persons may not be available in Cyprus.

660. For the sake of completeness of the analysis, it is noted that in relation to legal persons that are not administered by an ASP, BO information is accessed by competent authorities directly from the legal person or the DRCOR. As already stated in the introduction of this chapter, these legal persons do not feature nominee shareholders and the legal owner and the BO are the same. ASPs do not act as directors in these legal persons. BO information could also be obtained from banks, where these legal persons hold a bank account in Cyprus.

### *7.1.5. Effectiveness, proportionality and dissuasiveness of sanctions*

*Sanctions relating to basic information*

661. The DRCOR has taken significant measures in relation to legal persons which fail to submit or submit late annual returns. This has resulted in the imposition of effective and dissuasive sanctions. Sanctions amounting to over EUR 9.5 million were imposed during the period 2014 to 2018 for the late filing of annual returns by active companies (see Table 35). These measures have brought about an increase in the quality of information maintained by the DRCOR. In addition, by October 2018, more than 68,000 companies had been struck off the register for failure to submit an annual return.

**Table 35: Sanctions imposed for the late filing of annual returns**

| 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|
| EUR 3,016,020 | EUR 2,902,540 | EUR 1,471,760 | EUR 1,082,900 | EUR 1,034,060 |

*Sanctions relating to beneficial ownership information*

662. The statutory sanctions set out in the AML/CFT-Law for failure by FIs and DNFBPs to obtain and verify beneficial ownership information are relevant under IO 5. As noted under IO 3, the supervisors have issued very few sanctions for violations of the AML/CFT Law. The supervisors are of the view that so far no major problems have been identified with regards to the obligation to obtain and verify BO information. In some instances, obliged entities were found not to have gathered sufficient information on the economic profile of the customer, rather than failure to identify the BO. In this regard, consideration should be given as to how the lack of information on the customer's profile does in fact hamper the verification of BO information. The lack of application of dissuasive and effective sanctions under the AML/CFT Law is seen as a significant shortcoming and provides little incentive for the private sector, in particular, the ASP sector, to improve compliance.

663. There have also not been any sanctions in relation to other relevant requirements under the ASL. For instance, there have not been any sanctions for failure to appoint an ASP as a director/company secretary, failure to register a trust, failure to appoint a trustee for a Cyprus trust, provision of false or misleading BO information, etc.

*Overall conclusions on IO.5*

664. **Cyprus is rated as having a moderate level of effectiveness for IO.5.**

## 8. INTERNATIONAL COOPERATION

**Key Findings**

1. The Division for International Cooperation of the MJPO is an effective central authority for incoming and outgoing formal requests despite the fact that some of its processes are more informal in nature. It is positive that measures have been taken on occasion to clarify the procedure to be followed by foreign counterparts when requesting assistance, thereby expediting the process. However, the system could benefit from written guidance which is easily accessible to foreign counterparts.

2. Overall, Cyprus has been effective in executing requests in a timely and constructive manner in response to all types of formal requests from countries with which it cooperates most actively. The FIU has been instrumental in freezing and confiscating assets on behalf of foreign jurisdictions. Extradition requests have been processed effectively to extradite a number of high-profile, non-Cypriot fugitives wanted for prosecution in other countries. The Police have overcome challenges in responding to an increasing number of incoming requests by establishing the Office for the Execution/Handling of MLA Requests, which, however, is still in the process of removing a backlog of requests.

3. Cyprus has proactively sought legal assistance and extradition in relation to domestic ML and proceeds-generating offences committed in Cyprus with a foreign link. This has resulted in freezing and confiscation of assets abroad and assisted the Cypriot authorities in securing domestic convictions.

4. Since there have not been many investigations domestically concerning proceeds of crime generated outside of Cyprus and laundered in/through Cyprus (e.g. layering activities through banking transactions) international cooperation in these types of cases was sought to a much lesser extent. This is not in line with the type of threats that Cyprus faces as an IFC.

5. The FIU is generally effective in providing and seeking informal cooperation. Due to a heavy workload and limited human resources the FIU may not have always managed to meet the deadlines, particularly where the case involved the collection of significant volumes of information. On a positive note, the FIU spontaneously shares fully-fledged analysis products with foreign counterparts, which have been critical in assisting foreign counterparts in securing convictions and the seizure and confiscation of proceeds.

6. The Police, Customs and the supervisory authorities have mechanisms in place to provide and seek information informally in a swift, constructive and confidential manner.

7. Many incoming requests solicit information on basic and beneficial ownership since they involve legal entities registered in Cyprus. The authorities do not face any practical or statutory obstacles in providing this type of information and do so regularly.

**Recommended Actions**

1. The Office for the Execution/Handling of MLA Requests should, as a matter of priority, continue its efforts in clearing the backlog of pending MLA requests and ensure that timely and constructive assistance is provided in all cases going forward.

2. The Police should be more proactive in seeking MLA in relation to ML cases involving proceeds of funds in Cyprus originating from criminal activity outside of Cyprus.

3. The FIU should consider whether the current human resources to deal with international requests are sufficient to ensure that responses are provided in a timely manner in all cases. The

FIU should either enhance its existing case management system or install an automated system.

4. The International Cooperation Division at the MOJP is encouraged to develop more standardised and formalised operating procedures for the handling of MLA and extradition requests from non-EU countries including, but not limited to: (a) prioritisation criteria for the receipt of requests; (b) safeguards on confidentiality; (c) a more sophisticated case management system to monitor the progress of requests.

5. In order to further expedite cooperation, guidance on the process to be followed when seeking MLA and extradition should be made available publicly to assist non-EU foreign counterparts.

665. The relevant Immediate Outcome considered and assessed in this chapter is IO.2. The Recommendations relevant for the assessment of effectiveness under this section are R.36-40.

## *8.1. Immediate Outcome 2 (International Cooperation)*

666. As an IFC, Cyprus faces an elevated ML/FT risk of a cross-border nature, mainly emanating from layering activities through banking transactions. International cooperation is therefore very material in the context of Cyprus. While the Cypriot authorities have always endeavoured to extend the best possible assistance to their foreign counterparts, some operational aspects within the international assistance framework have posed challenges in the past. However, there has been an increased recognition across the board of Cyprus's critical role in assisting other jurisdictions in identifying and suppressing cross-border crime, including ML and FT. As a result, tangible efforts have been made to enhance the effectiveness of the system, which have already had a largely positive effect.

667. In assessing this Immediate Outcome, the assessment team considered the numerous case examples presented by Cyprus on international cooperation, statistics, discussions with the authorities during the on-site visit, the findings of the NRA (and its action plan), the AML/CFT National Strategy and the considerable feedback from countries in the Global Network on their experience in cooperating with Cyprus.

### *8.1.1. Providing constructive and timely MLA and extradition*

668. Cyprus displays characteristics of an effective system when providing international co-operation, particularly in the area of freezing and confiscation and extradition. In recent years, Cyprus has been able to render mutual legal assistance (MLA) and extradition in a constructive manner, especially with the top five countries with which it interacts most actively, which include both EU and non-EU countries.

669. The Ministry of Justice and Public Order (MJPO) is the central authority for the receipt of MLA (including European Investigation Orders (EIOs)) and extradition (including European Arrest Warrants (EAWs)) requests. Requests are transmitted by the MJPO to other domestic authorities for execution, depending on the nature of the request (except for requests dealing with Tax and Customs matters, that go directly to relevant authorities). The Police execute requests for the collection of evidence, such as bank information, etc. Requests relating to freezing and confiscation are executed by the FIU. Extradition requests and EAWs are executed by the Police and the Attorney General's Office. Requests may also be executed by the courts if these relate to the taking of testimonies on oath for cases the hearing of which is ongoing before a foreign court.

670. The number of MLAs and extradition orders received by the MJPO on criminal matters is presented in the table below.

**Table 36: Incoming MLA, EIO, Extradition and EAW requests**

| | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|
| **MLA requests** | 426 | 513 | 515 | 280 |
| **EIOs**[101] | - | - | - | 251 |
| **Extradition** | 10 | 15 | 14 | 16 |
| **EAWs** | 53 | 49 | 54 | 59 |
| **Total** | **489** | **577** | **583** | **605** |

671. The Division for International Cooperation within the MJPO is responsible for international cooperation with EU and third countries. It comprises 7 officers, 5 of whom deal with criminal cases. The authorities are of the view that the Division is suitably staffed in proportion to the number of requests received and the assessment team has not identified any issues in this respect. The representatives of the Division met on-site appeared to be very experienced and have sound knowledge of the legal framework in place governing international cooperation. All staff members receive regular training and participate in seminars and conferences both in Cyprus and abroad in the field of international cooperation in criminal law cases.

672. EIOs and EAWs, which since 2018 constitute roughly half of incoming requests, are handled in accordance with manuals and strict procedures (including timelines, prioritisation criteria and standardised response formats) issued at EU level. Requests from non-EU countries are handled according to a more informal, albeit relatively well-established, internal procedure. For instance, priority is assigned depending on the merits of the case based on the discretion of the case officers. There is no internal manual regulating the functioning of the Division, especially on matters dealing with confidentiality. Factors that are taken into account include the urgent nature of the request (as indicated by the requesting authority), the seriousness of the offence, the need to preserve evidential material, the likelihood of dissipation of assets or the risk of flight from the country. A more formalised and standardised procedure would further enhance the functioning of the Division, particularly since the number of incoming requests is on the rise.

673. As soon as a request is received by the Division, an acknowledgement is sent to the requesting authorities. For EIOs this is done within a week, while for other requests this is done as soon as reasonably practicable. The acknowledgement includes details of all contact persons in Cyprus involved in the execution of the request. The request is inputted in a database which operates autonomously from other systems within the MOJP. The database allows for swift retrieval of information on each case and is able to generate some statistics, though not on the nature of the offence. In parallel, the officers of the Division maintain an electronic system which includes information on the case, the file of the requesting authority, the date of receipt, the date the request is forwarded to the competent authority in Cyprus for execution, details of the legal and natural persons involved, the nature of the offence and the date the response is sent to the requesting country. Neither the database nor the electronic system appears to be sufficiently sophisticated to enable the authorities to automatically monitor progress on requests. In order to track the execution of a request, the officers of the Division will manually set a reminder to follow up on the request within three or four months of receipt, unless a reminder letter is received from the requesting authority beforehand.

674. According to Cyprus, some non-EU authorities may find it challenging to understand the process to be followed when seeking assistance from Cyprus. This is due to the fact that no external guidance has been developed by Cyprus to steer foreign authorities through the process, specifically with respect to freezing and confiscation. Nevertheless, it is to be underlined that, as a matter of good practice, in order to facilitate and speed up co-operation, Cypriot authorities have on a number of occasions visited countries (outside of the EU) with which they co-operate regularly to explain how the system functions. Similarly, meetings have been held with representatives from

[101] Cyprus implemented the EIO Directive in December 2017

embassies in Cyprus to discuss co-operation not only on specific cases but also on the general functioning of the system. Moreover, case officers will proactively seek to assist foreign authorities should the request not comply with the requirements of Cypriot law. There is also, to some extent, a practice of facilitating international cooperation through liaison officers. For instance, Cyprus has a liaison officer in Greece and has an agreement with Greece to make use of its own network of liaison officers. Foreign liaison officers in Cyprus are also asked to intervene in certain cases.

*Execution of MLA and EIO requests*

675. Requests are either received in the form of a MLA request when originating from non-EU countries or EIOs when sent by EU countries. The Police is in charge of executing requests for MLA and EIO relating to the collection of evidence, such as for instance, bank account information, witness statements, information on legal persons, interrogate suspects, search premises, etc. Although no statistics are maintained, the Police indicated that roughly two thirds of the requests relate to the production of financial records and assistance in identifying assets within Cyprus to aid investigations and asset recovery actions. The rest relate to more coercive actions such as search warrants, interrogation of suspects, etc. The Police have all domestic powers available to them under Cypriot legislation to process a foreign request. The police also utilise searches with central registries, such as the companies registry, land registry and registries on other property such as cars. The police have relatively convenient access to some of these registers and even direct access to others. Otherwise, the police may apply for production orders under the Criminal Procedure Law or disclosure orders under AML/CFT Law to seek the compulsory disclosure of information from banks and other institutions, or production orders to seek production of particular documents. As noted under IO 8, this is broadly an effective way to collect information.

676. The table below illustrates the number of incoming MLA requests broken down by nature of the offence. The large majority relate to ML and associated predicate offences, mainly of an economic nature. As expected, this is entirely in line with the risk profile of the country. The number of purely ML-related requests has been increasing. There have not been any FT-related requests. Requests for assistance most commonly come from Greece, Russia, Switzerland, Ukraine, the United Kingdom and the United States.

**Table 37: Incoming MLA requests (breakdown by nature of offence)**

| Offences | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|
| **Money Laundering** | 33 | 28 | 43 | 50 |
| **Money Laundering & Other Related Economic Crime Offences (Corruption, Fraud, Including Internet Fraud, False Pretences)** | 200 | 275 | 285 | 136 |
| **Drug Offences & Money Laundering** | 7 | 6 | 8 | 4 |
| **FT Offences** | 0 | 0 | 0 | 0 |
| **Other Offences** | 186 | 204 | 179 | 90 |
| **Total** | **426** | **513** | **515** | **280** |

677. The number of MLA and EIO requests received, executed, pending and refused are presented in Tables 40 and 41 respectively.

**Table 38: Incoming MLAs**

| Year | Received | Executed | Pending | Refused |
|---|---|---|---|---|
| **2015** | 426 | 420 | 1 | 5 |
| **2016** | 513 | 490 | 11 | 12 |
| **2017** | 515 | 350 | 158 | 7 |

| | | | | |
|---|---|---|---|---|
| **2018** | 280 | 75 | 201 | 4 |
| **Total** | **1,734** | **1,335** | **371** | **28** |

**Table 39: Incoming EIOs**

| Year | Received | Executed | Pending | Refused |
|---|---|---|---|---|
| **2018** | 253 | 244 | 0 | 9 |

678. The time taken to respond to MLAs and EIOs differs. There are set timeframes within which EIO requests must be satisfied. These timeframes are generally respected. With respect to MLAs, this generally depends on the type of assistance requested. The Police acknowledged that significant delays have been experienced in the past when executing MLA requests. They attribute the problem to limited resources at the Police, which have traditionally been allocated to the investigation of domestic cases rather than international assistance. This state of affairs has also had a negative impact on the quality of assistance provided. This matter was identified as a major vulnerability within the national system when the NRA was conducted and was the subject of discussions at senior governmental levels.

679. In response, the Office for the Execution/Handling of MLA Requests was created within the Police in order to expedite the execution of requests and improve the quality of the assistance provided. The Office comprises 15 members of staff, 12 of whom deal with the execution of requests. They were all previously involved in the execution of MLAs and EIOs and possess significant criminal investigation experience. It was stated that, on average, each officer executes 5 requests per month. Priority is given to EIOs with a 90-day time limit. Although the Office has only been operational since December 2018, statistics indicate that its existence has already started yielding results. At the time of the on-site visit, the Office was dealing with a backlog of 521 requests in addition to 235 new MLA/EIO requests which had come in since its inception i.e. a total of 756. In just 5 months, the Office had managed to execute almost half of the requests i.e. 387 (see Table 40 below).

**Table 40: statistics related to the Office for the Execution/Handling of MLA Requests**

| | |
|---|---|
| **MLAs & EIOs pending on the establishment of the Office** | **521** |
| **MLAs and EIOs received from date of establishment of the Office until the end of 2018** | **44** |
| **MLAs and EIOs received from 1/1/2019 until the date of the on-site visit** | **191** |
| **Total** | **756** |
| **MLAs and EIOs Executed** | **387** |
| **MLAs and EIOs Pending** | **369** |

680. Notwithstanding the above, the authorities presented many cases where the assistance provided to foreign authorities was very successful, even prior to the establishment of the Office for the Execution/Handling of MLA Requests. Indeed, many cases examined by the assessment team pre-dated the existence of the Office. Some examples are provided below.

**Box 2.1: Cases involving incoming EIOs and EAWs**

Case 1: In June 2018, the Police, through the MJPO, received an EIO from Country A in the course of a criminal investigation for the offences of participation in a criminal organisation and laundering of the proceeds of crime. The EIO involved a request for a disclosure order to be issued to obtain banking information. Country A requested the presence of its police officers in Cyprus. In October 2018, an EAW was sent by Country A requesting the arrest one of the persons (a foreign national) mentioned in the EIO. The EIO and the EAW were simultaneously executed in October 2018 in the presence of police officers from Country A. The suspect was arrested pursuant to the EAW and on the basis of a search warrant issued pursuant to the EIO, the residence of the suspect and the

premises of several companies connected to the suspect were searched and evidence (electronic pads, hard drives, computers, laptops, etc) was seized. Disclosure orders addressed to banks were issued upon application by the Police and financial information was gathered and provided to Country A. Freezing orders were also issued in Cyprus on the basis of an application made by the FIU to the courts based on the request of Country A. In December 2018, following a court procedure, the suspect was surrendered and transferred to Country A. All items seized and other evidence were handed over to Country A.

Case 2: In July 2017, the Police, through the MJPO, received a MLA request from Country A in relation to 17 persons for the offences of conspiracy to supply cocaine, conspiracy to supply heroin, ML and blackmail. Permission was requested to have the Police from Country A present during the execution of the MLA. The liaison officer from Country A posted in Cyprus contacted the Police in Cyprus in relation to a EAW issued by Country A against a person in relation to the offences mentioned above. The liaison officer requested that the MLA and the EAW be executed simultaneously, as an operation would also be conducted in Country A to apprehend other conspirators for the same case. In order to co-ordinate the operation, a meeting took place on in July 2017 with all involved parties namely the Drug Law Enforcement Representative, Larnaca District C.I.D., Members of INTERPOL Nicosia and the liaison officer and the Police from Country A who travelled to Cyprus for the execution of the MLA. Cypriot Police officers arrested the suspect on the basis of the EAW and on the basis of a warrant his residence was searched. During the search a number of items were seized (several mobile phones, credit cards, electronic pad, portable computer). Additionally, a disclosure order for telecommunication data was issued in relation to the suspect's mobile phones. Following a court procedure the suspect was surrendered in August 2017 and was transferred to Country A. All evidence and items seized during the execution of MLA was handed over to Country A. The subject pleaded guilty before the court. The level of detail in the evidence gathered by the Cyprus Police was critical to the defendant's early guilty plea.

Case 3: In December 2017, a request was received through Europol channels in relation to an operation conducted in Country A in relation to the offences of fraud and swindling. The case involved the wife of a person believed to be the leader of a criminal group. The operation was being conducted in the form of a joint investigation between Country A and Country B. Following information exchange through Europol channels, an EIO was received by the Cyprus Police through the MJPO, in which it was requested that coordinated and simultaneous action be taken in June 2018 in the presence of Police officers from Country A. In June 2018, Cyprus received an EAW issued by Country A requesting the arrest of the suspect in relation to the offences of fraud, theft and unlawful use of credit cards and computer fraud. Through coordinated action of various departments of the Cyprus Police, the EIO was executed in the presence of police officers from Country A and B, as well as representatives from Europol. During the operation the subject was arrested and her residence and vehicles were searched. A large number of electronic and other evidence was seized, including virtual assets. Court disclosure orders addressed to all banks in Cyprus were issued and banking information was secured as evidential material. Following a court procedure the subject was transferred to Country A including all the evidence collected during the operation.

681. The assessment team received substantial feedback from countries in the Global AML/CFT Network on their experience with Cyprus in relation to MLA, particularly those countries with which Cyprus co-operates extensively. Two of the countries that co-operate actively with Cyprus noted that their experience with Cyprus has been excellent. Positive feedback was received from other countries, especially in recent years both in relation to the timeliness and quality of the information. It was noted that there is a good level of communication, notably with the Police, likely due to the setting up of the Office for the Execution/Handling of MLA Requests. However, some countries indicated that significant delays were encountered in receiving a response to some, though not all, of their requests. Others noted that, while all the requests were satisfied, the information provided has not always been as comprehensive as needed. Out of all the countries that provided feedback, only one country expressed the view that Cyprus is generally not co-operative,

although the frequency of assistance requested by this country from Cyprus has been low.

682. In light of the above, the assessment team concluded that the level of co-operation is generally more timely and constructive with foreign counterparts with which Cyprus exchanges information on a regular basis and which the Cypriot authorities have specifically sought out to strengthen mutual cooperation. The other conclusion that can be drawn is that the framework for legal assistance has made a significant leap forward recently, bolstered by the setting up of the Office for the Execution/Handling of MLA Requests. However, these positive efforts should be sustained, if not further intensified, to continue reducing the remaining backlog of requests and guarantee the quality and timeliness of responses going forward.

683. Very few requests are refused outrightly, as evident from Tables 40 and 41. None of the feedback from the global network highlighted any concerns on this matter. Most cases appear to be isolated incidents. According to the authorities, refusals commonly relate to requests for evidence held in the occupied area, which is not under the control of the Republic. The authorities also cited instances where the requesting authority does not provide sufficient information substantiating the request. In such instances, the case is closed after a year if the country does not come back with further information.

*Execution of Freezing and Confiscation Requests*

684. The FIU handles requests for the freezing and confiscation of proceeds of crime. The FIU, including through its functions as an Asset Recovery Office, has been instrumental in freezing and confiscating assets on behalf of foreign jurisdictions. The FIU is endowed with far-reaching powers to trace assets and postpone transactions, even in the absence of a court order. The FIU is credited for using these powers proactively to secure freezing orders on behalf of foreign counterparts at its own initiative, even in the absence of a request to freeze assets.

685. Requests for freezing are treated with utmost priority and urgency. Since the FIU may conduct enquiries for the purposes of tracing of assets without the need to obtain a court order, the FIU immediately starts enquiries for the purposes of executing a freezing/confiscation-related request. Information is obtained from banking institutions as to the existence of or balance in a bank account, as well as the signatories of the bank account. If available balances are traced, pending a court order to obtain or register the freezing order in Cyprus, the FIU instructs obliged entities (most commonly banks) to suspend the execution of a transaction. This power is also exercised in cases where the FIU receives requests from foreign competent judicial authorities of EU Member States or a third country. In this manner, the property to be frozen or confiscated is secured immediately pending the issuing of a freezing order by the court or, as the case may be, the registration of a foreign freezing or confiscation order.

**Box 2.2: Freezing and Confiscation-related requests**

Case 1: A bank in Cyprus submitted an STR to the FIU regarding the transfer of a large sum from a bank in Country A due to a suspicion of possible fraud and ML. The FIU also received a request, through the MJPO, from Country A to freeze the funds in the bank account. The FIU conducted analysis and investigations and identified funds in another bank in Cyprus held in the accounts of three companies registered outside Cyprus. An application to the court to freeze the funds in the amount of approximately USD 8 million was made. The money remains frozen under a domestic freezing order.

Case 2: The FIU received an STR from a bank in Cyprus involving a company registered in Country B, having as beneficial owner a national from Country A. The company and the person were involved in a fraud on a grand scale in Country A. Following analysis and investigation, the FIU in Cyprus exchanged information with Country A through FIU channels and also through formal channels. A vast volume of evidential material was gathered in Cyprus on the basis of MLA requests and submitted to Country A. The proceeds of the fraud case amounting to EUR 20 million were identified in Cyprus and, following a MLA request, a domestic freezing order was obtained from the court. The court in Country A convicted a number of persons for the offences of fraud and money

laundering largely based on the evidence through the form of banking information submitted by the Cypriot Authorities. A confiscation order was issued. An appeal has been filed against the conviction. When the judgment will become final the confiscation order will be registered and enforced in Cyprus.

Case 3: The case related to a criminal investigation of a person for the offences of tax evasion, ML, human smuggling, forgery and fraud in another country. The suspect was on provisional detention and the foreign authorities were preparing a request for legal assistance to be sent to the Cypriot authorities for the freezing of the suspect's assets. Meanwhile, the foreign FIU made an urgent request to the FIU of Cyprus to exercise its power to postpone any transactions in the account of a company owned by the suspect kept at a domestic bank. The FIU Cyprus made inquiries with the bank, established that the company kept two accounts with available balances and issued instructions for the postponement of transactions from the said accounts. This provided the foreign authorities with sufficient time to obtain a freezing order from the court, which was eventually sent to Cyprus for registration and enforcement.

Case 4: This was an advance fee fraud carried out by persons located in Country B, who managed to convince elderly people in the Country A that they won a lottery but they first had to pay some money to receive their winnings. Upon a mutual legal assistance request submitted by Country A to the Cyprus Authorities property was frozen following both domestic freezing orders issued by Cyprus Courts as well as Court order for the registration and enforcement of a foreign freezing order for accounts held by Cyprus and foreign companies with banks in Cyprus. Following conviction in Country A, the authorities in Country A submitted a final order of forfeiture to be registered and enforced in Cyprus. The District Court of Nicosia issued the registration order for the enforcement of the final confiscation (forfeiture) order issued by the courts in Country A.

Type of order: Foreign Confiscation order registered in Cyprus

Date issued: 04/10/2018

Offences: Fraud

Property confiscated: USD 766,839

Case 5: Country A was investigating the activities of a company in Country B and other natural persons, who were involved in the installation of malicious software on millions of computers in Country A and elsewhere and laundering the proceeds from such criminal conduct. Country A had grounds to believe that part of the funds of such criminal conduct were laundered through banks in Cyprus. The Cyprus Police Authorities issued the relevant Disclosure Orders against certain banks in Cyprus and all the related documents were provided to Country A. Country A sent to the competent Authorities of Cyprus supplementary MLAs through the MJPO requesting the freezing of the funds transferred in Cyprus:

Domestic Freezing orders were issued by Cyprus Courts as follows:

- For a company registered in Seychelles for the amount of USD 118,910

- For a company registered in Cyprus for the amount of EUR 14,231

- Freezing orders against absent suspect for a company registered in Country C for the amount of USD 281,223. Renewed on 12/06/2012 and expired on 12/12/2012. Registration of a Freezing Order of Country A on 13/02/2013.

- Freezing orders against absent suspect for a company registered in Country D for the amounts of USD 3,244,396 and EUR 32,504. Renewed on 12/06/2012 and expired on 12/12/2012. Registration of a Freezing Order of Country A on 13/02/2013.

Following conviction of the accused in Country A, the Competent Authorities of Country A submitted to the Cypriot Authorities a request for the registration and enforcement in Cyprus of a final Order for Forfeiture (Confiscation) for the abovementioned restraint amounts.

Registration of Confiscation Order on 14/11/2016 for the abovementioned amounts. The proceeds of the confiscation, after the enforcement of the said order were distributed among the competent authorities of Country A and the Republic of Cyprus.

686. Cyprus has demonstrated its willingness to partake in asset sharing arrangements with the requesting countries, as demonstrated by case examples. As a matter of practice, when the requesting state indicates the existence of victims, the whole amount is repatriated to satisfy compensation requests. Where the confiscation involves real estate, the court appoints an official receiver to sell the property by auction. The proceeds are shared between Cyprus and the requesting state.

687. The table below present statistics on the number of MLA requests concerning freezing and confiscation, which were all executed.

**Table 41: foreign requests relating to freezing and confiscation**

| | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|---|
| **Freezing orders** | | | | | | |
| **Number of orders** | 11 | 6 | 5 | 7 | 1 | 1 |
| **Property (EUR)** | 23,771,999 | 5,821,271 | 8,870,347 | 28,931,505<br>2 real estate | 729,420 | 211,076 |
| **Registration of foreign freezing orders** | | | | | | |
| **Number of orders** | 8 | 4 | 2 | 2 | 7 | 4 |
| **Property (EUR)** | 4,530,383<br>1 real estate<br>1 motor vehicle | 15,795,640 | 372,259 | 90,776 | 521,466<br>1 real estate | 277,735 |
| **Confiscation (by consent of the account holder)** | | | | | | |
| **Number of orders** | 1 | 0 | 1 | 0 | 3 | 1 |
| **Property (EUR)** | 9,160 | 0 | 223,843 | 0 | 124,738 | 76,782 |
| **Registration of foreign confiscation orders** | | | | | | |
| **Number of orders** | 1 | 0 | 0 | 2 | 1 | 1 |
| **Property (EUR)** | 382,232 | 0 | 0 | 3,354,640<br>2 real estate | 3,393,192 | 696,605 |

688. Cyprus has also implemented provisions within the law for the registration and enforcement of civil confiscation orders. In an effort to provide the widest possible assistance in the area of freezing and confiscation, the AML/CFT Law was amended in 2018 to include civil confiscation orders (in rem) under the definition of foreign confiscation orders that can be registered and enforced in Cyprus. On the basis of this amendment, an application for such order has already been made following a request from another country.

*Extradition and EAWs*

689. Cyprus has demonstrated the ability to effectively process extradition requests and EAWs and has extradited a number of high-profile, non-Cypriot fugitives wanted for prosecution in other countries (see cases in Box 2.2). As noted, the MOJP also acts as the central authority for receiving and transferring such requests to the Police and the Attorney General's Office.

690. Between 2015 and 2018, Cyprus received 215 EAW requests. In 127 cases, a person was traced in Cyprus. In 122 cases an arrest warrant was issued while in only 5 cases the request was

refused. The reasons for refusal were either the absence of dual criminality or the court determined that the fugitive should serve the sentence in Cyprus. The number of extradition requests from non-EU countries was lower amounting to a total of 55. The courts decide whether to grant the extradition request. In 14 cases the Court refused the request on the grounds that either extradition would lead to a possible violation of the fugitive's human rights or the extradition request was based on ill-founded grounds by the requesting state.

691. Twenty-four cases were still pending at the time of the on-site visit. The authorities advised that in most of these cases, the fugitive had either lodged an appeal before the Supreme Court against the decision to extradite and the appeal was ongoing or filed a *Habeas Corpus* application. In some other cases, the procedure before the first level court had been prolonged due to procedural steps taken by the defence. In a small number of cases the fugitive had not yet been located.

692. The offences relating to extradition requests are mainly theft, appropriation of funds by abuse of an official position, cybercrime and human trafficking. The offences relating to EAW are mainly drug offences, tax-related offences, fraud and forgery. Cyprus demonstrated the ability generally to surrender a fugitive within 2-3 months of the request at the earliest (in case of EAWs) with more complex cases taking 16 to 24 months to complete. No negative feedback was received from foreign jurisdictions concerning Cyprus's ability to render extradition. Cyprus amended its Constitution in 2013 to extradite its own nationals. 32 Cypriot nationals were surrendered pursuant to an EAW request.

693. While dual criminality is required for extradition by Cyprus, the requirement is deemed to be satisfied provided that both countries criminalise the conduct underlying the offence. This principle was upheld by the Courts – in one case the court held that there is no need for absolute identification of the offences, nor is the description of the offences in the foreign arrest warrant of crucial significance and the requirement of double criminality is met because the actions referred to in the statement of facts constitute offences also in the Republic of Cyprus.

### *8.1.2. Seeking timely legal assistance to pursue domestic ML, associated predicates and TF cases with transnational elements*

694. Cyprus has demonstrated characteristics of an effective system also when seeking international co-operation. This is supported by the statistics on outgoing MLAs, EIOs, extradition and EAWs presented in Table 44 below and case-examples made available by the country. Feedback received from the Global Network was generally positive, indicating that requests are generally well-written, communication is clear and effective, and co-ordination, especially in relation to extradition, is efficient.

**Table 42: MJPO statistics on outgoing MLA, EIO, extradition and EAW requests**

| | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|
| MLAs | 188 | 170 | 183 | 127 |
| EIOs[102] | - | - | - | 35 |
| Extradition | 2 | 3 | 2 | 1 |
| EAWs | 56 | 56 | 50 | 49 |
| **Total** | **246** | **229** | **235** | **212** |

695. The MJPO acts as the central authority also for outgoing MLA, EIO, extradition and EAW requests. It receives requests from the domestic competent authorities and forwards them to the requested state. All requests are followed up with the requested state on an ongoing basis, particularly where the requests are urgent.

696. Table 45 suggests that the Police has been proactive in seeking legal assistance and extradition in relation to ML related to proceeds-generating offences committed in Cyprus, especially where these are followed by outward transfers of proceeds. It is estimated that in

[102] Cyprus implemented the EIO Directive in December 2017.

approximately 35-40% of the outgoing requests the police have suspicions, or identify trails, of proceeds leaving the island. The most common predicate offences are by far corruption and fraud – the highest domestic ML threats. Requests for assistance more or less go to the same countries which seek assistance from Cyprus i.e. Greece, Russia, the United Kingdom and the United States.

697. There have been some outgoing FT-related requests. With reference to case 2 presented in Box 9.2 under IO 9, the authorities sent 13 requests to foreign counterparts. With reference to case 1 in Box 9.2, the authorities stated that information gathered on the basis of a disclosure order was being analysed and requests were expected to be sent out in the near future.

**Table 43: Police statistics on outgoing MLA/EIOs requests (breakdown by nature of offence)[103]**

| Offences | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|
| **ML & Other Related Economic Crime Offences (Corruption, Fraud, Including Internet Fraud, False Pretences)** | 110 | 66 | 72 | 70 |
| **Drug Offences & ML** | 5 | 6 | 6 | 7 |
| **Other Offences** | 26 | 46 | 41 | 31 |
| **Total** | **141** | **119** | **120** | **110** |

698. Table 43 indicates that many outgoing requests involve ML. This would appear to contradict the findings under IO 7, which conclude that most ML investigations relate to domestic criminality. The authorities confirm that the figures are not contradictory. Many, although not all, outgoing requests do relate to investigations of a predicate offence in Cyprus together with self-laundering, which have a link to another country. The link to another country usually relates to the movement of proceeds of the domestic crime abroad, the suspect is abroad, or in the process of collecting evidence during the domestic investigation a witness statement or evidence from a foreign jurisdiction is deemed necessary. In many instances, while analysing the documentation received from a foreign jurisdiction, it becomes evident that there is a link with other jurisdictions – for example the funds are moved to a second jurisdiction. Hence, additional requests follow. The cases below are a good illustration of the type of domestic cases which give rise to outgoing requests.

**Box 2.3: Cases involving outgoing MLA and EAW**

Case 1: In one of the most serious corruption cases involving public officials, one of the accused persons was convicted by the Larnaca Assize Court for offences of corruption (receiving bribes for the total amount of EUR 300,000) and a confiscation order for the sum of EUR 300,000 was issued against him. Following co-operation between the ARO of Cyprus and ARO of Country A, it was determined that the accused had an account in the Country A. Subsequently, a MLA request was submitted by the Police, via the MJPO, requesting the freezing of the said amount, at the stage of the filing of the indictment before the Assize Court. The authorities of Country A, on the basis of the MLA Request, issued a restraint order on the said account. Following the conviction of the accused and the issue by the Larnaca Assize Court of the confiscation order (and following the decision on the appeal), the FIU contacted the accused and requested the enforcement of the confiscation order. The accused consented and gave instructions to the bank in Country A to execute the confiscation order. The whole amount was returned to Cyprus and was returned to the victim (i.e. the pension fund of a semi-governmental organisation).

Case 2: The Police (Economic Crime Unit) investigated a case (complaint made by OLAF) involving fraud, passive and active corruption in the private sector, abuse of authority by public officials,

[103] The statistics in Table 44 relate to MLAs/EIOs initiated by the Police, whereas those presented in Table 45 refer to the total outgoing MLAs by all competent authorities in Cyprus.

fraud affecting the financial interest of the European Union and ML. The case is now under trial before the District Court of Nicosia. Seven persons have been indicted out of which one is a legal person (company) and the rest are natural persons. During the investigation, a MLA request was sent to Country A to obtain evidence and trace illegal proceeds. The sum of EUR 500,000 was traced in Country A in the name of the accused legal person, which, following a relevant request by the Cyprus Authorities, has been frozen in Country A pending the hearing of the criminal case in Cyprus for the purposes of future confiscation.

Case 3: The Economic Crime Investigation Unit of the Police initiated investigations based on a complaint submitted by the director of a legal entity registered in Cyprus. According to the complaint, the company was defrauded via internet (internet fraud) and was given falsified instructions to transfer money to a bank account in Country A for the importation of products in Cyprus for the sum of EUR103,000. The FIU was informed by the Police accordingly and on the basis of FIU to FIU co-operation, a relevant request was sent to FIU in Country A. In parallel, an MLA request was sent by the Police to the competent authorities in Country A. The money was traced to a specific bank account and the bank in Country A returned the money to the account of the victim.

Case 4: On 12/02/2016 a European Arrest Warrant was issued against a German national against whom the offences of fraud, theft and money laundering for the total amount of EUR 108,000, were investigated by the Cyprus Police. On 20/02/2016 a diffusion message was issued by Interpol Nicosia by which the arrest of the subject was requested with a view to his surrender to the Republic of Cyprus. Additionally, the subject details were placed in Interpol's public website which is open to the public for the purpose of gathering information. On 31/12/2016 a message was received from Interpol Country A, by which Interpol Nicosia was informed that the subject was arrested in Country A and it was requested that the EAW be forwarded to Interpol Country A. Interpol Nicosia immediately informed the MJPO and on 01.01.2017 the EAW was sent to Interpol Country A. On 19/01/2017 Interpol Country A informed Interpol Nicosia that due to the fact that the original documents were not received, the subject was released from custody. On 23/08/2017 Interpol Nicosia received a message from Interpol's General Secretariat informing the Police that from information received from the public, the subject could be employed by a specific company. On 05/01/2018 Interpol Country A informed Interpol Nicosia that the subject was arrested and was presented before the court which decided that the subject should be surrender to the Cyprus Authorities. The subject appealed against the decision of the court, but the Supreme Court in Country A dismissed his appeal. Due to medical reasons, the transfer could not take place within the 10-day time limit. Finally, the subject was handed over to Cypriot Police Officers and was transferred to Cyprus on 08/02/2018.

699. The authorities have provided some statistics on the nature of outgoing requests, which are presented in Table 44 below. The same case will generally involve requesting the identification of a bank account, identifying a beneficial owner and the issuance of a freezing order. This is expected given the type of financial crime that the Police focus on, which often involves the concealment of identity of the perpetrators of crime behind a corporation and outward transfers of funds through different bank accounts.

**Table 44: type of outgoing requests by the Police**

| | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|
| Request to issue a freezing order | | | | |
| No. of orders | 69 | 45 | 47 | 52 |
| Requests to identify a bank account | | | | |
| No. of requests | 69 | 45 | 47 | 52 |
| Request to identify a beneficial owner | | | | |
| No. of requests | 69 | 45 | 47 | 52 |
| Request to obtain witness statements | | | | |
| No. of requests | 141 | 119 | 120 | 110 |

| Request to seize evidence | | | | |
|---|---|---|---|---|
| No. of requests | 69 | 45 | 47 | 52 |

700. International cooperation is sought to a much lesser extent in cases where the proceeds of crime are generated outside Cyprus and laundered in/through Cyprus (e.g. layering activities through banking transactions). This is evident from the statistics in the table below, which clearly show that requests for assistance purely for ML are extremely rare. This is consistent with the findings under IO 7, which indicate that while the jurisdiction accepts that there is a high threat of the proceeds of foreign crime being filtered into and/or through Cyprus, as it is an IFC, the focus of investigations and prosecutions has instead been on domestic crime proceeds.

**Table 45: Outgoing ML MLA requests**

| Offences | 2015 | 2016 | 2017 | 2018 | 2019 |
|---|---|---|---|---|---|
| **Money Laundering** | 0 | 1 | 1 | 2 | 0 |

701. The authorities advised that no cases have arisen where there was a conflict of jurisdiction of a case with another country.

### *8.1.3. Seeking and providing other forms of international cooperation for AML/CFT purposes*

702. Most competent authorities generally seek other (informal) forms of international co-operation in an appropriate and timely manner and provide information promptly and constructively when so requested by their foreign counterparts.

The FIU

703. The FIU is an active member of the Egmont Group and effectively uses the Egmont Secure Web (ESW) and FIU.Net (with EU FIUs) to provide and seek intelligence to and from foreign FIUs. The FIU has signed a significant number of Memoranda of Understanding despite this not being a requirement for the exchange of information under domestic law. There is a section within the FIU which is dedicated to international cooperation, staffed with five analysts who are highly qualified and well-attuned to the legislative framework, the principles governing information exchange and the risks and peculiarities of the AML/CFT system.

704. The FIU has an internal procedure in place governing the handling of FIU requests setting out the criteria on the basis of which requests are to be prioritised. Since 2017, incoming requests are uploaded into a case management system, which however does not appear capable of automatically picking up the most urgent requests on the basis of risk algorithms. Given the limited human resources and the numerous functions that the FIU performs, it may be advisable to automate the system in order to increase efficiency. Much attention is paid to the protection of confidential information. All databases held within the FIU are securely protected through various firewalls and passwords. All data is properly backed up on a daily basis. Only FIU personnel have access to FIU databases. Breaches of confidentiality are subject to severe penalties.

705. The statistics relating to incoming FIU requests are presented in the table below.

**Table 46: FIU Incoming Requests**

| | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|---|
| **Foreign requests received by the FIU** | 538 | 483 | 474 | 482 | 423 | 478 |
| **Foreign requests executed by the FIU[104]** | 538 | 483 | 474 | 482 | 423 | 478 |

[104] These figures refer to whether a request received in a particular year was executed, irrespective of whether this was done in the following year.

| | | | | | | |
|---|---|---|---|---|---|---|
| **Foreign requests refused by the FIU** | 0 | 0 | 0 | 0 | 0 | 0 |
| **Spontaneous sharing of information received by the FIU** | 14 | 42 | 56 | 62 | 68 | 92 |
| **TOTAL (incoming requests and information)** | 552 | 525 | 530 | 544 | 491 | 570 |
| **Average number of days to respond to requests from foreign FIUs** | 10 | 10 | 10 | 10 | 10 | 10 |
| **Refusal grounds applied** | n/a | n/a | n/a | n/a | n/a | n/a |

706. The FIU responds to all requests, generally within the timeframes stipulated under the Egmont Principles for Information Exchange. The foreign FIUs with whom the Cypriot FIU cooperates most actively were generally satisfied with respect to the FIU's response time. A small number of FIUs, which do not frequently request information from the FIU, expressed dissatisfaction with the timeliness of response. The assessment team attributes this issue to limited human resources, rather than reluctance or lack of diligence in handling requests. The FIU noted that in order to satisfy some requests a significant volume of information had to be collected, which may have prolonged the response time. Upon receipt of a request, information on the subject(s) is recorded in the FIU's database. Checks are performed to determine whether the subjects are known to the FIU. Other checks are subsequently carried out in other databases to which the FIU has access, including the Police database, the Company Registry, Land Registry, etc, depending on the nature of the request. The process is regulated by the internal procedure. Many foreign FIUs commented that the responses of the FIU are very comprehensive and oftentimes instrumental to progress their cases. The FIU also has the power to obtain information from obliged entities on behalf of foreign FIUs, including where banking or beneficial ownership information is solicited. This power was strengthened in 2013.

**Box 2.4: FIU to FIU co-operation**

Case 1: The FIU received an STR in 2018 from a bank in relation to the account of Company X registered in Cyprus. The BO of company X was a foreign national, individual A. An STR from a second Cypriot bank regarding Individual A was also received in 2017. Individual A was the BO of Company Y, also registered in Cyprus. The Cyprus account of company X had a remaining balance of around USD 6.5 million, which was frozen by the FIU. Based on the STR and on the analysis of the financial information contained therein, it was determined that the account of Company X had been credited with amounts from other countries. Funds were received from a number of foreign companies with accounts abroad and more specifically from accounts maintained in three foreign jurisdictions (Mauritius, Switzerland and Bahamas). The analysis performed also showed that the funds once received in the Cypriot account of Company X were transferred abroad and in particular to the accounts of foreign companies in 7 foreign jurisdictions (UAE, Switzerland, Spain, Italy, Liechtenstein, Mauritius and Portugal) related with company X and company Y, including the personal accounts of Individual A abroad. The Unit provided information, both upon request and spontaneously, to the FIUs of 9 FIUs namely those of UAE, Switzerland, Spain, Italy, Liechtenstein, Mauritius, Portugal, Angola and Bahamas.

Case 2: Two STRs were received in 2017 from the same bank in relation to a Cyprus registered company and a Spanish national named AB, director of the said company. The suspicion related to possible involvement of the company in carousel fraud. This became apparent from the analysis of the transactions in the bank accounts of the company. Notably, the credit turnover of the company

in a twelve month period amounted to EUR 37 million, as compared to the declared turnover of EUR 3 million. The principal activity of the company was stated to be general trade and the goods traded included mobile phones, PC laptops, tablets, PC components and other small appliances, in other words, small electronic items of significant value that could be traded in large quantities which is common in cases of VAT Carousel Fraud. Funds had also been transferred to Lithuania. In addition, the analysis of the transactions indicated that the Spanish national named AB had opened a personal account with the same bank in Cyprus. His personal account had been credited with funds from the Cypriot company which were further transferred to a personal account in Spain, as well as to the accounts of a different company in Estonia, whose BO was AB. The FIU exchanged information with the FIUs of Spain (country of nationality of individual AB and recipient of funds), Estonia (origin and destination of funds), UK (country of nationality of BO) and Lithuania (destination of funds).

707. Since a large proportion of cases that the FIU analyses have a cross-border element, the FIU often seeks information from other FIUs. It maintains close ties with its main partners and proactively seeks to resolve any issues that may arise in order to obtain information that it may require. It was noted positively that, where the FIU does not receive the requested information from foreign FIUs, it will attempt to obtain information through Police channels in order to further its analysis. The table below presents statistics on the number of outgoing requests sent by the FIU and spontaneous information sharing with foreign FIUs. As stated under IO 6, on average, the FIU analysis 315 STRs (categorised as medium/high risk) on an annual basis. The figures in Table 47 would suggest that the FIU is very proactive in seeking information from foreign FIUs to further the analysis of STRs.

**Table 47: FIU Outgoing Requests**

| | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|---|
| **Requests sent by the FIU** | 345 | 275 | 274 | 247 | 209 | 234 |
| **Spontaneous sharing of information sent by the FIU** | 50 | 98 | 93 | 126 | 242 | 135 |
| **TOTAL (outgoing requests and information)** | **395** | **373** | **367** | **373** | **451** | **369** |

708. The assessment team positively notes that the number of spontaneous disseminations to foreign FIUs has increased significantly over the period under review. As a best practice, the FIU has adopted a policy of providing complete analysis products to foreign FIUs, where following the analysis of an STR, grounds indicating the existence of criminal activity outside of Cyprus is identified. It is also positively noted that, in these cases, the FIU will generally authorise the foreign FIU to disseminate information to LEAs for further investigation.

709. The FIU also serves as the Asset Recovery Office set up pursuant to the requirements of the relevant EU legislation[105] concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds. The authorities provided the following statistics. All incoming ARO requests were executed.

**Table 48: ARO requests**

| | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|---|
| **Incoming ARO Requests** | 63 | 71 | 48 | 49 | 43 | 54 |
| **Outgoing ARO Requests** | 2 | 2 | 2 | 3 | 4 | 2 |

[105] COUNCIL DECISION 2007/845/JHA concerning co-operation between Asset Recovery Offices of the Member-States in field of tracing and identification of proceeds from or other property related to crime

The Police

710. The European Union and International Police Cooperation Directorate (EUIPCD) is responsible for international cooperation within the Police. It houses various bureaus dealing separately with requests through Interpol, Europol, SIENA, SIRENE (which is not yet operational[106]) and the Police Co-operation Unit, the latter serving as a point of contact between the Police and the MJPO for the execution of MLAs and between the Police and liaison officers. The centralisation of the various channels for informal cooperation within the EUIPCD has proven to be a useful asset as it facilitates co-ordination on all international cooperation matters internally within the Police among the different departments and also between the Police and other competent authorities.

711. The table below presents statistics on the number of incoming and outgoing requests from Interpol and Europol.

**Table 49: Police Incoming and Outgoing Requests**

| | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|---|
| **Incoming Interpol requests** | 797 | 971 | 819 | 837 | 1090 | 1283 |
| **Outgoing Interpol requests** | 231 | 294 | 293 | 360 | 364 | 393 |
| **Incoming Europol requests** | 91 | 95 | 90 | 98 | 102 | 117 |
| **Outgoing Europol requests** | 2 | 0 | 0 | 0 | 5 | 0 |
| **TOTAL** | 233 | 294 | 293 | 360 | 369 | 393 |

712. As a strategic choice, the Interpol communication channel is employed on a much more frequent basis than Europol, even when communicating with EU member states. The Police attribute this to Interpol's much wider global reach. Responses are sent within reasonably short timeframes. Delays happen in isolated cases. No request has ever been refused.

713. Cooperation through Interpol and Europol, both in terms of the nature of offences and types of requests, is broadly in line with the risks that Cyprus faces. Requests relate primarily to fraud, ML and suspicious banking activity. The majority of requests received through Europol channels involve company checks and bank account information, including ARO requests which are forwarded to the FIU for execution. With respect to Interpol channels, the requests mainly concern location of persons, arrest of persons, company checks, stolen / lost passports, forged driving licenses and forged marriage certificates. In case the execution of any requests requires the undertaking of coercive measures, the requesting country is advised to forward an MLA or an EIO request through the appropriate channels.

714. The Police attributes the reasons for the overall increase in incoming and outgoing requests to various factors, including the increased flow of irregular migrants to the EU including Cyprus, the installation of FIND (Fixed Interpol Network Databases) at arrival and departure points and the Green Line crossing points, the horizontal access to Europol's SIENA system of several Police Departments and other domestic LEAs (FIU and Customs Department) which simplifies the procedure, the promotion of Interpol's and Europol's tools and services offered by the two Organizations via presentations to the Cyprus Police Academy to new recruits and specialized courses (i.e. Sergeant, C.I.D. Inspectors course, LETS seminars etc), the increased measures taken at European and international level for combating terrorism and the increased incidents of cyber fraud.

[106] SIRENE will become operational once the Republic of Cyprus will apply the respective Schengen acquis on the Schengen Information System upon its accession to the Schengen area.

715. The EUIPCD is empowered to share any type of information and data maintained by the Police and any type of information or data held by other public authorities, by the private sector and which is available to the Police without the need to apply coercive measures. The EUIPCD has access to all police databases (including criminal records) and other governmental databases. If the request relates to this type of information, it is communicated directly in a prompt manner by the personnel of the EUIPCD. Where the request concerns information that is not accessible to the EUIPCD, the request is forwarded to the relevant authority to collect and provide this information and followed up through a BU (Bring Up) System. Where spontaneous intelligence is received from foreign authorities, which is a common occurrence, the EUIPCD will consider the information, assess its usefulness in terms of evidence and forward it to the relevant competent authority for further action. The EUIPCD records all the information in incoming/outgoing requests concerning the individuals/legal entities involved. This data is accessible to all police investigators, the FIU and the Customs and Excise Department through a joint law enforcement database. Therefore, this information is available to investigators in the process of a criminal investigation.

716. In 2018, the EUIPCD issued an internal manual to formalise the procedure on the handling of incoming requests and information sharing. The manual covers cooperation through Interpol, Europol and Sirene Offices (not yet operational) and stipulates procedures concerning the cooperation of these Offices with other Police Departments/ Services/Offices, as well as with other national law enforcement authorities (the FIU, the Customs and Excise Department, the Tax Department) in the processing of incoming and outgoing messages (requests for information), the handling of urgent messages, the handling of messages relating in particular to terrorism, the handling of classified correspondence, the coordination of the contribution of Cyprus to the Europol Analysis Work Files (AWF), the participation of the Cyprus Police to the projects under EMPACT (European Multi-Disciplinary Platform Against Criminal Threats) and the pan-European Operations and Joint Action Days, as well as the access to the Europol Information System and SIENA. The manual also describes in detail the procedure to be followed with respect to cooperation via SIRENE, though not yet operational. Due to an exponential increase in incoming requests, the EUIPCD is in the process of implementing a case management system to be able to control the flow of information in a more organised and efficient fashion.

717. The Police Cooperation Unit functions as a contact point for cooperation through liaison officers of foreign countries posted or accredited to Cyprus (Police Standing Order 1/24). Currently, police liaison officers from France, United Kingdom, Greece, Russia and the U.S.A, which are the countries that Cyprus cooperates with most extensively, are posted to Cyprus. Liaison officers from Germany, Italy, Japan, Romania, Israel, Canada, Australia and Spain, who are posted in neighbouring countries are accredited to Cyprus as well. The Police also have arrangements in place with Greece to use their much broader network of police liaison officers. The use of police liaison officers is used extensively during the investigation of domestic cases. In addition, the Police have also concluded bilateral agreements with foreign counterparts. These agreements tend to go beyond information exchange and cover a range of additional issues, such as joint training and exchange of expertise.

The Customs Department

718. The Customs Department provides assistance to member states of the EU on the basis of various legislative instruments and to third countries on the basis of bilateral and multilateral agreements, MoUs and the International Customs Organisation Recommendation for Mutual Administrative Assistance of 5 December 1953. The Customs Department has a well-established relationship with foreign counterparts and intelligence exchanges take place on a daily basis. The customs authority of the country which co-operates most actively with the Customs Department in Cyprus noted that the level of cooperation is very good.

719. A special unit within the Investigation Section of Customs Headquarters deals with international cooperation. This unit handles all the incoming mutual assistance and administrative requests from EU and non-EU countries. These requests are received through AFIS MAIL from EU (OLAF) or from other EU countries based on Regulations 515/1997, 389/2012 and protected channels when made under Naples II Convention or other conventions. Mutual assistance requests

are also received from non-EU countries based on bilateral agreements among EU and third countries or on Protocols on mutual administrative assistance in custom matters signed between the Republic of Cyprus and these countries. The confidentiality of the information shared is protected through AFIS MAIL and the correspondence is treated as confidential. Spontaneous information from EU countries is recorded, evaluated and in case this information can be connected with other information which already exists in the Customs databases and may lead to suspicions of the commission of customs offences, then further action is taken and the case is investigated.

**Box 2.5 – Joint Investigation Team (JIT)**

The Customs Department requested administrative assistance from the United Kingdom Customs Authorities in accordance with the provisions of the Treaty on Mutual Assistance and Cooperation between Customs Administrations (Naples II Treaty - Ratification Law 29 (III), 2004), the Regulation on mutual administrative assistance in Customs matters of the European Union no. 515/1997 and the Convention on Cooperation between Customs Services (Ratification) Law no. 29 (III) / 2004.

According to this request, a Joint Investigation Team was set up and an agreement was signed in 2014 between the United Kingdom Customs Authorities and the Law Enforcement Agencies of Cyprus, the Customs Authorities, the Police Authorities and the FIU, for joint investigation of a large scale cigarette smuggling case investigated by the United Kingdom Customs Authorities, in which Cyprus was involved.

Specifically, two Cypriot nationals and other persons were arrested in the United Kingdom by UK Customs Officers in connection with the illegal importation of a large number of 10 (ten) million cigarettes into the United Kingdom.

A disclosure order was issued by the Nicosia District Court under reference number, for the bank accounts of the suspects. The disclosure of data was deemed necessary for investigations carried out to collect evidence connected to the offense of cigarettes smuggling which was under investigation, but also for the detection and identification of illegal proceeds. All the evidential material gathered was shared between the authorities of the two countries participating in the JIT.

720. In the period under review, there were 16 requests sent to EU countries and 16 to third countries. Most of the requests were received from the UK (133), Ukraine (24), Greece (19) and Russia (16), which are the countries which pose the highest threat to Cyprus. The cases presented by the Customs Department indicate the involvement of legal persons in these countries in collusion with legal persons in Cyprus for the avoidance of payment of excise duties in most cases concerning the overpricing or devaluation of goods.

Supervisory Authorities

721. The supervisory authorities in Cyprus have mechanisms in place to exchange information in a timely and constructive manner with foreign counterparts. The Real Estate Agency Board and the Casino Commission were entrusted with supervisory responsibilities close to the date of the on-site visit and therefore had not yet engaged in international cooperation.

722. **CBC**: The legal framework governing the functioning of the CBC provides for the possibility of international cooperation, including on AML/CFT matters, with foreign authorities supervising credit and financial institutions. The requests received at the CBC are submitted to the Supervision Division and, where they relate to AML/CFT, are forwarded to the AML/CFT team which will examine the precise circumstances of the request and the nature of the information provided. If it is established that the case involves information as part of an ongoing ML/TF related investigation, the applicant is directed to the appropriate channel (FIU or MJPO). If the request is of supervisory nature, the CBC will respond accordingly. The responses are sent in the manner the request has come, i.e. via e-mail, fax or letter.

723. The Central Bank of Cyprus fosters the development of its bilateral relations by entering into negotiations for the signing of Memoranda of Understanding (MOUs) with a number of foreign

Central Banks and Supervisory/Regulatory Authorities of countries specifically whose banks and/or other financial institutions have an active presence in Cyprus. This practice is in accordance with the relevant recommendation of the Basel Committee on Banking Supervision, which aims at strengthening the supervision of cross-border activities of banking institutions. In this respect, MOUs setting out the general framework of mutual cooperation and exchange of information have been signed. The CBC has entered into MOU agreements with 24 countries of which 14 are third countries. In January 2019, the CBC entered into a multilateral agreement with the European Central Bank on the practical modalities for exchange of information pursuant to article 57a(2) of Directive (EU) 2015/849

724. There are seven domestically authorised banks which have no foreign presence and 24 subsidiaries or branches of foreign banks in Cyprus, as indicated in the table below:

**Table 50: number of branches or subsidiaries of foreign banks**

| | Type of bank | No. |
|---|---|---|
| 1. | Subsidiaries of EU banks | 3 |
| 2. | Subsidiaries of non-EU banks | 1 |
| 3. | Branches of EU banks | 6 |
| 4. | Subsidiaries of non-EU banks | 14 |

725. In relation to subsidiaries and branches of foreign banks, the CBC shares the findings of its AML/CFT on-site examinations with the home supervisor, both within the EU and outside the EU. There have also been a number of joint onsite examinations, for example, together with the Bank of Greece in relation to banks of Greek origin. Since the CBC is part of the Eurosystem of central banks sharing of prudential takes place through the ECB. For instance, it facilitates onsite examinations for prudential matters at Greek subsidiaries by the ECB. With respect to branches from non-EU member states, the CBC has met on a number of occasions with all counterparts (Jordan, Lebanon, Russia and Ukraine) and has exchanged information in writing for both prudential and AML/CFT matters. In particular, information was provided to the National Bank of Ukrainian on a complex and serious widely publicised case (see Box 2.6 below).

**Box 2.6: exchange of information with foreign supervisors**

In 2015, the CBC conducted an on-site inspection of one credit institution operating in Cyprus in the form of a branch. The inspection was both for prudential and AML/CFT purposes. While the AML/CFT examination revealed significant deficiencies in the preventive measures, the prudential examination on credit risk revealed unusual lending patterns which were further investigated jointly between the prudential and AML/CFT supervisors. This examination resulted in the CBC filing a SAR with the FIU and a fine for the AML/CFT findings. Subsequently, the CBC cooperated closely with the home supervisor and divulged all information related to the suspicious loan activity to the home supervisor who conducted similar onsite examinations at their end and took legal action against the owners.

726. The three largest Cyprus-incorporated banks are prudentially supervised by the ECB directly since November 2014. The CBC signed a MoU with the ECB in January 2019 for the exchange of AML/CFT information on these three banks. At its own initiative, the CBC presented the AML/CFT regulatory framework of the three banks to the ECB and shares the findings of its AML/CFT onsite inspections.

727. Up until 2013, Cyprus-incorporated banks had a presence in Greece and the UK. The CBC exchanged information formally i.e. in writing and informally i.e. in joint meetings with its counterparts on the following types of information: the regulatory framework in Cyprus, prudential

matters and AML/CFT issues. The CBC conducted onsite examinations both for prudential and AML/CFT matters of the Cyprus banks in these two countries and held closing meetings with the authorities to share its findings. In one case, the CBC conducted a joint AML/CFT onsite examination with the Bank of Greece. Measures were taken in collaboration with the foreign counterparts e.g. for a bank in the UK liquidity measures were taken in coordination between the two and warning letters were issued to the banks for AML/CFT breaches which were communicated to the host supervisor.

728. In addition to sharing information with home supervisors in relation to branches and subsidiaries operating in Cyprus, for licensing purposes and enquiries into the fitness and probity of qualifying shareholdings and directors, the CBC's licensing section has a very active exchange of information with foreign counterparts. The following statistics were provided:

**Table 51: CBC incoming and outgoing requests for information**

| | **2018** | **2019** |
|---|---|---|
| **(A) CBC requested and received information from the following competent authorities:** | | |
| Bank of Greece | 5 | 2 |
| FCA/PRA | 7 | 2 |
| CSSFC (Luxembourg) | 1 | 0 |
| Banque du Liban | 1 | 0 |
| Hong Kong Police Force | 0 | 1 |
| Banque de France | 3 | 0 |
| Bafin | 10 | 2 |
| National Bank of Czech Republic | 1 | 0 |
| Belarus Insurance Supervision | 1 | 0 |
| Central Bank of Russia | 2 | 1 |
| National Bank of Belgium | 1 | 0 |
| Financial Supervision Commission, Bulgaria | 1 | 0 |
| Bank of Mauritius | 1 | 0 |
| Financial and Capital Market Commission, Latvia | 4 | 0 |
| National Bank of Kazakhstan | 1 | 0 |
| **Total** | 39 | 8 |
| | | |
| **(B) CBC responded to enquiries from the following competent authorities:** | | |
| Finansinspektionen | 1 | 0 |
| Bank of Greece | 2 | 0 |
| Malta Financial Services Authority | 1 | 0 |
| **Total** | 4 | 0 |

729. In relation to payment and e-money institutions licenced by the CBC, activity is limited to cross border provision of services on the basis of EU passporting without physical presence in Cyprus. The CBC initiated contacts with one country on the basis of a risk assessment (Lithuania). This activity occurred in 2019. One e-money institution with a sister company in a non-European state was the subject of exchange of information for prudential purposes between the CBC and the foreign counterpart. Also, the CBC participated twice in an AML/CFT supervisory college in relation to an international money service business provider in the EU.

730. .

731. **CySEC**: CySEC cooperates effectively with its foreign counterparts through the Strategy, International Relations and Communications Department. Cooperation involves the exchange of information and mutual assistance between supervisory authorities to strengthen supervision and investigate potential violations of the legislation. CySEC actively exchanges information through the International Organization of Securities Commissions (IOSCO) and ESMA MMOU channels. CySEC is ranked as one of the top ten users of the IOSCO MMoU. The assistance provided by CySEC to foreign counterparts has been publicly acknowledged on numerous occasions, particularly in relation to assistance provided to further investigations of serious violations of securities laws.

732. During 2018, CySEC received 310 requests for assistance (2017 – 344 requests) to assist its overseas counterparts from 48 countries (2017 – 52 countries) with their authorisation process, supervision procedures and enforcement investigations. This included, *inter alia*, conducting interviews, obtaining bank records and transaction data, and providing information on shareholding structures. During the assessment of an application for authorisation and in case of a subsequent change in the shareholder and management structure, there is consultation between CySEC and other supervisory authorities in order to form an opinion on the "fitness and probity" of shareholders, directors and other key persons.

733. The average response time was 30 days. CySEC aims to execute international requests in the most efficient, effective and expedient manner depending on the extent and complexity of the request. Requests asking for a more expedient execution are discussed with the requesting authority and are executed accordingly. To monitor progress on the execution of requests, a case management system is maintained. The exchange of information is conducted through clear and secure gateways. Information is exchanged via password protected documents. When available, the exchange of information is conducted via encrypted emails. Communication with other competent authorities is stored in a special location in the server with limited access and in the Document Management System (eOASIS), where there is an audit trail feature, allowing the logging of every activity happening on a file. Furthermore, CySEC has in place controls and safeguards to ensure that information received is used only for the intended purpose, unless prior authorisation has been given by the requested authority. The confidentiality of information is strictly protected by virtue of the CySEC Law.

734. All information received is treated in the strictest confidence in accordance with the confidentiality rules set out in the CySEC Law, the IOSCO MMoU and the ESMA MMoU as well as the EU General Data Protection Regulation 2016/679, ("the GDPR"). Furthermore, confidentiality of information exchanged pursuant to the IOSCO and ESMA MMOU, is protected and may only be used for the purpose it has been requested unless the authority that provided the information consents. The same applies for any disclosure or onward sharing of information received.

735. **ICCS:** Most exchanges take place within the context of supervisory colleges, where there is a special co-ordination agreement in place between the ICCS and the foreign supervisory authority for the exchange of information when companies within the same group operating in different countries are involved. Information is also exchanged in relation to the assessment of acquisitions of qualifying holdings or withdrawal of authorisations. Within the framework of the decision of the Board of Supervisors on the cooperation of the competent authorities of the EU Member States, the ICCS has regular exchanges (i.e. on a daily/weekly basis) of information with regards to insurance undertakings and insurance distributors that carry out business in Cyprus from other EU countries and from Cyprus to other EU countries under the freedom of services (FOS) and freedom of establishment (FOE) regimes. This information includes notifications for business carried out for the first time, additional classes of business, portfolio transfers between insurance undertakings, changes of names and changes of addresses. Regarding FOS for new business carried out in Cyprus by insurance undertakings on 2018 the ICCS received 30 notifications,17 notifications on 2017, 31 notifications on 2016, 45 notifications on 2015 and 24 notifications on 2014. In 2018, the ICCS received 2 notifications for insurance intermediaries that carried out business in Cyprus under FOE.

736. Apart from the above, the European Insurance and Occupational Pensions Authority (EIOPA) organises regular meetings for Supervisors for exchange of information in relation to

supervisory practices and other relevant matters. The ICCS attends these meetings. Also, EIOPA notifies all national competent authorities when a licence of a company in a Member State is withdrawn.

737. The following statistics were provided:

**Table 52: ICCS international cooperation**

| Year | Type of exchange |
|---|---|
| **2014** | 3 supervisory colleges<br>1 formal complaint by an EU supervisory for activities carried out by two intermediaries in the UK not covered by their insurance mediation licence issued by the ICCS |
| **2015** | 5 supervisory colleges |
| **2016** | 5 supervisory colleges<br>2 assessments of acquisitions of qualifying holdings<br>1 complaint |
| **2017** | 6 supervisory colleges<br>1 formal complaint by an EU supervisory for activities carried out by two intermediaries in the UK not covered by their insurance mediation licence issued by the ICCS |
| **2018** | 6 assessments of acquisitions of qualifying holdings<br>5 supervisory colleges<br>As part of the withdrawal of authorisation of an insurance undertaking, the ICCS was in continuous contact and co-operation with the foreign supervisory authority |
| **2019** | 4 supervisory colleges<br>As part of the withdrawal of authorisation of an insurance undertaking, the ICCS was in continuous contact and co-operation with the foreign supervisory authority (continued from 2018) |

### *8.1.4. International exchange of basic and beneficial ownership information of legal persons and arrangements*

738. The Cyprus authorities regularly provide basic information of legal persons in a timely manner. Information on companies and businesses, such as date of the registration of the company, its shareholders, directors, secretary, and registered address is publicly available at the Registrar of Companies and easily shared upon request. The feedback provided by the AML/CFT global network does not suggest particular concerns in this respect. The assessment team had sight of actual (sanitised) correspondence with foreign authorities which contained detailed information on legal persons.

739. Requests concerning beneficial ownership either through incoming MLAs/EIOs or through informal FIU channels are very common. For instance, the statistics furnished by the FIU show that BO information was provided in 64 cases to 33 countries in 2017 and in 126 cases to 37 countries in 2018. The Police stated that the majority of incoming MLAs/EIOs involve legal persons/arrangements and are generally accompanied by a request for BO information. The assessment team confirms this as in nearly all the international cooperation cases viewed by the assessment team (at least 90) one or more legal persons/arrangements were implicated. BO information is retrieved in a timely manner by the Police on the basis of court disclosure orders (Police) and by the FIU pursuant to its information gathering powers under the AML/CFT Law. In most cases, BO information is obtained from banks since requests for assistance generally involve fund transfers to or through Cypriot bank accounts held by legal persons/arrangements (foreign and domestic).

740. The assessment team did not identify any major issues where BO information is maintained by banks. However, not all legal persons/arrangements registered in Cyprus maintain bank accounts in Cyprus. In theory, BO information on these legal persons/arrangements would be held

by ASPs. As noted under IO 4 and 5, the measures applied by ASPs have not been found to be as rigorous as those of banks. This could potentially limit the authorities' ability to identify and share such information with foreign counterparts, albeit there has not been any feedback suggesting that the BO information provided by the FIU or Police has not been accurate.

741. Numerous examples have been provided by the FIU demonstrating that BO information is effectively exchanged, some of which are presented below.

**Box 2.7: FIU to FIU sharing of BO information**

Case 1: The proceeds of a predicate offence committed in Country A involving significant proceeds were deposited in a bank account in Cyprus through a number of complex transactions. The bank account was held in the name of a company registered outside of Cyprus. The BO of the company (a national residing in Country A) was unknown to the authorities of Country A since he was not among the primary suspects of the case. The BO information of the company together with basic company information and financial information was provided to the authorities of Country A initially through FIU to FIU channels and later in response to a MLA request. This led to the arrest of the BO in country A, who was subsequently prosecuted and convicted of ML in Country A.

Case 2: The case involved an advance fee fraud carried out by persons located in Country A, who defrauded elderly people in Country B. The proceeds were transferred through bank accounts of foreign and Cypriot companies held with banks in Cyprus. A MLA request submitted by the authorities of Country B included, *inter alia*, a request to determine who the BOs of the companies were. The Cypriot authorities executed the request through court disclosure orders and determined that the BOs of the companies were the same persons located in Country A who had committed the fraud.

Case 3: A MLA request was received from the authorities in Country A requesting assistance to obtain BO information and bank documents in relation to the accounts in Cyprus of one foreign company, which had received the illegal proceeds. The offences under investigation were fraud and forgery. A disclosure order was obtained the following day to retrieve the information on the suspect company. Documents and information, including on the BO, were collected and sent to the authorities of Country A. The accounts were frozen.

742. Two foreign FIUs noted that the FIU of Cyprus has on occasion directed them to obtain information through MLA channels. The FIU's view is that in these cases insufficient background information had been provided to substantiate the request. In order to support this statement, the FIU presented various sanitised case examples demonstrating that BO information had been shared with these two FIUs on a number of occasions.

743. Case examples were also provided by the Police in relation to MLAs requesting BO information. The cases involved provision of information from an ASP. One such examples is presented below.

**Box 2.8: MLA requests for BO information**

The Office for the Execution/Handling of MLA request received a letter of request from the authorities of Country A, in relation to an investigation involving company X. The request required included a request to identify the BO of company X, whose director was an ASP licenced in Cyprus. The ASP was called in for questioning and requested to provide documentary evidence identifying the BO. The ASP complied with the request.

744. Supervisors also occasionally receive such requests. While the CBC has never received a specific request to disclose the BO of a licenced person, it actively exchanges information with host and home supervisors where there are changes in qualifying shareholdings of entities it regulates. The CySEC handled various requests for the identification and exchange of BO information: 32 in 2016, 25 in 2017 and 20 in 2018. These requests involved, for instance, cases where the foreign authorities were investigating market abuse/insider dealing/violations of the securities laws (e.g. failing to maintain appropriate internal accounting controls)/fraudulent schemes and sought to

determine the BOs of the entities involved.

*Overall conclusions on IO.2*

745. **Cyprus is rated as having a substantial level of effectiveness for IO.2.**

# TECHNICAL COMPLIANCE ANNEX

This annex provides detailed analysis of the level of compliance with the FATF 40 Recommendations in numerical order. It does not include descriptive text on the country situation or risks and is limited to the analysis of technical criteria for each Recommendation. It should be read in conjunction with the Mutual Evaluation Report.

Where both the FATF requirements and national laws or regulations remain the same, this report refers to analysis conducted as part of the previous Mutual Evaluation in 2011. This report is available from https://rm.coe.int/report-on-fourth-assessment-visit-anti-money-laundering-and-combating-/1680715f1f.

## Recommendation 1 – Assessing risks and applying a risk-based approach

These requirements were added to the FATF standards during the revision that took place in 2012, therefore, were not assessed during the previous evaluation of Cyprus that occurred prior to this date.

**Criterion 1.1** – Cyprus conducted a national risk assessment (NRA) based on the World Bank methodology to identify and assess the ML/FT risks for the country. The process was managed by the CBC and the FIU with the engagement of all the government authorities and services represented on the Advisory Authority and the private sector. The assessment was based on public sector and private sector workshops, surveys and interviews and the analysis of a wide set of qualitative and quantitative data. The final NRA report was published in November 2018. The NRA analyses the ML threat from both a domestic and international perspective, and the ML vulnerability at national and sectorial levels. TF risk is considered separately. The level of threat identified, and the overall vulnerability assessment determine the final risk assessment. The NRA adequately identifies and assesses most of the risks facing the country. It recognises that, as an international financial centre, Cyprus faces an elevated external ML/FT threat and that the banking and ASP sectors are the most exposed to the external threat given their interaction with international clientele. Some ML risks specific to Cyprus, including those emanating from legal persons owned by non-residents and the CIP, have not been formally identified and assessed and, consequently, the precise nature and extent of the risks are not yet known, although mitigating measures have been undertaken to mitigate these risks. While many factors were considered in the assessment of TF risk, some elements were not identified and assessed to their greatest extent (e.g. an assessment of money flows to and from high risk areas, the implications associated with the country of origin or of continuing family ties for an apparently large population of temporary resident workers, etc).

**Criterion 1.2** – The Advisory Authority for Combatting Money Laundering and Terrorism Financing coordinates actions aimed at assessing ML/FT risks (Art. 57(b1) AML/CFT Law).

**Criterion 1.3** – The Advisory Authority is required to update the assessment of risk (Art. 57(b1) AML/CFT Law). It has determined that the NRA should be conducted at four-year intervals. This is also required by the National AML/CFT Strategy.

**Criterion 1.4** – The Advisory Authority communicates the results of the NRA to other competent authorities and the private sector (Art. 57(b1) AML/CFT Law).

**Criterion 1.5** – The Advisory Authority has a general oversight function in relation to the implementation of AML/CFT measures at the national level. Within this role, it discusses and coordinates the allocation and prioritisation of resources required for the combating of ML/FT in response to the risks facing Cyprus. In 2018, the Advisory Authority developed an action plan which addresses the risks identified in the NRA. The action plan includes the allocation of resources within relevant authorities and the implementation of other measures to prevent and mitigate ML/FT.

**Criterion 1.6** – Section 61(6) of the AML/CFT Law provides for a limited exemption in relation to

electronic money. Obliged entities are permitted not to apply certain CDD requirements based on an appropriate risk assessment indicating that the risk is low provided that certain mitigating conditions are met (e.g. limited re-loadability and lack of anonymity). The exemption has been directly transposed from the 4th AML Directive. However, the NRA concludes that the risk posed by electronic money is low in Cyprus.

**Criterion 1.7** – The Advisory Authority is required to identify areas of greater risk, areas where obliged entities are to apply enhanced measures, and, where appropriate, specifying the measures to be adopted (Sec. 57(b1)(i) and (ii), AML/CFT Law). Obliged entities are required to apply enhanced CDD in cases which by their nature present a high risk of ML/FT, provided that when assessing the risks a list of factors of potentially higher risk situations set out in the AML/CFT Law are taken into account (Sec. 64(3), AML/CFT Law). Although obliged entities are not expressly required to take into account the higher risks identified in the NRA, the list of factors of potentially higher risk situations cover the higher risk areas identified in the NRA. In addition, obliged entities are required to manage and mitigate higher risks in specific cases i.e. in relation to high risk countries, correspondent relationships and politically exposed persons (Sec. 64(3), AML/CFT Law).

**Criterion 1.8** – The Advisory Authority is required to identify areas of lower risk (Sec. 57(b1)(ii), AML/CFT Law), which in practice are set out in the NRA. Obliged entities may apply simplified CDD as long as they have previously ensured that the business relationship or transaction presents a lower degree of risk, provided that, at least, the factors of potentially lower risk situations set out in the AML/CFT Law are taken into account (Sec. 63, AML/CFT Law).

**Criterion 1.9** – The AML/CFT Law determines the supervisory authority for each category of FI and DNFBP (Sec. 59, AML/CFT Law). Supervisory authorities are responsible for monitoring, evaluating and supervising the provisions of the AML/CFT Law and any implementing directives (Sec. 59(5a), AML/CFT Law). This includes requirements set out under Rec. 1. See analysis of R. 26 and R. 28 for more information.

**Criterion 1.10** – Obliged entities are required to take appropriate steps to identify and assess ML/FT risks, taking into account risk factors, including factors which relate to their customers, countries and geographical areas, products, services transactions or delivery channels. The risk assessment should be proportionate to the nature and size of the obliged entity, be documented, kept updated and made available to the relevant supervisory authorities. (Sec. 58A, AML/CFT Law) Further detailed requirements are set out in the binding directives issued by supervisory authorities.

**Criterion 1.11** – Obliged entities are required to have adequate and appropriate policies, controls and procedures in place, which are proportionate to their nature and size, to mitigate and manage ML/FT risks effectively (Sec. 58, AML/CFT Law). These measures should be approved by senior management, monitored and, where appropriate, enhanced (Sec. 58C, AML/CFT Law). Enhanced measures are required to be taken as noted under c.1.7.

**Criterion 1.12** – Simplified CDD is permitted only where low risk has been identified (see analysis of c.1.8). Criteria 1.9 to 1.11 are met. Situations in which obliged entities can apply simplified CDD do not expressly exclude situations where there is suspicion of ML/TF. However, Sec. 63(1) requires obliged entities to carry out sufficient monitoring of transactions and business relationships subject to simplified CDD to enable the detection of unusual or suspicious transactions.

***Weighting and Conclusion***

Cyprus meets all the criteria under R. 1, except for c.1.1 and c.1.12, which are mostly met. Some ML risks specific to Cyprus have not been formally identified and assessed and, consequently, the precise nature and extent of the risks are not yet known. While many factors were considered in the assessment of TF risk, some elements were not identified and assessed to their greatest extent. Simplified due diligence is not expressly prohibited where there is suspicion of ML/TF. **R. 1 is rated largely compliant.**

### Recommendation 2 - National Cooperation and Coordination

In the 2011 MER, the former R.31 was rated Compliant.

**Criterion 2.1** – Following the publication of the NRA in October 2018, the Advisory Authority developed an action plan which contains policies and measures intended to mitigate the risks identified in the NRA. The action plan was endorsed by the Council of Ministers of Cyprus in November 2018 and, at the time of the on-site visit, was being implemented by the relevant authorities.

**Criterion 2.2** – The authority designated to develop national AML/CFT policies is the Advisory Authority. It is responsible for advising and informing the Council of Ministers on policy and other measures to be taken in the fight against ML/FT (Sec. 57, AML/CFT Law).

**Criterion 2.3** – The Advisory Authority serves as a mechanism for co-operation among all AML/CFT stakeholders and co-ordination for the development and implementation of policies and activities. It is a body established by the Council of Ministers composed of a representative of the FIU, the CBC, CySEC, ICCS, the MoF, the MJPO, the MFA, the Customs Department, the Cyprus Police, the Company Registry, the association of international banks, the association of commercial banks, the CBA, the ICPAC, the Tax Commissioner, the National Betting Authority, the National Authority for Gambling and Casino Supervision and the Real Estate Registry Board. At the operational level, co-operation is underpinned by legislative provisions in the AML/CFT Law. Practical arrangements also facilitate cooperation. For instance, officers of the Police and the Customs Department are seconded to the FIU. The FIU has direct access to various databases held by other public authorities (see R. 29). The FIU regularly holds joint training with the Police and prosecutors and provides guidelines on ML/FT and confiscation. A memorandum of understanding exists between all financial sector supervisors. All supervisors (including those of DNFBPs) have set up a Special AML/CFT Technical Committee to develop common supervisory practices on the implementation of AML/CFT requirements.

**Criterion 2.4** – Cyprus has mechanisms in place to coordinate national efforts in combatting the proliferation of weapons of mass destruction and PF; the National Committee for the Implementation of the Convention on the Prohibition of Chemical Weapons and the Committee on Export Control of the Ministry of Trade and Industry. More specifically, action is coordinated through the Coordinating Unit to Combat International Terrorism, which was set up for the purpose of coordinating the activities of the relevant Ministries and Departments in the fight against terrorism and in the suppression of illegal activities, but also co-ordinates the combating of trafficking of harmful chemical substances and dual-use goods. There are also two bodies dealing specifically with aspects of PF-related TFS. The first is the Advisory Body on Financial Sanctions[107] set up by the Council of Ministers and chaired by the MoF dealing with (1) requests for the release of funds and financial resources falling within the exceptions/derogations provided for in the relevant resolutions and decisions of the UNSC and the EU and (2) the notification via the MFA of the release of funds and financial resources to the relevant UNSC Sanctions Committees, as well as the European Commission and EU Member States as necessary. The other body is the Unit for the Implementation of Sanctions in the Financial Sector[108], which is chaired by the MoF and deals with the examination of requests pertaining to UN and EU restrictive measures that fall within the financial sector. In addition, the Advisory Authority also serves as a platform for the discussion of PF issues, since the public authorities with ML/TF competences also deal with PF-related matters, with the exception of the Ministry of Energy, Commerce, Industry and Tourism. However, overall, a more active and joined up approach, intelligence and information-sharing on PF is needed

[107] Membership includes representatives of the MoF, the FIU, the MFA, the CBC, CySEC, the MJPO and the Ministry of Energy, Commerce, Industry and Tourism, which includes both the Company Registry and the Trade Services (Imports/Exports Licensing Section)

[108] Membership includes representatives of the Ministries of Finance, Foreign Affairs and Energy, Commerce, Industry and Tourism, the AG's Office, the CBC and CySEC

**Criterion 2.5** – The Commissioner for Data Protection has met with AML/CFT supervisory authorities on a number of occasions and also attended informative sessions organised by DNFBPs for their members, in order to clarify and explain situations of particular interest to obliged entities relating to Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR). Section 70B of the AML/CFT law contains specific references to the Data Protection legislation and ultimately in paragraph (6) it is recognised that the processing of personal data in accordance with the provisions of the AML/CFT law is considered as a matter of public interest for the purposes of the GDPR.

**Weighting and Conclusion**

Cyprus meets most of the criteria under R.2, except for C.2.4 which is mostly met since coordination of policies and activities in the area of PF is somewhat fragmented. **R. 2 is largely compliant with R. 2**.

### Recommendation 3 - Money laundering offence

Cyprus was rated LC for Rec. 1 in the 2011 MER and C for Rec. 2 in the third round. The previous report found that there was a technical deficiency in that TF was not fully covered as a predicate offence for ML (which is now a criterion under Rec. 5).

**Criterion 3.1** – ML is criminalised by Section 4 of the Prevention and Suppression of Money Laundering Activities and Terrorist Financing Laws of 2007-2018 ("**AML/CFT Law**"). The ML offence incorporates the elements from Article 6(1) of the Palermo Convention and Article 3(1) (b) & (c) of the Vienna Convention including the purpose requirements and the ancillary offences (aiding, abetting etc.). The offence also goes beyond the Convention standards by including an offence of negligent ML ("ought to have known"). Section 370 of the Criminal Code provides for the offence of inciting or attempting to induce another to commit an offence.

**Criterion 3.2** – Section 4 AML/CFT Law criminalises the laundering of proceeds from "the commission of illegal activities". "Illegal activities" is defined in Section 2 to mean the predicate offences mentioned in s.5 which in turn provides that a predicate offence is any offence which is defined as an offence by the law of the Republic. Therefore, Cyprus has an "all crimes" approach as all offences are capable of being predicate offences for ML. It is noted that in the previous rounds, Cyprus had a 1-year imprisonment threshold approach but that has now been replaced by an all crimes approach. As also noted in the 4th round, all the FATF predicate offences are adequately criminalised in domestic law.

Difficulties were expressed in the last MER (Paras 54-55) that it was necessary to prove that proceeds came from a specific predicate offence committed on a specific occasion due to the reference, in s.4 as was then in force, of the proceeds coming from "the commission of a predicate offence." This no longer appears to be a technical issue. However, effectiveness issues are discussed in IO7. It is noted that predicate offences are mentioned as one of the purpose requirements in s.4(1)(a)(i) and the purpose requirement in s.4(1)(a)(v).

**Criterion 3.3** – This criterion is not applicable because all criminal offences may be predicate offences for ML.

**Criterion 3.4** – In Section 2 of the AML/CFT Law, "property" is widely defined to mean "*assets of any kind, whether corporeal or incorporeal, movable assets including cash, immovable assets, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such asset*." The definition does not specify that the assets must be located in Cyprus or elsewhere so it is assumed that property may be caught wherever located (and indeed this was the view formed by the previous assessment team).

**Criterion 3.5** – Section 4(2)(d) of the AML/CFT Law explicitly provides that "*No previous or simultaneous conviction for a predicate offence is required, from which the proceeds were derived*."

**Criterion 3.6** – Section 4(2)(a) of the AML/CFT Law provides that it shall not matter whether the

predicate offence is subject to the jurisdiction of the Cyprus Courts or not.

**Criterion 3.7** – the offence of self-laundering is covered explicitly by s.4(2)(b) of the AML/CFT Law: "*a laundering offence may be committed by the offenders of a predicate offence as well*."

**Criterion 3.8** – s.4(2)(c) AML/CFT Law provides that the knowledge, intention or purpose which are required as elements of the offences referred to in s.4 (1) may be inferred from objective and factual circumstances.

**Criterion 3.9** – The sanctions can be considered proportionate and dissuasive:

Knowingly committing the ML offence in s.4 is punishable by a maximum of fourteen years' imprisonment or by a financial penalty of up to €500,000 or by both; and

Negligently committing the ML offence ("ought to have known") is punishable by a maximum of five years' imprisonment or by a pecuniary penalty of up to €50,000 or by both.

**Criterion 3.10** – Section 2(1) of the AML/CFT Law defines "person" to mean any natural or legal person. Thus, criminal liability (including when the offence lacks the mental element i.e. where it is negligence) and the financial penalties, as rehearsed above, apply equally to legal persons. There is no obstacle to parallel criminal, civil, or administrative proceedings with respect to legal persons. Administrative measures may also be taken against legal persons such as exclusion from entitlement to public tenders and disqualification from the practice of commercial activities. The financial sanctions for legal persons (see 3.9 above) are proportionate and dissuasive.

**Criterion 3.11** – s.4(1)(a)(iv) AML/CFT Law contains the ancillary offences of participating in, associating, co-operating, conspiring to commit, aiding and abetting, providing counselling or advice, for the commission of any of the substantive ML offences in s.4. The maximum sanctions are the same as described under Criterion 3.9 above.

**Weighting and Conclusion**

The criteria are fully met and therefore **Cyprus is rated Compliant for Recommendation 3.**

### Recommendation 4 - Confiscation and provisional measures

Cyprus was rated LC under the former Recommendation 3 in the 2011 MER. In addition to making recommendations regarding effectiveness, the assessment team in 2011 also noted that the deficiencies in the TF offence could have a knock-on effect in exercising the powers to freeze and confiscate assets in accordance with the standards.

**Criterion 4.1** – Cyprus' framework for the confiscation of assets is provided for in PART II of the AML/CFT Law. It should be noted that the law does not restrict the powers to confiscating property held by the defendant but also that held by third parties by way of prohibited gifts as per the definition of "realisable property" in s.13 AML/CFT Law.

a) Property Laundered/Proceeds: Part II of the AML/CFT Law enables the authorities to confiscate property laundered and the proceeds of crime. Section 6 provides that where a court has convicted a person for a prescribed offence (defined in sections 1 and 3 to mean "laundering offences" and "predicate offences"), then before sentencing it shall proceed with an inquiry in order to determine whether the accused acquired any proceeds from the commission of illegal activities or an ML offence. "Proceeds" is defined in s.1 to mean "*any kind of property or economic benefit which has been generated directly or indirectly from the commission of illegal activities and includes every subsequent reinvestment or conversion of direct products and every substantial gain*."

Section 7 AML/CFT Law provides that all payments which have been made to the accused or to any other person at any time before or after the commencement of this Law in connection with the commission of illegal activities or of a money laundering offence are deemed to be proceeds of the accused from the commission of illegal activities or the commission of a money laundering offence irrespective of whether this has been committed by the accused himself or another person, and the value of the proceeds acquired by the accused from the commission of illegal activities or of a

money laundering offence is the aggregate value of payments or other rewards made to him or the product of illegal activities or of a money laundering offence or proceeds. Section 7(2) enables the Court to make assumptions in that any property acquired by the accused after committing the offence or transferred into his name at any time during the six years before the commencement of proceedings against him constitutes proceeds, any expenditure made by him during that period was met out of proceeds from illegal activities, an ML offence or payments/rewards made to him in connection with either, and that for the purpose of valuing such property that he received it free of any charge or any interest of others. These assumptions apply unless the contrary is proven, or the Court considers that in making such assumptions there would be a serious risk of injustice to the accused, however, in that case, the court has to set out the reasons for reaching that conclusion regarding property acquired after the criminality, for the purposes of determining if the accused has acquired proceeds and for assessing the value of the proceeds. Section 8 provides that, where the court determines that the accused has acquired proceeds, it shall make a confiscation order of the proceeds in the possession of the accused or a third person.

It is noted that the Court may elect to conduct a summary enquiry under Part VI AML/CFT Law where the kind or amount of the benefit may be more easily determined by an evaluation of the financial position of the accused and his family. The outcome in such cases is the imposition of a pecuniary penalty in respect of the proceeds the accused might have acquired from the offending.

b) Instrumentalities: Regarding instrumentalities, Section 8(1)(b) AML/CFT Law empowers the Court to make a confiscation order for instrumentalities. However, this provision is only triggered where the Court has determined that the defendant has benefitted from proceeds. According to the authorities, the Court may order the seizure and disposal of any items used for the commission of offence on the basis of general powers under sections 32 and 33 of the Criminal Procedure Law or specific legislative provisions in e.g. the Law on Narcotic Drugs and Psychotropic Substances (s.31).

c) TF or Terrorism property: Section 5 AML/CFT Law defines predicate offences as any offence which is defined as a criminal offence by a law of the Republic. Therefore, under Part II AML/CFT Law where a person is convicted of a predicate offence, including TF or terrorism, then property which is the proceeds of the financing of terrorism, terrorist acts or terrorist organisations may be liable to confiscation. As Section 8(2) provides the for the confiscation of instrumentalities, this in theory provides the basis for confiscating property which is or is intended or allocated for use in TF, terrorist acts or terrorist organisations. However, the powers under s.8(2) are only triggered when the Court determines that an accused has acquired proceeds, and therefore the powers under CPL are used as standalone powers for forfeiture (there being no specific standalone provision in the Combating of Terrorism Law).

d) Property of corresponding value: Section 12 AML/CFT Law provides that the confiscation order is to be satisfied through recovery from the "realisable property." S.13(1) AML/CFT Law defines "realisable property" to mean any property held by the accused whether situated in Cyprus or elsewhere and includes property held by others as part of a prohibited gift made by the accused.

**Criterion 4.2** –

a) Identify, trace and evaluate**:** Part V AML/CFT Law contains powers for orders for the disclosure of information. An investigator may apply, in the context of an inquiry conducted in Cyprus or abroad, to the Court under s.45 for a disclosure order. If the court is satisfied, it may make a disclosure order addressed to the person who appears to be in possession of the information (to which the application relates) requiring the person to disclose or produce the said information to the investigator and/or any other person specified in the order within seven days or within such a longer or shorter period of time as the court may specify in the order if it considers expedient under the circumstances. *Inter alia*, the order shall have effect despite any obligation for secrecy or other restriction upon the disclosure of information imposed by law or otherwise. Section 137 of the Criminal Code provides that disobeying a court order is an offence carrying a maximum penalty of two years' imprisonment. Furthermore, the FIU has powers, without the need to obtain a court order, to request and obtain information and/or documents regarding beneficial owners, the

existence of business relationships, beneficiaries, signatories and balances of bank accounts, when deemed necessary for the purposes of analysing suspicious transactions which may relate to ML, TF or predicate offences (s.55(2)(c) AML/CFT Law). Measures can also be taken on the basis of Part II of the Criminal Procedure Law cap. 155. Sections 27-33 provide for search warrants and for the seizure of items mentioned in the warrant or not. Furthermore, s.6 Criminal Procedure Law empowers an investigating officer to issue a written order for the production of a document he considered necessary or desirable for the purposes of such investigation, with failure to do so without reasonable excuse being an offence.

b) Provisional measures**:** Section 14 AML/CFT Law provides for restraint orders which can be made both before and after the issuing of a confiscation order. A restraint order may be made, *inter alia*, (i) where criminal proceedings have been instituted and not concluded or are about to be instituted against a person for the commission of a predicate offence or a laundering offence, (ii) where the Attorney General has made a particular application such as for when a defendant has absconded or died, or (iii) the FIU possesses information which creates a reasonable suspicion that a person may be charged with ML or a predicate offence in Cyprus or elsewhere. A restraint order may be made following an *ex parte* application by the Attorney-General (s.14(5). A restraint order prohibits transactions in any way in realisable property and captures not only that held by the respondent to the order, but anything transferred to him after the order was made, and the court may order the seizure of the restrained property. Charging orders may also be made under s.15 AML/CFT Law on the same grounds as restraint orders and shall create a charge on realisable property specified in the order. A charging order is made following an *ex parte* application by the Attorney General (s.15(3). They take precedence over restraint orders (s.14(4) AML/CFT Law). Charging orders can be made against a wide range of assets including immovable property, bonds, units in a unit trust, and funds in court. Freezing orders against absent suspects are provided for under s.32 AML/CFT Law. Provisional orders may be made following *ex parte* applications.

The FIU has the statutory power to postpone transactions in a bank account pending the issue of a freezing order, whether the case is domestic or foreign (s.55(2)(e) AML/CFT Law).

c) Preventing or voiding actions**:** Section 73 AML/CFT Law empowers the Court to make an order setting aside any prohibited gift with a view to enforcing a confiscation order or a pecuniary penalty. "Prohibited gifts" are defined in s. 13(7) to mean gifts made by the accused at any time during the last six years prior to, or after, the institution of criminal proceedings against him, or made at any time and relating to property received in connection with, or which represents property received in connection with, a predicate offence committed by him or another. Moreover, pursuant to the Contract Law Cap. 149 as amended, contracts may be held null and void in different circumstances, including where the consideration and objects are unlawful (s.24), or where the contract is induced by fraud, coercion, misrepresentation (s.19) or undue influence (s.20). As mentioned above, charging orders may be made at early stages which is an important tool for preventing actions prejudicing the ability to freeze, or recover confiscated property.

d) Appropriate investigative measures**:** see (a) above for the investigative measures.

**Criterion 4.3** – Common law rights of *bona fide* third parties are safeguarded. Section 14(5)(b) AML/CFT Law provides for notice to be given to all parties affected by a restraint order (notwithstanding that the application is initially made on an *ex parte* basis). The powers to make restraint/charging orders are to be exercised with a view to allowing any person other than the accused or the recipient of any prohibited gift, to retain or recover the value of any property belonging to him (s.20(b)) and section 8(3) specifies that where the victim or the complainant in relation to a prescribed offence has claims against the accused, the order, or the potential enforcement of the confiscation order, does not prevent the victim/complainant from seeking compensation through civil action. Finally, claims against the accused by *bona fide* third parties are given priority over the realisation of the confiscation order (s.13(4)(b)).

**Criterion 4.4** – Receivers may be appointed both at the freezing and confiscation stage (sections 14(7), 17(1) AML/CFT Law) to, respectively, take property into possession and deal with it or to

execute the confiscation order and realise the property. It is noted that the court may appoint a receiver as the Official Receiver.

**Weighting and Conclusion**

Cyprus achieves compliance with the criteria under Recommendation 4. **Therefore, Cyprus is rated Compliant for Recommendation 4**.

### Recommendation 5 - Terrorist financing offence

Cyprus was rated LC on the former Special Recommendation II in the previous evaluation (PC in the third round). The 2011 MER assessment team remained unconvinced that the legislation adequately criminalised the collection and providing of funds in knowledge they would be used by terrorists. Cyprus was recommended to introduce a clear and separate criminal offence of TF which covered all the elements of SRII (in addition to already covering the TF Convention).

**Criterion 5.1** – The Law to Ratify the International Convention for the Suppression of the Financing of Terrorism 2001 (Law No.29) ("**the Ratification Law**") ratifies and implements the TF Convention. Section 4 of the Ratification Law provides that "*the offences referred to in article 2 of the Convention are punishable up to fifteen years or to a fine or [€1,700,000] or both."* Therefore Article 2 TF Convention is directly implemented in Cypriot Law and it is an offence to finance (a) the acts constituting offences of the Conventions listed in the Annex to the TF Convention or (b) other acts intended to cause death or serious injury to civilians for the purposes of intimidating a population, or compelling a government/international organisation to do/abstain from doing an act.

**Criterion 5.2** – As mentioned above in 5.1, the Ratification Law gives the TF Convention direct application under Cypriot Law and this ensures compliance with Criterion 5.2(a). However, Recommendation 5 goes further than the TF Convention and 5.2(b) requires the TF offence to extend to any person who wilfully provides or collects funds (by any means, directly or indirectly) with the intention that they should be used or the knowledge that they will be used, in full or in part, by terrorist organisations or individual terrorists even in the absence of a link to specific terrorist act(s). The assessment teams in both the third and fourth rounds highlighted this deficiency and were not satisfied that s.5(b) AML/CFT Law covered this. The Combating of Terrorism Law of 2010 (No 110(I)), as amended by Law No. 94(I)/2017 ("the Combating of Terrorism Law) provides in section 8 for the criminalisation of the provision of "support in any way" including the financing of terrorist groups, members of such groups, any other person for the benefit of a terrorist group/member, any other person for the commission of a terrorism offence or persons included in the catalogues, with knowledge that such support will "contribute to the activities" of the terrorist group etc. This offence seems to adequately cover the providing of funds and making the other provision (such as food and lodgings) for terrorists/terrorist groups. Furthermore, the authorities are also satisfied that the wide language also covers the collection of funds with the intention or knowledge that they will be used by a terrorist or terrorist organisation. However, this language has not been tested in Court and the assessment team considers that there could be ambiguity in whether the mere collecting of funds is covered by "providing support" if the funds are not transmitted to a terrorist/terrorist organisation.

**Criterion 5.2 bis** – During the on-site visit, Cyprus brought into force an amendment to the Combating of Terrorism Law, which criminalises the so-called phenomenon of foreign terrorist fighters and also provides that where "A person who intentionally does any act of organisation or takes part in any action that assist any person in travelling for the purposes of committing a terrorist offence and has knowledge that the assistance rendered is for that purpose, is guilty of an offence". This wide language therefore adequately captures all of the activities set out in UNSCR 2178, such as the financing of an individual's travel to undertake training.

**Criterion 5.3** – "funds" is defined in the TF Convention (which is directly incorporated into domestic law by the Ratification Law) to include assets of every kind… "*however acquired"* and therefore they can be from legitimate or illegitimate sources.

**Criterion 5.4** – Article 2(3) of the TF Convention (as incorporated by the Ratification Law)

provides that for an act to constitute an offence in Article 2(1) it shall not be necessary that the funds were actually used to carry out an offence under Article 2(1). Therefore, it is also not necessary that the funds be linked to a specific terrorist act.

**Criterion 5.5** – The authorities state that according to the Evidence Law and because Cyprus is a common law jurisdiction, that the intention and knowledge required to prove offences can be inferred from objective factual circumstances. The previous assessment team agreed. It is noted that the Cypriot authorities have put the equivalent point beyond any doubt as regards ML (see Criterion 3.8 above) and the absence of such a provision for TF could potentially cause ambiguity and the authorities may wish to consider an equivalent provision.

**Criterion 5.6** – A person convicted of an offence under the TF Convention is liable up to 15 years' imprisonment and/or a fine of EUR 1.7 million (Section 4(1) Ratification Law). A person convicted of an offence under the Combating of Terrorism Law is liable to a maximum imprisonment of 8 years and/or a fine of up to EUR 150,000 which is a modest financial penalty. The sanctions under the TF Convention can be regarded as dissuasive and proportionate. The imprisonment penalty under the Combating of Terrorism Law may also be regarded so but the financial penalty is not dissuasive and there does not seem to be an explanation as to why the penalties under the Combating of Terrorism Law are significantly less.

**Criterion 5.7** – Section 5 of the Ratification Law provides that a legal person of any nature is subject to the same criminal and civil liability in any case where any person, in charge of the administration or control of the said legal person, commits under the said capacity an offence in violation of the TF Convention. Section 14 of the Combating of Terrorism Law provides that, without prejudice to the criminal liability of any natural person who commits a terrorist offence under that law, a legal person has the same liability and may be prosecuted for any offence provided in this law, which was committed on behalf of the legal person from a person who holds management powers.

Section 14 of the Combating of Terrorism Law also provides that the legal person has the same liability and may be prosecuted in a case where the lack of supervision or control from the person referred to above, made possible the commission of an offence provided in that law on behalf of the legal person.

Where a legal person is found guilty of an offence under section 14, it may be subject to a penalty of up to EUR 850,000.

Civil measures may also be taken such as the crossing out of the relevant registry of a legal person or the postponement of its operation for a time considered necessary (s.5(2) Ratification Law) or the permanent or temporary ban on commercial activity; exclusion from public benefits or aid; dissolution; or temporary or permanent closure of premises used for the commission of terrorist offences (section 14, Combating of Terrorism Law).

**Criterion 5.8** – The ancillary TF offences are covered by the direct incorporation, under the Ratification Law, of Article 2 (4) and (5) of the TF Convention.

**Criterion 5.9** – As discussed under Criterion 3.2, section 4 AML/CFT Law criminalises the money laundering of the proceeds from "*the commission of criminal activities*" and therefore that wide language would most probably capture all TF. Also, section 8 of the Ratification Law provides that acts constituting offences under that Law/the Convention are considered predicate offences and there is of course also section 5 of the AML/CFT Law which provides that predicate offences are any offences defined as criminal offences by a law of the Republic of Cyprus. However, the issue identified in 5.2 regarding collection of funds may have a cascading effect such that if the TF offence is not fully implemented, not all TF is a predicate offence for ML.

**Criterion 5.10** – The authorities state that TF offences apply regardless of whether the person alleged to have committed the offence is in the same country or a different country from the one in which the terrorist/terrorist organisation is located, or the terrorist act occurred/will occur. There does not appear to be anything in the legislation which limits the TF offences in contravention of

this criterion and a previous gap regarding non-applicability to Cyprus citizens in Cyprus was removed in 2005.

**Weighting and Conclusion**

Cyprus has met the majority of the criteria for Recommendation 5 and their approach of directly implementing the TF Convention helps them to achieve compliance in many areas. However, the issue regarding the criminalisation of the wilful collection/providing funds with the intention or knowledge of their being used in full or part by an individual terrorist or a terrorist organisation (even in the absence of a link to a specific terrorist act(s)) remains a potential issue. It has been commented on by the previous two assessment teams and despite Cyprus having gone some way to addressing this through the Combating of Terrorism Law, there is still a potential risk that the offence only covers the provision of support and not collection. Cyprus **is rated Largely Compliant for Recommendation 5**.

### Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing

In the 2011 MER, Cyprus was rated Partly Compliant with Special Recommendation III, the equivalent Recommendation under the 2004 FATF Methodology. Deficiencies were numerous and serious; they included that Cypriot law did not encompass the full scope of UNSCR 1267, that funds and assets apparently could not be frozen without delay, that there were no delisting or unfreezing procedures, that there was no guidance on measures that needed to be taken concerning designated persons, and that the financing of terrorism was incompletely criminalized, making coordination with other countries difficult.

As an EU member state, Cyprus is bound by the EU framework implementing UN targeted financial sanctions ("TFS"), which is complemented by provisions in the Suppression of Terrorism Law of 2010 (Law No. 110(I)/2010), the Law for the Implementation of the Provisions of the UN Security Council Resolutions (Sanctions) and the Decisions and Regulations of the Council of the European Union (restrictive measures) of 2016 (Law No. 58(I)/2016)(Law on International Sanctions), Council of Ministers' Decision 73.606 of 25 May 2012 (establishing the Advisory Body on Financial Sanctions) and Council of Ministers' Decision E80.305 of 25 February 2016 (establishing the Unit for the Implementation of Sanctions in the Financial Sector).

**Criterion 6.1** –

a) At the EU level, Cyprus implements UNSCR 1267/1988 (on Afghanistan) through EU Regulation 753/2011 and Council Decision 2011/486/CFSP, and UNSCR 1267/1989 (on Al Qaida) through EU Regulation 881/2002 (and its successors) and Common Position 2002/402/CFSP. These Regulations have direct legal effect in Cyprus. At the national level, designation proposals would be made, if the situation arises, by the MFA by virtue of powers conferred to it by the Constitution of Cyprus as the representative of the country on issues pertaining to the imposition of UN and European sanctions. Cyprus has not made any proposals for designation to date.

b) – e) There are no formal procedures in place establishing a domestic process for identifying targets and the criteria to be applied under that process, or for procedures to be followed when making a designation proposal to the UN. However, the absence of a formal procedure or other mechanism does not prevent the MFA from obtaining input from the other authorities and would not appear to prevent it from coordinating a designation proposal to the UN. There are legal provisions to permit information-sharing in respect of possible designation targets. The MFA has a coordinating role in relation to proposals for designation which would involve obtaining input from other authorities, primarily the Police, the CIS, the FIU and other public authorities. It is likely that Cyprus would apply an evidentiary standard compatible with that in EU Common Position 931/2001, which is equivalent to an evidentiary standard of "reasonable grounds", but in the absence of any formal procedures this cannot be confirmed.

**Criterion 6.2** –

a) At the EU level, the Council of the EU is the competent authority for making EU designations in order to implement UNSCR 1373. This is prepared by the Working Party on restrictive measures to combat terrorism (COMET) of the Council of the EU, which applies designation criteria consistent with the designation criteria in UNSCR 1373. Persons, groups or entities can be included on the list on the basis of proposals submitted by the EU Member States or third countries. At national level, if accounts are held by persons listed in the annex of the relevant EU Regulation that do not fall under the competence of the Common Foreign and Security Policy of the EU (EU internals), Cyprus can freeze these accounts on the basis of Sec. 16B of the Suppression of Terrorism Law. There is no legal basis for a competent authority in Cyprus to make domestic designations on the country's own motion or at the request of another country. To date, Cyprus states that it has not identified the need to make domestic designations nor has it received requests from other countries under pursuant to UNSCR 1373.

b) At the EU level, the COMET Working Party of the Council of the EU applies designation criteria consistent with the designation criteria in UNSCR 1373. For domestic designations, there is no formal mechanism for identifying targets for possible designation on the country's own motion. In relation to actions initiated under the freezing mechanisms of other countries, as noted under criterion 6.1, the MFA has a coordinating role in relation to proposals for designation. This would involve obtaining input from other authorities, primarily the Police, the CIS, the FIU and other public authorities.

c) At the EU level, requests are received and examined by the COMET. All Council working parties consist of representatives of the governments of the Member States. EU designations are directly applicable in all EU Member States and must include sufficient identifying information to exclude those with similar names. Cyprus has never received a request from a third country in the context of UNSCR 1373 and does not have a formal procedure to ensure that a prompt determination is made when it receives a request from another country. However, once, a request was received in relation to an EU sanctions regime concerning Syria. The MFA received intelligence from another country concerning two individuals which had the potential of falling within the listing criteria of that sanctioning regime. Cyprus, on the basis of an informal procedure, was able to make a prompt determination that the proposed designees met the criteria for designation and forwarded the information to the European External Action Service[109].

d) At the EU level the COMET working party, during the designation assessment process, applies the standard of proof of "reasonable basis". The relevant decision is not conditional upon the existence of a criminal proceeding. At the national level, there are no formal procedures to deal with UNSCR 1373 related requests.

e) Cyprus has not requested another country to give effect to actions under domestic freezing mechanisms.

**Criterion 6.3** –

a) At EU level, all Member States are required to provide each other with the widest possible range of police and judicial assistance in matters related to persons/entities that meet the criteria for designation, inform each other of any measures taken, and cooperate and supply information to the relevant UN Sanctions Committee. The Cypriot authorities, particularly the Police, the CIS and the FIU have broad powers to request and receive information when performing their functions on the basis of the Suppression of Terrorism Law, the CC, AML/CFT Law and the Sanctions Law.

b) At the EU level, designations take place without prior notice to the person/entity identified (Art. 7a(1) Regulation 881/2002 and EC Regulation 1286/2009 preamble para.5). For asset freezing, the Court of Justice of the EU makes an exception to the general rule that notice must be given before the decision is taken in order not to compromise the effect of the first freezing order. The listed

[109] The EEAS eventually determined that these two individuals did not meet the listing criteria.

individual or entity has the right to appeal against the listing decision in Court and seek to have the listing annulled. At the national level, the powers of the Police, the SIS and the FIU to obtain information in the course of their functions may be applied *ex parte* (see for instance c29.3 and c.31.3). However, there are neither legal authorities nor procedures or mechanisms which expressly state that the authorities may operate *ex parte* against a person or entity who has been identified and whose proposal for designation is being considered.

**Criterion 6.4** – At the EU level, the implementation of TFS pursuant to UNSCRs 1267/1989 and 1988 does not occur "without delay" due to the time required to transpose UNSC designation decisions into EU framework (consultations between European Commission departments, translations into all official EU languages, etc.). An expedited procedure has been adopted by the Commission for implementation of new listings required by for UNSCR 1989 transposed under EU Regulation 881/2002. The delay between the date of designation by the UN and the date of its transposition into EU framework has consequently shortened to an average of 3-4 days in 2016 and 2017. This is still not consistent with the requirement to implement sanctions "without delay". For resolution 1373, TFS are implemented without delay because, once the decision to freeze has been taken, Council Regulation 2580/2001 is immediately applicable within all EU Member States. At the national level, Cyprus has enacted domestic legal provisions to ensure that designations under UNSCRs 1267/1989 and 1988 are implemented immediately as soon as designations are made by the UNSC without the need to rely on the EU mechanism. This is achieved through Sec. 16B of the Suppression of Terrorism Law and Sec. 4(1) of Law on International Sanctions (see c.6.5(a)).

**Criterion 6.5** –

a) Sec. 16B of the Suppression of Terrorism Law requires all natural and legal persons, including FIs and DNFBPs, to determine whether designated persons and/or entities included in the UN and EU lists have any assets in Cyprus and if such assets are identified, these are frozen without delay and without prior notice. This is purely an administrative procedure without the involvement of any court proceedings. In addition, Sec. 4(1) of the Law on International Sanctions provides that any person who infringes any of the provisions of UN and EU TFS is guilty of an offence.

b) Sec. 16B of the Suppression of Terrorism Law extends to all types of funds and other assets covered under (i) to (iv) of this sub-criterion. Funds or other assets which are jointly owned or controlled are not included. Instead Sec. 16B(1)(b) refers to funds or other assets partly owned by the designated person or entity. This would in effect capture funds or other assets jointly owned with another person. It is not clear whether all the elements of the definition of funds and other assets under the glossary of the FATF Methodology are covered since these terms are not defined in the Suppression of Terrorism Law. However, these elements are fully covered under the relevant EU legislation.

c) EU nationals and legal persons incorporated or constituted under the laws of EU Member States are prohibited from making funds or other economic resources available to designated persons and entities (EC Regulations 881/2002 art.2(2), 753/2011 art.3(2), 2580/2001 art 2(1)(b)). Regulations apply to any natural or legal person, entity, body or group in respect of any business done in whole or in part within the Union. There is no similar prohibition in the Suppression of Terrorism Law. At the national level, this obligation is immediately applicable in Cyprus on the basis of Sec. 4(1) of the Law on International Sanctions.

d) EU legal acts are published in the Official Journal of the EU and information on the designations is included in the Financial Sanctions Database maintained by the European Commission. In addition to EU mechanisms, pursuant to Sec. 17 of the Suppression of Terrorism Law, the Minister for Justice and Public Order publishes a national list of all designations made by the UN and EU designations, including EU internals, in the Government Gazette. The list is available online. Guidance is provided in the form of binding directives issued by all supervisory authorities. The large majority of obliged entities subscribe to the EU Financial Sanctions database – FSF Platform which contains a consolidated list of designated persons and entities). In addition, the MFA circulates any updates to the UN and EU lists received from the Permanent Representations of the

Republic of Cyprus to the United Nations and the European Union to the competent authorities and in particular to the Police, the Ministry of Justice and Public Order, the Ministry of Finance, the Ministry of Interior, the Ministry of Defence, the Ministry of Communications and Works, the Ministry of Industry Commerce and Tourism, the Intelligence Service, the Cyprus Ports Authority, the FIU and the supervisory authorities. The supervisory authorities maintain up-to-date contact lists that allow them to send notice of such actions to obliged entities by email immediately.

e) FIs and DNFBPs are required to immediately inform their supervisory authority upon taking any freezing or other measures in compliance with their requirements under the TFS regime (which would include reporting attempted transactions). The supervisory authorities are required, in turn, to inform the MFA (Sec. 16C(1)) Suppression of Terrorism Law).

f) EU Regulations protect third parties acting in good faith (Regulations 881/2002 art.6; 753/2011). In addition, Section 71 of the AML/CFT Law states, that obliged entities, having in good faith refrained in executing or suspending (delaying) a transaction due to the knowledge that the money held to the credit of the account or the transaction, may be connected with money laundering or terrorist financing offences or with the commission of other criminal offence, shall not constitute breach of any contractual or other obligation towards their customers.

**Criterion 6.6** –

a) At EU level, there are procedures to seek de-listing through EU Regulations (EC Regulation 753/2011, Art. 11(4) for designations under UNSCR 1988 and EC Regulation 881/2002, art. 7a and 7b1 for UNSCR 1267/1989). At the national level, if the MFA receives a request for a delisting, it will advise the relevant parties on the procedure to be followed and would forward all relevant information to the UN Sanctions Committee. The website of the MFA provides information, inter alia, on the role of the MFA, as well all the relevant links to UN and EU websites whereby the procedures to be followed are explained. However, Cyprus has not developed its own procedures to submit de-listing requests to the relevant UN Committee.

b) At EU level, for 1373 designations, the EU has de-listing procedures under Regulation 2580/2001. De-listing is immediately effective and may occur ad hoc or after mandatory 6-monthly reviews. At the national level, since Cyprus does not have the legal authority to make domestic designations on the country's own motion or at the request of another country, there are no legal authorities and procedures or mechanisms to de-list and unfreeze the funds or other assets of persons and entities designated pursuant to UNSCR 1373.

c) At the EU level, a listed individual or entity can write to the EU Council to have the designation reviewed or can challenge the relevant Council Regulation, a Commission Implementing Regulation, or a Council Implementing Regulation in Court, per Treaty on the Functioning of the European Union (TFEU) (article 263 (4)). Article 275 also allows legal challenges of a relevant CFSP Decision. At the national level, as noted under c.6.2, Cyprus does not have the legal authority to make domestic designations on the country's own motion or at the request of another country. There are therefore no procedures to allow, upon request, a review of the designation decision before a court or other independent competent authority.

d) & e) For 1267/1989 and 1988, designated persons/entities are informed of the listing, its reasons and legal consequences, their rights of due process and the availability of de-listing procedures including the UN Office of the Ombudsperson (UNSCR 1267/1989 designations) or the UN Focal Point mechanism (UNSCR 1988 designations).There are EU procedures that provide for de-listing names, unfreezing funds and reviews of designation decisions by the Council of the EU (EC Regulation 753/2011, art.11; EC Regulation 881/2002, art.7a and 7e).

f) At EU level, upon verification that the person/entity involved is not designated, the funds/assets must be unfrozen (EU Regulations 881/2002, 753/2011 and 2580/2001). The EU Best Practices on the implementation of restrictive measures provide guidance on the procedure for cases of mistaken identity (see paras 8-17).

g) At EU level, legal acts on delisting are published in the Official Journal of the EU and information

on the de-listings is included in the Financial Sanctions Database maintained by the European Commission (EC Regulation 881/2002, Art.13; 753/2011, Art. 15; 2580/2011, Art.11). At the national level, the Unit for the Implementation of Sanctions in the Financial Sector deals with the release of funds frozen under all TFS regimes (see criterion 2.4).

**Criterion 6.7** – *(Met)* At EU level, there are mechanisms for authorizing access to frozen funds or other assets which have been determined to be necessary for basic expenses, the payment of certain types of expenses, or for extraordinary expenses (articles 2a of EU Regulation 881/2002, EU Regulation 753/2011, and 5–6 of EU Regulation 2580/2001). At the national level, see c. 7.4.

**Weighting and Conclusion**

Cyprus has in place a framework to ensure that TFS are implemented without delay. However, there are some shortcomings. There are no formal procedures in place establishing a domestic process for identifying targets and the criteria to be applied under that process, or for procedures to be followed when making a designation proposal to the UN. There is no legal basis, and related procedures, to make domestic designations on the country's own motion or after examining and giving effect to, the request of another country. There are neither legal authorities nor procedures or mechanisms which expressly state that the authorities may operate *ex parte* against a person or entity who has been identified and whose proposal for designation is being considered. Cyprus has not developed its own procedures to submit de-listing requests to the relevant UN Committee. There are no legal authorities and procedures or mechanisms to de-list and unfreeze the funds or other assets of persons and entities designated pursuant to UNSCR 1373. There are therefore no procedures to allow, upon request, a review of the designation decision pursuant to UNSCR 1373 before a court or other independent competent authority. It should be noted that all of these shortcomings are, to a significant extent, mitigated by the existence of an EU framework on which Cyprus relies. Cyprus has never had the need to make domestic designations nor has it ever been requested to give effect to freezing measures taken by another country. **R. 6 is Largely Compliant.**

### Recommendation 7 – Targeted financial sanctions related to proliferation

The previous mutual evaluation of Cyprus was conducted prior to the adoption of R.7. This Recommendation concerns an issue for which there is no equivalent under the 2004 FATF methodology. As in the case of R. 6, Cyprus relies on a combination of EU and domestic legislation for compliance with this recommendation. The same domestic legislation and mechanisms apply since reference is made to all UNSCRs irrespective of the sanctions regime.

**Criterion 7.1** – At the EU level, UNSCR 1718 and successor Resolutions on the Democratic People's Republic of Korea (DPRK) is transposed into the EU legal framework (the current legislative framework is based on Council Decision (CFSP) 2016/849 and Regulation (EU) 2017/1509)). UNSCR 2231 on Iran is transposed into the EU Legal framework through EC Regulation 267/2012 as amended by EC Regulations 2015/1861 and 1862. EU regulations are directly applicable in Cyprus, as explained under c.6.4. In addition, Cyprus has legal provisions that would enable it to implement without delay UNSCR obligations (Sec. 16B, Suppression of Terrorism Law and Sec. 4(1) of the Law on International Sanctions), without relying on the EU implementation process.

**Criterion 7.2** –

a) Sec. 16B of the Suppression of Terrorism Law requires all natural and legal persons, including FIs and DNFBPs, to determine whether designated persons and/or entities included in the UN and EU lists have any assets in Cyprus and if such assets are identified, these are frozen immediately and without prior notice. This is purely an administrative procedure without the involvement of any court proceedings.

b) Sec. 16B of the Suppression of Terrorism Law extends to all types of funds and other assets covered under (i) to (iv) of this sub-criterion. Funds or other assets which are jointly owned or controlled are not included. Instead Sec. 16B(1)(b) refers to funds or other assets partly owned by the designated person or entity. This would in effect capture funds or other assets jointly owned with another person. It is not clear whether all the elements of the definition of funds and other

assets under the glossary of the FATF Methodology are covered since these terms are not defined in the Suppression of Terrorism Law. However, these elements are fully covered under the relevant EU legislation.

c) EU nationals and persons within the EU are prohibited from making funds and other assets available to designated persons and entities unless otherwise authorised or notified in compliance with the relevant UNSCRs (Chapter IV (Restrictions on Transfers of Funds and Financial Services) and Articles 21-33 of Regulation 2017/1509, as well as Chapter V (Freezing of Funds and Economic Resources) and in particular Articles 35 and 36). At the national level, this obligation is immediately applicable in Cyprus on the basis of Sec. 4(1) of the Law on International Sanctions.

d) The same domestic mechanism described under c.6.5(d) applies.

e) FIs and DNFBPs are required to immediately inform their supervisory authority upon taking any freezing or other measures in compliance with their requirements under the TFS regime (which would include reporting attempted transactions). The supervisory authorities are required, in turn, to inform the MFA (Sec. 16C(1)) Suppression of Terrorism Law)..

f) EU Regulations protect third parties acting in good faith (Council Regulation (EU) 2017/1509, art.50; Council Regulation (EU) No 267/2012, art.42). For domestic provisions, see c.6.5(f).

**Criterion 7.3** – All supervisory institutions are responsible for monitoring and ensuring compliance by FIs and DNFBPs with the requirements under Recommendation 7. Sanctions for non-compliance with the aforementioned obligations are set out in the Section 4 of the Law N. 58 (I) / 2016 and include: a) in the case of an individual, imprisonment not exceeding two years or to a fine not exceeding €100.000 (one hundred thousand Euro) or both these penalties; b) In the case of a legal entity, a fine not exceeding €300.000 (three hundred thousand Euro). In addition, according to the Article 59(6) of the AML/CFT Law, supervisory authorities have a right to impose sanctions for non-compliance with the requirements of binding directives which they issue for their supervised entities.

**Criterion 7.4** –

a) The EU Regulations contain procedures for submitting de-listing requests to the UN Security Council for designated persons or entities that, in the view of the EU, no longer meet the criteria for designation. Where the UN de-lists a person/entity, the EU amends the relevant EU Regulations accordingly. There are no domestic publicly known procedures enabling listed persons and entities to petition a request for de-listing. Cyprus has to date not received any de-listing requests.

b) At EU level, the EU Best Practices on the implementation of restrictive measures provide guidance on the procedure on the cases of mistaken identity (see paras 8- 17). There are no publicly known procedures available domestically.

c) At the EU level, there are specific provisions for authorising access to funds or other assets, where the competent authorities of Member States have determined that the exemption conditions set out in resolutions 1718 and 2231 are met, and in accordance with the procedures set out in those resolutions (EU Regulation 329/2007 articles 7 and 8, and EU Regulation 267/2012 articles 24, 26, and 27). At the national level, in 2012, Cyprus established the Advisory Committee on Economic Sanctions (Advisory Committee) which deals with the examination of requests for the release of funds from frozen accounts, (affected by UN sanctions and/or EU restrictive measures) which are submitted by credit institutions and are accompanied by the necessary supporting documents and information. The credit institution acts on behalf of the account holder whose account has been frozen. The Advisory Committee submits relevant recommendations for approval or rejection to the Minister of Finance, who subsequently takes the final decision. The decision is based on determination made by the Member States of the EU concerning the exemption conditions set out in resolutions 1718 and 2231. In addition, in 2016 the specialized Unit was set up for the Implementation of Sanctions in the Financial Sector in relation to Sanctions imposed by UNSC Resolutions and Restrictive Measures imposed by EU Council Regulations. The Unit, which is chaired by the Ministry of Finance, deals with the examination of requests that fall within the

financial sector affected by UN sanctions and/or EU restrictive measures. It submits relevant recommendations for approval or rejection, with the final decision to be taken collectively or by a majority of the Ministers of Finance, Foreign Affairs and Energy, Commerce, Industry and Tourism or their representatives.

d) At EU level, legal acts on de-listings are published in the Official Journal of the EU and information on the de-listings is included in the Financial Sanctions Database maintained by the European Commission (EC Regulation 881/2002, Art.13; 753/2011, Art. 15; 2580/2011, Art.11). At the national level, the Ministry of Foreign Affairs informs the relevant departments and authorities of the Republic of the adoption and/or amendment and or expiration of SC/UN sanctions and EU restrictive measures, including de-listing and un-freezing. All the authorities are required to communicate any changes to the entities they supervise.

**Criterion 7.5** –

a) The EU Regulations permit the payment to the frozen accounts of interests or other sums due on those accounts or payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of this resolution, provided that these amounts are also subject to freezing measures (Regulation 329/2007, Art. 9 and Regulation 267/2012, Art. 29).

b) Provisions in the EU Regulations also authorize the payment of sums due under a contract entered into prior to the designation of such person or entity, provided that this payment does not contribute to an activity prohibited by the regulation, and after prior notice is given to the UN Sanctions Committee (Regulation 267/2012, Art. 24 and 25).

**Weighting and Conclusion**

Cyprus meets most of the criteria under this Recommendation. However, there are no domestic publicly-available procedures to submit de-listing requests and unfreeze funds or other assets. . **R. 7 is Largely Compliant**.

### Recommendation 8 – Non-profit organisations

In its 2011 MER, Cyprus was rated PC with the former SRVIII due to the absence of a comprehensive domestic review of the NPO sector's vulnerabilities, absence of outreach to the NPO sector and deficiencies in the sanctioning regime. Since the adoption of the 2011 MER, R.8 has changed significantly.

**Criterion 8.1 –**

a) Societies, institutions, federations/associations, charities and certain non-profit companies have all been identified as falling within the FATF definition of NPO. Societies, institutions and federations/associations are categorised in the electronic register maintained by the MoI by type of activities which include the following: sports, human rights, humanitarian aid, persons with disabilities, international organisations, volunteering in hospitals, research and development, immigration issues, discrimination issues, active citizen issues, environmental issues, community services, family issues, education arts and culture issues, animal welfare issues, health and welfare issues and others. Charities may only be set up for educational, literary, scientific or public charitable purpose. Non-profit companies are registered to promote art, science, religion, charity or any other similar cause/objective. The only subset of NPOs in Cyprus that do not fall within the FATF definition are non-profit companies set up to promote commerce. It is not clear that the authorities apply this distinction, and any risk-based actions flowing from such a distinction, to this type of NPO. With the coming into force of the LSI in 2017, existing societies, institutions and federations/associations were required to revise their statutory documents and provide updated information on their activities to the MoI within a transitionary period which ended on 30 June 2019 (after the date of the on-site visit). The MoI stated that once it was in possession of all the information it would proceed with identifying the features of societies, institutions and federations/associations in Cyprus which by virtue of their activities or characteristics are likely to

be at risk of terrorist financing abuse. The features of charities and non-profit companies that may be at risk of FT abuse have also not been identified. The NRA contains a section on NPOs. While the sector as a whole is assessed as posing a medium-low risk, there is no analysis justifying the rating. It is said that the rating is based on the absence of evidence or case law indicating that the sector has been misused for FT purposes.

b) Cyprus has not identified the nature of threats posed by terrorist entities to the NPOs which are at risk as well as how terrorist actors abuse those NPOs.

c) The LSI was adopted in 2017 to update the legislative framework governing the activities of societies and institutions and ensure that it is in line with the requirements under Rec.8. The process also involves shifting the regulation of charities from under the Charities Law to the LSI by requiring them to re-register as institutions under the LSI. The Charities Law will eventually be superseded by the LSI. The authorities have also clarified that most charities in Cyprus are state-funded and therefore they are unlikely to pose a high risk for TF. There has been no similar review in relation to non-profit companies, although these constitute a smaller portion of NPOs in Cyprus.

d) No reassessment has been carried out since the sector has not been subject to an initial assessment.

**Criterion 8.2** –

a) Cyprus has taken measures to promote accountability, integrity and public confidence in the administration and management of NPOs. One such measures was the establishment of the Office of the Commissioner for Volunteering and non-governmental organisations in 2018. The Commissioner is appointed by, and accountable to, the President of the Republic. The Commissioner is responsible for promoting policies that encourage the establishment of NPOs and their good functioning. The coming into force of the LSI, once implemented, will also significantly enhance the accountability and integrity of NPOs and, as a result, increase public confidence in the sector.

*Societies, institutions and federations/associations:* Art. 4 of the LSI states that an NPO which is unlawful within the meaning of Art. 63 of the CC (unlawful association) or the object or operation of which aims or tends to undermine the Republic, the democratic institutions of the Republic, the security of the Republic, public order, public safety, public health, public morals, fundamental rights and freedoms of the individual or the rights of persons with disabilities, shall have no legal existence and shall not be capable of being registered or if already registered may be dissolved. The LSI requires NPOs to be registered (Art. 7, Art. 26, Art. 44). Registration is refused where a founding member or proposed member by the administration has been convicted of a crime due to lack of honesty or moral disgrace. Applicants must submit a certificate on their criminal record of the members (Art. 6). On a yearly basis, NPOs are required to submit audited financial statements (Art. 49) and notify the Registrar of certain changes (e.g. information of expulsion/registration of new members, change in the address and contact details, whether minimum number of meetings stipulated in the Articles of Association was held, etc)(Art. 10). The Registrar is required to keep the information in the register up to date (Art. 7, Art. 26, Art. 44). Certificates of registration of NPOs are published in the Official Gazette (Art. 7, 26, Art. 44).

*Charities:* Charities are incorporated upon an application by the trustee for a certificate of registration (Art. 2, Charities Law). Every application for a certificate shall, *inter alia*, contain the objects of the charity, a description of the property belonging to or in the possession of the charity, and the name and address of the trustees (Art. 4). The trustees are required to submit an annual return with details of the trustees (Art. 5). The certificate of registration shall be published in the Official Gazette (Art. 6). The trustees of the charity shall keep an account of all moneys received and paid on account of the charity. The accounts shall be certified by the trustees (Art. 10). The Council of Ministers may order that the accounts are audited (Art. 11). The Supreme Court shall have the power and jurisdiction to enforce every charity, give direction and order as may appear necessary or expedient for the administration of a charity and sanction the sale or other disposition of any

property subject to a charity on being satisfied that such sale or disposition is for the benefit and advantage of the charity (Art. 13).

*Non-profit companies:* It is not clear that any measures have been taken to promote accountability, integrity and public confidence in the administration and management of non-profit companies.

b) Cyprus has undertaken a number of initiatives to promote the uniform enforcement and interpretation of the new provisions under the LSI. Seminars have been organised at the Cyprus Academy of Public Administration and in the different districts. A public campaign was also launched on national media outlets. However, the focus of the outreach was on the new law and not on the potential vulnerabilities of NPOs to terrorist financing abuse and terrorist financing risks, and the measures that NPOs can take to protect themselves against such abuse. The assessment team is not convinced that the persons responsible for these initiatives have the necessary expertise to undertake TF-related outreach.

c) No best practices have been developed together with NPOs to address TF risk and vulnerabilities;

d) No measures have been taken to encourage NPOs to conduct transactions via regulated financial channels. However, NPOs regulated by the LSI are required to keep audited accounts that provide detailed breakdowns of income and expenditure and have appropriate controls in place to ensure that all funds are fully accounted for and are spent in a manner that is consistent with the purpose and objectives of the NPO's stated activities.

**Criterion 8.3 –** There are measures in place to ensure that NPOs are effectively supervised and monitored. Supervision is carried out by the General Registrar (and District Registrars) within the Ministry of Interior (MoI) for socieities, institutions, federations/associations and by the MCEI for non-profit companies. However, since Cyprus has not identified the subset of NPOs which are at risk of FT misuse, these requirements apply in the same manner to all NPOs and not on a risk-sensitive basis.

*Societies, institutions, federations/associations:* The LSI sets out a list of measures which broadly correspond to the measures detailed in sub-paragraph 6(b) of INR. 8. These types of NPOs are required to be registered (Art. 7, Art. 26, Art. 44). They must maintain information on the purpose and objectives (Art. 8, 26(3), Art. 44(3)) and the identity of the persons who own, control or direct their activities (Art. 8(e), 26(2), 44(2)). The board of directors of a society is required to keep a fully updated register of its members, which shall be updated at least once a year and shall be available for inspection by the Registrar and any other third party with a legitimate interest (Art 18(5)). All of this information is available to the competent authorities (see for instance Rec. 29 and Rec. 31). Some information is also available publicly on the electronic register maintained by the MoI. NPOs are required to issue financial statements that provide a breakdown of incomes and expenditures (Art. 49). There are no requirements to confirm the identity, credentials and good standing of beneficiaries and associate NPOs and that they are not involved with and/or using the charitable funds to support terrorists or terrorist organisations. Equally, there are no requirements to take reasonable measures to document the identity of their significant donors and to respect donor confidentiality and maintain records on transactions for a period of at least 5 years.

*Charities:* Charities are required to be registered under the Charities Law (Art. 2). They are required to maintain information on their objectives and the trustees (Art. 4) and issue financial statements (Art. 10). There are no requirements to confirm the identity, credentials and good standing of beneficiaries and associate NPOs and that they are not involved with and/or using the charitable funds to support terrorists or terrorist organisations. Equally, there are no requirements to take reasonable measures to document the identity of their significant donors and to respect donor confidentiality and maintain records on transactions for a period of at least 5 years.

*Non-profit companies:* No information is available on these types of NPOs.

**Criterion 8.4** –

a) *Societies, institutions, federations/associations, charities:* The implementation of the requirements under the LSI is monitored by the General Registrar (and District Registrars) within the Ministry of Interior (MoI). Monitoring is conducted off-site on the basis of information (e.g. mandatory notifications, audited financial statements) submitted by the NPOs to the registrar. With respect to societies only, the General and District Registrars may carry out inspections, acting on a complaint or on their own initiative, to ascertain whether the conditions laid down in the LSI are fulfilled (Art.7(6)). In addition, the registrar or any person who may establish a legitimate interest may go to the court and the request the issue of an order for auditing the accounts of a society, institution or federation/association. The auditing is carried out by the Auditor General.

*Non-profit companies* are registered with the DRCOR and have an obligation to file changes and annual return forms.

b) Article 4 of the LSI provides that societies, institutions or federations/associations that are unlawful in the meaning of Article 63 of the Criminal Code (unlawful association) or the object or operation of which aims or tends to undermine the Republic, the democratic institutions, the security of the Republic, the public interests, the fundamental rights and freedoms of all persons, shall have no legal existence, and should be either refused registration, or dissolved by order of the Court. Additionally, any person who is a member of the unlawful society, institution or federation/association, shall be guilty of an offence and liable to imprisonment not exceeding three (3) years or a fine not exceeding three thousand euros (€3,000) or to both such penalties. There are no sanctions for breaches of the provisions of the LSI. There are no sanctions for charities and non-profit companies.

**Criterion 8.5** –

a) Information on societies, institutions and federations/associations is held by the General Registrar and the District Registrars. There are effective systems in place to ensure cooperation, coordination and information sharing between them. Information on charities and non-profit companies is held centrally by Tax Authority and the MCEI respectively. There are no other authorities which hold relevant information on NPOs within Cyprus.

b) Although the Police have received some training on the investigation of FT, it is doubtful that there is any investigative expertise and capability to examine those NPOs suspected of either being exploited by, or actively supporting, terrorist activity or terrorist organisations.

c) The LSI and the Charities Law require NPOs to submit information on their administration and management, which information is maintained by the respective registrars. This information is available to all competent authorities during the course of an investigation on the basis of the powers described under Rec. 31.

d) There is no specific mechanism to ensure that, when there is a TF suspicion involving an NPO, information is shared promptly with competent authorities. However, in such instances, the General/District Registrars would inform the FIU, the Police and the CIS.

**Criterion 8.6** – (*Mostly met*) International requests involving NPOs, if they had to arise, would be received either through the formal channels (i.e. the MJPO) or informally by the Police or the FIU. The Police and the FIU would obtain the requested information from the General/District Registrar. However, there are no points of contact or procedures specific to requests related to NPOs suspected of TF or other forms of terrorist support.

*Weighting and Conclusion*

Cyprus has not identified the subset of NPOs which may be vulnerable to TF abuse. It is, therefore, not in a position to apply measures to the sector on a risk-sensitive basis. It has not been demonstrated that TF outreach has been undertaken by the authorities. However, measures have been taken to promote accountability and integrity of the sector, thereby increasing public confidence in the sector and, with the enactment of the LSI, there are now measures in place to

guard NPOs from abuse. The sanctions do not appear to be proportionate. There are some issues with respect to mechanisms for effective information gathering and investigations of TF cases involving NPOs.

**Cyprus is rated Partially Compliant with Rec. 8.**

### Recommendation 9 – Financial institution secrecy laws

In the 2011 MER, Cyprus was rated compliant on the equivalent recommendation under the 2004 FATF methodology.

**Criterion 9.1 –** There are no financial secrecy laws that impede the implementation of the FATF recommendations. Sec. 46 (3) (c) of the AML/CFT Law explicitly provides that an order for disclosure of information shall have effect despite any obligation for secrecy or other restriction upon the disclosure of information imposed by law or otherwise. The FIU may use the provisions of section 55 (2) (c) of the AML/CFT Law, for obtaining financial information without the need to obtain a court order. In section 49 of the AML/CFT Law it is stated that information relating to the same customer and the same transaction may be exchanged between obliged entities which are subject to the same AML/CFT requirements and are subject to obligations as regards professional secrecy and personal data protection. Section 59(8) of the AML/CFT Law provides that the Unit and the Supervisory Authorities may exchange information within the framework of their obligations, emanating from the AML/CFT Law. Even the exception from access to the registry of beneficial ownership for information that may expose beneficial owners to the risk of fraud, kidnapping, blackmail, violence, or intimidation does not apply to credit institutions and financial institutions (which together cover the FATF definition of "financial institutions") and some DNFBPs. See AML/CFT Law Sec. 61A(9)(a).

**Weighting and Conclusion**

The criterion is met. Recommendation 9 is rated compliant.

### Recommendation 10 – Customer due diligence

In the 2011 MER, Cyprus was rated Largely Compliant on the equivalent Recommendation under the 2004 FATF methodology. Main deficiencies noted were the possibility for low-risk businesses to be exempted from CDD and EDD entirely (rather than just having simplified or reduced requirements, that EDD was required on correspondent banking only for non-EU countries, that there was a general lack of awareness of the CDD concept and process, and that the Registrar of beneficial ownership information was significantly backlogged.

**Criterion 10.1** – Section 66 (2) of the AML/CFT Law explicitly prohibits obliged entities from opening or maintaining anonymous or numbered accounts or accounts in names other than those stated in official identity documents.

**Criterion 10.2 –** Obliged entities are required to apply customer due diligence measures in the following cases: (i) when establishing a business relationship; (ii) when carrying out an occasional transaction which amounts to an amount equal to or higher than EUR 15,000 whether the transaction is carried out in a single operation or in several operations which appear to be linked; (iii) ) when carrying out an occasional transaction which constitutes a transfer of funds as defined in EU Regulation 2015/847[110]; (iv) when there is a suspicion of money laundering or terrorist financing, regardless of the amount or any derogation, exemption or minimum threshold pursuant to the provisions of the present Law; (v) when there are doubts about the veracity or adequacy of previously obtained customer identification data. See AML/CFT Law Sec. 60.

**Criterion 10.3 –** Obliged entities are required to identify the customer and verify the customer's identity on the basis of documents, data or information obtained from a reliable and independent source; when identifying the beneficial owner, obliged entities shall take reasonable measures to

[110]See analysis of R.16

verify that person's identity so that the obliged entity is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer. See AML/CFT Law Sec. 61(1)(a) and (b).

**Criterion 10.4 –** Obliged entities are required to verify that any third person acting on behalf of the customer is authorised to do so and identify and verify the identity of that person. See AML/CFT Law Sec. 61(1)(d).

**Criterion 10.5 –** Obliged entities are required, when identifying the beneficial owner, to take reasonable measures to verify the identity so that the obliged entity is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer. See AML/CFT Law Sec. 61(1)(b).

**Criterion 10.6 –** Obliged entities are required to assess and, depending on the case, obtain information on the purpose and intended nature of the business relationship. See AML/CFT Law Sec. 61(1)(c).

**Criterion 10.7 –** Obliged entities are required to conduct ongoing monitoring of the business relationship with their customers, including scrutinizing transactions to ensure that the transactions are consistent with the obliged entity's information relating to the customer, including the customer's business and risk profile and (where necessary) the source of funds used. Obliged entities are also required to keep such information up to date. See AML/CFT Law Sec. 61(1)(d).

**Criterion 10.8 –** Obliged entities are required to understand the ownership and control structure of customers that are legal entities and arrangements. See AML/CFT Law Sec. 61(1)(b). in addition, binding guidance requires obliged entities to understand the customer's business. For credit institutions the requirement to ascertain the nature and size of business activities apply, see CBC AML/CFT Directive to Credit Institutions para. 75-76A, 85. For money transfer businesses the requirement to obtain information on customers' activities apply, see CBC AML/CFT Directive to Money Transfer Businesses, para. 28, though it should be noted that these requirements only apply with respect to transfers over EUR 1000, -. For securities regulated by CySEC, the requirement to obtain information customers' activities apply, see Cyprus SEC Directive on the Prevention of Money Laundering and Terrorist Financing, para. 21(1). For insurance sector firms the requirement to collect information on business profile, incl. nature and scale of activities, see Sec.3.3.2 of ICCS Order. There is no similar requirement for e-money institutions, Credit Acquiring Companies, Bureaux de Change. These sectors are not very material in Cyprus.

**Criterion 10.9 –** Obliged entities are required to identify a customer which is legal entity or arrangement and verify such a customer's identity on the basis of documents, data and information. See AML/CFT Law Sec. 61(1)(a). For some types of obliged entities, binding guidance fleshes out this general requirement, identifying specific categories and pieces of information that must be collected. For credit institutions, see CBC AML/CFT Directive to Credit Institutions, para. 99-112, 132-133, 135. For money transfer businesses, see CBC AML/CFT Directive to Money Transfer Businesses, para. 28, though it should be noted that some of these requirements only apply with respect to transfers of over EUR 1,000. For securities regulated by CySEC, see the Cyprus SEC Directive on the Prevention of Money Laundering and Terrorist Financing, para. 21(1). For insurance sector firms, see Sec.3.3.2 (3) of ICCS Order. Specific information covered under elements (a-c) are not listed in any binding legislation for other payment institutions that does not act as MVTS providers; for e-money institutions, Credit Acquiring Companies, Bureaux de Change. However, these sectors are not material in Cyprus.

**Criterion 10.10 –** Obliged entities are required, when identifying the beneficial owner, to take reasonable measures to verify the identity so that the obliged entity is satisfied that it knows who the beneficial owner is, including, as regards legal persons. See AML/CFT Law Sec. 61(1)(b). Beneficial owner is defined in Sec. 2(1) of the AML/CFT Law; definition comprises the following elements of legal persons: (i) the natural person who ultimately owns or controls a corporate entity

through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that legal person; (ii) the natural person who holds the position of senior managing official if, after having exhausted all possible means and provided there are no grounds for suspicion, no person under element (i) is identified; (iii) the natural person who holds the position of senior managing official if there is any doubt that the person identified under element (i) is the beneficial owner.

**Criterion 10.11 –** Obliged entities are required to identify the beneficial owners of legal arrangements that are customers, and to verify their identities, and statute specifies the pieces of information that need to be collected. See AML/CFT Law Sec. 61(1)(b), 61B(1), (2). Beneficial owner is defined in Sec. 2(1) of the AML/CFT Law; definition comprises all the elements of legal arrangements' beneficial ownership (b) in the case of trusts: (i) the settlor; (ii) the trustee or commissioner; (iii) the protector, if any; (iv) the beneficiary, or where the individual benefiting from the legal arrangement or legal entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates; (v) any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means; and (vi) in the case of legal entities, such as foundations, and legal arrangements similar to trusts, the natural person holding equivalent or similar positions to the person referred above has to be identified. For additional information also see c. 10.12. Obliged entities are required to identify the beneficial owners of legal arrangements that are customers, and to verify their identities, and statute specifies the pieces of information that need to be collected. See AML/CFT Law Sec. 61(1)(b), 61B(1), (2)

**Criterion 10.12 –** In addition to the CDD measures applied to customer and beneficial owner, obliged entities are required: (i) in the case of beneficiaries that are identified as specifically named persons or legal arrangements, to take the name of the person; (ii) in the case of beneficiaries that are designated by characteristics or by class or by other means, to obtain sufficient information concerning those beneficiaries to satisfy the credit institutions or financial institution that it will be able to establish the identity of the beneficiary at the time of the pay-out. See AML/CFT Law Sec 61(1)(4)(a-b); (iii) in the case of beneficiaries of trusts or of similar legal arrangements that are designated by particular characteristics or class, the obliged entities are required to obtain sufficient information concerning the beneficiary to be satisfied that they will be able to establish the identity of the beneficiary at the time of the pay-out or at the time of the exercise by the beneficiary of its vested rights. See AML/CFT Law Sec. 61(5) (a). See AML/CFT Law Sec. 61(4).

**Criterion 10.13 –** By the date of the on-site visit, no express requirement to take the beneficiary of a life insurance policy into account as a risk factor in determining whether enhanced CDD measures are appropriate had been imposed, and the identity of the beneficiary of a life insurance policy had not been identified as not one of the factors suggesting enhanced CDD may be appropriate. See AML/CFT Law, Annex III.

**Criterion 10.14 –** Obliged entities are allowed to complete the verification of the customer's and the beneficial owner's identity during the establishment of a business relationship, provided that: (i) this is necessary so as not to interrupt the normal conduct of business; (ii) there is low risk of money laundering or terrorist financing; (iii) the customer and beneficial owner identity verification procedures shall be completed as soon as possible after the initial contact. See AML/CFT Law Sec. 62(2).

**Criterion 10.15 –** Credit institutions and financial institutions (categories that comprise FATF "financial institutions") may open accounts pending completion of CDD, but such accounts may not carry out transactions until after CDD is completed. See AML/CFT Law Sec. 62(3). This satisfies the requirement to have risk management policies.

**Criterion 10.16 –** Obliged entities must apply CDD measures whenever there are doubts about the veracity or adequacy of previously obtained customer information data and must expressly apply CDD measures to existing customers at appropriate times on a risk-sensitive basis. See AML/CFT Law Sec. 60(d), 62(6).

**Criterion 10.17 –** Obliged entities are required to apply enhanced customer due diligence measures in the cases which by their nature present a high risk of money laundering or terrorist financing. See AML/CFT Law, Sec. 64 (3). Examples of factors of potentially risk situations are listed in Annex III of the AML/CFT Law. See AML/CFT Law Sec. 64(1)-(3).

**Criterion 10.18 –** Obliged entities are allowed to apply simplified customer due diligence measures, where it has identified that the business relationship or the transaction presents a lower degree of risk. In addition, there are additional safeguards imposed: (i) when carrying out simplified CDD, obliged entities must ensure that they carry out sufficient monitoring of the transactions and the business relationships to enable the detection of unusual or suspicious transactions; (ii) when assessing the risks of money laundering or terrorist financing which relate to types of customers, geographical areas and particular products, services, transactions or delivery channels, the obliged entities are required to take into account measures stipulated in Appendix II of the Law (lower risk scenarios). See AML/CFT Law Secs. 60(c), 63.

**Criterion 10.19 –** Where obliged entities are unable to comply with the customer due diligence requirements, they are required not carry out a transaction through a bank account, establish a business relationship or carry out the transaction, or shall terminate the business relationship and consider making suspicious transaction report to the FIU. See AML/CFT Law Sec. 62(4).

**Criterion 10.20 –** There is a provision allowing for processing of a transaction, followed by filing of a suspicious transaction report, if *not* processing that transaction would frustrate an enforcement action against a suspected money laundering or terrorist financing operation. See AML/CFT Law Sec. 70. This shows that the law can identify elements of AML/CFT compliance that can be superseded if necessary, for law enforcement purposes, such as to avoid tipping off a customer. At the same time, however, it highlights the fact that the law does no such thing with respect to the obligation to perform CDD.

**Weighting and Conclusion**

There is no express requirement to take the beneficiary of a life insurance policy into account as a risk factor in determining whether enhanced CDD measures are appropriate. There are no legal provisions under which obliged entities are allowed not to pursue CDD process, provided that continuation of CDD process will tip-off the customer. Some requirements covered under criterions 10.8-10.9 do not apply to some types of payment institutions (those that do not act as MVTS providers); e-money institutions, credit acquiring companies, bureaux de change. However, these sectors are not very material in Cyprus. **Cyprus is largely compliant with R.10.**

### Recommendation 11 – Record-keeping

In the 2011 MER, Cyprus was rated Compliant on the equivalent Recommendation under the 2004 FATF methodology.

**Criterion 11.1** – All obliged entities (defined by AML/CFT law Sec. 2A) are required to maintain records on transactions for 5 years after the end of a business relationship with a customer or after the date of an occasional transactions for compliance with CDD requirements. This encompasses records necessary to identify transactions and relevant correspondence with customers and other persons with whom they maintain a business relationship. See AML/CFT Law, Sec. 68(1).

**Criterion 11.2 –** For retention of records, see criterion 11.1. Analytical results are included in records required for compliance with CDD requirements, see AML/CTF Law Sec. 61(2), so are also required to be retained.

**Criterion 11.3 –** Credit institutions must ensure that in the case of a ML investigation by the FIU, they will be able to provide different information permitting reconstruction on individual transactions. See CBC AML/CFT Directive to credit institutions Sec. 191. The same applies to Money Transfer businesses (See CBC AML/CFT Directive to Money Transfer businesses Sec. 39), FIs under the CySEC supervision (See CySEC's AML/CFT Directive Paragraph 30), the ICCS supervision (See ICCS Orders – 3.9 (iii)) and IPAAC supervision (See ICPAC's AML Directive Paragraph 6.09).

**Criterion 11.4 –** Sec. 68(2) of the AML/CFT Law provides that financial institutions ensures that all information on CDD, transactions and correspondence are promptly and without delay made available to the FIU and the competent Supervisory Authority. Moreover, this information must be made available to the police on the basis of a disclosure order (Sec. 45 and 46 AML/CFT Law), which requires FIs and DNFBPs to provide information within seven days or within such a longer or shorter period of time as the court may specify if it considers expedient.

**Weighting and Conclusion**

**Compliant.**

### Recommendation 12 – Politically exposed persons

In the 2011 MER, Cyprus was rated Largely Compliant on the equivalent recommendation under the 2004 FATF methodology. Main deficiencies identified were that PEP-related requirements didn't apply to foreign PEPs resident in Cyprus, that there was no provision in statutes for confirming whether beneficial owners were PEPs (though this may have been covered by administrative directives), and that there was no provision for senior management approval to continue business relationship where the customer or beneficial owner of the customer was found to be a PEP subsequent to account opening.

**Criterion 12.1** – Obliged entities are required to have appropriate risk management systems to determine whether a customer or the beneficial owner of a customer is a PEP, must receive approval from senior management to establish or continue a business relationship with a PEP, must take adequate measures to establish the source of wealth and funds involved in business relationships or transactions with a PEP, and must conduct enhanced, ongoing monitoring of a business relationship with a PEP. See AML/CFT Law Sec. 64(1)(c). The definition of PEP encompasses both foreign and domestic PEPs (including PEPs from an international organisation). See AML/CFT Law Sec. 2(1). Where the PEP is no longer entrusted with a prominent public function, for at least 12 months, an obliged entity shall be required to take into account the continuing risk posed by that person and to apply appropriate and risk-sensitive measures until such time as that person is deemed not to pose any further risk specific to PEPs. Although EDD measures are subject to minimum twelve month limited, the risk-based approach would still require consideration by the subject person of the particular risks associated with the customer (and the appropriate mitigating measures).

**Criterion 12.2 –** See discussion of Criterion 12.1.

**Criterion 12.3 –** The definition of PEP includes family members and close associates of PEPs. See AML/CFT Law Sec. 2(1).

**Criterion 12.4 –** Obliged entities must take reasonable measures in order to determine whether the beneficiaries of a life insurance or other investment-related insurance policy, and/or where required the beneficial owner of the beneficiary, are PEPs. These measures shall be taken no later than at the time of the pay-out. Where higher risks are identified, obliged entities are required to inform senior management prior to pay-out of the policy proceeds, to conduct enhanced scrutiny of the entire business relationship with the policy holder. See AML/CFT Law Sec. 64(2). There is no specific requirement to consider making a STR where higher risks are identified in relation to life insurance policies with the involvement of a PEP as a beneficiary or the beneficial owner of the beneficiary.

**Weighting and Conclusion**

Cyprus law establishes a complete framework for financial institutions to handle customers that are PEPs. There is no specific requirement to consider making a STR where higher risks are identified in relation to life insurance policies with the involvement of a PEP as a beneficiary or the beneficial owner of the beneficiary. **R. 12 is largely compliant.**

### Recommendation 13 – Correspondent banking

In the 2011 MER, Cyprus was rated Largely Compliant on the equivalent recommendation under the 2004 FATF methodology. The main deficiency identified was that it had no guidance regarding payable-through accounts.

**Criterion 13.1** – Credit institutions and financial institutions (which together comprise all entities in the FATF definition of "financial institutions") must gather sufficient information about respondent institutions to fully understand the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of its supervision, must assess respondent institutions' prevention of money laundering and terrorist financing controls, must obtain approval from senior management before establishing new correspondent relationships, and must "document the respective AML/CFT responsibilities" of such institutions. See AML/CFT Law Sec. 64(1)(b)(i)-(iv). Documenting AML/CFT responsibilities includes understanding, and if necessary, specifying by contract, the respondent's AML/CFT responsibilities. See CBC Directive, para. 204(vii). The AML/CFT Law do not specify that credit institutions or financial institutions must collect information about whether their foreign correspondents have been subject to ML/TF investigations or regulatory actions. Also, these requirements do not apply to correspondent relationships with respondents situated in countries of the European Economic Area.

**Criterion 13.2 –** Credit institutions and financial institutions must be satisfied that respondent institutions have verified the identify and performed ongoing due diligence on customers having direct access to payable-through accounts, and that they are able to obtain relevant CDD data upon request from respondent institutions. See AML/CFT Law Sec. 64(1)(b)(v), CBC Directive para. 204(viii). The requirements do not apply to correspondent relationships with respondents situated in countries of the European Economic Area.

**Criterion 13.3 –** Credit institutions and financial institutions are clearly prohibited from entering into or continuing correspondent relationships with shell banks and must reach reasoned decisions as to whether potential respondent institutions are shell banks. See AML/CFT Law Sec. 66(1), CBC Directive para. 204(i). By contrast, credit institutions and financial institutions must take appropriate measures to ensure that they do not engage in correspondent relationships with other credit institutions or financial institutions "known to allow their accounts to be used by shell banks." See AML/CFT Law Sec. 66(1),. This suggests that credit institutions and financial institutions can accept third party evaluations of whether potential respondent institutions could allow their accounts to be used by shell banks, rather than requiring that the institution make its own evaluation on this issue.

**Weighting and Conclusion**

**R.13 is partially compliant.** The requirements do not apply to correspondent relationships with respondents situated in countries of the European Economic Area.

### Recommendation 14 – Money or value transfer services

In the 2011 MER, Cyprus was rated Largely Compliant on the equivalent Recommendation under the 2004 FATF Methodology. Deficiencies that were noted included that there were no rules on PEPs, no provisions concerning minimum data collection, no penalties for infringement of obligations, no requirement on MTBs to examine the purpose of transactions, and no requirement on value transfer businesses to be licensed or registered. Since the last evaluation, the provisions of Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market have been transposed into national law - the Provision and Use of Payment Services and Access to Payment Systems Law of 2018 (Payment Services Law) - regulating the provision of payment services.

**Criterion 14.1** – Legal persons that provide money and value transfer services are required to be licensed by the CBC (Section 5 and annex 1 (5) of the Payment Services Law). Only legal persons are licensed by the CBC as Payment Institutions which offer money remittance services. The CBC

maintains a public register of licensed MSBs.

**Criterion 14.2 –** Section 37. -(1) of the Payment Services Law provides that it is forbidden for natural or legal persons who are not payment service providers to provide payment services. Provision of services without a licence is an offence and upon conviction natural and legal persons are liable to a maximum of two years' imprisonment and/or a fine of up to a maximum amount of EUR 85, 000. With a view to identifying the provision of services without a licence, the CBC enquires with licenced entities whether they are aware of unlicensed activities and conducts periodic searches to identify any internet advertising of unlicensed operations.

**Criterion 14.3 –** According to Section 59. -(1) (a) AML/CFT Law, the CBC is designated supervisory authority for MVTS, including branches and agents, which hold a relevant operational license granted by a competent authority of a member state. Section 59. -(4) and (5) (a) of the AML/CFT Law elaborates on the modality of the CBC AML/CFT supervision and monitoring.

**Criterion 14.4 –** All agents of the licensed legal persons are subject to the prior approval of the Central Bank of Cyprus and a register is published on the CBC website.

**Criterion 14.5 –** MSB providers are required to have adequate policies, controls and procedures in place to mitigate and manage ML/TF risks (Sec. 58 AML/CFT Law), which should be communicated, *inter alia*, to authorised agents (Para 7 CBC Directive). There should be appropriate mechanisms, including on-site visits, to determine the level of compliance by authorised agents with the policies, procedures and controls of the MSB provider and provide training to agents (Para. 14 CBC Directive).

**Weighting and Conclusion**

Compliant.

### Recommendation 15 – New technologies[111]

In the 2011 MER, Cyprus was rated Largely Compliant with the equivalent Recommendation under the 2004 FATF methodology. The deficiency noted was that there were no provisions regarding misuse of technological developments.

**Criterion 15.1** – Cyprus obliged entities are all under an indirect obligation to identify and assess the ML/TF risks that may arise in relation to new technologies. They are required to undertake enhanced customer due diligence in situations that present a high risk of ML/TF, and in assessing situations that pose high risks they are required to consider, among other things, "new products and new business practices, including new delivery mechanism[s], and the use of new or developing technologies for both new and pre-existing products". AML/CFT Law, Sec. 64(3) and Annex III, para. 2(e). Banks are also subject to a more direct requirement: credit institutions must apply policies, procedures and measures to identify, assess and manage ML/TF risk during the day-to-day operations of the credit institution in relation to (a) the development of new products, services, new business practices, including new delivery channels (b) the use of new or developing technologies for both new and existing products and (c) possible changes in the business profile of the credit institution (e.g. penetration to new markets by opening branches/subsidiaries in new countries/areas). CBC AML Directive, para. 13(xi). S Securities are specifically required to comply with the European Supervisory Authorities' Risk Factor Guidelines, which requires that they understand the risks associated with new or innovative products or services, particularly where this involves the use of new technologies. CySEC Circular C276, ESA Risk Factor Guidelines paras. 30, 67. Insurance companies are required to evaluate risks arising from "new customers, new products, and updating and amending systems and procedures." ICCS Revised AML Orders, sec.

[111] The FATF revised R.15 in October 2018 and its interpretive note in June 2019 to require countries to apply preventive and other measures to virtual asset service providers and virtual asset activity. This evaluation does not assess Cyprus's compliance with revised R.15 because, at the time of the on-site visit, the FATF had not yet revised its assessment Methodology accordingly. Cyprus will be assessed for technical compliance with revised R.15 in due course, in the context of its mutual evaluation follow-up process.

4.2(xii). There is no similarly explicit requirement for other types of obliged entities. Apart from the requirements under Sec. 64(3) of AML/CFT Law, there are no more detailed requirements for payment institutions, for e-money institutions, credit acquiring companies, bureaux de change. However, these sectors are not material in Cyprus. Cypriot authorities have taken actions to understand the risk of new technologies. That has resulted in issuing public warnings to the obliged entities on the risks posed by virtual currencies, attending training seminars to increase supervisory expertise in virtual currencies and other FinTech related products, examining features of FinTech-related products by closely engaging in consultations with the private sector entities, etc. In relation to virtual currencies, supervisory authorities closely monitor international practices, in particular, taking into consideration results of the supranational (EU level) risk assessment, warnings issued by EU bodies (such as ECB, ESAs, EC, etc.) on risks posed by virtual currencies, recent guidance issued by the FATF, etc. Cyprus is in the process of introducing the amendments to the AML/CFT Law aiming to regulate virtual currency exchange operators and custodian wallet providers (as required by the 5th AMLD).

Cyprus also considers the risks of new delivery mechanisms. The authorities reported that private sector firms recently expressed a huge interest to introduce new regulatory requirements which would allow them to identify the customer using mobile phone solutions (following the example of some other EU FinTech companies). However, after careful examination of new delivery mechanism-related risks, the country decided not to legally approve this innovation. And on the other hand, where similar requirements in relation to new delivery channels have been introduced (e.g. requirement to meet introduced customers provided that such a meeting is held using controlled video streaming tools), certain regulatory measures have been imposed to have adequate safeguards in place (e.g. quality of the sound/view, record keeping, etc.).

**Criterion 15.2** – (*Mostly Met*) For credit institutions, the risk assessment must be conducted prior to the launch of the new products, business practices or the use of new or developing technologies and there must be measures in place to manage and mitigate the risks, see section 13 of the CBC directive. Entities regulated by CySEC, Securities, similarly, must specifically undertake "measures and procedures for the prevention of the abuse of new technologies and systems providing financial services, for money laundering and terrorist financing.", see CySEC AML/CFT Directive, para. 9(1)(a). Other obliged entities more generally must take measures to prevent the use of products or transactions that may favour anonymity and must apply reasonable measures and procedures to address the risks of technological developments and new financial products. See AML/CFT Law Sec. 66(3). This obligation does not clearly extend to new business practices in general, or to new delivery mechanisms in particular, and does not require that risk assessment and mitigation take place before launch of a new technology. Apart from the requirements under Sec. 64(3) of AML/CFT Law, there are no more detailed requirements for insurance firms, payment institutions, for e-money institutions, credit acquiring companies, bureaux de change. However, these sectors are not material in Cyprus.

*Weighting and Conclusion*

Credit institutions, securities and insurance firms are required to identify, assess, and manage the ML/TF risks that may arise in relation to new technologies. More detailed requirements for other type of financial institutions are missing. In general, there is no explicit requirement for risk assessment and mitigation to take place before launch of a new technology, product or service. **R. 15 is rated Largely Compliant**.

### Recommendation 16 – Wire transfers

In the 2011 MER, Cyprus was rated Compliant with the equivalent Recommendation under the 2004 FATF methodology. Since that time, the EU has promulgated Regulation 2015/847 on information accompanying transfers of funds, to which Cyprus is subject.

**Criterion 16.1** – The obligation to ensure that wire transfers are accompanied by specific information about the originator and beneficiary, with originator information being verified, is implemented by Art. 4(1) and (2) of EU Reg. 2015/847.

**Criterion 16.2 –** This criterion on batch files is implemented through Art. 6, 7(2) and 11(2)c) of EU Reg. 2015/847, with relevant references to Art. 4 for required and accurate originator information, as well as for required beneficiary information.

**Criterion 16.3 –** Under Art. 6 of EU Reg. 2015/847, cross-border wire transfers below EUR 1,000 should always be accompanied by the required originator and beneficiary information.

**Criterion 16.4 –** According to Art. 6 of EU Reg. 2015/847, FIs need not verify the information on the originator unless, inter alia, they have reasonable grounds for suspecting ML/FT.

**Criterion 16.5 and 16.6 –** Wire transfers within the EEA are considered domestic transfers for the purposes of R.16, consistent with the FATF Standards. Art. 5 of EU Reg. 2015/847 prescribes that such transfers shall be accompanied by at least the payment account number of both the originator and the beneficiary, or by the unique transaction identifier. There is a 3 working day period established for the ordering FI to make available required originator information whenever requested to do so by the beneficiary or intermediary FI. In addition, Art. 14 of EU Reg. 2015/847 requires FIs to respond fully and without delay to enquiries from appropriate AML/CFT authorities.

**Criterion 16.7 –** Art. 16 of EU Reg. 2015/847 establishes a 5-year period for FIs to maintain records of originator and beneficiary. Upon expiry of this period, personal data is to be deleted, unless provided for otherwise by national law. The Regulation allows Member States to decide upon further retention only after carrying out a thorough assessment of the necessity and proportionality of such further retention, and where it is justified for the ML/FT purposes. That further retention period shall not exceed five years.

**Criterion 16.8 –** EU Reg. 2015/847 (Art. 4) prohibits the ordering FI to execute any transfer of funds before ensuring full compliance with its obligations concerning the information accompanying transfers of funds.

**Criterion 16.9 –** Art. 10 of EU Reg. 2015/847 requires intermediary FIs to ensure that all the information received on the originator and the beneficiary accompanying a transfer of funds is retained with the transfer.

**Criterion 16.10 –** EU Reg. 2015/847 does not provide for the exemption specified in this criterion regarding technical limitations preventing the appropriate implementation of the requirements on domestic wire transfers.

**Criterion 16.11 –** Art. 11 of EU Reg. 2015/847 obliges the intermediary FI to implement effective procedures including, where appropriate, ex-post or real-time monitoring, in order to detect whether required originator or beneficiary information in a transfer of funds is missing.

**Criterion 16.12 –** The intermediary FI should have effective risk-based procedures for determining whether to execute, reject or suspend a transfer of funds lacking the required payer and payee information and for taking the appropriate follow up action (Art. 12 of EU Reg. 2015/847). If the service provider has not been provided with the required payer or payee data, it shall reject the transfer or ask for the required information on the payer and the payee before or after the transmission of the transfer of funds, on a risk-sensitive basis.

**Criterion 16.13 –** According to Art. 7 of EU Reg. 2015/847, the obliged entity of the beneficiary shall implement effective procedures, including, where appropriate, ex-post monitoring or real-time monitoring, in order to detect whether information on the payer or the payee is missing for transfers of funds where the PSP of the payer is established outside the EU, as well as for batch file transfers where the PSP of the payer is established outside the EU.

**Criterion 16.14 –** Art. 7 of EU Reg. 2015/847 provides that, in the case of transfers of funds exceeding EUR 1,000, the beneficiary FI shall verify the accuracy of the identification information on the beneficiaries before crediting their payment account or making the funds available to them.

**Criterion 16.15 –** Art. 8 of EU Reg. 2015/847 obliges the beneficiary FI to implement effective risk-based procedures for determining whether to execute, reject or suspend a transfer of funds lacking

the required originator and beneficiary information and for taking the appropriate follow-up action.

**Criterion 16.16 –** The obligations listed above also apply to MVTS providers and their agents (EU Reg. 2015/847, art.2(1)).

**Criterion 16.17 –** The payment service provider of the payee shall take into account missing or incomplete information on the payer or the payee as a factor when assessing whether a transfer of funds, or any related transaction, is suspicious and whether it is to be reported to the FIU (EU Reg. 2015/847, art. 9). There is no explicit obligation requiring payment service providers to file an STR in any country affected by the suspicious wire transfer, in cases where a payment service provider controls both the sending and receiving end of the transfer.

**Criterion 16.18 –** FIs that conduct wire transfers are subject to the EU requirements that give effect to UNSCRs 1267 and 1373, and successor resolutions.

**Weighting and Conclusion**

Cyprus meets of the criteria under R. 16. However, there is no explicit obligation requiring payment service providers to file an STR in any country affected by the suspicious wire transfer, in cases where a payment service provider controls both the sending and receiving end of the transfer. R. 16 is rated **Largely Compliant.**

### Recommendation 17 – Reliance on third parties

In the 2011 MER, Cyprus was rated Compliant with the equivalent Recommendation under the 2004 FATF methodology. The 2013 methodology broadened the Recommendation to address reliance on third parties within financial groups.

**Criterion 17.1** – Obliged entities are permitted to rely on third parties to perform elements of CDD (customer identification, beneficial owner identification, understanding the nature of the business relationship), so long as those third parties are themselves "obliged entities" (roughly equivalent to FATF financial institutions plus some DNFBPs) that apply CDD and recordkeeping measures consistent with those required by the EU's Fourth Anti-Money Laundering Directive, and that are supervised consistent with the requirements of that Directive. See AML/CFT Law Sec. 67(1), (2). Such persons, while they may rely on such third parties, retain ultimate responsibility for compliance with CDD requirements. See AML/CFT Law Sec. 67(1). Such third parties must make CDD information immediately available to such persons and forward immediately to them copies of data, information and identification documents obtained as a result of the CDD procedures. See AML/CFT Law Sec. 67(3).

**Criterion 17.2** – Cyprus law leaves to obliged entities the decision as to whether the home jurisdiction of a third party is a "high-risk third country" – in which case the third party would be disqualified from performing CDD elements as provided above. See AML/CFT Law Sec. 67(2)(b)(i). However, it establishes clear criteria for such persons to determine what is a high-risk third country, including adopting the European Commission's categorical definition of countries or territories having strategic deficiencies in the AML/CFT regimes and posing significant threats to the financial system of the European Union as well as a risk-based component. See AML/CFT Law Sec. 2(1).

**Criterion 17.3** – Cyprus law permits an obliged entity to rely on a third party from the same group as the obliged entity, so long as the group is subject to appropriate CDD, recordkeeping and AML program obligations and is subject to effective supervision at group level by the supervisory authority of the group's home state. See AML/CFT Law Sec. 67(4). This permission is subject to the obligation that the group's AML/CFT policies take into account at a minimum the risk factors identified in Annex III to the AML/CFT Law, which include geographic risk factors associated with reliance on the third party.

**Weighting and Conclusion**

Cyprus is **Compliant with R. 17.**

### Recommendation 18 – Internal controls and foreign branches and subsidiaries

In the 2011 MER, Cyprus was rated Largely Compliant with the equivalent Recommendation under the 2004 FATF methodology. Deficiencies that were noted include that there was is no explicit requirement to establish independent audit for all insurance and MTBs. The 2013 methodology broadened the Recommendation to address group-wide programs and situations in which the AML/CFT obligations of home and host countries varied.

**Criterion 18.1** – Obliged entities are required to implement risk-based programmes to mitigate and manage money laundering and terrorist financing risks, and those programmes must include compliance management arrangements (including appointing a money laundering compliance officer), screening procedures for employees, training for employees on recognizing and handling ML/TF-related transactions, and the possibility of an independent audit. See AML/CFT Law Sec. 58, 58B, 58C, 58D, 69. It is possible for an obliged entity to conclude that its own size and nature of activities make it unnecessary to have an independent audit, but the obliged entity's supervisor retains the authority to require an independent audit despite the obliged entity's conclusion to the contrary. See, e.g., CySEC Circular C056, para. 28.

**Criterion 18.2** – Financial groups must implement group-wide AML/CFT policies, including policies for sharing information within the group and data protection policies and procedures. See AML/CFT Law Sec. 68A.

**Criterion 18.3** – Branches or subsidiaries of obliged entities in third countries must implement AML/CFT requirements of Cyprus if the requirements of host countries are less strict than those of Cyprus, or if that is not permitted must take additional measures to effectively deal with ML/TF risks and must notify their supervisory authorities. See AML/CFT Law Sec. 68A.

**Weighting and Conclusion**

Cyprus has a well-developed legal framework for requiring financial institutions to maintain AML/CFT programs with most of the necessary elements. It is still the case that there is no general, universal requirement for independent audit, however. **Largely Compliant.**

### Recommendation 19 – Higher-risk countries

In the 2011 MER, Cyprus was rated Largely Compliant on the equivalent recommendation under the 2004 FATF methodology. Deficiencies noted were the lack of requirements for Investment Brokers, Insurers or International Businesses to give special attention to business relationships and transaction with persons from or in countries not applying FATF Recommendations.

**Criterion 19.1** – Obliged entities must apply enhanced due diligence when transacting with legal or natural persons with establishments in "high-risk countries." See AML/CFT Law Sec. 64(1)(a). High-risk countries are defined according to designation by the EC, see AML/CFT Law Sec. 2(1), and when identifying countries, the EC is required to take into account relevant evaluations by international organisations in relation to the ML/TF risks posed by individual third countries. See 4AMLD, Art. 9(4). The EC has interpreted this to include FATF and has adopted the FATF public statement. See Commission Delegated Regulation 2016/4180. In addition, obliged entities must apply EDD in cases which "by their nature" present high risks, and must take into account geographic risk factors that include identification of countries by credible sources that include mutual evaluations and detailed assessment reports as not having effective AML/CFT regimes (i.e. third countries which, on the basis of credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, do not effectively implement FATF requirements). See AML/CFT Law Sec. 64(3) and Annex III.

Binding directives issued by the financial supervisors further clarify this requirement. to the directive for credit institutions provides they are required to apply enhanced due diligence and

monitoring measures with business relationships or transactions with natural or legal persons or financial institutions that originate from countries that do not or inadequately apply the FATF recommendations (see section 211). In addition, Section 210 of the said directive provides that the FATF publishes the list of countries having strategic weaknesses/deficiencies in AML/CFT regime. Binding guidance directive provides that Money Transfer Businesses (MTBs) are required to apply EDD measures for transfers of funds from or to countries which do not apply or inadequately apply FATF's recommendations (i.e. MTBs are required to perform additional monitoring procedures and pay special attention to money transfer transactions with persons, including companies and financial institutions, from countries which do not apply or apply inadequately FATF recommendations. In addition, MTBs are required thoroughly examine such transactions in order to establish their economic, commercial or investment purposes; and file a STR to FIU in case of suspicion). See the CBC AML/CFT Directive to MTBs, Sec. 33-34. Binding guidance to insurance companies (ICCS orders, see section 3.6.4 (1-2)) provides that insurance companies are required to apply specific additional CDD measures (i.e. exercise additional monitoring procedures and pay special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not apply or they apply inadequately FATF Recommendations; insurance companies are required examine such transactions in order to establish their background and purpose; and file a STR to FIU in case of suspicion.

Apart from the requirement under Sec. 64(1)(a) of the AML/CFT Law, no binding guidance on high risk third countries has been issued for payment institutions that do not act as MTBs providers; e-money institutions, credit acquiring companies, bureaux de change. However, these sectors are not material in Cyprus.

**Criterion 19.2** – The enhanced due diligence that obliged entities are required to undertake when transacting with establishments in high-risk countries can, but is not required to, include countermeasures of the kind typically imposed by FATF. As discussed above (see c.19.1), countermeasures typically include enhanced monitoring of business relationships and transactions. As per section 57 of the AML/CFT Law, the Advisory authority has the right to identify any areas where obliged entities are to apply enhanced measures and, where appropriate, specify the measures to be adopted. There is a domestic mechanism in place to apply countermeasures proportionate to the risks when the need arise (albeit not directly linked to third country risks, this can cover all the risk areas whenever the need arise).

**Criterion 19.3** – The CBC circulates to all supervised entities the FATF public statements and asks for compliance with the said statements. Binding guidance requires that MLCOs of credit institutions should obtain and study the announcements and the country assessment reports prepared by the FATF, MONEYVAL and other FSRBs, the IMF and the World Bank in order to implement additional due diligence measures for identifying and monitoring transactions of persons from countries with significant shortcomings in their legal and administrative systems for the prevention of ML/TF. See CBC AML/CFT Directive to Credit Institutions, Sec. 161. Moreover, the CBC indicated to the assessment team that it notifies credit institutions via email whenever FATF issues public statements. The CBC also informs MTBs about countries which do not apply or inadequately apply FATF's recommendations and by binding guidance requires them to take appropriate steps. See CBC AML/CFT Directive to MTBs, Sec. 35. CySEC publishes on its website and sends obliged entities it regulates advisory emails about changes to the EC delegated regulation concerning high-risk third countries with strategic deficiencies, and requires AML officers of entities it regulates to consult sources of information on high-risk third countries that include FATF, MONEYVAL, and the UN among others. CySEC AML/CFT Directive, para.17. ICPAC, CBA, and ICCS impose similar requirements on obliged entities they regulate. No information has been provided by the ICCS on actions taken to advice insurance firms about the weaknesses in the AML/CFT systems in other countries.

**Weighting and Conclusion**

Apart from the requirement under Sec. 64(1)(a) of the AML/CFT Law, no binding guidance on high risk third countries has been issued for payment institutions that do not act as MTBs providers; e-

money institutions, credit acquiring companies, bureaux de change. However, these sectors are not material in Cyprus. No information has been provided by the ICCS on actions taken to advice insurance firms about the weaknesses in the AML/CFT systems in other countries**. Cyprus is rated as largely compliant.**

### Recommendation 20 – Reporting of suspicious transaction

In the 2011 MER, Cyprus was rated Largely Compliant on the equivalent Recommendation under the 2004 FATF methodology. Deficiencies that were noted included a failure to harmonize laws punishing a failure to report suspicious transactions and imposing an obligation to file such reports.

**Criterion 20.1** – All financial institutions (using the FATF definition of the term) are covered by the requirement for obliged entities (the term used in the AML/CFT Law, defined at Sec. 2A) to file with the FIU reports on transactions suspected of involving proceeds of illegal activity or of relating to terrorist financing irrespective of the amount. Reports are required to be submitted to the FIU immediately upon suspicion. See AML/CFT Law Sec. 58, 69 (d).

**Criterion 20.2** – The STR filing obligation applies with respect to attempted transactions, and without respect to the size of the transaction. See AML/CFT Law Sec. 69(d).

**Weighting and Conclusion**

Cyprus has a comprehensive legal requirement for financial institutions to report suspicious transactions and attempted transactions. **Compliant.**

### Recommendation 21 – Tipping-off and confidentiality

In the 2011 MER, Cyprus was rated Largely Compliant on the equivalent Recommendation under the 2004 FATF methodology. The deficiency noted was that the prohibition on tipping off didn't cover all cases where an STR was reported or was in the process of being prepared.

**Criterion 21.1** – Obliged entities under Sec. 69A and Sec. 2A AML/CFT law embrace FIs. Disclosure of information in an STR shall not constitute a breach of any restriction on disclosure and shall not result in liability of any kind, even when the filing entity was not precisely aware of the underlying criminal activity. These provisions are applicable to obliged entities, their employees or directors See AML/CFT Law Sec. 69A.

**Criterion 21.2** – Obliged entities under Sec. 69A and Sec. 2A AML/CFT law embrace FIs. Their directors and employees may not notify clients or third parties that information relating to suspicious transactions has been, is being, or will be transmitted to the FIU, or that an analysis of information relating to suspicious transactions is being or will be carried out. See AML/CFT Law Sec. 48.

**Weighting and Conclusion**

Cyprus has clear legal standards enforcing STR confidentiality and protecting filers of STRs. **Compliant.**

### Recommendation 22 – DNFBPs: Customer due diligence

In the 2011 MER, Cyprus was rated Partly Compliant on the equivalent Recommendation under the 2004 FATF Methodology. Deficiencies included lack of a legal framework covering TCSPs, no identification of other activities where it was the case that cash payments above € 15,000 were OK, uncertainty about the coverage of accountancy, the fact that lawyers were permitted to forego the customer identity verification process upon declaration, and the lack of adequate requirements to pay special attention to risks arising from new or developing technologies. This Recommendation was largely unchanged under the 2013 methodology.

**Criterion 22.1** – The types of DNFBPs specifically identified in the Criterion are all required, in the circumstances identified in the Criterion, to comply with CDD requirements that are themselves largely compliant (see Recommendation 10 above). See AML/CFT Law Sec. 2A(1). Casinos are separately required to comply with CDD requirements with respect to transactions over EUR 2,000,

which is stricter than demanded by Rec. 22.1.(a). See AML/CFT Law Sec. 60(e). Dealers in precious metals and stones are prohibited from engaging in transactions over EUR 10,000, so they are not permitted to engage in transactions at the threshold where the requirements of this criterion would apply to them. See AML/CFT Law Sec. 5A.

**Criterion 22.2** – AML/CFT Law Sec. 68 requires all obliged entities, including DNFBPs, subject to Rec.22, to comply with record retention requirements. No shortcoming identified under Rec.11.

**Criterion 22.3** – Obliged entities have obligations with respect to PEPs that are themselves compliant. See AML/CFT Law Sec. 64. No shortcoming identified under Rec.12.

**Criterion 22.4** – All obliged entities are all under an indirect obligation to identify and assess the ML/TF risks that may arise in relation to new technologies. They are required to undertake enhanced customer due diligence in situations that present a high risk of ML/TF, and in assessing situations that pose high risks they are required to consider, among other things, "new products and new business practices, including new delivery mechanism(s), and the use of new or developing technologies for both new and pre-existing products.", see AML/CFT Law, Sec. 64(3) and Annex III, para. 2(e). In addition, obliged entities have an obligation to take measures to prevent the use of products or transactions that may favour anonymity, and to apply reasonable measures and procedures to address the risks of technological developments and new financial products. AML/CFT Law Sec. 66(3). In general, there is no explicit requirement that obliged entities risk assessment and mitigation take place before launch of a new technology, product or service.

**Criterion 22.5** – Obliged entities are permitted to rely on third parties for CDD purposes. See AML/CFT Law Sec. 67(1), (2), (3). Such persons, while they may rely on such third parties, retain ultimate responsibility for compliance with CDD requirements. No shortcoming identified under Rec.17.

**Weighting and Conclusion**

Shortcomings identified under Rec. 15 equally apply for DNFBPs. **Largely Compliant.**

### Recommendation 23 – DNFBPs: Other measures

In the 2011 MER, Cyprus was rated Partly Compliant on the equivalent Recommendation under the 2004 FATF Methodology. Deficiencies included a need to enhance awareness of STR requirements for some DNFBPs, uncertainty about accountancy coverage, that there was no law governing TCSPs, and that there were no requirements for real estate agents and dealers in precious stones and metals. This Recommendation was largely unchanged under the 2013 methodology.

**Criterion 23.1** – All obliged entities are covered by the requirement (obliged entities defined at Sec. 2A, AML/CFT Law) to file with the FIU reports on transactions suspected of involving proceeds of illegal activity or of relating to terrorist financing irrespective of the amount. Reports are required to be submitted to the FIU immediately upon suspicion, see AML/CFT Law Sec. 58, 69 (d). In addition, there is a general obligation for all persons in Cyprus to file a suspicious transaction report if they know or reasonably suspect that another person is engaged in ML/TF and the information on which that knowledge or reasonable suspicion is based comes to their attention in the course of their trade, profession, business or employment, see AML/CFT Law Sec. 27(1).

**Criterion 23.2** – *(Mostly met)* All obliged entities, are required to implement risk-based programs to mitigate and manage money laundering and terrorist financing risks, and those programs must include compliance management arrangements (including appointing a money laundering compliance officer), screening procedures for employees, training for employees on recognizing and handling ML/TF-related transactions, and the possibility of an independent audit. See AML/CFT Law Sec. 58, 58B, 58C, 58D, 69. Shortcomings identified under Rec.18 equally apply here.

**Criterion 23.3** – Obliged entities must apply enhanced due diligence when transacting with legal or natural persons with establishments in "high-risk countries." See AML/CFT Law Sec. 64(1)(a). Deficiencies identified at Rec.19 apply here. ASP supervisors notify their supervised entities of weaknesses in third countries' AML/CFT regimes. Limited information has been provided by other

competent authorities on actions taken to advice their supervised about the weaknesses in the AML/CFT systems in other countries (e.g. Casino Commission, RE Council.

**Criterion 23.4** – Obliged entities may not notify clients or third persons about the filing of an STR.

**Weighting and Conclusion**

Cyprus is largely compliant with R. 23. Shortcomings identified under R.18 and R.19 equally apply here.

### Recommendation 24

In the 3rd round Cyprus was rated as Largely Compliant with Recommendation 33. It was determined that mainly lawyers subject to the AML/CFT-Law were forming and administering companies, but not all of the entities (including trust and company service providers) were required to ascertain beneficial owners and controller information by law and guidance. Moreover, supervision was lacking insofar as there were no on-site inspections conducted of lawyers by the competent authority.

Since the last evaluation, there have been significant amendments to the AML/CFT-Law. The most recent amendment was enacted and published on 3 April 2018 and mainly incorporated the provisions of the 4th Anti-Money Laundering Directive of the European Union.

**Criterion 24.1** –

*(a) Types, forms and basic features of legal persons* – The types of companies that may be established in Cyprus are provided under Chapter 113 of the Companies Law (Sec. 3(2)), namely companies limited by shares and companies limited by guarantee (with or without share capital). Both types of companies can be either private or public. Additionally**,** the Companies Law contains provisions on the establishment and registration of a place of business of foreign companies in Cyprus (overseas companies). Provisions on the European Company (SE) are made by the Council Regulation (EC) No. 2157/2001, which is directly applicable to Cyprus.

Partnerships are governed by the Partnerships and Business Names Law. According to Section 5 (1) of the said law, a partnership is defined as the relation which subsists between persons carrying on a business in common with a view of profit. There are two types of partnerships: limited and general.

The LSI contains provisions on the features and incorporation of societies, federations and associations (see also Rec. 8).

*(b) Processes for creation of legal persons and obtaining information* – Part I of the Cyprus Companies Law contains provisions on the incorporation and registration of limited companies. For the creation of such companies under Cypriot law a memorandum of association and articles of association are required, whereby the latter are only mandatory for the creation of a company limited by guarantee. In practice, articles of association are submitted by all companies. With respect to partnerships, provisions for their registration are prescribed in Section 51 of the Partnerships and Business Names Law.

Pursuant to Section 11 (5) (a) of the Advocates Law, the drafting of the memorandum or articles of association of a company (including European Companies (SE)) constitutes the exclusive work of an advocate. Any memorandum or articles of association of a company drafted in violation of that rule shall be deemed void and shall have no legal effect (Section 11 (5) (b) of the Advocates Law).

The Department of Registrar of Companies and Official Receiver (DRCOR) is responsible for keeping the register of companies, overseas companies and partnerships. This register is accessible online at the website of DRCOR[112] and is free of charge regarding the basic information as mentioned in Criterion 24.3. All other information and documents on the company, for instance, shareholders, memorandum and articles of association, are provided to the public upon payment of

[112] www.mcit.gov.cy/mcit/drcor/drcor.nsf/index_en/index_en

a flat fee of EUR 10 per legal person. All the necessary statutory forms (in Greek) that are used for creating a legal person in Cyprus and updating the relevant information, is available on the official website of the DRCOR, together with guidance on the processes for the creation of legal persons and for obtaining and recording of basic information. Additionally, relevant guidance (in Greek and English) and the statutory forms for the creation of legal persons can be found on a website of the Cyprus government.[113]. Moreover, a publicly accessible general database containing the entire legislation of Cyprus can be found on www.cylaw.org (free of charge and in Greek). In addition, access to official English translations of various legislation, including laws for incorporation/registration of legal persons and arrangements can be found on the website of the Office of the Law Commissioner[114].

The Societies and Institutions Law deals with the incorporation of societies, institutions, federations and associations. The responsible registrar (i.e. District Officer of the relevant District) must keep a Register that may be inspected by any interested party. Information (in Greek) on how these entities can be established and the legal basis for their registration is provided on the website of the MoI (http://www.moi.gov.cy/moi/moi.nsf/page61_gr/page61_gr?OpenDocument). Information (in Greek) on registered entities is publicly available on a website of the MoI (http://www.moi.gov.cy/moi/moi.nsf/All/EB27634CFA8868DAC2257B5D002CAF58?OpenDocument).

**Criterion 24.2 –** Cyprus has not conducted a formal assessment of the ML/TF risks and vulnerabilities of the entire sector of legal persons or identified the extent to which legal persons created in the country can be or are being misused for ML or TF. However, through various initiatives, such as the implementation of the action plan deriving from the 2013 Special Assessment, some aspects of risks relating to legal persons were identified (see core issue 5.1).

**Criterion 24.3** – Sections 14 and 15 of the Companies Law deal with the registration of limited companies with the registrar of companies (i.e. DRCOR). The information required to be recorded in the register is mainly included in the memorandum of a company and the relevant accompanying documents (i.e. notification of the company's registered office address and of the first directors and secretary) that have to be submitted to the registrar. The memorandum and the articles have to be in accordance with the templates in Tables A, B, C and D, in the First Schedule of the Companies Law. Those templates provide the information that has to be included in the company's memorandum and articles of association.

Section 58 of the Partnerships and Business Names Law stipulates that the registrar (i.e. DRCOR) keeps the register of partnerships.

The following basic information is accessible online at the website of DRCOR: entity name, registration number, registration date, legal form and status, address of registered office and names of current directors and secretary. Access to all other information and documents pertaining to a company, partnership or overseas company can be achieved upon payment of a fee and retrieved electronically.

With respect to societies, federations and associations, the LSI requires these entities to be registered with the Registrar of Societies (i.e. District Officer of the relevant District). For this purpose, a written application has to be submitted to the registrar by the founders or the board of directors of the entities, to which the articles of association, the names and addresses of the administration members as well as their contact details, the emblem of the society and a description of the property of the society must be attached. The contents of the articles of association are set out under the Societies and Institutions Law. The Register is in possession of the required information and this may be inspected by any interested party without paying any fee. An

[113]http://www.businessincyprus.gov.cy/mcit/psc/psc.nsf/All/A2E29870C32D7F17C2257857002E18C9?OpenDocument

[114] http://www.olc.gov.cy/olc/olc.nsf/dmllegislation_en/dmllegislation_en?OpenDocument

updated list of entities can be found online.

**Criterion 24.4** – Companies are required to maintain the information provided under Criterion 24.3 in the memorandum of the company, the register of its members (Section105(1)(a) of the Companies Law) and, the register of its directors and secretaries (Section 192 of the Companies Law). The register of members and the register of directors and secretaries are usually kept at the company's registered office (sections 105(3) and 192(1) of the Companies Law respectively) and, if kept at a different place it cannot be outside the Republic (section 105(2)(b)).The registered office of a company has to be in the Republic of Cyprus to which all communications and notices may be addressed. The registrar of companies shall be informed of the place of the registered office at the day the company begins to carry on business and of any changes thereafter within fourteen days of the change (Section 102 of the Companies Law). Every company shall send notice to the registrar of companies of the place where its register of members and its register of directors and secretaries are kept and any change of that place (Sections 105 (3) and 192 (4) (a) of the Companies Law).

In the case of a company with a share capital, the register of members has to contain the names and addresses of the members, a statement of the shares held by each member, distinguishing each share by its number so long as the share has a number, and the amount paid or agreed to be paid on the shares of each member (Section 105 (1) (a) of the Companies Law). This information is available to any person including creditors and members of the company (Section 108 (1) of the Companies Law). While the Companies Law regulates the voting rights of shares, it does not specifically require the register of members to include information on nature of the voting rights associated with shares. However, Companies Law provides that all relevant information regarding the voting rights is included in the Articles of Association of the company (CL, First Schedule, Tables A, C and D).

Any transfer of shares of a private company with a share capital shall be notified to the registrar of companies within fourteen days from the registration of this transfer in its register of members (Section 113A of the Companies Law). Notice of any change of the registered office shall be given within fourteen days after the date of the change to the registrar of companies (Section 102 of the Companies Law). Additionally, companies are required to prepare and submit to the registrar once a year an annual return regardless of whether they have a share capital (Section 118 of the Companies Law) or not (Section 119 of the Companies Law). These annual returns provide an overview of the company with information on its members, directors, secretaries, registered office and further details. In case of failure to submit the annual return to the registrar, pecuniary fines are applicable and as ultima ratio the striking off of the company may be initiated by the DRCOR.

Any amendments of the particulars of partnerships have to be notified to the registrar within seven days (Section 54 (1) of the Partnerships and Business Names Law). Additionally, since 2012 certain partnerships (i.e. partnerships having a company or a partnership as a general partner) must file an annual return to the registrar with current information regarding the registered particulars (Section 64A of the Partnerships and Business Names Law).

**Criterion 24.5** – Changes to the share capital and transfers of shares of a private company with a share capital, changes of the registered office as well as changes of register of directors and secretaries have to be notified to the registrar of companies within fourteen days, at the latest. Additionally, once a year an annual return has to be submitted by each company to the registrar of companies including current information on the company (see the analysis for Criterion 24.4 above). With regards to public companies with a share capital, the register of members has to be updated when changes occur and the DRCOR will be provided with that updated information through the submission of the annual return.

Any amendments of the particulars of partnerships have to be notified to the registrar within seven days (Section 54 (1) of the Partnerships and Business Names Law). Additionally, since 2012 certain partnerships must file an annual return to the registrar with current information regarding the registered particulars (Section 64A of the Partnerships and Business Names Law).

**Criterion 24.6** – Cyprus uses a combination of mechanisms to ensure that information on the BO of

a company is available. Cyprus introduced provisions in the AML/CFT Law which provide the legal basis for the setting up of a BO registry. These provisions, which are found under Sec. 61A, require legal persons to obtain and hold adequate, accurate and current BO information and for that information to be held in a registry. At the time of the on-site visit, arrangements had been initiated to set the registry up. As a second mechanism, beneficial ownership may be obtained from FIs and DNFBPs (mainly banks and ASPs) on the basis of information gathered as part of the implementation of CDD requirements. The supervisory authorities, the FIU, the Customs Department, the Tax Department and the Police, within the framework of exercising their competencies, have access to the information held with a company and any other legal entity in a timely manner pursuant to Section 61A (3) of the AML/CFT-Law.

**Criterion 24.7** – Companies and any other legal entities incorporated in Cyprus, are required to obtain and hold adequate, accurate and current information on their beneficial ownership (Section 61A (1) of the AML/CFT-Law). FIs and DNFBPs are required to keep CDD information up-to-date and relevant.

**Criterion 24.8** – The ASL requires legal persons to engage the services of a Cyprus-licensed ASP – as a minimum the ASP must act as the company secretary of the legal person and must be a natural person resident in Cyprus (cf. Section 6 of the Administrative Services Law). ASPs are fully accountable to the competent authorities due to their qualification as obliged entities under the AML/CFT Law. Where a legal persons is exempt from the requirement to engage the services of an ASP i.e. the director/company secretary of the legal person owns at least 25 % of the legal person and the share capital is not held on behalf of third persons, the director or secretary of the company would be accountable to the authorities for providing all basic and beneficial ownership information by virtue of its obligations as a director under the Companies Law.

**Criterion 24.9** – Pursuant to Section 68 (1) of the AML/CFT-Law, obliged entities which maintain a business relationship with a company have to maintain records for a period of five years after the end of the business relationship with the customer or after the date of an occasional transaction. Pursuant to Sections 141(3), 320 of the Companies Law, a company is required to keep its books and papers for at least five years from the date of its dissolution and, the books of account and records for a period of six (6) years after the end of the calendar year to which these refer to. In addition, the DRCOR as the competent body to maintain basic information keeps the records of all registered entities for a period of 20 years from the date of its strike off from the register (cf. Section 327 (7) of the Companies Law). However, it is not clear whether the companies themselves are required to maintain a record of beneficial ownership information for a period of at least five years.

**Criterion 24.10** – Pursuant to Section 61A (3) of the AML/CFT-Law, competent authorities have access in a timely manner to information on beneficial ownership held by a company and any other legal entity according to Section 61A (1) of the AML/CFT-Law. Access to information on beneficial ownership of partnerships can be obtained by competent authorities from FIs and DNFBPs. Supervisory authorities may also request information on beneficial owners held by obliged entities pursuant to Section 59 (9) of the AML/CFT-Law. The FIU has the power to request and obtain information and/or documents with regard to the beneficial owners of legal persons and entities on the basis of Section 55 (2) (c) of the AML/CFT-Law. The Police may obtain information through an order for disclosure by the court under the provisions of Sections 45 and 46 of the AML/CFT-Law.

**Criterion 24.11** – The Cyprus Companies Law does not provide for the issue of bearer shares. According to Section 27 of the Companies Law, the subscribers of the memorandum of a company shall be deemed to have agreed to become members of the company and on its registration shall be entered as members in its register of members. Every other person who agrees to become a member of a company, and whose name is entered in its register of members, shall be a member of the company. Also see the analysis for Criterion 24.1 (b) above. However, it is noted that public companies limited by shares and listed on a regulated market may, if so authorised by their articles of association, issue share warrants to a bearer. These share warrants have characteristics that are similar to bearer shares. Before December 2012, this possibility also existed for other public

companies. As the possibility to issue bearer share warrants is limited to public companies limited by shares that are listed on a regulated market, mitigation of a potential misuse for ML/TF is ensured to some extent.

**Criterion 24.12** – The Administrative Services Law regulates directorship and shareholding services (Section 4 (1) (b) (i) and (iii)), referred to under the law as administrative services. These services may only be provided by eligible persons who are required to be licensed as advocates, lawyers' companies or ASPs as required under c. 24.12 (b)[115]. Eligible persons are required to comply with the AML/CFT-Law (including the identification of the BO) and, therefore, required to maintain information on their nominator (the BO). As obliged entities, they are required to make this information available to competent authorities upon request (see for instance c. 29.3). Eligible persons must be registered with the CySEC, the CBA or the ICPAC (Sec. 25 ASL) and these three authorities are required to maintain a register. These registers include information on the administrative services provided. The status of shareholders or directors as "nominees" may be determined through these publicly accessible registers.

**Criterion 24.13** – Section 59 (6) of the AML/CFT-Law provides for measures in cases where a person falling under the AML/CFT-Law fails to comply with the provisions of Part VII of this Law or with the Directives issued by the competent supervisory authority. These measures may be imposed on natural persons having managerial responsibilities in an obliged entity or any other person held responsible for a breach as well as on the legal person itself.

The Companies Law contains sanctioning provisions applicable in the case that a company does not notify the registrar of companies of:

- the place of the register of its members (Section 105 of the Companies Law),
- the registered office or any changes thereof (Section 102 of the Companies Law),
- any allotment or transfer of its shares (Sections 51, 76 and 375 of the Companies Law),
- the register of directors and secretaries or any changes thereof (Section 192 of the Companies Law),
- the annual return and accounts on a yearly basis (Section 120 (3) of the Companies Law).

In addition to the above, a company and every officer is liable to a default fine for every day the status of non-compliance continues (Section 375 (1) of the Companies Law). Finally, a company may be struck off the register if the requirements of Section 327 of the Companies Law are fulfilled.

With respect to societies, the competent registrar may carry out inspections to ascertain whether the conditions of the Societies and Institutions Law are fulfilled. In case of non-compliance with the requirements for mandatory notifications, the registrar does have the ability to appeal to the court requesting the dissolution of the society.

**Criterion 24.14** – The competent authorities, particularly the MJPO, the Police, the FIU, the the CBC, the CySEC, the ICPAC and the CBA, have effective gateways to exchange basic and BO information in a constructive and timely manner. These are described under Rec. 37 and 40. Basic information held by the DRCOR is available publicly and can be easily accessed by foreign authorities. Information on shareholders and beneficial owners can be shared by the MJPO, Police and the FIU pursuant to their exchange of information powers (see Recs. 37 and 40)..

In addition, competent authorities may exchange BO information with their EU counterparts pursuant to sections 61A (8) and 61B (6) of the AML/CFT-Law

**Criterion 24.15** – All competent authorities keep a record of the assistance requested from other

[115] In the cases mentioned in Section 4 (3) (a) of the Administrative Services Law, the provision of director services does not require any licensing or authorisation by any supervisory authority. For instance, these cases refer to companies where at least 25 % of the shares are owned by the person providing the director services.

countries. In discussions with the authorities, particularly the FIU and the Police, which are the most active in requesting basic and BO information, they were able to point out which foreign counterparts are, as a rule, unresponsive. This indicates that the monitoring of the quality of assistance does take place, albeit on an informal and less systematic basis.

**Weighting and Conclusion**

Cyprus meets or mostly meets most criteria. However, there are some weaknesses in relation to the country's assessment of risks associated with legal persons. While the Companies Law regulates the voting rights of shares, it does not specifically require the register of members to include information on nature of the voting rights associated with shares. Monitoring of quality of assistance provided by other countries in response to requests for BO and basic information is not done on a formal and systematic basis. **Cyprus is Largely Compliant with Recommendation 24.**

### Recommendation 25 – Transparency and beneficial ownership of legal arrangements

In the 3rd round Cyprus was rated as Largely Compliant with Recommendation 34. It was concluded that trust service providers, who were not lawyers, were not explicitly covered by the AML/CFT-Law. Moreover, it was found that lawyers had not been subject to any on-site inspections.

Since the last evaluation, there have been significant amendments to the AML/CFT-Law. Management and administration services for trusts are now explicitly covered by Section 2 of the AML/CFT-Law irrespective of who provides those services and wherever the corporate entity or trust is registered, established or set up (cf. Sections 3 (7), 4 (1) (a) and 23 (2) of the Administrative Services Law).

**Criterion 25.1** – Pursuant to Section 61B (1) of the AML/CFT-Law, a trustee or commissioner of any express trust has to obtain and hold adequate, accurate and up-to-date information on beneficial ownership regarding the trust, which shall include the identity of: the settlor; the trustee or commissioner; the protector; the beneficiary or class of beneficiaries; and any other natural person exercising effective control over the trust.

The definition of a beneficial owner of a trust is contained in Section 2 (1) of the AML/CFT-Law and corresponds to the information mentioned in Section 61B (1) of the AML/CFT-Law.

In addition, Section 3 (7) of the Administrative Services Law states that any person providing services of management and administration of trusts must identify and verify the identity of the beneficial owners of the trust. This should include accurate and updated information on the following categories, where and if they are applicable: trustees; settlors; beneficiaries or information on the class of beneficiaries including the beneficiaries to whom any distributions have been made pursuant to the trust; protector, where applicable; investment advisor, accountant, tax consultant, where applicable; the activities of the trust; any other person who exercises effective control over the trust.

Section 3 (7) of the Administrative Services Law applies not only to eligible persons, but also to those who are exempt from the authorisation requirement pursuant to Section 4 (3) of the said law.

Section 68 (1) of the AML/CFT-Law provides for a retention period of five years for documents and information gathered under the provisions of this law after the end of the business relationship with the customer or after the date of an occasional transaction. The Administrative Services Law, while requiring that information on service providers to the trust, such as investment advisors, accountants and tax consultants, be maintained, does not state that information has to be maintained for at least five years after the end of the business relationship or the trust ceases to exist.

With respect to institutions, it is foreseen that registered institutions must be administered by three or more persons. The board of directors of an institution attends to the affairs of the institution and represents the same in court and out of court (Sections 32 (1) and 34 (1) of the Societies and Institutions Law). According to Section 52 of the Societies and Institutions Law, the administrative organs of societies shall be obliged to comply with and apply the provisions of the

AML/CFT-Law. Institutions acquire legal personality from the date of its registration in the Registry of Institutions and therefore, are qualified as "other legal entities" when it comes to the application of the AML/CFT-Law. Accordingly, institutions are required to obtain and hold BO information according to Section 61A of the AML/CFT-Law. A Register of Institutions is kept by the registrar (i.e. District Officer of the relevant District) and open to the public.

**Criterion 25.2** – A trustee or commissioner of any express trust is required to obtain and hold adequate, accurate and up-to-date information on beneficial ownership regarding the trust (Section 61B (1) of the AML/CFT-Law). Additionally, Section 3 (7) of the Administrative Services Law requires that information on the beneficial owners of a trust needs to be accurate and updated. This includes information on investment advisors, accountants and tax consultants providing services to the trust. For institutions the provisions of Section 61A (1) of the AML/CFT-Law are applicable.

**Criterion 25.3** – When a trustee or commissioner establishes a business relationship or carries out an occasional transaction, it discloses to financial institutions and DNFBPs its status and provides the information referred to in Section 61B (1) of the AML/CFT-Law. With respect to institutions, a provision comparable to that of Section 61B (2) of the AML/CFT-Law does not exist.

**Criterion 25.4** – There are no provisions in law or enforceable means which would prevent trustees from providing information to the competent authorities or to financial institutions and DNFBPs. On the contrary, trustees are expressly obliged to share this information (cf. Section 61B (2) and (3) of the AML/CFT-Law and Section 3 (7) of the Administrative Services Law). There are no provisions preventing the members of an institution to provide authorities with any available information.

**Criterion 25.5** – Pursuant to Section 61B (3) of the AML/CFT-Law, the supervisory authorities, the Customs and Excise Department, the Inland Revenue, the FIU and the Police, within the framework of exercising their competencies, shall have timely access to the information on beneficial ownership regarding trusts according to Section 61B (1) of the AML/CFT-Law.

The FIU also has the power to request and obtain information and/or documents with regard to the beneficial owners of legal persons and entities, including trusts on the basis of Section 55 (2) (c) of the AML/CFT-Law. The Police may obtain information on beneficial ownership through an order for disclosure by the court under the provisions of Sections 45 and 46 of the AML/CFT-Law.

In addition to the provisions of the AML/CFT-Law, Section 3 (7) of the Administrative Services Law stipulates that the person providing the services of management and administration of trusts must keep the information on the beneficial ownership in the Republic of Cyprus and make them available for disclosure to and inspection by the relevant competent authority at all times. Competent authority means the authorities defined in Section 59 of the AML/CFT-Law.

Additionally, the information on beneficial ownership regarding trusts will be kept in the future central register of trusts, when the express trust generates tax consequences in Cyprus (Section 61B (4) (a) of the AML/CFT-Law). The supervisory authorities, the Customs and Excise Department, the Inland Revenue, the Unit and the Police shall have timely and unrestricted access to the information relating to beneficial owners of the trust without the trust concerned (Section 61B (5) of the AML/CFT-Law).

With respect to the residence of trustees, the AML/CFT-Law does not contain any provisions stating that such information has to be documented and recorded. However, the various AML Directives issued by the ICPAC, the CBA, the CySEC, the ICCS and the CBC contain provisions to establish and verify the address of customers and beneficial owners.

Pursuant to Section 59 (9) of the AML/CFT-Law, the supervisory authorities ask and collect from persons under their supervision any useful information necessary for the performance of their duties and request within a specified deadline the provision of relevant information, documents and data. This encompasses information on any assets held or managed by a financial institution or DNFBP in relation to any trustees with which they have a business relationship or for which they undertake an occasional transaction. The Unit can access this information based on Section 55 (2)

(c) of the AML/CFT-Law. The law enforcement authorities may obtain this information through an order for disclosure by the court under the provisions of Sections 45 and 46 of the AML/CFT-Law, whereby this way of information procurement is not seen to be timely.

Apart from the AML/CFT-Law, Section 25A of the Administrative Services Law foresees that the CySEC, the CBA and the ICPAC each establish and keep a trust register with respect to each trust governed by Cyprus law and where one of its trustees is an eligible person resident in Cyprus and supervised by the CySEC, the CBA or the ICPAC in its capacity as a competent supervisory authority. The trust registers are not available to the public but shall be available for inspection by the competent authorities. The following information is contained therein: the name of the trust; the name and full address of every trustee at all relevant times; the date of establishment of the trust; the date of any change in the law governing the trust; the date of termination of the trust. Any changes to this information must be notified to the competent authority that keeps the relevant trust register (Section 25A (8) and (9) of the Administrative Services Law).

**Criterion 25.6** – See analysis under c.24.14**.**

**Criterion 25.7** – According to Section 2A (1) of the AML/CFT-Law, natural and legal persons offering services to trusts and similar legal arrangements are obliged entities. In order to ensure that all persons offering such services are covered by the obligations of the AML/CFT-Law, Section 23 of the Administrative Services Law states that also those persons exempt from the licensing requirement must at all times comply with the AML/CFT-Law. Even if Section 4 (4) of the Administrative Services Law refers to the reservation of Section 23 (2) of the Administrative Services Law, for reasons of ensuring completeness, Section 23 (2) of the Administrative Services Law should refer to Section 4 (4) of the Administrative Services Law too.

Section 59 (6) of the AML/CFT-Law provides for sanctions and supervisory measures that the supervisory authorities may take where an obliged entity fails to comply with the provisions of the AML/CFT-Law. Additionally, Sections 24, 26, 27 and 29 of the Administrative Services Law provide for criminal, administrative and civil sanctions in the case of non-compliance with the provisions of the Administrative Services Law and the AML/CFT-Law. For institutions the provisions of Section 2A (1) (i to iii) in connection with Section 59 (6) of the AML/CFT-Law are applicable.

**Criterion 25.8** – As outlined in the previous Criterion 25.7, sanctions and supervisory measures may be imposed by competent supervisory authorities on persons offering services to trusts and similar legal arrangements in the case of non-compliance with the provisions of the AML/CFT-Law. This covers the case where (timely) access to information on beneficial ownership of a trust or a similar legal arrangement is declined or deferred.

**Weighting and Conclusion**

Cyprus meets most of the criteria under R. 25. There is one minor deficiency. The Administrative Services Law, while requiring that information on service providers to the trust, such as investment advisors, accountants and tax consultants, be maintained, does not state that information has to be maintained for at least five years after the end of the business relationship or the trust ceases to exist. **Cyprus is Largely Compliant with Recommendation 25.**

### Recommendation 26 – Regulation and supervision of financial institutions

In the 2011 MER, Cyprus was rated as Largely Compliant with the requirements of former Recommendation 23 due to the following deficiencies: limited coverage of on-site supervision of MTBs was demonstrated by the CBC (limited number of on-site inspections and their agents) as well as very low number of on-site inspections conducted by CySEC). In the 5th round the effectiveness issues are no longer analysed in the TC Annex.

**Criterion 26.1** –

AML/CFT supervisory authorities are designated as follows: (i) CBC supervises credit institutions (incl. branches of foreign institutions), e-money institutions (incl. branches of foreign institutions and agents of EU institutions), Payment institutions (incl. branches of foreign institutions and

agents of EU institutions), other persons (Credit Acquiring Companies, Leasing116, Bureaux de Change, MVTSs117); (ii) CySEC supervises Investment companies (CIFs), External Investment Fund Managers, Internally managed Investment Funds, Undertakings for Collective Investment in Transferable Securities (UCITS), UCITS Management Companies (UCITS MC), Alternative Investment Fund Managers (AIFMs), Alternative Investment Funds (AIFs), Alternative Investment Funds with a Limited Number of Persons (AIFLPNs); (iii) ICCS supervises Life insurance companies and intermediaries. See section 59 of the AML/CFT Law.

**Criterion 26.2** –

*Core Principle financial institutions*

All core principles financial institutions are required to be licensed.

*Credit institutions* are licensed under Section 4 of the Business of Credit Institution Laws 1997-2018 Law. As from November 2014 the decision to grant a licence has been made through the EU Single Supervisory Mechanism: in accordance with EU Council Regulation (EU) 1024/2013, the ECB has the ultimate decision making responsibility with respect to authorisation of credit institutions to be incorporated in Cyprus; relevant applications are submitted to the CBC which in turn notifies the ECB accordingly.

*Securities institutions* are licensed by CySEC:

- Cyprus Investment Firms (CIFS) are subject to authorisation (Section 5 of Investment Services and Activities and Regulated Markets Law of 2017 (CIF Law)).
- UCITS Management Companies (UCITS MC) are subject to authorisation (Sections 109 and 111 of the Open-ended Undertakings for Collective Investment (UCI) Law).
- Alternative Investment Fund Managers (AIFMs) are subject to authorisation (Sections 6 and 7 of the Alternative Investment Fund Managers Law of 2013 (AIFM law)).
- Alternative Investment Funds (AIFs) are subject to authorisation (Section 13 of the Alternative Investment Fund Law of 2018).
- Undertakings for Collective Investment in Transferable Securities (UCITS) are subject to authorisation (Section 9 of the Open-ended Undertakings for Collective Investment (UCI) Law).
- Alternative Investment Funds with a Limited Number of Persons (AIFLPNs) are subject to authorisation (Section 126 of the Alternative Investment Fund Law of 2018).
- UCITS and AIFLNPs, which can be internally managed investment funds, are subject to authorisation under Section 9 of the UCITS Law.

*Insurance companies and intermediaries* are licensed under Articles 14 and 375 of the Insurance and Reinsurance Business and other Related Issues Law of 2016.

*Other FIs* are licensed by the CBC: payment Institutions are authorised under the Provision and Use of Payment Services and Access to Payment Systems Law of 2018 (Section 11); e-money Institutions are authorised under the Electronic Money Laws of 2012 and 2018 (Section 5); mortgage credit institutions are authorised under the Credit Agreements for Consumers relating to Residential Immovable Property Law of 2017 (Law 41(I)/2017) and Credit Agreements for Consumers relating to Residential Immovable Property Amendment Law (Law 149(I)/2017) (Section 34(A)); credit acquiring companies are authorised under the Sale of Credit Facilities and Related Matters Laws of 2015 and 2018 (Laws 169(I)/2015 and 86(I)/2018) (Section 5); bureaux de change are authorised under Sections 16(a) and 36 of the Central Bank of Cyprus Laws of 2002

[116] Leasing Companies are regulated under Financial leasing and the Activities of Financial leasing Companies Law, 2016. To date, no leasing companies have been licenced by the CBC and operating.

[117] Money value transfer services providers fall into the scope of payment institutions sector. MVTS is one of the 8 business activities that could be offered by a payment institution. The provision of payment services is regulated by the Provision and Use of Payment Services and Access to Payment Systems Law of 2018 (hereinafter – Payment Services Law).

to (No. 3) 2014 and Section 35 of the Bureaux de Change Businesses Directive of 2014; Financial Leasing Companies are authorised under the Financial Leasing and the Activities of Financial Leasing Companies Law, 2016 (Section 15).

*Shell banks*

Under Section 4. (1)(b)(ii) of the Business of Credit Institutions Law of 1997, a credit institution incorporated in Cyprus is required to have its registered and head office in the Cyprus. Under Section 4(1)(b)(iii) of the Law, credit institutions other than those referred to in sub-point (ii), have their head office in the Member State which granted their authorisation and in which they actually carry out their business. Banks are required to have substance and shell banks are not permitted.

**Criterion 26.3** –

*Banks and other institutions supervised by the CBC*

Section 17A of the Business of Credit Institutions Law 1997 sets out criteria for authorisation, including: (i) the reputation of the proposed acquirer (covering all layers of natural or legal persons or persons acting in concert who have taken a decision to acquire directly or indirectly, a qualifying holding (proposed acquirer) or to further increase directly or indirectly such a qualifying holding as a result of which the proportion of the voting rights of the capital held in the credit institution would reach or exceed 20%, 30% or 50% or so that the credit institution would become the subsidiary of the proposed acquirer, (ii) the reputation, knowledge, competencies and the experience of any member of the management body, senior management and key functionaries (iii) the financial soundness of the proposed acquirer, (iv) whether there are any reasonable grounds to suspect that, in connection with the acquisition, ML or FT is being or has been committed or attempted or that the proposed acquisition could increase the risk of ML/FT.

Section 18 of the law contains criteria to assess the fitness and probity of the proposed members of the management body, senior management and key function holders. The assessment procedure and the criteria for the fitness and probity of the members of the management body, senior management and key function holders are set out in the 2014 Directive on the Assessment of the Fitness and Probity of Members of the Management Body and Managers of Authorised Credit Institutions.

Sections 17A, 17D and 18 permit the CBC to remove persons who do not meet the statutory criteria.

The reputational elements in the law would largely allow the CBC to ensure that associates of criminals are prevented from being a controller of a bank in at least most circumstances. There are regulatory measures in place in practice which would detect associates of criminals. See IO.3.

Similar frameworks apply in relation to payment institutions, e-money institutions, mortgage credit companies, financial leasing companies, credit acquiring companies and bureaux de change (EMI Law of 2012, Electronic Money Institutions Directive of 2012, Payment Services Law, Bureaux de Change Directive of 2014, Sale of Credit Facilities and Related Matters Law of 2015 and Authorisation of Credit Acquiring Companies Directive).

*Securities*

Sections 9, 11, 12, 14 and 47 of the CIF Law specify fitness and properness or suitability requirements for beneficial owners, shareholder, directors and senior management (key function holders) and the ability for CySEC to prevent their appointment and remove them. In addition, CySEC has issued guidelines on the assessment of acquisitions and increases of qualifying holdings and guidelines on the assessment of the suitability of members of the management body and key function holders. However, there are no provisions in relation to managers other than key function holders. The reputational and suitability elements of the legal provisions would largely seem to allow CySEC to prevent associates from controlling supervised entities. There are regulatory measures in place in practice which would detect associates of criminals. There are regulatory

measures in place: CySEC conducts fit and proper checks and this would allow associates to be detected. Similar requirements apply in relation to other market participants supervised by CySEC. See IO.3.

*Insurance*

Similar provisions to those for credit institutions apply under articles 25, 44, 58, 60, 62 and 63 of the Insurance and Reinsurance Business and other Related Issues Law 2016. At the operational level, the Law refers to the board of directors and any other persons who run the undertaking. This language would not necessarily cover all relevant management. The reputational elements of the legal provisions would largely seem to allow the ICCS to prevent associates from controlling supervised entities. There are regulatory measures in place in practice which would detect associates of criminals. See IO.3.

**Criterion 26.4** –

*Core Principles institutions*

Cyprus was subject to an FSAP update concluded by the IMF in May 2009, which included an assessment of compliance with the Basel Committee Core Principles (BCPs) for effective Banking Supervision. Cyprus took measures to address IMF's recommendations and has taken strong steps to comply with the current BCPs. There has not been a recent external assessment of compliance with the BCPs, but it appeared to the assessment team that there is a good level of compliance with those which are relevant to criterion 26.4.

The first assessment of observance of the IOSCO Objectives and Principles of Securities Regulation (IOSCO Principles) in Cyprus was undertaken in 2005 as part of the offshore financial centre (OFC) assessment program by the International Monetary Fund (IMF). The most recent IMF report (2009) was a Technical Note – Factual Update of IOSCO Core Principles of Securities Regulation. Cyprus has taken strong steps to comply with the current IOSCO Core Principles. There has not been a recent external assessment of compliance, but it appeared to the assessment team that there is a good level of compliance with those IOSCO Core Principles which are relevant to criterion 26.4.

With referenced to the IAIS Insurance Core Principles, Cyprus has provided information on Insurance Core Principle relating specifically to AML/CFT (ICP22). As information on the other relevant Core Principles has not been provided, the assessment team cannot conclude whether the regulation and supervision of insurance undertakings is in line with criterion 26.4 (and footnote 62 of the methodology). The impact of this has been assessed taking into account compliance with the analysis in relevant parts of this Technical Annex (in particular R.40), the intent at legislative and operational level to comply with the EU's Solvency II framework, and the low materiality of insurance sector in Cyprus.

*Other FIs*

All other FIs, for which the CBC is the responsible supervisory authority (see c. 26.1), are subject to monitoring and onsite examinations under legislation and the CBC's supervisory policy.

**Criterion 26.5** – According to the Section 59(5)(b) of the AML/CFT Law, the supervisory authorities, when implementing a risk-based approach to supervision, base the frequency and intensity of on-site and off-site supervision on the risk profile of obliged entities, and on the risks of ML/TF in Cyprus. The assessment of the ML/TF risk profile, including the risks of non-compliance must be reviewed both periodically and when there are major events or developments in their management and operations. Furthermore, the supervisory authorities take into account the degree of discretion allowed to the obliged entities and appropriately review the risk assessments underlying this discretion and the adequacy and implementation of their internal policies, controls and procedures. There is no explicit provision in the AML/CFT Law to take into account

characteristics of groups of financial institutions, but this has been addressed when incorporating the ESAs' risk-based supervision guidelines into internal supervisory procedures. It is not clear that all elements of sub-criterion (a) are met.

**Criterion 26.6** – Section 59(5)(b) of the AML/CFT Law sets out the requirements for supervisory authorities to assess the risk profile of financial institutions, including the risks of non-compliance, providing that such assessments shall be reviewed both periodically and when there are major events or developments in their management and operations. The law is complemented by procedures adopted by each FI supervisory authority. In addition, the FI supervisory authorities incorporate the ESAs' Risk Based Supervision Guidelines (including in relation to cases when an obliged entity is part of a financial group established in another member state or third country or has any other relevant link to other countries).

**Weighting and Conclusion**

**R.26 is rated largely compliant.** Not all relevant management is covered by the legislative frameworks for the securities and insurance sectors and the framework to address associates of criminal is not necessarily complete. It is not clear that all elements of sub-criterion (a) of c.26.5 have been met. Limited information has been provided on the level of compliance with the IAIS Core Principles (c.26.4).

### Recommendation 27 – Powers of supervisors

In the 2011 MER, Cyprus was rated as Largely Compliant with the requirements of former Recommendation 29 due to the following deficiencies: there was legal uncertainty on the applicability of the AML/CFT sanctions to the directors and senior management; very low number of CYSEC onsite examinations; The CySEC law was restrictive in terms of powers to obtain a full range of information.

Cyprus addressed some of these deficiencies and improved their legislative framework by introducing increased fining powers, which are also applicable to the senior management, including officers (directors), see R.35.

**Criterion 27.1** –

As per section 59(4) of the AML/CFT Law, the supervisory authorities are required to issue directives that are applicable to persons falling under their supervision. Section 59(5)(a) of the law requires the supervisory authorities to monitor, evaluate and supervise the application of the provisions of the Part VIII of the AML/CFT law (where all the requirements of AML/CFT preventive measures are listed) and of the directives issued.

**Criterion 27.2** –

Section 59(9)(b) of the AML/CFT Law provides that supervisory authorities, in order to verify the compliance of persons under their supervision, may carry out inspections, request and collect information; enter the premises of the supervised persons and inspect documents; records and accounts and any data stored in computers or other electronic means; and receive copies or extracts of these data.

**Criterion 27.3** –

Section 59(9) (a) of the AML/CFT Law provides that supervisory authorities have the right to ask and collect information from supervised persons that is necessary for the performance of their supervisory duties. Relevant information, documents and data can be requested giving specified deadline for their submission. In cases where a supervised person might refuse to comply with a request to provide the information within the specified deadline or in cases where a person refuses to provide any information or provides insufficient, false or forged information, supervisory authorities have the power to impose sanctions stipulated in section 59(6) of the AML/CFT Law (for further information on the range of sanctions available see R.35). Sectorial Laws also contain similar provisions to the Section 59(9) of the AML/CFT Law: Section 26(11) of the Business of

Credit Institutions Law, Section 24(1)(a) of the Payment Services Law, Section 33 of the CySEC Law and Articles 396-397 of the Insurance and Reinsurance Business and other Related issues Law, Section 33(2) of the CySEC Law[118]).

**Criterion 27.4** –

Supervisors are authorised to impose a range of sanctions for AML/CFT breaches, including disciplinary and financial sanctions, as well as withdrawal, restriction or suspension of a licence. For additional information see R.35.

**Weighting and Conclusion**

**R. 27 is rated compliant.**

### Recommendation 28 – Regulation and supervision of DNFBPs

In the 2011 MER, Cyprus was rated as Partially Compliant with the requirements of Recommendations 24 and 30 due to the following deficiencies: there was no legislation regulating company service providers and professional intermediaries, the draft law regulating trust and company service providers' activities was in the amendment process during 4th round evaluation visit, according to which it appeared that trust and company service providers are to be supervised by three separate supervisory authorities depending on the profession of the service provider, which could lead to an uneven playing field in monitoring this activity; no supervisory action on compliance checking was taken in respect of the real estate and dealers in precious metals and stones' sectors; there were insufficient resources and capacity for all DNFBP supervisors in order to ensure adequate execution of their supervisory activities; there was no indication of sanctions imposed on the DNFBP sectors.

Cyprus addressed some of these issues and improved its supervisory system of DNFBPs from a legal perspective.

**Criterion 28.1** – The Casino Operations and Control Law of 2015 ("Casino Law") contains provisions for the licensing and operation of casinos in Cyprus and for the establishment of the National Gaming and Casino Supervision Commission ("Casino Commission"). The Casino Law does not regulate betting, lotteries, horseracing or online gaming; those activities are subject to other national legislation and regulations. Betting activities – carried out land based or online – are regulated by the Betting Law and supervised by the National Betting Authority. Online casinos are strictly prohibited by the Betting Law. Lotteries are also prohibited with the exception of lotteries conducted by the National Lottery and other charitable purpose lotteries.[119]

According to Section 15 of the Casino Law, a single integrated casino resort shall be licensed, and the operator shall be given a 15-year exclusivity period. The integrated casino resort license issued to the respective operator shall be for a single integrated casino resort on the site selected by the operator and authorise, but not require, the operator to develop and operate up to four satellite casino premises (Section 16 of the Casino Law).

Pursuant to Section 8 of the Casino Law, one of the objectives of the Casino Commission is to maintain and administer systems for the licensing, supervision and control of the casino, in order to ensure that the management and operation of the integrated casino resort is carried out by persons who are suitable and remain free from criminal influence or exploitation. In detail, the Steering Committee shall not approve a person to hold a casino resort license unless it is satisfied that the selected candidate, each shareholder holding 10 % or more of the shares and/or voting rights of the candidate for public listed companies and each shareholder holding 5 %or more of the shares and/or voting rights of the candidate for all other shareholders, and every associate of the

[118] The CySEC law (section 33) was last amended in April 2019, lifting the restrictive provisions in relation to CySEC's powers to obtain a full range of information required for the supervisory purposes from its supervised entities.

[119] This report assesses solely the activities of casinos (land- and internet based) as it is foreseen by the FATF Recommendations. Other gambling activities like betting or lotteries are excluded.

candidate, are suitable persons for the management or operation of the casino resort (Section 22 of the Casino Law). On a positive note, it should be mentioned that the applicable thresholds for the determination of the BO of a casino are lower than the general thresholds in case of corporate entities pursuant to Section 2 (1) of the AML/CFT-Law. The detailed requirements are stipulated in Section 10 of the Casino Operations and Control Regulations of 2016 ("Casino Regulations"). These requirements are very comprehensive and contain also provisions on the identification of the (ultimate) beneficial owners. If the casino applicant is owned by other companies or entities, it is required to submit the ownership structure of the entire group and to disclose details of all the shareholders in the group up to the ultimate beneficial owners. For the disclosure, the above described thresholds are applicable (Section 10 (j) and (k) of the Casino Regulations).

Furthermore, all employees and key employees of a casino require a valid casino employee and casino key employee license issued by the Casino Commission. The licensing process entails investigation of the suitability of each employee by the Casino Commission which includes criminal checks. The detailed process is described in Section 28 of the Casino Regulations.

Pursuant to Section 59 (1) (h) of the AML/CFT-Law, the National Authority for Gambling and Casino Supervision is designated as a supervisory authority for providers of gambling services as provided in the Casino Law according to Section 2A (f) of the AML/CFT-Law. Section 18 (2) of the Casino Regulations establishes the Casino Commission as the supervisory authority to monitor compliance with the AML/CFT-Law. Accordingly, the titles of the supervisory authorities used in the different laws do not match each other. Nevertheless, the competent Cypriot authorities confirmed that a single authority (i.e. Casino Commission) is responsible for supervision of casinos.

As a supervisory authority, the Casino Commission monitors, evaluates and supervises the application of the provisions of Part VII of the AML/CFT-Law and of the directives issued pursuant to the provisions of Section 59 (4) of the AML/CFT-Law (cf. Section 59 (5) (a) of the AML/CFT-Law). Furthermore, the Casino Commission has the power to sanction violations of the AML/CFT-Law according to the provisions of Section 59 (6) of the AML/CFT-Law. It can require remedial actions, impose administrative fines, amend, suspend or withdraw the license of a casino, impose a temporary ban on any person discharging managerial responsibilities in a casino or any other natural person, held responsible for the breach from exercising managerial functions in an obliged entity.

**Criterion 28.2** – All DNFBPs[120] are subject to monitoring by a designated competent authority or SRB, namely either by the CBA, the ICPAC, the CySEC or the Estate Agents Registration Council according to Section 59 (1) of the AML/CFT-Law (see the table below).

At the time of the on-site visit, dealers in precious stones and metals were not covered by the AML/CFT-Law because trading in precious stones and/or precious metals, mechanical vehicles and works of art and/or antiques in cash equal to or higher than EUR 10,000 was prohibited (Section 5A of the AML/CFT-Law).

Notaries are also not mentioned in the AML/CFT-Law as the profession of a notary does not exist in Cyprus. The Ministry of Justice is exclusively responsible for issuing certifications of apostilles.

**Criterion 28.3** – All DNFBPs who are subject to the AML/CFT-Law are also subject to supervision for AML/CFT compliance (Section 59 (1) of the AML/CFT-Law). The Estate Agents Registration Council took over competency from the FIU in May 2018 and since then supervises real estate agents. The CBA is responsible for the supervision of advocates and LLCs and the ICPAC supervises accountants and auditors. With respect to ASPs or TCSPs, supervision is performed by three separate supervisors depending on the profession of the service provider, respectively the type of license:

[120] Auditors and tax advisors are also covered by the AML/CFT-Law, although they do not fall under the FATF definition of DNFBPs.

- The CBA supervises ASPs providing administrative services according to the Administrative Services Law that do not fall under the supervision of the ICPAC or the CySEC;
- The ICPAC supervises ASPs providing administrative services according to the Administrative Services Law that do not fall under the supervision of the CBA or the CySEC;
- The CySEC supervises ASPs providing administrative services according to the Administrative Services Law that do not fall under the supervision of the ICPAC or the CBA.

Pursuant to Section 25 (1) and (2) of the Administrative Services Law, the CySEC keeps a register of all persons licensed to provide administrative services. This register contains information on the licensed person, the administrative services provided, the names of its fully owned subsidiaries which offer administrative services, the names of its employees, the name and communication information of the compliance officer, and any other information deemed necessary.

The other supervisors, namely the CBA and the ICPAC must also maintain respective registers that contain the same information. Such registers could be found on the websites of all three supervisors. However, the ASP register maintained by the CBA does not contain full information as required by Section 25 (2) of the Administrative Services Law.

Pursuant to Section 23 (2) of the Administrative Services Law, persons exempt from the licensing requirement are subject to the obligations of the AML/CFT-Law and therefore, are under the supervision of the supervisory authorities.

**Criterion 28.4** – The CySEC has adequate legal powers to supervise AML/CFT compliance. The comprehensive powers of the CySEC to monitor AML/CFT compliance are the same for financial institutions and ASPs (see also Rec.27).

The CBA, the ICPAC and the Estate Agents Registration Council also have adequate and comprehensive powers to supervise AML/CFT compliance based on the AML/CFT-Law. Pursuant to Section 59 (5) (a) of the AML/CFT-Law, the supervisory authorities monitor, evaluate and supervise the application of the provisions of the AML/CFT-Law and of the issued directives. Furthermore, they ask and collect from persons under their supervision any useful information necessary for the performance of their duties and request within a specified deadline the provision of relevant information, documents and data (Section 59 (9) of the AML/CFT-Law). The supervisory authorities also have the power to carry out inspections, to request and collect information, to enter the premises of the supervised persons and to inspect documents, records and accounts and any data stored in computers or other electronic means and to receive copies or extracts of these data.

According to the definition of FATF, the CBA, the ICPAC and the Estate Agents Registration Council qualify as SRBs. On the basis of the FATF definition of "supervisors" it is required that such non-public bodies are supervised by a competent authority in relation to the functions they perform. The ICPAC's activities are supervised by the CyPAOB and the CBA by the Attorney-General, both being public bodies. The Estate Agents Registration Council as SRB is not subject to any supervision/oversight by a competent authority.

ASPs have to fulfil comprehensive requirements when they apply for a license from the CySEC on the basis of the Administrative Services Law. ASPs are required to comply with the licensing requirements at all times, which includes the continuous assessment by the ASP of the appropriateness of shareholders, persons managing the business and the AMLCO (Section 23 of the Administrative Services Law) and therefore, should notify the CySEC of any changes of the licensing requirements.

The above provisions of the Administrative Services Law only apply to applicants who apply for a license from the CySEC. They do not apply to the so-called "exempted persons" providing administrative services (Sec. 2 of the Administrative Services Law). Those are advocates and LLCs under the supervision of the CBA and members of the ICPAC who are under the supervision of the ICPAC.

With respect to advocates, market entry requirements are stipulated in the Advocates Law.

However, there is no requirement for applicants to submit a criminal record certificate or any other confirmation from a competent third party. The incorporation of a LLC is approved by the CBA, if all of the partners or a general or limited partnership or if all of the intended shareholders and members of the board of directors of a private limited liability company are advocates enrolled in the Register of Practising Advocates. The Advocates Law does not foresee any measures by the CBA in order to reaffirm fit and properness of partners, shareholders and/or directors. Furthermore, there are no specific provisions in the Advocates Law ensuring on-going monitoring of fit and properness of license holders (e.g. notification obligations in case of changes) and to prevent that close associates of criminals act as license holders or partners, shareholders or directors of Lawyers' Companies. The same deficiencies apply to holders of an ASP license issued by the CBA.

With respect to auditors and accountants, requirements regarding measures to prevent criminals from being professionally accredited or holding a management function in an entity or holding or being the beneficial owner of a significant or controlling interest are foreseen in Section 1.201 of the Members Handbook. Applicants have to comply with various fit and proper requirements, *inter alia*, applicants must declare that they have not been convicted of any criminal offence and a copy of a valid, recent criminal record certificate (not older than three months prior to the application date) has to be submitted. The requirement to submit a criminal record certificate was introduced as of 1 January 2019. All of the practising licenses issued by the ICPAC have to be renewed on an annual basis. In the course of renewal, declarations to confirm compliance with the licensing requirements have to be made by the license holders (including partners, shareholders and directors in the case of partnerships and companies). Moreover, each licensed member is obliged to notify the ICPAC on an on-going basis of any matters affecting fitness and propriety that may occur in between the renewal of each license.

In order to be registered in the Real Estate Agents Registry, natural persons have to comply with the qualifications for registration as outlined in the Real Estate Agents Law (sections 11 and 12). Besides educational and training qualifications, applicants have to prove that they are not under bankruptcy (or under any other penal incapacity under the law or any court order) and have not been convicted of any offence involving a lack of honesty or moral disgrace or, if convicted, have been reinstated in accordance with the provisions of the Reinstating of Convicts Act by submitting a criminal record certificate to the Council.

The registration of a legal person in the Real Estate Agents Registry is a separate and independent registration and is carried out in parallel with the registration of any natural person related to a legal entity. The legal entity has to be established under the laws of the Republic of Cyprus or any other EU member state, has to have a registered office in Cyprus and must prove that it is not in the process of liquidation or resolution (section 11 of the Real Estate Agents Law). According to the Council, shareholders, partners and beneficial owners have to prove that they have not been convicted of any offence by submitting a criminal record certificate to the Council. This could not be verified by the assessment team due to a lack of corresponding legal provisions. Moreover, there is no requirement for directors of real estate entities to undergo a licensing/verification process.

Every licence has to be renewed every year under the same terms and conditions as its issuance (section 17 of the Real Estate agent Law). No specific measures are foreseen to prevent close associates of criminals acting as license holders or partners, shareholders, BOs or directors of license holders.

There are sanctions available for failures to comply with AML/CFT requirements for all DNFBPs. The competent authorities and supervisors are responsible for imposing sanctions (cf. Section 59 (6) of the AML/CFT-Law).

**Criterion 28.5** – According to the Section 59 (5) (b) of the AML/CFT, the supervisory authorities, when implementing a risk-based approach to supervision, base the frequency and intensity of on-site and off-site supervision on the risk profile of obliged entities, and on the risks of money laundering and terrorist financing in Cyprus. Furthermore, supervisory authorities take into account the degree of discretion allowed to the obliged entities and appropriately review the risk

assessments underlying this discretion and the adequacy and implementation of their internal policies, controls and procedures.

Pursuant to the CySEC, it applies a unified risk-based approach to supervision and monitoring of all entities under its supervision that is based on data collected through off-site monitoring. Hence, the same principles and procedures are applicable to financial institutions and ASPs under its supervision. The supervisory system provides four risk categories determining the frequency of on-site inspections as follows: high risk (annually); medium-high risk (2 to 5 years); medium-low risk (5 to 8 years); low risk (ad hoc).

The risk assessment process of the ICPAC is based on off-site monitoring, which is conducted on an annual basis, whereby the ICPAC collects all necessary information via an AML questionnaire and the Annual Compliance Officers Report. The frequency of on-site monitoring depends on the risk assessment of each practitioner with a maximum cycle of six years (high risk: every 1 to 2 years; medium high risk: every 2 to 4 years; medium low risk: every 3 to 5 years; low risk: every 6 years).

The CBA also uses off-site analytical tools in order to determine the on-site visit strategy. On-site visits are conducted to all categories of advocates, LLCs and ASPs with priority given to high-risk advocates, LLCs and ASPs. On-site visits to high risk entities are performed at least annually, to medium-high risk firms every 2 years, to medium-low risk firms every 3 to 4 years and to advocates providing only litigation services, every 5 years.

The Casino Commission has started with the implementation of a risk-based approach to supervision since it started its supervisory work only recently in 2018. The Estate Agents Registration Council does not apply a risk-based approach to supervision.

**Weighting and Conclusion**

Cyprus meets c.28.1-28.3 and mostly meets c. 28.4, 28.5. The Estate Agents Registration Council as SRB is not supervised by the competent authority; market entry measures for the prevention of criminals being professionally accredited, or holding a management function or being the beneficial owner of an obliged entity are not fully adequate for real estate agents and entities supervised by the CBA (advocates, ASPs). The Real Estate Agents Registration Council does not apply a risk-based approach to supervision**. Cyprus is Largely Compliant with Recommendation 28.**

### Recommendation 29 - Financial intelligence units

In the 2011 MER, Cyprus was rated LC with the previous R. 26 due to minor issues related to guidance on reporting and matters related to effectiveness.

**Criterion 29.1** – Section 54 of the AML/CFT Law provides for the establishment of the FIU. It is a multidisciplinary unit established within the Law Office of the Republic and is composed of representatives of the Attorney-General, the Chief of Police and the Director of the Department of Customs and Excise as well as financial analysts. Sec. 55 AML/CFT law sets out the functions of the FIU in detail, according to which, among others, the FIU is the national centre for the receipt and analysis of suspicious transaction reports and other information relevant to money laundering, associated predicate offences and terrorist financing; and for the dissemination of the results of that analysis to the Police and other public authorities such as the Inland Revenue and the Customs and Excise Department, when it is deemed appropriate.

**Criterion 29.2 –**The FIU serves as the central agency for the receipt of Suspicious Transaction Reports (STRs) filed by reporting entities pursuant to Sec. 69(d) of the AML/CFT Law. There is no requirement to submit other types of reports (such as cash transaction reports) to the FIU, in Cyprus.

**Criterion 29.3 –** (a) The FIU may obtain additional information not only from the reporting entity which filed a report but also from all other obliged entities. (Sec. 55(2)(c) AML/CFT Law) (b) The FIU has timely direct or indirect access to the widest possible range of financial, administrative and

law enforcement information[121]. (Sec. 55(a)(a1) AML/CFT Law)

**Criterion 29.4 –** Pursuant to Sec. 55 (2) (a) (i) (ii) of the AML/CFT Law the FIU's functions include: (i) operational analysis which focuses on individual cases and specific targets or on appropriate selected information depending on the type and volume of the disclosures received and the expected use of the information after dissemination; and (ii) a strategic analysis addressing money laundering and terrorist financing trends and patterns.

**Criterion 29.5 –**According to Sec. 55 (1) (b) and 55 (1) (a1) of the AML/CFT Law, the FIU is able to disseminate the results of its analysis to the Police and other public authorities and respond, at its discretion, to requests for information from competent authorities of the Republic of Cyprus, which relate to suspicions for money laundering, associated predicate offences or terrorist financing. The FIU uses the protected and secured electronic system of the FIU for such purposes.

**Criterion 29.6 –** (a) All information, written or oral, which comes to the knowledge of an officer of the FIU, in the execution of his duties, shall be confidential and its communication to any person shall be prohibited except for the proper performance of an official duty or at the express direction of the appropriate authority (Section 67 of the Public Service Law). In addition, FIU staff is subject to Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. (b) Newly recruited members of the FIU must have a clean criminal record and checks are carried out to ensure that they are of good character. They are trained on their responsibilities in handling and disseminating sensitive and confidential information. (c) All databases held within the FIU are securely protected through various firewalls and passwords. All data is also properly backed up on a daily basis. Only FIU personnel have access to FIU databases. The FIU's intranet is isolated from any other networks and a firewall protects FIU data on intranet level. A second firewall on the government hub level exists. The premises of the FIU are protected by an electronic alarm system and a CCTV system. Each office floor is equipped with an access control system which allows entry only to authorised personnel. All documents are stored in archives which are controlled by an electronic alarm and CCTV systems. The server room is equipped with an alarm system, CCTV cameras and fire extinguishing system. In addition, the area around the premises of the FIU is patrolled by the Police on a 24-hour basis.

**Criterion 29.7** – (a) The FIU is an autonomous and independent body (Sec. 55(1) AML/CFT Law). (b) As an independent body it makes arrangements and engages independently with both domestic and foreign authorities. (c) While the FIU is established with the Law Office of the Republic, the AML/CFT clearly sets out its functions, which are distinct from those of the Law Office. (d) Sufficient financial, human and technical resources are provided to the FIU so as to be in a position to execute and deliver its duties (Sec. 54(6) AML/CFT Law).

**Criterion 29.8** – The FIU has been a member of the Egmont Group since 1998.

**Weighting and Conclusion**

Cyprus is rated as Compliant with R. 29.

### Recommendation 30 – Responsibilities of law enforcement and investigative authorities

Cyprus was evaluated as Largely Complaint for former Recommendation 27 in the 3rd round. The previous Assessment team commented that the competencies of the designated investigative authorities could be more usefully delineated.

[121] Direct access to Police database (including information about criminal convictions, investigations, StopList, arrivals and departures from Cyprus), Car registry, Customs Database (containing information on cash declarations in ports and airports as well as Custom's seizures) and Registrar of Companies website for information about companies registered in Cyprus (shareholders, directors, secretary, status of registration, share capital, registered office address). Moreover, the FIU can obtain information (indirect access) from the Department of Lands and Surveys, Cyprus Securities and Exchange Commission, Tax Department, Social Insurance Services, Civil Registry and Migration Department, Registrar of Companies for involvement of persons or entities in Cyprus registered companies and from other government departments based on the provisions of article 55(2)(c) of the domestic AML/CFT Law.

**Criterion 30.1** –

The National Police Service is the security force for the Republic (Article 130 of the Constitution) and pursuant to s.6 of the Police Law acts for law and order, preserving the peace, preventing and detecting crime and apprehending offenders. Any police officer may investigate the commission of an offence (s.4(1) Criminal Procedure Law). The Police are therefore the primary authority for the investigation of ML/TF and associated predicate offences and can be said to be the designated LEA for ensuring the investigation of ML, associated predicate offences and TF. Police Standing Orders ("PSO") provide for the allocation of responsibilities. There are a myriad of offices within the Police who have investigative roles:

1) District Crime Investigation Departments at the local level, and in Nicosia and Limassol there are Economic Crime Sections;

2) Crime Combating Department ("CCD"): the general supervision and coordination of the investigation of all serious criminal offences vests with the Director of the CCD. The CCD receives and analyses files of SARs from the FIU then if there is reasonable suspicion it distributes the files to the appropriate investigating offices. The CCD has the following sub-offices;

- CCD Operations Office (when the investigation involves serious or complicated cases, prominent persons or cases of public interest);
- CCD Economic Crime Investigation Office (which investigates serious financial crime), acts throughout Cyprus and investigates cases in practice which involve more than one district or are of "a particular nature". According to the authorities this means where the case under investigation is serious or complicated economic crime, where it involves "prominent" persons or where it might cause public interest. The ECIO's responsibilities are set out in PSO 3/40(4) including the investigation of serious and complicated cases of an economic nature. What is serious or complicated is not specifically defined yet the authorities note that seriousness is judged on the penalty attaching to the defence and whether something is complicated or not shall depend on the complexity of the *modus operandi* involving complicated financial transactions, schemes and structures;
- CCD Office for Combating Terrorism which co-ordinates all activities of the Police for the prevention and combating of terrorism. PSO 3/39 provides that a criminal investigation regarding terrorism or TF may be initiated on the basis of intelligence or information received by this office, and the office may provide support to local investigators;
- Drug Law Enforcement Service (and each district has its own unit);
- Internal Affairs Service: responsible for investigating allegations and/or complaints regarding corrupt practices or omissions of police officers. It is vested with powers and competencies to conduct investigations, detect and prosecute corruption offences committed by members of the Police or in which members of the Police participate in any way, including ML/TF offences.

According to the authorities, criminal cases are distributed to the sub-offices of the CCD according to the nature and seriousness of the offences, the place it occurred, the nature of the complaint and possible public attention the case might attract.

Up until March 2016, the FIU, using mainly their Police officers-members, conducted investigations, usually in co-operation with the Police. However, since then the situation changed, in practice as well as in law. Section 55(1)(b) of the AML/CFT Law provides that the FIU transmits to the Police and other public authorities information and data for investigation purposes. However, members of the FIU, according to section 54(3) of the AML/CFT Law are deemed to be investigators. This power of the members of the FIU, may be used at the analysis stage if it is necessary to take some further actions, such as the taking of written statements from persons. Also, since the FIU executes formal Mutual Legal Assistance Requests for freezing and confiscation, this power may be used in the course of the execution of such requests in order to get evidence (not simply intelligence) for the

purposes of applying to Court for freezing orders or registering foreign confiscation orders.

The Customs Department investigates customs offences and co-operates with the Police and the FIU in case of an ML/TF investigation, if necessary, with the exchange of information and joint actions.

The Attorney General/Law Office give guidance to the Police, during the criminal investigation when requested, in order to establish the necessary evidence and decides on prosecutions.

Intelligence is provided by the Central Information Service; it does not have investigative powers.

**Criterion 30.2** – The authorities state that a parallel financial investigation can be carried out when traditional investigation is being carried out into serious criminal offences. It is not however abundantly clear on what basis the judgment is made, i.e. "serious" is relatively wide although the authorities said this covers drug trafficking, corruption and large-scale fraud, but the list of crimes is not exhaustive. Instructions to carry out a PFI can be issued by the CCD Director or the Heads of District CIDs. For the reasons discussed in Recommendation 3 (particularly criterion 3.6), there is no bar to initiating PFI based on where the predicate offence occurred.

**Criterion 30.3** – The Police are the designated LEA for investigating ML, associated predicates and TF pursuant to the Constitution and Police Standing Orders. According to the authorities, the identification, tracing and initiation of freezing is part of "the investigation procedure." The investigator or investigation team, which may be supported by accountants or other experts, conduct investigations and this may involve the identification and tracing of assets. The Attorney General is the designated authority for applying for provisional orders (ss. 14-15 AML/CFT Law) although in practice these are done by lawyer members of the FIU, who also belong to the Law Office of the Republic. Section 55(1)(g) AML/CFT Law also provides that the FIU "carries out investigations for identification of illegal proceeds and other related assets, which may be the subject matter of a restraint and/or confiscation order."

**Criterion 30.4** – Not applicable

**Criterion 30.5** – There are no separate anti-corruption units others than the Internal Affairs Service which does not investigate and pursue corruption only, but all offences committed by police officers, which includes ML/TF. The Internal Affairs Service has powers to identify and trace, seize or initiate freezing of property, and have unhindered access to information, documents etc. pursuant to section 5 of the Establishment and Functioning of the Internal Affairs Service of the Police Law of 2018 (Law 3(I)/2018).

**Weighting and Conclusion**

Cyprus meets most of requirements of Recommendation 30 but it is still not clear on what basis a particular office of the police/CCD takes the lead on ML investigations. It is not abundantly clear on what basis the judgment is made to determine that a criminal offence is serious enough to warrant a parallel financial investigation. **Cyprus is rated Largely Compliant for Recommendation 30.**

### Recommendation 31 - Powers of law enforcement and investigative authorities

Cyprus was evaluated as Compliant with the previous Recommendation 28 in the 3rd round.

**Criterion 31.1** –

a) Production of records: In addition to the powers for the Court to order disclosure under ss. 45-46 AML/CFT Law (failure to obey being an offence under s.137 of the Criminal Code), s.6(1) of the Criminal Procedure Law empowers investigating officers to issue a written order requiring the production of a document he considers necessary or desirable for the purposes of an investigation. The "production order" may be issued to a person under whose possession or control is under or is believed to be under to produce it at such reasonable time and place as may be specified in the order. Refusal to comply with a production order is an offence which carries a maximum sentence of imprisonment for three years and/or a fine.

b) Search of persons and premises: Section 25 of the Criminal Procedure Law empowers any police officer to detain and search any person or enter upon and search any place, even without a warrant in certain circumstances such as where he reasonably suspects any offence is about to be committed, is being committed or has recently been committed. Anything found during such search can be seized if it would have been seized in a search under warrant. Section 28 of the Police Act also empowers the police with stop and search powers and s.26 Criminal Procedure Law allows for the search of transport. The Court may issue a search warrant under s.27 of the Criminal Procedure Law on the basis of a sworn statement by a police officer that there is a reasonable ground for believing that there is in any place anything upon or in respect of which any offence has been or is suspected to have been committed, or anything which there is reasonable ground for believing will afford evidence as to the commission of any offence, or anything which there is reasonable ground for believing is intended to be used for the purpose of committing any offence.

c) Taking witness statements: An investigating officer may require any person to attend upon him, where he can examine the person and take a statement from them, if the officer believes the person to be acquainted with the facts and circumstances of the investigated offence (s.5 Criminal Procedure Law). Failure to comply with such a requirement is an offence punishable by up to one year's imprisonment.

d) Seizing and obtaining evidence: As mentioned above, there are production/disclosure orders available as tools for LEAs receiving documents/information (NB s.47 AML/CFT Law makes special provision for information contained in a computer to be disclosed in a visible/legible form). Furthermore, ss. 32-34 Criminal Procedure Law make provision for the detention of evidence collected by the police under warrant or without warrant, the seizure of property not mentioned in a warrant, and the impounding by the judge of anything traced under search warrant.

**Criterion 31.2** –

a) Undercover operations: Pursuant to the Regulation of Some Investigatory Powers (Undercover Police Officers) Law 2017, undercover operations can be carried out into the conduct of investigations into serious offences. "Serious offence" is defined as any offence *inter alia* which carries a maximum sentence of imprisonment of three or more years, so thus covering ML/TF and serious predicate offences. In addition to this specific power, the police are also empowered under section 24 of the Police Law to prevent the commission of offences and apprehend offenders and bring them to justice.

b) Communication Intercept: Pursuant to Art 17 of the Constitution, communication may be intercepted upon a court order without any limitations where this is necessary in the interest of the security of the Republic, in relation to prisoners, and for the prevention, investigation or prosecution of (a) murder/manslaughter; (b) trafficking in human beings; (c) offences related to child pornography; (d) serious drug-related offences; (e) offences relating to the coin/banknote of the Republic; and (f) serious corruption offences[122]. In relation to other serious offences (i.e. criminal offences carrying a maximum penalty of 5 years' imprisonment or more), including ML and FT, interceptions may be ordered by the court only in relation to traffic data, location data and related data necessary to identify the subscriber or user. Therefore, in relation to ML and FT, such orders do not allow for the actual interception of the content of communications. The Cyprus Authorities note that a draft law has been put before the House of Representatives in 2017 to regulate the interference with private communications. However, this can only be taken into account if in force by 7 June 2019, and in any event, it is not clear on the information provided that this law would mitigate the gaps in achieving full compliance with this criterion.

c) Accessing computer systems: The Ratification Law 22(III)/2004 is said to implement the Cybercrime Convention and all the offences contained in it (the evaluator has not been provided with a translated version of this law.) Importantly for this Criterion, the powers under Section II

[122] Such orders are governed by the Protection of the Secrecy of Private Communications (Interception of Communications and Access to a Recorded Content of Private Communication (Law of 1996).

Chapter II of the Convention are implemented into domestic law and are applied *mutatis mutandis* to the Criminal Procedure Law.

d) Controlled Delivery: The Crime Suppression (Controlled Delivery and other special provisions) Law 1995 provides for controlled delivery, with the Chief of Police and director of Customs able to act alone or together (they must notify the AG who can issue instructions). The offences for which controlled delivery can be utilised are prescribed in s.3(2) of the 1995 Law and are limited to drug trafficking, firearms trafficking, stolen objects or nuclear items (no further offences have been prescribed under Regulations). Therefore, the power cannot be used for cash/BNIs being moved (which are related to ML/TF) and indeed in the previous round the assessment team noted that there was no practice of controlled delivery for cash.

**Criterion 31.3** –

a) Section 61A(6)(a) AML/CFT Law enables, in theory at least, for the police to have timely and unrestricted access in all cases to beneficial ownership info held in the Central Register without alerting the entity concerned. However, this Central Register is yet to be established and reliance is instead placed on the use of disclosure orders etc. under AML/CFT Law or Production Orders under the Criminal Procedure Law which may be addressed to all banking institutions. The authorities reported that the vast majority of banks usually reply within the time frame stated in the order(s).

b) Disclosure orders (ss.45-46 AML/CFT Law) and productions orders (s.6 CPL) enable LEAs to identify assets without prior notification to the owner.

It is noted that a tipping off offence is provided for under section 48(2) of the AML/CFT Law: any person who makes any disclosure which may impede or prejudice the interrogation and investigation carried out in respect of prescribed offences or the ascertainment of proceeds, knowing or suspecting that the said interrogation and investigation are taking place, shall be guilty of an offence punishable by imprisonment not exceeding two year and/or a fine of EUR 50,000.

**Criterion 31.4** – The police may ask the FIU for relevant information it holds, and the FIU is required to do so when it deems it appropriate by section 55(1)(b) AML/CFT Law.

**Weighting and Conclusion**

Cyprus has a comprehensive framework for the powers given to the law enforcement and investigative authorities. However, the limited powers for interception of communications is a major shortcoming and together with the gaps for controlled delivery means that **Cyprus is rated as Partially Compliant for Recommendation 31**.

### Recommendation 32 – Cash Couriers

Cyprus was evaluated as Largely Compliant for SRIX under the 3rd round with the assessment team noting that the Special Recommendation was not entirely fulfilled as the declaration system appeared not to cover bearer negotiable instruments.

**Criterion 32.1** - Cyprus operates a declaration system pursuant to the Control of Cash Entering or Leaving the Community and the Exercise of Intra-Community Cash Controls Law no. 53(I) of 2009 ("**Control of Cash Law**"). Under section 4 of the Control of Cash Law, any natural person entering or leaving Cyprus (whether from/to another member state of the EU or a third country), carrying cash or gold of a value of €10,000 or more, shall declare that sum in writing to the competent Customs Officer during his arrival or departure. The definition of "cash" now includes BNIs. There is a gap acknowledged by the Cyprus authorities that this statute does not cover mail or cargo such that there is no requirement to make a similar declaration (or alternatively a disclosure) for cross-border cash/BNIs movement through mail or cargo. The authorities note that this gap will eventually be covered by the entering into force of EU Reg 2018/1672, however as this is not due to come into force until June 2021 it falls well outside the period under evaluation.

**Criterion 32.2** – Cyprus requires, in its declaration system, for all persons entering/leaving the jurisdiction with cash/BNIs to make a written declaration if carrying amounts of €10.000 or more.

**Criterion 32.3** – Not applicable as Cyprus operates a declaration system.

**Criterion 32.4** – According to the authorities, where there has been a false declaration or a failure to declare, such matters are thoroughly investigated. The matter is assigned to a competent customs officer who proceeds with the investigation and he obtains information and clarifications by taking a statement from the offender and requesting information on the evidence of the origin of the cash. Compounding powers will be used when the officer is satisfied that the defendant has no intention to defraud the authorities. Where there is suspicion of ML/TF then the Customs Departments co-operates closely with the FIU and Police for further investigation.

**Criterion 32.5 –** Section 5 of the Control of Cash Law provides that if any person fails to make a declaration under the conditions of section 4, or who makes false, inaccurate or incomplete statement shall be guilty of an offence and liable to a fine of up to €50,000. In such cases, the total amount of cash can be detained or seized as liable to forfeiture, according to the provisions of the Customs Code Law, under conditions laid down by the Director. It is not accepted that the sanctions available for failure/false declarations are proportionate. For example, the difference in penalty between a person who innocently fails to make a declaration of an amount over the threshold and a person who knowingly and fraudulently declares a false amount which is greatly over the threshold is not significant. Therefore, it cannot be said that the penalty is proportionate and furthermore that 50,000 may not be deemed to be dissuasive enough where there are significant false declarations. However, the availability of confiscation arguably mitigates the latter point. It is noted that the Customs Code Law enables an offence to be compounded on acceptance of a payment not exceeding the maximum penalty for that offence; various criteria are taken into account for this compromise such as ignorance, systematic negligence, intended fraud etc., with the compounding amount said to vary from between 10% and 60%. Where there are suspicions of ML.TF, predicate offending then the matter is referred to the Police for further investigation and possible prosecution for the offences and/or confiscation.

**Criterion 32.6** – Customs are required to transmit information obtained based on declarations and failure/false declarations to the FIU (section 9, Control of Cash Law). Further, when upon inquiries carried out by the Department of Customs & Excise, according to the provisions of the sections 4 and 5 of the law, there are implications or reasonable suspicions for the commission of money laundering offences; Customs reports that case to the FIU for further "investigations" which the FIU say means further analysis, conducting domestic queries or contacting foreign FIUs for intelligence purposes.

**Criterion 32.7** – As mentioned above in 32.6, there are specific triggers for when Customs are required to transmit information to the FIU. Furthermore, information is also forwarded onto the Police based on a Memorandum of Understanding (according to the authorities; an English translation of this MoU has not been provided to the Assessment team) and to the tax authorities based on EC Directive 2011/16. There are otherwise no guidelines/framework for domestic co-operation amongst authorities for implementing R32, but it is reported that two customs officers are on secondment to the FIU which will no doubt assist in the co-operation between those two agencies.

**Criterion 32.8** – The Control of Cash Law provides for the restraining of currency/BNI when it is liable to forfeiture due to a failure/false declaration. It is also the case that where there is a suspicion of ML/TF or predicate offences (regardless of whether or not there is also a failure to declare or a false declaration) the customs authorities can inform the police who can then consider exercising the powers under AML/CFT Law and CPL for stopping/restraining cash/BNIs for a reasonable time.

**Criterion 32.9** – The FIU has the ability to inform counterpart FIUs of the data transmitted by the Customs, either in the form of request or spontaneous dissemination. Article 55(1)(c) of the AML/CFT Law provides that amongst its powers and competencies, the FIU shall co-operate with the corresponding Units abroad irrespective of the type of organizational structure of the said Units, spontaneously or upon request, for the purposes of analysis of information and/or

investigation of money laundering offences and financing of terrorism offences, as well as associated predicate offences, with the exchange of information which the Unit has the power to obtain at a domestic level even if the type of predicate offences which it may relate to are not determined at the time of the exchange of information. It also provides for co-operation with corresponding Asset Recovery Offices for the tracing and identification of proceeds of crime or other related property.

**Criterion 32.10** – According to the authorities, the information obtained through the declaration system is registered in a designated electronic registry which is password protected. The use of this information, as well as the information exchanged is said to be conducted under the written authorization of the Personal Data Protection Commissioner.

**Criterion 32.11** –

(a) Where a person is convicted of ML/TF they are subject to the sanctions discussed under Recommendations 3 and 5, and persons transporting cash across the border which is related to ML/TF could be prosecuted for concealing, possessing etc. (ML) or providing/collecting (TF) under the provisions of the AML/CFT Law and the TF Convention. Failing prosecution for the principal ML/TF offences, cash couriers could also be liable for aiding and abetting offences.

(b) Regarding forfeiture, as detailed above, there are sufficient powers in place for the forfeiture of cross-border cash/BNIs.

**Weighting and Conclusion**

Cyprus has a shortcoming in that there is no declaration/disclosure system for cross-border movements of cash/BNIs through mail cargo. **Cyprus is therefore rated Largely Compliant for Recommendation 32**.

### Recommendation 33 – Statistics

In the 2011 MER, Cyprus was rated PC with the previous R. 32 since it was not demonstrated that Cyprus reviewed the performance of the AML/CFT regime on a regular basis. Complete statistics were not available.

**Criterion 33.1** – **Pursuant** to Sec. 76, AML/CFT Law, the competent supervisory authorities, the FIU, the Ministry of Justice and Public Order, the Police, and the Customs and Excise Department, are required to maintain comprehensive statistics on matters related to their competences. Such statistics shall as a minimum cover the suspicious transaction reports made to the Unit, the inspections made by the supervisory authorities, the administrative penalties and the disciplinary sanctions imposed by the supervisory authorities, the number of cases investigated, the number of criminal prosecutions, the number of convictions and the assets frozen, seized or confiscated as well as the types of predicate offences and applications received or sent by the FIU, within the scope of the cooperation with respective Units of other countries. All statistical data is transmitted to the Commission and is available for the assessment of risks in accordance with paragraph (b1) of section 57, the national valuations including the National Risk Assessment and Evaluation of the Council of Europe's "Moneyval" Commission. In practice, statistics on STRs/SARs received and disseminated are kept by the FIU as well as statistics on freezing and confiscation on the basis of the AML/CFT Law. Statistics on Mutual Legal Assistance and European Investigation Orders requests for co-operation made and received are held by the Ministry of Justice and Public Order. Statistics on ML/TF investigations, prosecutions and convictions are kept by the Police.

**Weighting and Conclusion**

R. 33 is rated as C.

### Recommendation 34 – Guidance and feedback

In the 2011 MER, Cyprus was rated as Largely Compliant with the requirements of former Recommendation 25 due to the following deficiencies: Guidance Notes for financial institutions and DNFBPs did not cover financing of terrorism. No guidelines were issued to domestic trust and

company service providers and some other DNFBPs.

Cyprus addressed some of these deficiencies by amending/issuing a number of supervisory directives and providing AML/CFT trainings, guidance and feedback.

**Criterion 34.1** –

*FIU Feedback and Outreach*

Section 55(1)(f) of the AML/CFT Law requires the FIU to inform, where practicable, the obliged entities of the effectiveness and results of the STRs/SARs submitted to it. In 2016 the FIU issued "New Feedback Procedures", which explains the procedure for feedback by the FIU. Individual feedback is given through an IT system on specific STRs/SARs when such communication is deemed necessary or useful. For example, if useful information arises following communication with other FIUs, the Police, or other sources, such feedback is provided through the system, which enables timely and efficient information exchange; or when postponement of transaction is deemed necessary, such directions are given immediately and directly to the reporting entity. Moreover, each reporting entity, mainly banking institutions, may send a request for feedback providing a list of the STRs/SARs submitted, requesting the status of them. The FIU also communicates with AMLCOs using other means (e.g. telephone) to exchange the views or provide further guidance.

The FIU issues aggregated feedback and guidance on STR/SAR reporting: the most recent guidance was issued in January 2019 "General Feedback – indicators" addressed to all reporting entities; feedback was also issued in April 2018 ("Guidelines for Reporting"), July 2018 and May 2016. In addition, AML/CFT trainings have been delivered to obliged entities by the FIU itself and/or in cooperation with other supervisory authorities.

*Supervisory authorities Guidance and Outreach*

Section 59(4) of the AML/CFT Law provides an obligation for supervisory authorities to issue directives to supervised entities. The directives are binding in nature and provide further details/ guidance on the implementation of AML/CFT requirements stipulated in the AML/CFT Law. Directives have been issued by the CBC, CySEC, ICCS, ICPAC, CBA and the RE Council. In addition, the supervisory authorities provide AML/CFT training/consultations and/or other forms of guidance and feedback to the entities under their supervision. The feedback is provided as part of on-site examination process and, where necessary, addressed during ongoing consultations, meetings and trainings to the obliged persons.

CBC. The CBC has issued directives for credit institutions and MTBs[123]. In addition, a number of additional Guidelines have been issued by the CBC for credit institutions on Sound and effective risk management systems to identify and understand ML/TF risks; Customer Due Diligence and construction of customer's business/risk profile; Enhanced Due Diligence measures in relation to Politically Exposed Persons; Ongoing Monitoring of business relationships and transactions; Education and Training to staff in relation to money laundering and terrorist financing; Fraudulent tax crimes as a predicate offence. No guidelines have been issued by the CBC specifically to credit acquiring companies, currency exchange offices, e-money institutions and payment institutions. However, the CBC directive for MTBs can be considered as covering part of the financial services activities provided by payment and e-money institutions. The CBC also provides specialized AML/CFT trainings to employees of all supervised institutions and hosts meetings with AMLCOs.

CySEC. CySEC has issued an AML/CFT directive for its supervised entities. In addition, CySEC has issued a number of circulars, concerning, inter alia, guidance on new provisions of the AML/CFT Law; guidance on legislative changes at an EU level; serious tax offenses; and guidance on the content of the annual report of the compliance officers in relation to issues which have arisen in relation to preventing money laundering and terrorist financing. Furthermore, CySEC has issued feedback (in the form of circulars) to supervised entities in relation to common and recurring weaknesses and/or deficiencies and best/poor practices identified during the onsite and offsite

[123] Directive for MTBs was last amended in 2011.

inspections. The CySEC provides guidance to its regulated entities by addressing enquiries of legal nature on the application of the AML/CFT Law and CySEC's AML/CFT Directive. Circulars issued for AML/CFT purposes are addressed to all entities under the supervision of CySEC and are publically available on CySEC's website.
ICCS. In accordance with Article 59(4) of the AML/CFT Law, the ICCS has issued Orders for life-insurance companies and life insurance intermediaries (Orders are legally binding). In addition, through its off-site and on-site supervision the ICCS has provided guidance to supervised entities on the submission of the AMLCO annual report and in response to ad hoc queries, as well as providing formal feedback from on-site visits to the senior management and the Board of Directors. While, the ICCS does not deliver any formal AML/CFT training itself to the supervised entities, it encourages insurance firms to take part in the trainings, delivered by other supervisory authorities, international organisations or similar. For monitoring purposes, ICCS requests supervised entities to include data and information on the AML/CFT trainings taken in their offsite returns.
ICPAC. ICPAC has issued a directive for its supervised entities. In cooperation with other professionals and the competent authorities, ICPAC has provided AML/CFT seminars for its members. Other forms of guidance are delivered by ICPAC to its members in the forms of circulars, guidance notes, free access to e-learning seminars and a free helpline.
CBA. The CBA issues directives, guidelines and circulars to its members and also provides targeted seminars to its members.

Casino Commission. No directives or guidance have been issued by the Casino Commission. However, the supervisor is very closely engaged in monitoring of sole casino operator in Cyprus and provides constant feedback and consultations.

RE Council. The RE Council, which took over supervisory duties from the FIU in 2018, issued a directive for real estate agents in April 2019.

The directives issued by the supervisory authorities - the CBC, CySEC, ICPAC - do include lists of examples of potentially suspicious transactions/activities, related to ML and, separately, to TF. However, examples of suspicious TF criteria in the instruments are almost identical in different supervisory directives, thus do not take into account sectorial specificities (i.e. different features of products and services offered by each sector). The most material sector in Cyprus received more attention in this respect: in 2016 CBC issued an additional comprehensive guidance paper on TF for credit institutions.
Guidelines issued by the ICCS, CBA and RE Council do not cover financing of terrorism.

**Weighting and Conclusion**

**R. 34 rated largely compliant.** The CBC has not issued guidelines to credit acquiring companies, currency exchange offices, e-money institutions and payment institutions that do not operate as MSBs. The Casino Commission has not issued guidelines for casinos. There is scope for supervisory authorities and the FIU to take further steps to enhance guidance on identifying TF suspicion.

### Recommendation 35 – Sanctions

In the 2011 MER, Cyprus was rated as Partly Compliant with the requirements of former Recommendation 17 due to the following deficiencies: there was legal uncertainty on the applicability of the AML/CFT sanctions to the directors and senior management; sanctions applied were not considered as proportionate and were applied mainly in the form of warning letters; no sanctions were imposed in the sectors of insurance and credit cooperatives.

**Criterion 35.1 –**

*Financial institutions and DNFBPs*

Supervisory authorities have the power to require supervised entities to remediate deficiencies within a specified time frame and apply administrative sanctions for supervised entities for non-compliance with the AML/CFT Law and directives issued by the authorities (section 59(6) of the

AML/CFT law), namely: 1. To impose administrative fines: a) up to one million euro (€1.000.000) for DNFBPs and up to five million euro (€5.000.000) for FIs; b) where the benefit derived from the breach exceeds the amount of the maximum permissible administrative fine, an administrative fine up to an amount of at least twice the amount of the benefit derived from the breach might be applied; c) in the event the breach continues, an administrative fine of up to one thousand euro (€1.000) for each day the breach continues; 2. to amend[124], suspend or withdraw the licence of the supervised person; 3. to make a public statement about the legal person responsible for the breach and the nature of the breach[125].

As per section 59(6)(b) of the AML/CFT Law, an independent legal professional or auditor or external accountant who fails to comply with that part of the law or the directives issued by the competent supervisory authority is referred by the competent supervisory authority to the relevant disciplinary committee to make a decision in relation to the issue of a sanction.

In addition to the administrative sanctions specified above, criminal sanctions are applicable in some circumstances.

According to the section 27(1)(4) of the AML/CFT Law, failure to report suspicion to the FIU is a criminal offence (this applies to any person, including obliged entities). Upon conviction persons can be subject to imprisonment not exceeding two years or a penalty not exceeding €5.000 or both these sentences.

According to the section 48(3) of the AML/CFT Law, tipping off is a criminal offence, and, upon conviction, persons can be subject to imprisonment not exceeding two years or a penalty not exceeding €50.000 or both these sentences.

Section 68.C. of the AML/CFT Law imposes sanctions for non-compliance for any persons that knowingly provide false or misleading evidence or information for the identity of the customer or of the ultimate beneficial owner or provides false or forged identification documents. A person found guilty of the offence, upon conviction, is subject to imprisonment not exceeding two years or to a pecuniary penalty of up to hundred thousand euro (€100.000) or to both of these penalties. In addition, according to the Section 59(9) of the AML/CFT law, the supervisory authorities have the power to take all and/or any of the measures mentioned in section 59(6) of the Law, in case any person under their supervision refuses to comply with the request of supervisory authorities to provide the information within the specified deadline or in case that the person refuses to provide any information or provides insufficient, false or forged information.

*Targeted Financial Sanctions*

The section 3(1) and 3(2) of the Law 58(1)/2016 on UNSCR and EU sanctions imposes obligation for supervisory authorities to monitor the implementation of TFS and, thus, to apply sanctions, that are stipulated under the section 59(6) of the AML/CFT law.

Section 4(1) of Law 58(I)/2016 on UNSCR and EU sanctions provides that any person in violation of these sanctions is guilty of an offence and in case of conviction a legal person is subject to a pecuniary fine not exceeding €300.000.

*NPOs*

See criterion 8.4(b).

**Criterion 35.2** –

Administrative fines for AML/CFT breaches, as stipulated in the section 59(6) of the AML/CFT Law, are applicable to a person discharging managerial responsibilities in an obliged entity or to any other person, whenever it is established that the failure to comply was due to their fault, intentional omission or negligence. Supervisory institutions also have a right to temporarily

[124] For the purpose of AML/CFT Law, "amend" shall be understood as any changes to the terms of the licence, including restriction (i.e. amending the licence can affect the services and products provided by the supervisory authorities).

[125] Supervisory authorities may at their discretion make public statements for any kind of sanctions imposed to the supervised persons.

prohibit any person held responsible for a breach from exercising managerial responsibilities/functions in an obliged entity. A supervisory authority may also make a public statement about natural persons held responsible for a breach and nature of the breach. The penalties for failure to report suspicion mentioned in c.35.1 also apply to any person who fails to comply with the AML/CFT Law. The provisions cover senior managers and directors.

With regard to tipping off, natural person is subject to the same criminal penalties as legal persons (see c.35.1).

*Targeted Financial Sanctions*

The section 3(1) of the Law 58(1)/2016 on UNSCR and EU sanctions imposes obligation for supervisory authorities to monitor the implementation of TFS and, thus, to apply sanctions, that are stipulated under the section 59(6) of the AML/CFT law.

In addition, section 4(1) of Law 58(1)/2016 on UNSCR and EU sanctions provides that a natural person in violation of these sanctions is guilty of an offence and in case of conviction can be subject to imprisonment of up to two years, a fine not exceeding €100,000 or both.

**Weighting and Conclusion**

**Rec. 35 is rated compliant.**

### Recommendation 36 – International instruments

In the 2011 MER, Cyprus was rated LC with the previous R. 35 since it had not fully implemented the Palermo and Vienna conventions.

**Criterion 36.1** – Cyprus has signed and ratified the Vienna Convention (Ratification Law 49/1990), the Palermo Convention (Ratification Law 11(III)/2003), the Merida Convention (Ratification Law 25(III)/2008) and the TF Convention (Ratification Law 29(III)/2001).

**Criterion 36.2** –All the conventions were fully implemented without any reservations (including through the Drugs and Psychotropic Substances Law of 1977 (L.29/1977), AML/CFT Law, CPC, CC, Extradition Law (L.95 and 97/1970), Law on International Cooperation (Law 23(I)/2001), Protection of Witnesses Law (Law 95(I)/2001), Law establishing minimum standards on rights, support and protection of victims of crime (Law 51(I)/2016), Prevention of Corruption Offences Law (Cap.161), The Control of Cash Entering or Leaving the Community and the Exercise of Intra-community Cash Control Law (L.53(I)/2009), Suppression of Terrorism Law).

***Weighting and Conclusion***

**R. 36 is Compliant.**

### Recommendation 37 - Mutual legal assistance

In the 2011 MER, Cyprus was rated LC with the previous R. 36. The assessment team considered that the incomplete criminalisation of FT restricted the authorities' ability to provide MLA in circumstances where dual criminality was required.

**Criterion 37.1** – Pursuant to the Law Providing for International Co-operation in Criminal Matters (Law 23(I)/2001), the ratification of all major multilateral conventions (Council of Europe, UN and EU) on MLA in criminal matters, Parts IV and IVA of the AML/CFT Law and Law 181/2017 (transposing the EIO Directive), Cyprus has a legal basis to provide a wide range of mutual legal assistance in relation to ML, associated predicate offences, and FT. Assistance can be provided in relation to: the production of records (Section 45(1) and (2) AML/CFT Law), search and seizure of evidence (Section 9 Law 23(I)/2001), taking witness statements (Section 9 Law 23(I)/2001), freezing and confiscation of proceeds and instrumentalities (Parts IV and V AML/CFT Law); taking witness statements (Sec.5, CPC); effecting service of judicial documents (Art. 3 and 4 Law 23(I)/2001); etc.

**Criterion 37.2** –The authority responsible for the transmission and execution of requests is the

Ministry of Justice and Public Order (MJPO). The MJPO co-operates closely with the FIU and the Police for the execution of requests. The MJPO has clear processes in place to handle MLA requests. However, there are no formal prioritisation criteria. The timely execution of MLA requests has improved significantly since the setting up of the Office for the Execution/Handling of MLA Requests. There is a case management system in place.

**Criterion 37.3** – MLA is not prohibited or made subject to unreasonable or unduly restrictive conditions. In accordance with Section 9(2) of Law 23(I)/2001, MLA requests may only be executed if the manner in which they are to be executed is not contrary to the Constitution or international conventions on human rights to which Cyprus is a party. According to Section 9(5)(b), in executing a request, the Court shall not compel a witness to testify if the testimony may be harmful to the security of Cyprus. This decision should be issued by the Minister of Foreign Affairs in agreement with the Minister of Defence.

**Criterion 37.4** –There is nothing in Law 23(I)/2001 which restricts the provision of MLA on the sole ground that the offence is considered to involve fiscal matters or on the grounds of secrecy or confidentiality requirements on FIs or DNFBPs, except in those instances where the legal professional privilege applies (Art. 44, AML/CFT Law).

**Criterion 37.5 –**Cyprus, having ratified the 2nd Additional Protocol to the CoE Convention on Mutual Assistance in Criminal Matters (Ratification Law 5(III)/2012), applies the provisions of section 25 which provides that at the request of the requesting party, the requested party shall keep confidential the fact and substance of the request, except to the extent necessary to execute the request. The MJPO, the Police, the FIU and the other competent authorities involved in the execution of requests are all required by law to keep confidential any information that comes into their possession in the exercise of their functions.

**Criterion 37.6 –** Legal assistance requires dual criminality. However, where the request involves non-coercive measures, the authorities may deploy informal channels to provide assistance.

**Criterion 37.7** – The requirement of dual criminality is not applied strictly, and offences are interpreted in a wide manner.

**Criterion 37.8** –Pursuant to Art 9 subsections (5) to (8) Law 23(I)/2001, the Courts, the Prosecution, the Police and Customs have all the powers available to them in the course of domestic proceedings when executing a MLA request. However, the issues identified under R. 31have a negative bearing on this criterion.

**Weighting and Conclusion**

Cyprus meets most of the criteria under R. 37. The issues identified under R. 31 have a negative bearing on c.37.8. Cyprus is rated Largely Compliant with R. 37.

### Recommendation 38 – Mutual legal assistance: freezing and confiscation

In the 2011 MER, Cyprus was rated C with the previous R. 38.

**Criterion 38.1** – Cyprus has the authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate property. This applies to all types of property referred to under (a) to (e) (see definition of "foreign order" under Section 37, AML/CFT Law).

**Identification:** Art. 45 (2), AML/CFT Law, specifically states that disclosure orders (see c.4.2(a) and c. 31.1(a)) and may be applied for upon the request of a foreign LEA in the course of an investigation outside of Cyprus.

**Freezing, seizure and confiscation:** MLA requests of this nature are governed by Art. 14(1)(b), Art. 15(1)(b), Art. 43(3), Part IV and IVA of the AML/CFT Law. Under Arts. 14, 15 and Art. 43(3) the Cypriot authorities may secure a domestic restraint or charging order (see c. 4.2(b)) on behalf of foreign authorities. Part IV deals with the registration and enforcement of freezing, seizure and confiscation requests from foreign countries which are parties to the Conventions referred to under

R. 36, except for the USA. Cyprus cooperates with the USA on the basis of a bilateral treaty on MLA in penal matters with Cyprus and an agreement on MLA between the EU and the USA. Part IV A deals with the registration and enforcement of freezing, seizure and confiscation requests from the member states of the EU.

**Criterion 38.2** – The Cypriot authorities may enforce a foreign non-conviction-based confiscation order pursuant to Section 37 AML/CFT Law. This is defined as an order which must result in the deprivation of property and does not constitute a criminal sanction, to the extent that it is ordered by the court of a foreign country in relation to a criminal offence, provided that it has been proven that the property constitutes proceeds. Provisional measures referred to under Sections 14 and 15 of the AML/CFT Law apply.

**Criterion 38.3** – (a) There are adequate statutory and practical arrangements in place in relation to the FIU and the courts, which ensure that the execution of seizure and confiscation orders are adequately co-ordinated with foreign authorities. (b) The mechanism described under c.4.4 applies pursuant to the application of Section 43(1) in relation to orders from foreign countries which are parties to the Conventions referred to under R. 36, (except with the USA, where cooperation is based on a bilateral treaty and the agreement on MLA between the EU and the USA) and Section 43HF(1) in relation to orders from the member states of the EU.

**Criterion 38.4** –The AML/CFT Law, Sections 39(3) and 43JA(4), provides for the sharing of confiscated property with other countries.

**Weighting and Conclusion**

**Cyprus is compliant with R. 38.**

### Recommendation 39 – Extradition

In the 2011 MER, Cyprus was rated C with the previous R. 39.

**Criterion 39.1** – *(Met)* (a) Extradition is governed by the Law on the Extradition of Fugitive Offenders, L.97/70 (as amended by L.97/90, L.154(I)/2011 and L.175(I)/2013), the ratification of the European Convention on Extradition, L.95/70 and its Protocols, L.23/79 and L.17/84, the Law on the European Arrest Warrant and the Procedures for surrender between the Member States of the European Union, L.133(I)/2004 (as amended by L.112(I)/2006 and L.30(I)/2014). All these laws ensure that ML and TF are extraditable offences. (b) In the case of extradition requests by third countries i.e. under the European Convention on Extradition or a bilateral agreement, a case management system is maintained by the Ministry of Justice and Public Order in its capacity as the national Central Authority. In addition, the case is managed judicially in the course of judicial proceedings leading to a Court decision on the success or rejection of the request. Under European Arrest Warrant proceedings, case management is carried out solely by the Court. The European Arrest Warrant does not provide for designated central authorities. (c) Bilateral agreements signed by Cyprus are always in line with the provisions and the conditions of the European Convention on Extradition. This also holds truth regarding L.97/70. This ensures that no unreasonable or unduly restrictive conditions are in any way placed on the execution of requests. That being said, there are a few examples where more relaxed conditions apply under L.97/70 than under the Convention. For instance, whereas Art.12 of the Convention provides for "an authenticated copy" of the conviction and sentence or detention order or of the arrest warrant as part of the supporting documents, an "arrest warrant" would suffice under art.7(2)(a) of L.97/70.

**Criterion 39.2** – Extradition of Cypriot nationals is permissible provided that the requesting party also allows for extradition of its nationals to Cyprus – Laws 127(I)/2006 and L.68(I)/2013 amending the Constitution of Cyprus and provided that the fundamental human rights of the extradited person are protected, particularly the right to fair trial/treatment as protected by the UN Convention on Human Rights, the European Convention on Human Rights and the Cyprus Constitution (Art. 12) and as guaranteed by the European Convention on Extradition.

**Criterion 39.3** –While dual criminality is required for extradition by Cyprus, the requirement is

deemed to be satisfied provided that both countries criminalise the conduct underlying the offence. This principle was upheld by the Courts – in one case the court held that there is no need for absolute identification of the offences, nor is the description of the offences in the foreign arrest warrant of crucial significance and the requirement of double criminality is met because the actions referred to in the statement of facts constitute offences also in the Republic of Cyprus.

**Criterion 39.4** – Regarding simplified extradition proceedings, these are regulated by the European Convention on Simplified Extradition Proceedings as ratified by L.12(III)/2004; the Law on the European Arrest Warrant and the Procedures for surrender between the Member States of the European Union, L.133(I)/2004 (as amended by L.112(I)/2006 and L.30(I)/2014) and, to the extent possible, the bilateral agreements between the Republic of Cyprus and third countries.

**Weighting and Conclusion**

**Cyprus is compliant with R. 39.**

### Recommendation 40 – Other forms of international cooperation

R. 40 was rated PC in the 2010 MER[126] due to restrictions which unduly limited FIU co-operation with its counterparts and lack of broad statutory powers for supervisors, which had a bearing on the effectiveness of supervisory co-operation (except for the CBC).

Since the 2010 MER, the restrictions which applied to the FIU have been remedied and it is now in a position to utilise all the powers it can avail itself of for domestic purposes to process requests from foreign FIUs (Section 55(1)(c)(i)). The powers of the CBC and the CySEC to co-operate with foreign counterparts now appear to be broad enough. The situation does not appear to have changed with respect to other financial supervisory authorities and DNFBP supervisors.

**Criterion 40.1** – The FIU (Sec. 55(1)(c)(i),(ii) and (2A), AML/CFT Law), LEAs (various international instruments to which Cyprus is a party, EU Acquis, Police Standing Order 1/74), Customs (Customs Code article 4(4) of the Customs Code Law no. 94(I)/2004, Law ratifying the Naples II Convention, EU Acquis and bilateral and multilateral conventions), the CBC (Sec. 27, Business of Credit Institutions Law), the CySEC (Sec. 28 and 29, CySEC Law), the ICCS (Section 66 and 67 of the Law on Insurance) and the Casino Commission (Sec 98 of the Casino Control Law) can rapidly provide the widest range of international co-operation, spontaneously and upon request, in relation to ML, associated predicate offences and FT.

**Criterion 40.2 –**

(a) See criterion 40.1

(b) Nothing prevents the competent authorities from using the most efficient means to co-operate. The relevant authorities can co-operate directly with their counterparts.

(c) Competent authorities have clear and secure gateways, mechanisms or channels to facilitate, transmit and execute requests for assistance. Co-operation largely occurs through mechanisms established by the EU, Egmont, Europol, Interpol, SIRENE. For example, the Police uses Interpol and Europol mechanisms and police liaison officers; the FIU uses Egmont Secure Web and FIU.net; the supervisory authorities use designated electronic mailboxes; and Customs uses AFIS Mail and SIENA (EUROPOL).

(d) Competent authorities have processes in place to assess and prioritise requests and ensure timely assistance is provided. For example, the FIU is required to respond to requests in a timely manner based on Sec. 55(2A)(c) AML/CFT Law. It has developed an internal procedure for the prioritisation of requests depending on their urgency. The Police has developed a manual for international police cooperation. CySEC and CBC have a designated electronic mailbox for the receipt and transmission of international requests which are

[126] The relevant following paragraphs in the 2010 MER for all competent authorities are the following: (a) FIU/ARO: 789-790, 796-803, 816, 818-820 (b) LEAs: 791, 804-806, 821 (c) Customs: 792, 807-808, 821 (d) supervisory authorities: 793-795, 809 – 815, 817.

monitored by the International Cooperation Department of CySEC and AML/CFT team respectively.

(e) For FIU staff see c.29.6(a). Additionally, Sec. 55(2A), AML/CFT Law provides that information exchanged between FIUs shall only be used for the purpose for which it was sought and provided and any dissemination of the said information by the receiving FIU to another authority, agency or department or any use of such information for purposes beyond those originally approved is made subject to prior consent by the FIU providing the information. At the Police a Protocol for Handling Information sets out in detail all procedures to be followed with respect to receiving, managing and storing information held by the Europol National Unit, Interpol National Bureau, the Police cooperation Office and the SIRENE Office. In case of CySEC all information received is treated in the strictest confidence in accordance with the confidentiality rules set out in the CySEC Law and the IOSCO MMoU and the ESMA MMoU. At the CBC sections 26, 27B, 28B and 28A of the Business of Credit Institutions Law provide proper confidentiality of the information.

**Criterion 40.3** –None of the competent authorities require a bilateral or multilateral agreement to co-operate with their counterparts.

**Criterion 40.4** –As a member of the Egmont Group, the FIU is required to provide feedback when so required pursuant to Egmont Principles for Information Exchange. CySEC is required, as the signatory of IOSCO MMoU, provide information to the IOSCO MMoU Monitoring Group, which collects the yearly statistics on the requests for assistance (including the timeliness of execution and the use and usefulness of the information) sent by all signatories and some non-members. The Police may upon request, provide feedback to competent authorities from it has received assistance, on the use and usefulness of the information obtained.

**Criterion 40.5** –The FIU does not prohibit or place any unreasonable or unduly restrictive conditions on the exchange of information or assistance: the FIU may only refuse assistance in exceptional circumstances where the exchange could by contrary to fundamental principles of the law of the Republic (Sec 55(2A)(d) AML/CFT Law); assistance is provided regardless of any differences between national law definitions of tax crimes (Sec 55(2A)(e) AML/CFT Law); financial/professional secrecy does not inhibit the exchange of information (see R. 9); assistance is not withheld if there is an inquiry, investigation or proceeding underway in Cyprus – the FIU may only refuse to provide consent to the requesting the FIU to disseminate the information to another authority if this could to the impairment of a criminal investigation process in Cyprus (Sec 55(2A)(g) para. 3, AML/CFT Law); the FIU may co-operate with any type of FIU (Section 55(1)(c)(i), AML/CFT Law). The Police may only refuse to provide assistance in a limited number of instances: co-operation through Interpol/Europol may be refused if this is contrary to the essential interests of the security of Cyprus, assistance would jeopardise the success of an ongoing investigation or the safety of an individual, if the information requested relates to the Cyprus Intelligence Service. Similar conditions apply within the context of cooperation under the auspices of the Swedish initiative. Within the framework of other international instruments, restrictions are only imposed where these are explicitly provided for in the instruments.

**Criterion 40.6** –In relation to the FIU, Sec. 55(2A)(g), AML/CFT Law provides that information exchanged between FIUs is used only for the purpose for which it was sought and provided and any dissemination of the said information by the receiving FIU to another authority, agency or department or any use of such information for purposes beyond those originally approved is made subject to prior consent by the FIU providing the information. In relation to Custom article 78(8) and article 89(6) of the Customs Code Law no. 94(I)/2004 prohibit to authorized officers in any way to provide any collected or transmitted confidential information to third parties unless upon authorization by the minister and prescribes punishment in case of violation. In relation to Police relevant provisions are provided under criterion 40.1 above, which are also reflected in the Manual for International Police Cooperation (July 2016) that has been issued by the EUIPCD.

**Criterion 40.7** – Requests for co-operation and exchanges of information are subject to the same

confidentiality rules which apply to competent authorities when handling information from domestic sources.

**Criterion 40.8** – The broad powers for information exchange permit the competent authorities to conduct inquiries on behalf of foreign counterparts and share information that would obtainable by them if such inquiries were being carried out domestically.

**Criterion 40.9** – see criterion 40.1 and 40.5(d).

**Criterion 40.10** – As a member of the Egmont Group, the FIU is bound by Egmont Group Principles and, as such, pursuant to the Egmont Group Principles on Information Exchange, it generally provides feedback to its counterparts when so requested.

**Criterion 40.11** – According to Sec.55(1)(c)(i), AML/CFT Law, the FIU can co-operate and exchange information with its counterparts and provide information which it has the power to obtain domestically, even if the type of the predicate offences which it may relate to has not been determined at the time of the exchange of information.

**Criterion 40.12** – The CBC, CySEC and the ICCS has the legal basis for cooperation with their foreign counterparts (see c. 40.1). This includes exchanging supervisory information for AML/CFT purposes.

**Criterion 40.13** - Pursuant to the Section 27 of the Banking Law, CBC is able to exchange information with foreign competent authorities to assist them in the conduct of their duties and responsibilities or to enable the effective conduct of its own duties, including the supervision on a consolidated basis. Pursuant to the Section 29 of the CySEC Law, CySEC may cooperate and exchange information with other foreign competent supervisory authorities and organisations. CySEC may establish protocols for the cooperation with supervisory authorities or other organisations abroad in the form of MoU. These MoUs provide for the exchange of information, cross-border inspections and the collection of information by one authority on behalf of another in view of ongoing investigations, and generally to provide mutual assistance in order to ensure compliance with the relevant laws governing securities markets. According to Articles 66-67 of the Insurance and Reinsurance Business and Other Related Issues Law of 2016, ICCS is able to exchange information with foreign superintendent of insurance and the supervisory authorities.

**Criterion 40.14** – As mentioned criterion 40.13, CySEC has a framework and procedures for cooperation to facilitate the exchange of information between the parties for the better monitoring of transactions and activities in the field of securities markets. Information is exchanged on the basis of the IOSCO and ESMA MMoU, to which CySEC is a signatory. In relation to the CBC, exchange of the information on the basis of the MoUs includes any type of relevant for AML/CFT purposes information – regulatory, prudential and AML/CFT specific. Information can also be exchanged on the basis of the Banking Law.

**Criterion 40.15 -** The CBC, CySEC and ICCS may conduct inquiries on behalf of their foreign counterparts, and exchange with them all information obtained, and have done so in practice.

**Criterion 40.16 -** Pursuant to article 7 of the ESMA MMoU CySEC can make disclosure after it has discussed the nature and extent of the disclosure required with the requesting authority and obtained its consent to the disclosure. Also, according to article 10 of the IOSCO MMoU if CySEC intends to use information for any purpose other than stated in the MoU, it must obtain the consent of the requested authority. The MoUs signed by the CBC with foreign counterparts require prior authorisation of the requested supervisor before dissemination of information can take place.

**Criterion 40.17** – The Police has wide-ranging powers to exchange information with its foreign counterparts based on various legal instruments as indicated under c.40.1.

**Criterion 40.18** – Law enforcement authorities are able to conduct inquiries and use domestically-available, non-coercive powers and investigative techniques to conduct inquiries and obtain information on behalf of foreign counterparts.

**Criterion 40.19** –Cyprus may establish or participate in joint investigation teams with competent authorities of other jurisdictions for the investigation of any criminal offence including ML, associated predicate offences and FT. The relevant law is the Joint Investigations Teams Law of 2004 (L.244(I)/2004 as amended by L.98(I)/2011) which was enacted to align national law with Council Framework Decision 2002/465/JHA of 13 June 2002 on joint investigation teams and allows for the establishment of joint investigation teams in implementation of the provisions of the EU Convention on Mutual Legal Assistance in Criminal Matters between the Member States of the European Union and the provisions of any other Multilateral or Bilateral Convention to which the Republic is a party and which provides for the establishment of joint investigation teams.

**Criterion 40.20** –There is nothing which inhibits competent authorities' ability to exchange information indirectly with non-counterparts.

**Weighting and Conclusion**

**Cyprus is Compliant with R. 40.**

## Summary of Technical Compliance – Key Deficiencies

| Recommendation | Rating | Factor(s) underlying the rating |
|---|---|---|
| 1. Assessing risks & applying a risk-based approach | **LC** | • Some elements were not identified and assessed to their greatest extent in the NRA (e.g. an assessment of money flows to and from high risk areas, the implications associated with the country of origin or of continuing family ties for an apparently large population of temporary resident workers, etc).<br>• Simplified CDD is not expressly prohibited where there is suspicion of ML/TF. |
| 2. National cooperation and coordination | **LC** | • The PF coordination mechanism is somewhat fragmented. |
| 3. Money laundering offence | **C** | |
| 4. Confiscation and provisional measures | **C** | |
| 5. Terrorist financing offence | **LC** | • It is not unequivocally clear whether the mere collecting of funds is covered by "providing support" if the funds are not transmitted to a terrorist/terrorist organisation;<br>• Financial penalties under the Combating of Terrorism Law are not dissuasive;<br>• Issue identified in 5.2 regarding collection of funds may have a cascading effect such that if the TF offence is not fully implemented, not all TF is a predicate offence for ML. |
| 6. Targeted financial sanctions related to terrorism & FT | **LC** | • There are no formal procedures in place establishing a domestic process for identifying targets and the criteria to be applied under that process, or for procedures to be followed when making a designation proposal to the UN – reliance is made on the EU framework.<br>• There is no legal basis, and related procedures, to make domestic designations on the country's own motion or after examining and giving effect to, the request of another country – reliance is made on the EU framework.<br>• There are neither legal authorities nor procedures or mechanisms which expressly state that the authorities may operate *ex parte* against a person or entity who has been identified and whose proposal for designation is being considered.<br>• Cyprus has not developed its own procedures to submit de-listing requests to the relevant UN Committee – reliance is made on the EU framework.<br>• There are no legal authorities and procedures or |

## Summary of Technical Compliance – Key Deficiencies

| Recommendation | Rating | Factor(s) underlying the rating |
|---|---|---|
| | | mechanisms to de-list and unfreeze the funds or other assets of persons and entities designated pursuant to UNSCR 1373 – reliance is made on the EU framework.<br>• There are no procedures to allow, upon request, a review of the designation decision pursuant to UNSCR 1373 before a court or other independent competent authority. |
| 7. Targeted financial sanctions related to proliferation | **LC** | • There are no domestic publicly available procedures to submit de-listing requests and unfreeze funds or other assets. |
| 8. Non-profit organisations | **PC** | • Cyprus has not identified the subset of NPOs which may be vulnerable to TF abuse.<br>• Cyprus has not identified the nature of threats posed by terrorist entities to the NPOs which are at risk as well as how terrorist actors abuse those NPOs.<br>• No reassessment has been carried out since the sector has not been subject to an initial assessment.<br>• The focus of the outreach was not on the potential vulnerabilities of NPOs to terrorist financing abuse and terrorist financing risks, and the measures that NPOs can take to protect themselves against such abuse.<br>• No best practices have been developed together with NPOs to address TF risk and vulnerabilities.<br>• No measures have been taken to encourage NPOs to conduct transactions via regulated financial channels.<br>• NPOs are supervised and monitored not on a risk-sensitive basis.<br>• There are no sanctions for breaches of the provisions of the LSI. There are no sanctions for charities and non-profit companies.<br>• It is doubtful that there is any investigative expertise and capability to examine those NPOs suspected of either being exploited by, or actively supporting, terrorist activity or terrorist organisations.<br>• There is no specific mechanism to ensure that, when there is a TF suspicion involving an NPO, information is shared promptly with competent authorities.<br>• There are no points of contact or procedures specific to requests related to NPOs suspected of TF or other forms of terrorist support. |
| 9. Financial institution secrecy laws | **C** | |

## Summary of Technical Compliance – Key Deficiencies

| Recommendation | Rating | Factor(s) underlying the rating |
|---|---|---|
| 10. Customer due diligence | **LC** | • There is no express requirement to take the beneficiary of a life insurance policy into account as a risk factor in determining whether enhanced CDD measures are appropriate.<br>• There are no legal provisions under which obliged entities are allowed not to pursue CDD process, provided that continuation of CDD process will tip-off the customer.<br>• Some requirements covered under criterions 10.8-10.9 do not apply to some types of payment institutions (those that do not act as MVTS providers); e-money institutions, credit acquiring companies, bureaux de change. |
| 11. Record keeping | **C** | |
| 12. Politically exposed persons | **LC** | • There is no specific requirement to consider making a STR where higher risks are identified in relation to life insurance policies with the involvement of a PEP as a beneficiary or the beneficial owner of the beneficiary. |
| 13. Correspondent banking | **PC** | • The AML/CFT Law does not specify that credit institutions or financial institutions must collect information about whether their foreign correspondents have been subject to ML/TF investigations or regulatory actions;<br>• Measures taken by Cyprus under c.13.1 and 13.2 do not apply to correspondent relationships with respondents situated in countries of the European Economic Area;<br>• Credit institutions and financial institutions can accept third party evaluations of whether potential respondent institutions could allow their accounts to be used by shell banks, rather than requiring that the institution make its own evaluation on this issue. |
| 14. Money or value transfer services | **C** | |
| 15. New technologies | **LC** | • There are no requirements for FIs, other than credit institutions, securities and insurance firms, to identify, assess, and manage the ML/TF risks that may arise in relation to new technologies.<br>• There is no explicit requirement for risk assessment and mitigation to take place before launch of a new technology, product or service. |
| 16. Wire transfers | **LC** | • There is no explicit obligation requiring payment service providers to file an STR in any country affected by the suspicious wire transfer, in cases where a payment service provider controls both the sending |

## Summary of Technical Compliance – Key Deficiencies

| Recommendation | Rating | Factor(s) underlying the rating |
|---|---|---|
| | | and receiving end of the transfer. |
| 17. Reliance on third parties | **C** | |
| 18. Internal controls and foreign branches and subsidiaries | **LC** | • There is no general, universal requirement for independent audit. |
| 19. Higher-risk countries | **LC** | • Apart from the requirement under Sec. 64(1)(a) of the AML/CFT Law, no binding guidance on high risk third countries has been issued for payment institutions that do not act as MTBs providers; e-money institutions, credit acquiring companies, bureaux de change.<br>• No information has been provided by the ICCS on actions taken to advice insurance firms about the weaknesses in the AML/CFT systems in other countries. |
| 20. Reporting of suspicious transaction | **C** | |
| 21. Tipping-off and confidentiality | **C** | |
| 22. DNFBPs: Customer due diligence | **LC** | • Shortcomings identified under Rec. 15 equally apply to DNFBPs. |
| 23. DNFBPs: Other measures | **LC** | • Shortcomings identified under Rec. 19 equally apply to DNFBPs. |
| 24. Transparency and beneficial ownership of legal persons | **LC** | • Cyprus has not conducted a formal assessment of the ML/TF risks and vulnerabilities of the entire sector of legal persons or identified the extent to which legal persons created in the country can be or are being misused for ML or TF.<br>• While the Companies Law regulates the voting rights of shares, it does not specifically require the register of members to include information on nature of the voting rights associated with shares.<br>• Monitoring of quality of assistance provided by other countries in response to requests for BO and basic information is not done on a formal and systematic basis. |
| 25. Transparency and beneficial ownership of legal arrangements | **LC** | • The Administrative Services Law, while requiring that information on service providers to the trust, such as investment advisors, accountants and tax consultants, be maintained, does not state that information has to be maintained for at least five years after the end of the business relationship or the trust ceases to exist. |
| 26.Regulation and supervision of financial | **LC** | • Not all relevant management is covered by the legislative frameworks for the securities and insurance |

## Summary of Technical Compliance – Key Deficiencies

| Recommendation | Rating | Factor(s) underlying the rating |
|---|---|---|
| institutions | | sectors and the framework to address associates of criminal is not necessarily complete.<br>• It is not clear that all elements of sub-criterion (a) of c.26.5 have been met.<br>• Limited information has been provided on the level of compliance with the IAIS Core Principles (c.26.4). |
| 27. Powers of supervisors | **C** | |
| 28. Regulation and supervision of DNFBPs | **LC** | • Market entry measures for the prevention of criminals being professionally accredited or holding a management function or being the beneficial owner of an obliged entity are not fully adequate for real estate agents and entities supervised by the CBA.<br>• The Real Estate Agents Registration Council does not apply a risk-based approach to supervision.<br>• The Estate Agents Registration Council as SRB is not supervised by the competent authority |
| 29. Financial intelligence units | **C** | |
| 30. Responsibilities of law enforcement and investigative authorities | **LC** | • It is still not clear on what basis a particular office of the police/CCD takes the lead on ML investigations;<br>• It is not abundantly clear on what basis the judgment is made to determine that a criminal offence is serious enough to warrant a parallel financial investigation |
| 31. Powers of law enforcement and investigative authorities | **PC** | • In relation to ML and FT, court orders do not allow for the actual interception of the content of communications;<br>• Controlled delivery cannot be utilised for cash/BNIs being moved. |
| 32. Cash couriers | **LC** | • There is no requirement to make a declaration (or alternatively a disclosure) for cross-border cash/BNIs movement through mail or cargo;<br>• Sanctions available for failure/false declarations are not proportionate. |
| 33. Statistics | **C** | |
| 34. Guidance and feedback | **LC** | • The CBC has not issued guidelines to credit acquiring companies, currency exchange offices, e-money institutions and payment institutions that do not operate as MSBs.<br>• The Casino Commission has not issued guidelines for casinos.<br>• Guidance on identifying TF suspicions is limited. |

## Summary of Technical Compliance – Key Deficiencies

| Recommendation | Rating | Factor(s) underlying the rating |
|---|---|---|
| 35. Sanctions | **C** | |
| 36. International instruments | **C** | |
| 37. Mutual legal assistance | **LC** | • Deficiencies identified under R. 31 have a negative impact on c.37.8. |
| 38. Mutual legal assistance: freezing and confiscation | **C** | |
| 39. Extradition | **C** | |
| 40. Other forms of international cooperation | **C** | |

## GLOSSARY OF ACRONYMS

| | |
|---|---|
| **AG** | Attorney General |
| **AMLGN** | Anti-Money Laundering Guidance Notes |
| **AMON** | Anti-Money Laundering Operational Network |
| **BCC** | Board of Charity Commissioners |
| **BO** | Beneficial Owner |
| **BNRA** | Business Names Registration Act |
| **B2B** | Business to business |
| **CA** | Crimes Act |
| **CompA** | Companies Act |
| **CFT** | Combating the financing of terrorism |
| **CHG** | Companies House Registry |
| **CP&EA** | Criminal Procedure and Evidence Act |
| **CTR** | Cash Transaction Reports |
| **DLT** | Distributed Ledger Technology |
| **DPA** | Data Protection Act |
| **DTOA** | Drug Trafficking Offence Act |
| **EC** | European Commission |
| **ECDD** | Enhanced Client Due Diligence |
| **EFCO** | European Freezing and Confiscation Orders |
| **EIOs** | European Investigation Orders |
| **ESW** | Egmont Secure Web |
| **ETS** | European Treaty Series [since 1.1.2004: CETS = Council of Europe Treaty Series] |
| **EU** | European Union |
| **EUSNRA** | EU Supra National Risk Assessment |
| **EAWA** | European Arrest Warrant Act |
| **FATCA** | Foreign Account Tax Compliance Act |
| **FOA** | Fugitive Offenders Act |
| **FI** | Financial Institution |
| **Fintech** | Financial Technology |
| **FT** | Financing of terrorism |
| **GACO** | Gibraltar Association of Compliance Officers |
| **GBP** | British pound sterling |
| **GCID** | Gibraltar Coordinating Centre for Criminal Intelligence and Drugs |
| **GD** | Gambling Division |
| **GDP** | Gross Domestic Product |
| **GFIU** | Financial Intelligence Unit |
| **GFSC** | Gibraltar Financial Services Commission's |
| **GGC** | Gibraltar Gambling Commissioner |
| **GPO** | General Prosecutor's Office |
| **HMC** | HM Customs |
| **HR** | Human Resources |
| **HVDs** | High Value Dealers |
| **ICOs** | Initial coin offerings |
| **IFC** | International Financial Centre |

| | |
|---|---|
| **ILOR** | International Letter of Request |
| **IMF** | International Monetary Fund |
| **INTERPOL** | International Police Organisation |
| **IOSCO** | International Organisation for Securities Commissions |
| **IT** | Information Technology |
| **KRIs** | Key Risk Indicators |
| **LEA** | Law Enforcement Agency |
| **LoR** | Letter of Request |
| **MER** | Mutual Evaluation Report |
| **ML** | Money Laundering |
| **MLA** | Mutual Legal Assistance |
| **NCA** | UK National Crime Agency |
| **NCO** | National Co-Ordinator for AML/CFT |
| **NRA** | National Risk Assessment |
| **OAC** | Office of Advisory Council |
| **OCGs** | Organised Crime Groups |
| **OCPL** | Office of Criminal Prosecutions & Litigation |
| **OFT** | Office of Fair Trading |
| **OFSI** | Office of Financial Sanctions Implementation (UK) |
| **OPC** | Office of Parliamentary Counsel |
| **POCA** | Proceeds of Crime Act 2015 |
| **PSPs** | Payment Service Providers |
| **RBA** | Risk-based approach |
| **REAs** | Real estate agents |
| **REs** | Reporting entities |
| **FRB** | Relevant financial business (include FIs) |
| **RGP** | Royal Gibraltar Police |
| **RSC** | Registrar of the Supreme Court |
| **RUBO** | Register of Ultimate Beneficial Ownership |
| **SB** | RGP Special Branch |
| **TA** | Terrorism Act |
| **TAFR** | Terrorist-Asset Freezing Regulations 2011 |
| **TOCA** | Transnational Organised Crime Act |

www.coe.int/MONEYVAL

December 2019

Anti-money laundering and counter-terrorist financing measures

# Cyprus

*Fifth Round Mutual Evaluation Report*

This report provides a summary of the AML/CFT measures in place in Cyprus as at the date of the on-site visit (13 to 24 May 2019). It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Cyprus''s AML/CFT system and provides recommendations on how the system could be strengthened.