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(2018)8

Anti-money laundering and counter-terrorist financing measures

Latvia

Fifth Round Mutual Evaluation Report

July 2018

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 Latvia was adopted by the MONEYVAL Committee at its 56th Plenary Session (Strasbourg, 3-6 July 2018).

CONTENTS

EXECUTIVE SUMMARY

This report provides a summary of the anti-money laundering (AML) and countering the financing of terrorism (CFT) measures in place in Latvia as at the date of the onsite visit (between 30 October and 10 November 2017). It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Latvia's AML/CFT system and provides recommendations on how the system could be strengthened.

Key Findings

- Latvia produced the report on its most recent full-scope national assessment of money laundering (ML) and terrorist financing (FT) risks in April 2017, presenting it as a key document that comprehensively articulates the understanding of ML/FT threats, vulnerabilities and residual risks in the country. A high-level commitment and support for making the national assessment of ML and FT risks a systemic and consistent exercise was demonstrated through two rounds of elaborating a national risk assessment (NRA) in 2010 and 2014, respectively. Large financial flows passing through Latvia as a regional financial centre pose a significant threat. Certain authorities, such as the Control Service (FIU) and the Financial Capital Market Commission (FCMC), demonstrated a rather broad understanding of the risks within the AML/CFT system. However, there is uneven and overall inadequate appreciation of the potentially ML-related cross-border flows of funds passing through Latvia.

- Competent authorities have access to and use a broad range of financial intelligence. Unusual transaction reports (UTRs) and suspicious transaction reports (STRs) are not fully in line with Latvia's risk profile and their quality appears modest. Relevant factors for this include: confusion between UTRs and STRs; possible confusion with the parallel reporting system on tax suspicions; "defensive" reporting; insufficient supporting documentation attached to STRs; inaccurate or incomplete information related to the ultimate beneficial owner (UBO); and limited feedback provided to reporting entities (REs) by the FIU. The FIU's work feeds in a large number of law enforcement authorities' (LEA) investigations and is critical to the remarkable results in non-conviction-based confiscation. However, some LEAs also noted the limited quality of the FIU's analysis. Cooperation between the FIU and other authorities appears to be improving, although it remains to be more clearly established at the operational and policy level.

- Until recently, the judicial system of Latvia did not appear to consider ML as a priority and to approach ML in line with its risk profile as a regional financial centre. This appears to have changed lately to a certain extent, with some large-scale ML investigations underway, involving bank employees having actively facilitated the laundering of proceeds. The country has achieved a certain number of ML convictions in the five years prior to the onsite visit. ML convictions for both domestic and foreign predicate offences have been achieved. Latvia also demonstrated one conviction for third-party laundering and one conviction for stand-alone ML, the latter being possible only because the accused made a full confession. Otherwise, prosecutors still rely on the existence of a predicate offence to meet the prerequisite of proving that the accused had knowledge of the illegal origin of the laundered property. Sanctions for natural persons appear neither dissuasive nor proportionate due to the frequent reduction of sentences in light of the length of proceedings or the application of the legal possibility to suspend a custodial sentence of up to five years' imprisonment. Latvia demonstrated the application of coercive measures provided by the Criminal Law (CL) against legal persons. The country also uses a number of alternative criminal

measures where a ML conviction is not possible for justifiable reasons.

- The absence of a robust FT risk assessment, including in the non-profit organisations (NPO) sector, presents a major deficiency in Latvia's effective efforts to prevent and combat FT. The country has not yet achieved any prosecutions or convictions specifically for FT, while conducting a number of terrorism-related investigations. However, Latvia is largely able to demonstrate the application of alternative measures to disrupt potential FT activities.

- Latvia's legal basis for targeted financial sanctions (TFS) calls for urgent clarifications and improvements. Most reporting entities (REs) follow a list-based approach, which - associated with limited effectiveness in implementing customer due diligence (CDD) - appears highly insufficient in light of the sanctions-evasion risk of the country. In the case of proliferator-states such as Democratic People's Republic of Korea (DPRK), such evasion is perpetrated through highly sophisticated means. Cases of proliferation financing (PF)-related TFS evasion through Latvian banks detected in 2017 illustrated those vulnerabilities. It is unclear whether the authorities, including the FIU and the FCMC, have taken sufficient steps (and have the necessary means, including legal) to mitigate sanctions-evasion risks. Moreover, it remains uncertain whether other supervisors can and do include TFS compliance in their monitoring programme.

- Overall, the appreciation of ML/FT risk in the financial sector is not commensurate with the factual exposure of financial institutions (FIs) in general, and banks in particular, to the risk of being misused for ML and FT. The general understanding of risks among designated non-financial businesses and professions (DNFBPs) is limited to risks relevant for their particular businesses and professions; it does not amount to an appropriate perception and awareness of ML/FT risks. The NRA conducted by Latvia does not appear to facilitate better understanding of ML/FT risks and relevant AML/CFT obligations in the private sector. There are certain concerns about the insufficient independence of the compliance (as well as audit) function particularly regarding the decision-making on termination of business relationships and reporting of STRs.

- The supervisors demonstrate widely varying views and knowledge about ML/FT risks. The authorities are aware of this issue, as noted in the strategic plan of the Financial Sector Development Board (FSDB). The FCMC displays the highest level of risk-understanding. Despite the knowledgeable and persistent approach taken by the FCMC to the non-resident banking sector, change of risk-appetite in this sector remains slow. In practice, issues such as understanding the nature or significance of ML/FT risks, or a lack of knowledgeable resources, prevented the supervisory authorities from fully implementing programs focused on higher-risk market segments.

- The NRA acknowledges that a significant number of Latvian legal persons and foreign legal entities are very likely involved in ML/FT schemes. Nevertheless, the NRA does not consider them to be vulnerabilities in the AML/CFT system of the country. The interviews with the private sector highlighted insufficient understanding of AML/CFT risks in the company service providers sector. This is a concern, given that company service providers are among the medium to high risk-ranked groups in the NRA. As a result of recent legislative amendments, the Enterprise Register (ER) will include UBO information obtained from all legal entities. However, this functionality was not up and running as of the time of the visit.

- International cooperation constitutes a critical component of the country's AML/CFT system. Latvia demonstrates many of the characteristics of an effective system in that area. Overall, the

Latvian authorities proactively cooperate with foreign counterparts, effectively providing and seeking not only mutual legal assistance (MLA), but also exchanging financial intelligence, and engaging in joint investigations and cooperation meetings with positive results. However, with the exception of the FCMC, the supervisory authorities do not seem to take an active part in international cooperation. The main challenge appears to be connected with difficulties to obtain assistance from countries of the Commonwealth of Independent States (CIS), which should be critical partners given Latvia's risk profile.

Risks and General Situation

1. Given its geographic location, its European Union (EU) membership (including being part of both the Schengen and the euro area) and the ability of its FIs to provide services in Russian, Latvia is a major gateway between Western Europe and CIS countries. In particular, the country is a regional financial centre, with a majority of its commercial banks focusing on servicing foreign customers, mainly from the CIS countries, including the provision of investment services and management.

2. The vulnerability of CIS countries to economic crime, especially corruption, remains one of Latvia's key ML risks. Latvia's own level of corruption, vulnerability to international organised crime and significant shadow economy are also key factors of the overall ML risk faced by Latvia. The NRA assesses the overall ML risk of the country as "medium high". It notes that the main sources of criminal proceeds are corruption and bribery, tax offences, fraud and smuggling as confirmed by most judicial and LEAs met onsite. According to the NRA a significant part of laundered proceeds are generated abroad, while domestic ML mainly pertains to self-laundering. ML methods employed in Latvia are complex and wide-ranging and involve a number of sectors. FT is considered to pose a low risk in the NRA; however, the risk of FT does not appear to be appropriately identified and assessed by Latvia.

Overall Level of Effectiveness and Technical Compliance

3. Since the last evaluation, Latvia has taken steps to improve its AML/CFT framework. Notably, since 2012 the Law on the Prevention of Money Laundering and Terrorism Financing (AML/CFT Law) has been amended several times to widen the definition of politically exposed persons (PEPs), FIs, and FT; the regulation was updated regarding the identification of UBOs; and a set of other normative FCMC regulations were executed to achieve significant compliance with the FATF recommendations. The Latvian authorities also made amendments to the legal framework of Latvia in order to implement the 4th EU Directive. However, some deficiencies remain in Latvia's technical compliance framework, for example with respect to preventive measures, the TFS regime and international cooperation.

4. Certain Latvian authorities have demonstrated rather broad understanding of the risks within the AML/CFT system. However, there is uneven and overall inadequate appreciation of the threats emanating from large financial flows passing Latvia as a transit point in its capacity of a regional financial centre.

5. A substantial level of effectiveness has been achieved in international cooperation. A low level of effectiveness has been achieved in the areas of transparency of legal persons and arrangements and implementation of PF financial sanctions. Latvia has achieved moderate results in the other areas covered by the FATF standards.

Assessment of Risks, coordination and policy setting (Chapter 2 - IO.1; R.1, R.2, R.33)

6. Latvia adopted its NRA in 2017 presenting it as a key document that comprehensively articulates the understanding of ML/FT threats, vulnerabilities and residual risks in the country. Certain key authorities, such as the FIU and the FCMC, demonstrated rather broad understanding of the risks within the AML/CFT system. However, in the vast majority of cases participation of competent authorities in the NRA process was limited to providing information, with limited or no involvement in the analysis of collected data and drafting of relevant conclusions.

7. The key document defining nation-wide efforts aimed at effective implementation of AML/CFT measures is the 2017-2019 Action Plan. However, the action plan seems to fall short of specific targeted measures to address the major ML threat emanating from, *inter alia*, the high concentration of the foreign customer base of the credit institutions and the related large cross-border movements of funds.

8. The FSDB chaired by the Prime Minister and comprising representatives of all key public and private sector stakeholders is the coordinating authority with the objective to improve the cooperation between state authorities and the private sector in the prevention of ML/FT. The Advisory Board of the CS (ABCS) chaired by the General Prosecutor (GP) is tasked with, *inter alia*, facilitating the work of the FIU and coordinating its cooperation with pre-trial investigation agencies, the Prosecutor's Office, the judiciary and the subjects of the AML/CFT Law. Most of the government agencies (except for the Ministry of Economy and the Ministry of Foreign Affairs) that are members of the FSDB also sit at the ABCS.

9. The private sector showed little if any interest in using the results of the risk assessment for revisiting their relevant policies, procedures and controls. This may be partly due to the lack of previously unidentified threats, vulnerabilities and residual risks articulated in the 2017 NRA Report, and partly to the disagreement with its analysis and conclusions.

Financial Intelligence, Money Laundering and Confiscation (Chapter 3 - IOs 6-8; R.3, R.4, R.29-32)

10. All competent authorities report having access to and making use of necessary sources of financial intelligence to support their analytical and investigative activities. However, UBO information is of limited reliability. The general quality of UTRs/STRs is modest, given the confusion between UTRs and STRs; the possible confusion with the parallel reporting system on tax suspicions; "defensive" reporting; insufficient documentation attached to STRs; inadequate UBO-related information; and limited FIU feedback to REs. The reports do not fully reflect the country's risk profile. Although an important part of the FIU's disseminations leads to ML/FT investigations, the quality of FIU analysis is deemed unsatisfactory by some LEAs. However, FIU/State Police (SP) coordination efforts since 2015 have resulted in FIU disseminations progressively becoming the main source of ML prosecutions. More generally, coordination and cooperation efforts between the FIU and LEAs have increased since 2015, especially at the operational level, but no clear mechanisms have been established.

11. Latvia has a sound legal system and institutional framework for the investigation and prosecution of ML. Until recently, the judicial system of the country did not appear to consider ML as a priority and to approach ML in line with Latvia's risk profile as a regional financial centre. This appears to have lately changed to a certain extent, with some large-scale ML investigations underway, involving bank employees having actively facilitated the laundering of proceeds. The

country has achieved a certain number of ML convictions in the five years prior to the onsite visit, which however appears modest when compared with the high number of convictions for predicate offences during the same period. ML convictions for both domestic and foreign predicate offences have been achieved. Latvia also demonstrated one conviction for third-party laundering and one conviction for stand-alone ML, the latter however being possible only because the accused made a full confession. Otherwise, prosecutors still rely on the existence of a predicate offence to meet the prerequisite of proving that the accused had knowledge of the illegal origin of the laundered property. The large majority of custodial sentences are deferred. Sanctions for natural persons appear neither dissuasive nor proportionate due to the frequent reduction of sentences in light of the length of proceedings or the application of the legal possibility to suspend a custodial sentence of up to five years' imprisonment. Latvia demonstrated the application of coercive measures provided by the CL against legal persons. The country also uses a number of alternative criminal measures where a ML conviction is not possible for justifiable reasons.

12. Latvia has a sound and broad legal system for confiscation of criminal proceeds, which is based on two pillars, conviction-based and non-conviction-based confiscation. While results from conviction-based confiscation are hampered by previous evidentiary requirements to demonstrate the criminal origin of the property, the absence of routinely-performed parallel financial investigations and the modest number of ML-convictions achieved through the judicial system, non-conviction-based confiscation brought some encouraging results, enabling Latvian authorities to confiscate considerable amounts in both domestic and international cases. In individual cases, Latvia is able to demonstrate effective repatriation of large amounts of confiscated proceeds of crime to third states, as well as in a domestic context the restitution of victims of economic crime.

13. Latvia has not been able to demonstrate an effective system of confiscation of undeclared or falsely declared cross-border movement of currency and bearer negotiable instruments (BNIs). Given that smuggling is identified as one of the main ML risks in Latvia, the lack of effectiveness in that area raises concern. The authorities are actively freezing and seizing illegal property, especially bank account assets, which resulted in some cases with considerable amounts of confiscated illegal property. In order to reach the characteristics of an effective system to a large extent, the evaluators would however have expected Latvia to demonstrate even stronger confiscation results in line with the ML risks the country faces.

Terrorist Financing and Financing Proliferation (Chapter 4 - IOs 9-11; R.5-8)

14. The absence of a robust FT risk assessment presents a major deficiency in Latvia's effective implementation of IO.9. Without a thorough understanding of how its broader financial vulnerabilities expose Latvia to exploitation by terrorist actors, the country cannot provide a systematically effective response to the FT threat. The Security Police (SeP) appears to be both empowered and enabled to identify potential terrorism and FT risks emanating from within Latvia.

15. Latvia does not have a national counterterrorism or CFT strategy, instead incorporating CFT elements in other strategic policies. Latvian authorities are capable of cooperating to investigate cases of FT, but do not have a single platform for obtaining information on FT-related matters across all relevant agencies. Interagency awareness and cooperation has not been shown to suffer as a result, but could be enhanced. Latvia has not yet achieved any prosecutions or convictions specifically for FT, while it has had only a handful of terrorism-related investigations. This absence appears consistent with Latvia's terrorist threat level, if not necessarily with the level of its terrorist financing risks, since no assessment accounting for its role as a financial hub has been conducted.

The country is largely able to demonstrate the application of alternative measures to disrupt potential FT activities.

16. No relevant outreach has been conducted towards the NPO sector. However, the sector appears to be proactively monitored by a number of competent authorities, which seems to mitigate the potential risks of FT abuse.

17. There are major issues in the legal basis for the TFS in Latvia (both for FT and PF), which may have an impact on the effectiveness of its TFS regime, as they necessarily limit the authority to regulate, monitor and sanction breaches of TFS obligations. A list-based approach to compliance followed by most REs, large numbers of foreign shell companies, deficiencies in the effectiveness of CDD measures (IO.4) and limited penalties imposed to date, among other factors, create a permissive environment for sanctions evasion, as demonstrated by the exploitation of Latvian banks for the purposes of circumventing PF-related sanctions exposed in 2017. The detection of sanctions evasion schemes resulted in enforcement actions in mid-2017, an autonomous Latvian PF TFS designation, additional guidance to the financial sector and the implementation of improved internal control programmes by banks.

Preventive Measures (Chapter 5 - IO4; R.9-23)

18. The financial sector's appreciation of the ML/FT risk is not commensurate with the factual exposure of FIs in general, and banks in particular, to the risk of being misused specifically for ML as well as for FT. The general understanding of risk among DNFBPs which is virtually unrelated to the ML/FT implications relevant for individual businesses and professions does not amount to an appropriate perception and awareness of ML/FT risks.

19. Banks and other non-bank FIs demonstrated fair knowledge of the applicable requirements in the AML/CFT Law and relevant regulations regarding the pillars of the preventative regime, i.e. CDD (including identification of UBOs and on-going monitoring of transactions/business relationships) and record-keeping. Nonetheless, there are grounded concerns about the quality of the additional information/documents collected and maintained by banks in the CDD process for verifying the UBOs, obtaining proof of the source of funds and source of wealth, as well as for monitoring transactions in terms of legitimacy and economic rationale, where primary emphasis is made on self-identification and there is overreliance on internet data. Poor implementation of the preventive measures by many DNFBPs is the presumed direct result of their insufficient knowledge in the area of AML/CFT.

20. There are certain concerns about the insufficient independence of the compliance (as well as audit) function, particularly regarding the decision-making on termination of business relationships and reporting of STRs. Concentrated ownership structure of the banks is among the reasons for that.

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

21. The supervisors demonstrate widely varying views and knowledge about ML/FT risks. The FCMC displays the highest level of risk understanding demonstrated through multiple examples. Other supervisors often referred to mitigation as risks, and non-compliance with preventative measures as a risk.

22. All FI and DNFBP supervisors appear to understand the theory of paying more supervisory attention to their higher risk market segments. However, in practice, issues such as understanding

the nature or significance of ML/FT risk, or a lack of knowledgeable resources, prevented them from fully implementing such programs.

23. Despite the knowledgeable and persistent approach taken by the FCMC to the non-resident banking sector, the rate of change of risk appetite in this sector is slow.

24. Effective, proportionate and dissuasive sanctions are relatively new in Latvia as the AML/CFT Law provisions on sanctions entered into force (in the banking sector) between July 2016 and the date of the onsite visit.

25. The impact of the actions of supervisors on the FI and DNFBP sectors ranges from negligible (with regard to some DNFBP sectors) to fairly good (with regard to the FCMC).

Transparency of Legal Persons and Arrangements (Chapter 7 – IO.5; R. 24-25)

26. The NRA acknowledges that a significant number of Latvian legal persons and foreign legal entities are very likely involved in ML/FT schemes.

27. The interviews with the DNFBP sector have highlighted the involvement of company service providers to incorporate companies in Latvia. However, there is insufficient understanding of AML/CFT risks and measures in the company service providers sector.

28. BO information gathered by REs must conform to the AML/CFT Law but self-identification through a statement signed by the customer was used as a primary method for determining the BO of a transaction or a business relationship.

29. Under the amended provisions of the AML/CFT Law that were enacted during the onsite visit all legal persons in Latvia are obliged to collect and submit information about BO to the ER. However, this functionality was not up and running as of the time of the onsite visit.

30. The FIU, LEAs and control authorities in the field of tax administration, public procurement or public-private partnership have direct electronic access to a wide range of information and databases and indirect access to other databases. After enactment of the latest legislative amendments BO information contained in the ER will be publicly accessible.

International Cooperation (Chapter 8 – IO.2; R. 36-40)

31. International cooperation constitutes a critical component of Latvia's AML/CFT system. The country demonstrates many of the characteristics of an effective system in the area of international cooperation. Overall, the Latvian authorities proactively cooperate with foreign counterparts, effectively providing and seeking not only MLA, but also exchanging financial intelligence, and engaging in joint investigations and cooperation meetings with positive results. However, with the exception of the FCMC, the supervisory authorities do not seem to take an active part in international cooperation. The main challenge appears to be connected to difficulties to obtain assistance from CIS countries, which should be critical partners given Latvia's risk profile.

Priority Actions

- With regard to the proper understanding of its ML/FT risks, Latvia should take measures to:

1) ensure substantial participation of competent authorities in all stages of the NRA process; 2) improve the analysis and proper understanding of ML/FT threats and vulnerabilities.

- Latvia should take measures to ensure that obliged entities draw from the relevant outcomes of national ML/FT risk assessments to support or supplement their own risk assessments.

- Latvia should take measures to ensure that among the subjects of the AML/CFT Law: 1) the understanding of FT risk extends beyond the screening against "terrorist lists"; 2) the understanding of ML/FT risks is practicably facilitated by contributions to and feedback on national risk assessments.

- Latvia should take measures to enhance enforcement of the minimum requirements to the quality of additional information and documents collected and maintained by the subjects of the AML/CFT Law in the CDD process (e.g. verifying the UBOs).

- With regard to the internal controls and procedures, Latvia should take measures to: 1) consider introduction of additional (legislative) measures to ensure independence of the compliance (as well as audit) function; 2) ensure effective and substantial implementation of internal controls and procedures by all subjects of the AML/CFT Law, as ascertained through targeted supervisory action.

- Latvia should increase outreach to and eventually regulation of REs to develop and institute internal control systems capable of detecting potential PF activity, taking into account developments in efforts at detecting PF sanctions evasion and Latvia's PF vulnerabilities.

- Latvia should revise the legal framework for TFS and assign adequate resources to PF and FT TFS compliance supervision.

- The FCMC should substantially increase the frequency of AML/CFT supervisory visits to the foreign deposits banking sector.

- Latvia should ensure that the authorities have access to the relevant BO information as defined in the AML/CFT Law at the time of incorporation and throughout the lifetime of all legal persons. Priority should be given to the Limited Liability Company (LLC) sector as this is the most prevalent and also at the highest risk of ML/FT according to the NRA. Latvia should establish a mechanism to compel FIs/DNFBPs to take reasonable measures to determine the BO of their customers who are legal persons and actively verify such information.

- Latvia should take measures to revise the concepts of unusual transaction and suspicious transition to eliminate the overlap in the relevant definitions.

- Latvia should pursue ML as a priority and seek to systematically prosecute a wider range of ML offences, including third party and stand-alone/autonomous ML, for criminal activity which is in line with its profile as a regional financial center.

- Latvia should develop law enforcement guidance, backed up by corresponding training for all judicial stakeholders involved in the prosecution of proceeds-generating offences, on the minimum levels of evidence which the courts may require to establish underlying predicate criminality in a ML prosecution under the recently-changed legislation.

Effectiveness & Technical Compliance Ratings

Effectiveness Ratings

IO.1 – Risk, policy and coordination	**IO.2** – International cooperation	**IO.3** – Supervision	**IO.4** – Preventive measures	**IO.5** – Legal persons and arrangements	**IO.6** – Financial intelligence
Moderate	**Substantial**	**Moderate**	**Moderate**	**Low**	**Moderate**
IO.7 – ML investigation & prosecution	**IO.8** – Confiscation	**IO.9** – TF investigation & prosecution	**IO.10** – TF preventive measures & financial sanctions	**IO.11** – PF financial sanctions	
Moderate	**Moderate**	**Moderate**	**Moderate**	**Low**	

Technical Compliance Ratings (C – compliant, LC – largely compliant, PC – partially compliant, NC – non-compliant, N/A – not applicable)

R.1 - assessing risk & applying risk-based approach	**R.2 - national cooperation and coordination**	**R.3 - money laundering offence**	**R.4 - confiscation & provisional measures**	**R.5 - terrorist financing offence**	**R.6 - targeted financial sanctions – terrorism & terrorist financing**
C	**LC**	**LC**	**C**	**LC**	**PC**
R.7- targeted financial sanctions - proliferation	**R.8 -non-profit organisations**	**R.9 – financial institution secrecy laws**	**R.10 – Customer due diligence**	**R.11 – Record keeping**	**R.12 – Politically exposed persons**
PC	**PC**	**C**	**PC**	**LC**	**LC**
R.13 – Correspondent banking	**R.14 – Money or value transfer services**	**R.15 –New technologies**	**R.16 –Wire transfers**	**R.17 – Reliance on third parties**	**R.18 – Internal controls and foreign branches and subsidiaries**
LC	**LC**	**LC**	**LC**	**LC**	**LC**
R.19 – Higher-risk countries	**R.20 – Reporting of suspicious transactions**	**R.21 – Tipping-off and confidentiality**	**R.22 - DNFBPs: Customer due diligence**	**R.23 – DNFBPs: Other measures**	**R.24 – Transparency & BO of legal persons**
LC	**LC**	**C**	**PC**	**LC**	**LC**
R.25 - Transparency & BO of legal arrangements	**R.26 – Regulation and supervision of financial institutions**	**R.27 – Powers of supervision**	**R.28 – Regulation and supervision of DNFBPs**	**R.29 – Financial intelligence units**	**R.30 – Responsibilities of law enforcement and investigative authorities**
LC	**PC**	**C**	**PC**	**LC**	**LC**
R.31 – Powers of law enforcement and investigative authorities	**R.32 – Cash couriers**	**R.33 - Statistics**	**R.34 – Guidance and feedback**	**R.35 - Sanctions**	**R.36 – International instruments**
LC	**PC**	**LC**	**C**	**LC**	**LC**
R.37 – Mutual legal assistance	**R.38 – Mutual legal assistance: freezing and confiscation**	**R.39 – Extradition**	**R.40 – Other forms of international cooperation**		
LC	**LC**	**PC**	**PC**		

MUTUAL EVALUATION REPORT

Preface

This report summarises the AML/CFT measures in place as at the date of the onsite 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.

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 evaluation team during its onsite visit to the country from 30 October to 10 November 2017.

The evaluation was conducted by an assessment team consisting of:

- Mr Blaz Mozina - Senior Judicial Adviser Supreme Court, Slovenia (legal expert)
- Mr Borja Aguado Delgado - Prosecutor, General Prosecutor's Office, Andorra (law enforcement expert)
- Mr Michael Lieberman - U.S. Department of the Treasury, Office of Terrorist Financing and Financial Crimes, Assistant Director, USA (legal expert)
- Mr Nicolas Choules-Burbidge - formerly Senior Director, AML and Compliance Division, Office of the Superintendent of Financial Institutions, Canada (financial expert)
- Mr Arakel Meliksetyan - Deputy Director, Financial Monitoring Center, Central Bank, Armenia (financial expert)

MONEYVAL Secretariat

- Mr Matthias Kloth – Executive Secretary
- Ms Astghik Karamanukyan – Administrator
- Ms Solène Philippe – Administrator

The report was reviewed by Mr Boudewijn Verhelst (FIU Belgium), Mr Richard Walker (Policy Council of the States of Guernsey), Mr Andrew Le Brun (Jersey Financial Services Commission) and the FATF Secretariat.

Latvia previously underwent a MONEYVAL Mutual Evaluation in 2012, conducted according to the 2004 FATF Methodology. The 2012 evaluation and 2016 follow-up report have been published and are available at https://www.coe.int/en/web/moneyval/jurisdictions/latvia.

That Mutual Evaluation concluded that the country was compliant with 15 Recommendations; largely compliant with 19; and partially compliant with 14. 1 Recommendation (R.34) was considered to be not applicable. Latvia was rated compliant or largely compliant with 12 of the 16 Core and Key Recommendations. Latvia was placed under the regular follow-up process immediately after the adoption of its 4th Round Mutual Evaluation Report and was removed from the regular follow-up process in September 2016.

CHAPTER 1. ML/TF RISKS AND CONTEXT

1. Located in northern Europe, the Republic of Latvia is one of the three Baltic States, covering over 64,589 square kilometres. Latvia shares borders with Estonia to the north, Lithuania to the south, the Russian Federation to the east, and Belarus to the southeast, and it shares a maritime border to the west with Sweden. Riga is the capital of Latvia. The population of Latvia is 1.95 million (2016 Central Statistics Bureau of Latvia estimate as of November 2015). Latvia's GDP is about EUR 25.0 billion and its official currency is the Euro (EUR).

2. Latvia is a parliamentary republic. According to the constitution of Latvia, the National Assembly (*Saeima*) is the supreme representative body and holder of constitutional and legislative power in the country. The *Saeima* is composed of one hundred representatives, elected for a four-year term. The government is comprised of the Prime Minister (as the head of government) and a Cabinet of Ministers (CoM), who together are responsible for the executive affairs of the state. The head of state is the President, who holds a largely ceremonial position but also has a control function in the legislative process. Latvia's legal system is based on civil law principles.

3. Latvia joined the European Union (EU) in 2004 and the euro zone in 2014. The country is a member of numerous international organisations, such as the Council of Europe, the United Nations (UN), the North Atlantic Treaty Organisation (NATO), the Organisation for Security and Co-operation in Europe (OSCE), the Organisation for Economic Cooperation and Development (OECD), the World Trade Organisation (WTO), the International Monetary Fund (IMF), the World Bank (WB), the European Bank for Reconstruction and Development (EBRD) and Interpol.

ML/TF Risks and Scoping of Higher-Risk Issues

Overview of ML/TF Risks

ML Threats

4. The national risk assessment (NRA) identifies illicit economic activities – particularly corruption and bribery (including embezzlement of public funds)[1], fraud (including through fictitious companies[2]), and tax evasion – as Latvia's primary money laundering (ML) threats[3]. These crimes exceed other proceeds-generating offences such as drug trafficking[4].

5. The NRA identifies illegal economic activities as another major ML threat[5]. White collar crime has exceeded other more conventional proceeds-generating offences, such as drug trafficking, in terms of threat[6]. Indeed, the top three predicate offences in the period under review were tax evasion, fraud (including fictitious companies[7]), as well as corruption and bribery (including embezzlement of public funds)[8].

6. Organised crime is also a factor with a substantial impact on the overall ML risk situation in Latvia. According to the NRA, ML threats that arise from international organised criminal groups (OCGs) are rated as high. The proximity and strong financial ties of Latvia with members of the

[1] NRA, p. 22.
[2] NRA, p. 23.
[3] NRA, p. 41.
[4] NRA, p. 22.
[5] NRA, p. 41.
[6] NRA, p. 22.
[7] NRA, p. 23.
[8] NRA, p. 22.

Commonwealth of Independent States (CIS) facilitates the access of regional OCGs to the financial system of Latvia and the international one subsequently. OCGs from CIS are known to exercise influence on the domestic ones. In fact, Latvia hosts approximately 80 OCGs (in line with the definition of Sec.21 of CL)[9], out of which only 10-12 groups are active in the area of severe and organised crime with an international dimension[10]. OCG activities in Latvia are connected with publicly known criminal offences (CO) types: i.e. smuggling of narcotic/psychotropic substances; weapons/ammunition and products subject to excise duty; human trafficking, blackmail and collection of debts that is often covered behind legal commercial activity; as well as fraud and cybercrimes characteristic to Latvia[11].

7. The growing presence of organised crime in Latvia has also been reinforced by the high corruption levels within the state services, as well as by the shadow economy. In particular, both factors have helped feed the upsurge of a new type of OCG related to the insolvency abuse, in which the central role was taken by administrators of insolvency proceedings, but private and public sector representatives were involved in committing the CO[12].

8. The financial services and products offered by Latvian financial institutions (FIs) to foreign customers are considered as a high risk in the NRA. This is in conjunction with the very-high risk of the customer base profile (mainly CIS countries) of foreign customer serving banks; the high or medium high risk of funds turnover associated with named products; the high or medium-frequency of international transactions involving these products; and the availability of non-face-to-face use of these products. It is very likely that such products and services could be used for fiduciary trusts, loans against collateral, current accounts and wire transfers etc. and cause a number of negatives consequences to the financial system of the country[13].

FT Threats

9. Turning to the risk of financing of terrorism (FT), Latvia has had no specific cases of terrorist financing or terrorism. The NRA rates the risk of terrorism as low, primarily on the basis of Latvia's small (albeit growing) "at risk"-community, its limited interest for terrorist groups, and the fact that no groups or individuals engaged in terrorism have been found operating in Latvia[14]. However, Latvia recognises the presence of broader threats found elsewhere in Europe, such as internet-based terrorist propaganda and radicalised individuals. The greatest risk factor the country identifies is the participation of such individuals in the Syrian/Iraqi conflicts. Latvia also recognises the threat of "foreign sources" of financing more broadly.

10. The non-profit sector is considered by the NRA to pose a low FT risk. Latvian non-profit organisations (NPOs) that could be at risk from terrorist abuse are very small in number, given the country's general risk profile. However, at least one Latvian NPO was led by an individual who later became a foreign terrorist fighter (FTF) in Syria. Still the Latvian authorities do not consider that this case connotes a broader risk from the sector. The authorities require NPOs, including those potentially more at risk, to submit annual reports with financial and operational details. The State

[9] NRA, p. 25.
[10] European Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime.
[11] NRA, p. 24.
[12] NRA, p. 24.
[13] NRA, pp. 64-65.
[14] NRA, pp. 104-105.

Revenue Service (SRS) is responsible for the review of those reports, while two desk-based reviews on NPOs have already been conducted by the financial intelligence unit (FIU).

Country's risk assessment

11. Latvia accomplished its first NRA in 2012, under strictly confidential status. The second NRA was published in 2017. The NRA report considers both ML and FT. The FIU co-ordinated the development of the NRA using the National Money Laundering and Terrorist Financing Risk Assessment Tool provided by the WB.

12. Sources of information for the NRA include information and statistical data gathered from the FIU, supervisory bodies, law enforcement authorities (LEAs), the Ministry of Finance (MoF), the Ministry of Justice (MoJ), other public institutions and private entities[15]. Information has also been obtained from surveys, interviews and information requests.

13. The NRA methodology uses a risk assessment tool, which is developed in MS Excel and which helps the country to identify the key risks and vulnerabilities of ML/FT. This tool consists of nine interconnected modules within which a number of input variables are evaluated, which allows the assessors to judge the threats and vulnerability of ML/FT. The nine risk assessment tool modules are: 1) ML threats; 2) ML national vulnerability; 3) Vulnerability of the banking sector; 4) Vulnerability of the securities sector; 5) Vulnerability of the insurance sector; 6) Vulnerability of other FIs sector; 7) Vulnerability of designated non-financial businesses and professions (DNFBPs); 8) FT risk assessment; and 9) Risk assessment of financial inclusion products.

14. The completion of each module includes the collection of statistics and data, analysis, risk identification, conclusion drawing, and allocation of appropriate ratings based on the assessment. The risk assessment tool rates ML threats and vulnerabilities on a basis of a 5-grade scale (low, medium low, medium, medium high and high). The overall ML risk is determined as a combination of the relevant ratings for threats and vulnerabilities. The final ratings[16] for national and sectorial vulnerabilities are achieved through the scores assigned to various constituent factors of vulnerability within the range of 0.00-1.00[17] based on either "open door approach" or "weighted approach".

Scoping of Higher Risk Issues

15. The assessment team identified areas which required an increased focus through an analysis of information provided by the Latvian authorities, including the NRA, and by consulting various open sources. These were as follows:

16. **Foreign corruption and bribery**[18]**:** The level of understanding by all relevant stakeholders of the risks posed by corruption, as well as the effectiveness of the implementation and supervision

[15] In the assessment process these institutions were involved – MF, FIU, MoJ, MoI, MoT, GPOSP, SeP, SRS, FCMC, BoL, LGSI, SBC, RE, CA, CRPC, OCMA, LACA, LCSA, LCSN, LACB, LIA, CPCB, ARO, as well AML/CTF Law obliged entities.

[16] Ratings are a product of the initial vulnerability score adjusted for its weight in terms of AML/CFT significance.

[17] A score between 0.00 and 0.20 corresponds to low, 0.20-0.40 – low medium, 0.40-0.60 – medium, 0.60-0.80 – medium high and 0.80-1.00 – high level of vulnerability.

[18] Latvia is No. 44 on the list of countries of Transparency International's 2016 Corruption Perception Index. The Council of Europe's Group of States against Corruption (GRECO) found in March 2016 in its fourth round on "Corruption prevention in respect of members of parliament, judges and prosecutors" that Latvia's compliance with GRECO's recommendations was "globally unsatisfactory", but established in June 2017 that the country had made some measurable progress to no longer justify this low level of compliance (GRECO, Second Interim Compliance Report of Latvia, June 2017, paras. 3 and 79; available at: http://www.coe.int/en/web/greco/evaluations/round-4).

of the relevant AML/CFT preventive measures and of corruption-related ML investigation/prosecution processes, especially as carried out by Corruption Prevention and Combating Bureau (KNAB), received considerable attention.

17. **Economic crimes:** As noted previously, economic crimes have surpassed more conventional proceeds-generating crimes such as drug trafficking in Latvia. The assessment team therefore explored whether law enforcement objectives and activities have evolved to address these emerging threats.

18. **Correspondent banking:** Given the fact that the Latvian banks (focus on servicing foreign customers), which were involved in recent high-profile international ML schemes, provide correspondent services to CIS banks, the issues of risks associated with correspondent banking, preventive measures' effectiveness and supervision received particular attention by the assessors.

19. **Mutual legal assistance (MLA) and international cooperation:** Both ML and FT have a significant cross-border element in Latvia. The assessment team paid particular attention to the difficulties highlighted in the NRA[19] in cooperating with a number of relevant countries (especially from the CIS), as well as the effectiveness of the international cooperation of supervisory authorities with foreign counterparts.

20. **Shadow economy**[20]**:** The shadow economy accounts for a very significant part of the gross domestic product (GDP)[21] in Latvia. Thus the level of cash in circulation is high[22]. Taking into account the widespread use of cash and the fact that tax evasion is one of the most significant ML threats in Latvia, discussions were held with the tax authorities on the measures to mitigate these risks.

21. On the **supervisory side,** the assessment team considered the risks and vulnerabilities stemming from the current level of resources, sanctioning powers and prioritisation of inspections[23]. Considerable attention was also paid to the DNFBPs sector entry requirements and level of awareness of AML/CFT obligations.

22. **Transparency of legal entities and beneficial ownership:** Shell companies[24], often incorporated abroad, are extensively relied on to hide the ultimate beneficiaries of ML schemes, as illustrated in the already-mentioned recent high-profile ML cases. The NRA highlights the risks related to services provided to foreign trusts. The NRA also points to the use of inexperienced persons, or persons in need or without a declared place of residence, as frontmen for ML purposes. The assessment team thus discussed with the authorities whether the current arrangements in Latvia are sufficient to prevent legal persons and arrangements from misuse for ML or FT.

---

[19] NRA, p. 21.

[20] According to the NRA the main components of the shadow economy include, *inter alia*, underreporting of business income, employees or envelope wages.

[21] According to the NRA, the shadow economy comprised 20-25% of the official GDP (or EUR 5-6 billion per year). See F. Schneider: "Size and Development of the Shadow Economy of 31 European and 5 other OECD Countries from 2003 to 2015: Different Developments" (Study by the Department of Economics, Johannes Kepler University, Linz (Austria), available online).

[22] NRA, p. 29.

[23] OECD, Working Group on Bribery, *Phase 2 Report on Implementing the OECD Anti-Bribery Convention*, p. 31.

[24] Shell arrangements are defined in Paragraph 15[1] of Sec.1 AML/CFT Law as having characteristic features that impede transparency of beneficial ownership and, subsequently, enable their use for various financial manoeuvres.

23. **ML prosecution and convictions:** The assessment team sought to determine whether the focus of criminal investigations is still preponderantly on the predicate criminality and whether recent prosecution efforts are actually bearing fruits. Issues such as the lack of autonomous ML convictions, the lack of convictions of bank employees involved in the reported ML schemes, and the possible lack of application of existing sanctions to legal persons under criminal law in these cases, received considerable attention.

Materiality

24. Latvia is a regional financial centre. The banks are considered to be the driving force in the whole financial sector, holding 90 % of financial system assets[25]. The share of the banking system in total financial system assets is roughly 90%[26]. The total assets of the banking sector amounted to EUR 21.36 billion in 2016 and its profitability reached EUR 454 million[27], while the amount of incoming and outgoing client payments through banks through the NOSTRO correspondent network (including accounts held with the Bank of Latvia) totalled EUR 312.2 billion (and EUR 235.3 billion for the first nine months of 2017). The banking sector in Latvia is split in two segments: domestic-centred banks, where Nordic banking groups holding 54% of shareholder capital have a dominant role[28], and banks focusing mainly on servicing non-residents while having no close links with the domestic economy. The latter banks are mainly domestically-owned (only 10% of banking sector capital originates from the CIS)[29]. Overall, non-resident share in banks' capital has been reduced in size to 43% in 2017. The banking services provided include deposits (both resident and non-resident), loans, money transfers, foreign exchange, guarantees, shell company accounts and payment services.

25. The size of the shadow economy in Latvia, which is exacerbated by the widespread use of cash, constitutes a significant ML vulnerability. According to official sources, the size of the shadow economy in the country is around 20-25% of the GDP and the proportion of cash in the supply of money is high, as the shadow economy is mainly based around cash turnover.

26. As indicated in the NRA, certain persons (e.g. inexperienced persons, persons in need or without a declared place of residence) may be used and act as frontmen of an unlimited number of companies (fictitious companies), as the effective legal regulations do not impose any limitations in this regard. The NRA also indicates that legal entities registered in Latvia or abroad (mostly Limited Liability Companies (LLCs)), associations, foundations and funds with a good reputation and operational background, as well as off-shore companies holding current accounts at Latvian banks, pose similar risks if misused for illegal activities.

Structural Elements

27. The key structural elements necessary for an effective AML/CFT regime are generally present in Latvia. There is a high-level commitment to address AML/CFT issues. AML/CFT policy-making and coordination is conducted through the Financial Sector Development Board (FSDB). The Board

[25] OECD, *Latvia: Review Of The Financial System*, April 2016, p. 6, available at: https://www.oecd.org/finance/Latvia-financial-markets-2016.pdf
[26] OECD, *Latvia: Review Of The Financial System*, April 2016, p. 6, available at: https://www.oecd.org/finance/Latvia-financial-markets-2016.pdf
[27] See, https://www.ebf.eu/latvia/
[28] The structure of bank capital by country is Latvia with 18%, Sweden 43%, Norway 11%, US 5% and UK 4%. See, https://www.ebf.eu/latvia/
[29] OECD, *Latvia: Review Of The Financial System*, April 2016, p. 6, available at: https://www.oecd.org/finance/Latvia-financial-markets-2016.pdf

is composed of senior officials representing all relevant authorities involved in the prevention of ML/FT[30].

Background and other Contextual Factors

28. Corruption is widespread and permeates all levels of the public administration to varying degrees[31]. This seriously undermines public confidence in the civil service and the criminal justice system and encourages criminals to act with impunity[32]. In 2016, the Transparency International Corruption Perception Index ranked Latvia 44th out of 176 countries. The KNAB coordinated the fight against corruption in Latvia through its 2014-2016 operation strategy and the 2014-2016 action plan on combating and preventing organised crime[33].

29. The level of financial inclusion is considered high, with 90% of the adult population maintaining an account at a formal FI[34]. The Financial and Capital Market Commission (FCMC) has drawn up a national financial literacy strategy (2014-2020) which aims to gradually enhance the financial literacy level of Latvian population[35]. In spite of these facts, the use of cash is still identified as a risk factor for ML[36], which the evaluation team took into close consideration.

AML/CFT strategy

30. The 2017-2019 Strategy of Measures for Prevention of Money Laundering and Terrorism Financing Risks was approved by the Cabinet of Ministers (CoM) following the approval of the NRA. The Strategy specifies that it will guide the activities of the FIU. It is planned to update the strategy every three years. In addition to the Strategy, AML/CFT is set as a priority and integrated into the work plan of state institutions to restrain the shadow economy for 2016-2020[37]; the MoF strategy to reduce shadow economy for 2015-2020[38]; the State Police (SP) plan of activity priorities for 2016[39]; the CoM guidance on combating and preventing corruption for 2015-2020[40]; the KNAB activity strategy for 2014-2016[41]; the CoM plan on combating and preventing organised crime for 2014-2016[42]; and the Operational Strategy of the FIU for 2017-2019.

31. The 2017-2019 national strategy aims to restrict general ML/FT risks by taking measures oriented towards reducing the ML/FT threats and the vulnerability of the financial and non-financial sector, and to ensure conformity with the international commitments and standards in the field of AML/CFT, promoting the public safety, competitiveness of the economic environment and

[30] The FSDB is composed of: (1) Prime Minister (Chairman of the Board); (2) Minister of Economics; (3) Minister of Foreign Affairs; (4) Minister of Internal Affairs; (5) Minister of Finance; (6) Minister of Justice; (7) General Prosecutor; (8) President of the Central Bank; (9) Chairman of the FCMC; (10) Head of the FIU; (11) President of the Latvian Association of Commercial Banks; (12) President of the Latvian Association of Insurers; (13) Executive Director of the Latvian Association of Securities Market Professionals; (14) President of the Union 'Association of Latvian Private Banks'.
[31] The NRA sets corruption as the ML threat with the highest importance in Latvia (p. 25).
[32] It is to be noted, however, that various country-wide measures have been instituted in recent years to fight corruption.
[33] Cabinet order No 276 of June 5, 2014 "On Organized Crime Prevention and Combating plan for 2014-2016".
[34] See, http://databank.worldbank.org/data/reports.aspx?source=1228
[35] See, http://www.fktk.lv/texts_files/FIN_STRATEGIJA-ENG.pdf
[36] There is widespread use of cash in gambling, currency exchange operations below the identification threshold of EUR 8000, use of proxies/frontmen in real estate transactions and non-regulated activities of certain professions such as legal advice, tax consultancy and similar services for onshore and offshore company formation, and real estate brokerage.
[37] Action plan of state authorities for limiting the shadow economy for 2016-2020 (adopted on June 10, 2016)
[38] MoF presentation "Strategy for limiting shadow economy for 2015-2020"
[39] Annex to the SP order No 4981 of December 29, 2015 "Work Plan for SP for 2016"
[40] Cabinet order No. 393 of 16 July 2015, "Guidance for Corruption Prevention and Combating for 2015-2020"
[41] Operation strategy of CPCB for 2014-2016
[42] Cabinet order No 276 of 5 June 2014, "On Organized Crime Prevention and Combating plan for 2014-2016"

confidence in the jurisdiction of Latvia. In order to achieve these objectives it defines seven courses of action, by means of: 1) enhancing the coordination in the development and introduction of the AML/CFT strategy and policy; 2) improving the statutory regulation of AML/CFT; 3) improving the effectiveness of investigation, indictment and adjudication; ensuring effective application of preventive measures and penalties; 4) improving the effectiveness of FIU activities; 5) building the capacity of subjects in the AML/CFT field; 6) building the capacity of the supervisory and control authorities in the AML/CFT field; and 7) improving data aggregation and analysis for ML/FT risk assessment and other AML/CFT purposes. Each course of action defines a set of specific measures to be implemented, their expected outcomes, the indicators against which implementation is measured, the agencies (co)responsible and the deadline established for implementation of such measures.

Legal & institutional framework

32. The AML/CFT legal and organisational framework in Latvia is principally governed by the Law on the Prevention of Money Laundering and Terrorism Financing (AML/CFT Law), along with acts of the CoM, FSDB and FIU as well as other government agencies' acts. The AML/CFT Law is supplemented by certain provisions in the Latvian Criminal Law (CL), the Latvian Criminal Procedure Law (CPL), the Latvian Administrative Violations Code (AVC), the Civil Law, the Law of the Bank of Latvia, the Gambling and Lotteries Law, the Commercial Law, the Law on Sanctions and other (international) regulatory enactments.

33. Since the last evaluation, Latvia has taken steps to improve the AML/CFT framework. Notably, since 2012 the AML/CFT Law has been amended several times to widen the definition of politically exposed persons (PEPs), FIs, and FT; the regulation was updated regarding the identification of ultimate beneficial owners (UBOs)[43]; and a set of normative FCMC regulations[44] were executed to achieve significant compliance with the FATF recommendations. The Latvian authorities made also amendments to the legal framework of Latvia in order to implement the 4th EU Directive.

34. In addition, an array of delegated laws and regulations[45] has been issued by the CoM, the FCMC and the Bank of Latvia (BoL) to regulate in details certain requirements of the AML/CFT Law.

35. The main agencies involved in Latvia's institutional structure to implement its AML/CFT regime are the following:

36. **The FSDB** is a high-level AML/CFT policy-making and coordination body, which coordinates the activities between the various State authorities and the private sector in the prevention of ML/FT (AML/CFT Law, Sec.61). The FSDB is headed by the Prime Minister and comprises

[43] 13.08.2014 amendments in AML/CTF Law

[44] For instance, the responsibility of banks to develop a numerical assessment system of customers' risk, training requirements for staff; the authorisation to issue binding regulatory enactments that are relevant to obliged entities has also been delegated to several AML/CTF Law supervisory bodies (FCMC, BoL); etc.

[45] Cabinet 08.03.2016 regulations No. 138 On countries and international organisations that have prepared lists of those persons that are suspected of participating in terroristic activities or creating, holding, moving, using or distributing weapons of mass destruction; Cabinet 22.12.2008 regulations No. 1092 Order in which state and municipality institutions provide information to Office for Prevention of Laundering of Proceeds Derived from Criminal Activity;
FCMC 23.12.2015 regulations No. 234 on enhanced customer due diligence, 27.08.2008 FCMC regulations No. 125; BoL 30.10.2017 regulations No. 158 Money laundering and terrorism financing prevention requirements when buying and selling foreign currencies; etc.

representatives of all government agencies involved in AML/CFT and representatives of self-regulatory organisations (SRO) [46]. The FSDB's main tasks include:

i) assessing the risk of ML/FT possibilities;
ii) developing an action plan, stipulating country's priorities in promoting the development of the financial sector and preventing ML/FT; and
iii) considering proposals on the development of laws and regulations necessary to promote the development of the financial sector and to reduce the possibility of carrying out ML/FT in Latvia, as well as to decide on the further progress of the referred to proposals.

37. **The Office for the Prevention of Laundering of Proceeds Derived from Criminal Activity (Control Service/FIU)** is an administrative-type of FIU. It operates under the supervision of the Prosecutor's Office and, pursuant to the procedure provided for by law, it receives, processes, and analyses reports on unusual and suspicious financial transactions. It also provides this information to control, pre-trial investigation and judicial authorities, including the Prosecutor's Office.

38. **The Office of the Prosecutor of Latvia (GPO)** is an institution of judicial power, which independently carries out supervision of the observance of law within the scope of the competence determined by the Law on the Prosecution Office. It is tasked to react to a violation of law and to ensure the deciding of matters relating to such in accordance with the procedures prescribed by law. The GPO supervises the work of investigative institutions and the investigatory operations of other institutions; organises, manages, and conducts pre-trial investigations; initiates and conducts criminal prosecutions; maintains charges of the State; supervises the execution of sentences; protects the rights and lawful interests of persons and the State in accordance with the procedures prescribed by law; submits a complaint or a submission to a court in cases provided for by law; and takes part in the adjudication of matters by a court in the cases provided for by law[47].

39. In addition, the GPO is one of the three central authorities granting MLA requests[48], is in charge of extradition matters[49]; and is amongst the competent authorities authorising the establishment of a joint investigation team[50].

40. **The Security Police (SeP)** is an internal counterintelligence and security service, which gathers information from different sources, carries out analysis, and informs senior officials about the threats identified to national security. It also takes measures to neutralise these threats.

41. The SeP's responsibility is the conduction of counter-intelligence activities, protection of state secrets, protection of the constitutional order, economic security, coordination and conduction of counterterrorism measures as well as protection of dignitaries (more detailed under Competencies). The SeP is also the only security and intelligence service with the right to carry out pre-trial investigations (to initiate criminal proceedings, initiate criminal prosecution as well as arrest persons).

42. The work of the SeP is supervised by the Minister of Interior, while the operational activities and the legitimacy of the pre-trial investigation process are supervised by the General Prosecutor

[46] For its full composition, see above.
[47] Office of the Prosecutor Law, Ch.1(Sec.2)
[48] Sec.846 of the CPL
[49] Sec.704 of the CPL
[50] Sec.889 of the CPL

(GP). The Parliamentary control over the SeP is performed by the National Security Committee of the *Saeima*.

43. **The SP** is a state institution to protect the State and society from criminal and other illegal threats to life, health, rights and freedoms, property and interests. The SP is also responsible for the execution of incoming and outgoing MLA requests.

44. The central authority of the SP organises and co-ordinates activities of the structural units of the SP. The SP of Latvia consists of the SP Central Criminal Police Authority; the SP Central Civil Police Authority; the SP Central Administrative Authority; and five regional authorities.

45. **The SRS** is a direct administrative authority under the supervision of the Minister of Finance, which ensures the accounting of tax payments and taxpayers; the collection of taxes, duties and other mandatory payments; and the implementation of the customs policy and customs control. In accordance with its activities, it has set the following priorities: the fight against organised crime in the matters of state revenue; the shift of maximum resources to investigate serious and especially serious crimes in the matters of state revenue; and the possibility to recover assets to the state budget by solving financial matters in criminal proceedings.

46. The SRS is responsible for the AML/CFT supervision (Sec.45 AML/CFT Law) of the following entities: tax consultants and outsourced accountants; independent providers of legal services; providers of services of establishment of a legal entity and ensuring its operation; persons who act as agents or intermediaries in transactions with immovable property; other legal or natural persons trading in vehicles, precious metals or precious stones, articles thereof and other types of goods, as well as acting as intermediaries in such transactions or providing other type of services; and other FIs (not supervised by financial supervisors).

47. **The KNAB** is the leading specialised anti-corruption authority of Latvia. Its aim is to fight corruption in a coordinated and comprehensive way through prevention, investigation and education. The KNAB has jurisdiction over the following violations related to corruption: exceeding a public official's authority; using an official position in bad faith; public official's failure to act, i.e. a public official fails to perform his or her assigned duties, intentionally or through negligence and thus causes harm to a state authority, its rights and interests; accepting and giving bribes, including misappropriation of a bribe and intermediation in a bribery; violating restrictions imposed on a public official repeatedly or if substantial harm is caused to the state interests; unlawful participation in property transactions by a public official; trading in influence, i.e. giving/accepting material value, property or other kind of benefits to/by a public official to personally influence the activities or decisions of a public official; and illicit financing of political parties on a large scale.

48. The KNAB is under the supervision of the Prime Minister and the CoM, which is limited to the control of the lawfulness of decisions. The KNAB is also a pre-trial investigatory body with traditional police powers.

49. **Latvijas Banka (hereinafter the Bank of Latvia (BoL))** is the central bank of Latvia, whose main responsibility is to ensure price stability. To achieve this, the BoL participates in the formulation of the Euro monetary policy, related decision-making and implementation. The main tasks carried out by the BoL include: managing foreign reserves; issuing cash in Latvia and participating in ensuring the cash circulation process in the euro area; promoting smooth operation of the payment systems; compiling financial and monetary statistics, as well as balance of payments statistics; and maintaining and developing the Credit Register.

50. In addition, the BoL issues licenses for purchasing and selling cash of foreign currencies and carries out AML/CFT supervision of currency exchange offices at the national level[51], in accordance with the requirements of the AML/CFT law.

51. **The FCMC** is a lawful autonomous public institution, which is responsible for AML/CFT and sanctions supervision and control of Latvian banks; credit institutions; electronic money institutions (EMI); insurance companies carrying out life insurance; private pension funds; insurance intermediaries providing life insurance services; investment brokerage companies; alternative investment fund managers; investment management companies; credit unions; and providers of reinsurance services and payment institutions (PI). The FCMC is responsible for ensuring stability, competitiveness and development of the financial and capital markets, as well as protection of the interests of investors, depositors and insured persons. Under the Single Supervisory Mechanism (SSM) the European Central Bank (ECB), is responsible for the direct prudential supervision of significant banks and groups in the participating Member States, and monitors national authorities' prudential supervision of less significant banks. The criteria for determining significance are laid down in Union law and the ECB issues yearly a list confirming the categorization of all banks in the Banking Union. The ECB also grants and withdraws banking licenses and assess acquisitions of qualifying holdings for both significant and less significant banks. For significant institutions, the ECB may take supervisory measures and may apply directly or in cooperation with national authorities sanctions in the cases specified under relevant Union law. For less significant institutions only national authorities may take supervisory measures and impose sanctions. The ECB may issue guidance to national authorities on how they should perform supervision of less significant banks and can decide to directly supervise any one of these banks if necessary to ensure that high supervisory standards are applied consistently.

52. **The Ministry of Transport (MoT)** is the leading institution of the state administration of transport and communication branches. The MoT elaborates legal acts and policy planning documents regulating the branches. According to its internal regulations, the MoT assesses compliance of operations by *Latvijas Pasts* (Latvian post) in accordance with the requirements set forth in the AML/CFT law and respective legislation. However, it is not authorised to impose sanctions and the FCMC is authorised to impose sanctions for breaches of the AML/CFT law.

53. **The Ministry of Interior (MoI)** is the leading institution in the home affairs sector, which includes subsectors such as: the fight against crime, protection of public order and security, protection of individual rights and lawful interests, state border security, fire safety, fire security, rescue, civil protection, record keeping and documentation of population, as well as migration.

54. **The MoF** develops financial policy, coordinates and organises its implementation, as well as performs other functions stated in external regulatory enactments. In the AML/CFT area it is one of the main policy-making actors, responsible for ML/FT risk prevention policy according its areas of competency[52]. During the preparation period of the NRA, the MoF was responsible for the development of ML/FT risk prevention and developing an action plan for the mitigation of ML/FT risks. In addition, the MoF has adopted a strategy to reduce the shadow economy for the period 2015-2020[53].

[51] Law on Bank of Latvia, Sec.11(2); AML/CTF Law, Sec.45(1)(6).
[52] Cabinet decision No 49 of 16.09.2014 "On preparation of the national ML/FT risk assessment"
[53] MoF presentation "Strategy for limiting shadow economy for 2015-2020"

55. **The MoJ** is the national executive body responsible for developing, organising and coordinating the implementation of state policy in the area of criminal law, criminal procedure law, public registers, development of policies of rights and administration policy of regional and district courts etc. Within the AML/CFT framework, the MoJ is one of the main policy-making actors and responsible for international cooperation.

56. **The Ministry of Foreign Affairs (MFA)** is the national executive body in charge of formulating and implementing the government's policy in the area of foreign affairs. Within the AML/CFT framework, the MFA is responsible for submitting proposals to committees of the UN Security Council/EU to include/remove natural or legal persons to its sanctions lists. In addition, the MFA coordinates the conclusion and implementation of international treaties, coordinates membership of the country (and of its representative bodies) in international organisations, and regularly updates competent national authorities on the UN Security Council Resolutions/EU regulations on sanctions in connection with FT and proliferation financing (PF).

57. **The Lotteries and Gambling Supervision Inspection (LGSI)** is responsible for licencing and regulating all lotteries and gambling operators in Latvia, under the aegis of the MoF. The LGSI also carries out the supervision of lottery and gambling providers in the area of AML/CFT. Most recently, the LGSI has issued recommendations in September 2017 setting out the principles for creating an internal control system and defining certain indicators of unusual and suspicious transactions.

58. **The Latvian Association of Certified Auditors (LACA)** is an independent professional corporation aiming at promoting the improvement of professional qualifications, refining creative skills and acquiring new experience as well as fostering the reputation and legal protection of the profession. According to the Law on Certified Auditors, the Association should act in order to: ensure monitoring over compliance with professional standards and norms of ethics as well as other applicable professional norms and regulations and professional activities of its members; represent and protect the interests of its members, organise qualification examinations of professional auditors and decide on issuing certificates to certified auditors as well as issuing licences to firms of certified auditors; keep the register of certified auditors and firms of certified auditors; review disputes between certified auditors and clients based on the request of an involved party; organise professional training and qualification improvement courses for certified auditors; develop and submit to legislative institutions recommendations in the field of bookkeeping standards and audit; and provide quality control over activities of certified auditors.

59. **The Enterprise Register (ER)** is an administrative institution that registers enterprises (companies), merchants[54], their subsidiaries and representative offices within the territory of the Republic of Latvia, as well as all amendments to the basic documents of their activity and takes other actions envisaged by legislative acts. It also registers mass media, public organisations, commercial pledges, decisive influences, marriage contracts, public and private partnership agreements, religious organisations, political parties, trade unions, arbitrages and processes of insolvency. Beyond registration, the ER is responsible to provide information regarding the registered entities and legal facts; to provide the operation and development of the information system of the ER; and to perform other functions laid down in laws and regulations.

[54] A merchant is a natural person (an individual merchant) or a legal person (a partnership or a company), who engages in comercial activities.

60. The ER is a legal person that acts under the supervision of the MoJ and its activity is regulated by Register of Enterprises Law.

Financial sector

61. Due to its EU membership, Latvia is part of a single internal market that fully integrates 28 countries and, based on bilateral agreements, at least an additional 18 countries, where there is a free flow of capital and where financial and other services can be provided freely either through establishment, or as a cross-border service.

62. As of 10 November 2017, the Latvian financial system was comprised of 23 banks (seven of them are foreign banks' branches), four investment brokerage and 12 investment management companies, 2 life insurance companies and 55 intermediaries, 29 payment institutions, 15 EMI, 39 exchange offices, 6 private pension funds, 34 credit unions, 13 alternative investments funds managers, and 1 postal services provider. Banks are required to be authorised by the ECB.

63. The number of licensed institutions remained largely stable since the 4th round report. A decrease has been observed regarding the number of domestic-centered banks (by 1/3), which reflects the concentration in the sector. A decrease has also been observed with regard to currency exchange offices. Such a decrease appears to be the result of the accession of Latvia to the Eurozone in 2014.

64. AML/CFT and sanctions supervision of FIs is within the responsibility of the FCMC. Except in relation to targeted financial sanctions (TFS), an area in which the FCMC considers the current legal framework does not provide it with sufficient regulatory authority (see below) the FCMC is assigned with adequate powers which are widely used. It has categorised the banks for the purposes of AML/CFT risks and applies resources accordingly. Such powers are used to carry out off-site and onsite inspections ("comprehensive", "thematic" or "target", which differ in content and duration).

Table 1: Financial Institutions

Financial Institutions	2010	2011	2012	2013	2014	2015	2016	10.11.2017
Licensed Banks	21	22	20	19	17	17	16	16
Licenced Foreign Bank Branches	10	9	9	9	9	9	7	7
Currency Exchange Offices	68	68	68	66	58	50	42	39
Securities Investment Companies	25	21	20	16	17	16	16	16
Life Insurance Companies and Life Insurance Brokers	65	59	56	57	62	65	57	57
State Joint Stock Company "Latvijas Pasts"	1	1	1	1	1	1	1	1
Payment Institutions	15	34	34	36	34	37	29	29
Financial Leasing Companies	N/A	N/A	16	14	13	15	15	15
Lending (inc. factoring; forfeiting; etc.) Companies[55]	N/A	N/A	36	39	44	42	44	44
Electronic Money Institutions	0	8	14	14	14	15	15	15
Private Pension Funds	7	7	7	7	6	6	6	6
Credit Unions	34	33	34	35	32	34	34	34
Alternative Investment Fund Managers	N/A	N/A	N/A	N/A	9	12	13	13

[55] Other licenced non-bank lenders (without Financial leasing companies)

DNFBPs

65. The sector is dominated by lawyers, real estate agents, accountants and other independent legal professionals. Lawyers are regulated by the Advocacy Law; real estate agents operate in accordance with the Real Estate Association Code of Ethics; and accountants are regulated by the Code of Ethics of Professional Accountants. Other independent legal professionals are not regulated. The SRS is the supervisory authority of all these professionals that are subject to compliance with the AML/CFT law.

66. Casinos and gambling operators are licenced and regulated by the LGSI. Casinos are subject to compliance with the Gambling and Lotteries Law which contains provisions relevant to their compliance with AML/CFT requirements. This Law defines two modes of gambling – on-spot (at the premises of the operator) and interactive (through electronic communication). Inspections are carried out both onsite and remotely (for instance, by observing a casino's collection process, which happens daily)[56].

Table 2: Gambling Entities

Casinos	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**
Land based Casinos	6	6	6	6	5	5	6
Internet casinos (webpages)	1	1	1	4	6	6	7
Gaming halls	327	321	328	324	321	322	317
Bingo halls	2	3	3	2	2	2	2
Betting points	18	14	21	19	26	42	57
Total	**354**	**345**	**359**	**354**	**360**	**377**	**389**

67. The remaining DNFBPs have been assigned to the SRS for AML/CFT supervision. Trust and company service providers (TCSPs) are also supervised by the SRS[57] and subject to compliance with the AML/CFT law, although there is no sector-specific legislation setting out additional specific provisions relevant for AML/CFT compliance.

68. The following statistics were provided by the Latvian authorities in relation to the DNFBP sector:

Table 3: Number of DNFBPs

DNFBP	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**
Real estate agents	N/A	N/A	1038	1999	2492	2170	2415
Dealers in Precious Stones and Precious Metals (DPMS)	N/A	N/A	47	314	448	388	339
Sworn Notaries	120	117	114	112	112	108	107
Lawyers	N/A	N/A	N/A	1340	1349	1363	1376
Other Independent Legal Professionals	N/A	N/A	N/A	N/A	N/A	N/A	5568
Auditors, Audit Companies	N/A	298	296	310	311	293	286
Accountants (tax advisors)	N/A	N/A	6453	9722	10975	11182	10811
TCSPs	N/A	N/A	781	1358	1537	1583	1415
Others (sellers of vehicles, goods and provision of services)	N/A	N/A	763	1456	1881	1958	1720
Total	**7139**	**7674**	**7884**	**8052**	**7769**	**7674**	**7460**

Preventive measures

69. The cornerstone of the Latvian AML/CFT regime is the AML/CFT Law. The law was amended several times since the 2012 Moneyval mutual evaluation in order to implement the 4th round

[56] NRA, p. 133.
[57] Latvian law does not recognise trusts as a distinct type of legal arrangement.

recommendations; relevant international conventions and standards; and lessons drawn from experience on AML/CFT issues gathered in previous years[58].

70. The amended law expands the definition of PEPs in order to cover domestic PEPs (according to the 4th EU AML Directive), management bodies of international organisations (4th EU AML Directive) and grandparents (2012 FATF Recommendations). The law also amended the legislation on FIs, notably in relation to banks, payment institutions and EMIs so that they develop compliance policies for individuals (compliance officers) and board members responsible for compliance with the AML/CFT law. In addition, the FCMC is empowered to adopt regulatory requirements on different AML/CFT areas (i.e. correspondent banking, identification of source of wealth and source of funds, for non-face-to-face identification etc.).

71. The AML/CFT Law is supported by a number of laws governing specific categories of designated entities. A number of regulations adopted by the CoM, as well as by-laws issued by the respective AML/CFT regulators, provide more detailed obligations for the implementation of the aforementioned laws. The provision of guidance by supervisors is part of the missions the AML/CFT Law has assigned to them.

72. The AML/CFT Law has addressed many gaps with regard to preventive measures highlighted in the 2012 mutual evaluation. A number of deficiencies remain, as noted in the TC Annex.

Legal persons and arrangements

73. Numerous types of legal person can be formed in Latvia (see the table below). Most legal persons have been formed as LLCs by individuals for commercial purposes. At the time of the onsite element of the evaluation, a total of around 189,000 were in existence. All legal persons are obliged to register with the ER (residing at the MoJ) upon formation. Legal personality is granted upon registration or re-registration with the ER. The ER consists of 13 registers, of which the most essential ones are the Commercial Register (for partnerships (general partnerships and limited partnerships); and companies (LLCs and stock companies)), the ER Journal (for co-operative societies) and the Register of Associations and Foundations (for associations, foundations, and trade unions).

74. The ER performs a number of inspections and verification controls in order to ensure the accuracy, currency and validity of information. Legal persons are obliged to inform the ER on any change of their information. With regard to legal persons registered abroad, the ER shall request their representatives in Latvia to submit proof of registration/foundation and proof of the rights of representation. Administrative liability for non-compliance/violation by legal persons to submit accurate and up-to-date information is foreseen by the law[59].

Table 4: Legal Persons

Type of Legal Persons	Number of legal persons registered:			
	2014	2015	2016	As of 12.03.2017
General partnerships	96	60	53	600
Limited partnerships	19	3	8	127
LLCs	13991	12555	10318	163 847
Stock Companies	57	55	43	1 015

[58] The last amendments took place in November 2017.
[59] Sec.166.3 of the AVC.

Type of Legal Persons	Number of legal persons registered:			
	2014	2015	2016	As of 12.03.2017
European companies	0	1	0	5
Co-operative societies	12	8	7	1 873
Associations (including trade unions)	1196	1302	1259	19 857
Foundations	86	95	81	1 416

75. Legal persons are either "Private Law" or "Public Law" entities. "Private Law legal persons" must be organised on the basis of constituent documents and can be established and operate under the model statute in the manner specified by law. "Public Law legal persons" can be established on the basis of a regulatory Act by the President of Latvia, the state power authority, or the local self-government body. Foreign companies or other legal persons established under the laws of another jurisdiction can conduct economic activities in Latvia through branches or permanent establishments. Branches must be registered with the ER.

76. As of November 2017, according to information from the ER 70% of all registered subjects are legal entities registered in the Commercial Register.

77. The most common form of legal persons in Latvia is the company. There are three main categories of companies under Latvia's law:

- The most popular type of company is the LLC. It is a commercial company, the equity capital of which consists of the total sum of the nominal value of equity capital shares and the shares of which are not publicly tradable objects (Commercial Law, Sec.134(1)(3)).
- A stock company is a commercial company, the equity capital of which consists of the total sum of the nominal value of equity capital stock and the shares (stock) of which may be publicly tradable objects (Commercial Law, Sec.134(1)and(4)).
- A European company may be formed by merging stock companies of Member States; by stock companies or LLCs of a Member State promoting the formation of a holding company; by transforming a stock company of a Member State; or as a subsidiary stock company within the meaning of Art.2, Par. 3 of Regulation No. 2157/2001.

78. Under commercial law, upon registration with the ER, legal personality[60] is also conferred to two categories of partnerships:

- Under a general partnership, members carry out entrepreneurial activities on behalf of the partnership and incur joint subsidiary liability in respect of the partnership's obligation by all property they own.
- A limited partnership is a partnership, the purpose of which is the performance of commercial activities utilising a joint firm name, and in which two or more persons (members) have agreed on the basis of a partnership agreement, if the liability of at least one of the members of the partnership (limited partner) in relation to the creditors of the partnership is limited to the amount of their contribution, but the liability of the other personal liability members of the partnership (general partners) is not limited.

79. Latvia stands at 19 in the ranking on the "Ease of Doing Business"-index and 21 on the "Ease of Starting a Business"-index in the *WB Report 2018*. The country is thus in the third place among

[60] They do not have the status of a legal person but they have rights similar to a legal person.

the Baltic states under both indexes. The report highlights the overall friendly legal and political environment of Latvia in terms of business doing.

80. The AML/CFT Law requires the reporting entities (REs) to determine, as part of the CDD measures set out in Sec.17(1) of the Law, the BO of natural and legal persons if it is known or suspected that the transaction is carried out in the interests or on behalf of another person, *inter alia*, the commercial law, requires legal persons to declare BO information to the ER. The ER contains information on the BOs of legal persons, but it is believed that there are cases when information is submitted to the ER only on the economic owners of legal persons (shareholders, stockholders, persons who have the right to vote) and not on other economic beneficiaries, since the legislation does not require explicitly that, where no natural person with ultimate effective ownership or control is identified, the REs should obtain information on the identity of the relevant natural person who holds the position of senior managing official of the legal person.

81. Administrative and criminal liability for not submitting information or providing false information on BOs of legal persons was introduced thereafter.

82. The AML/CFT Law (Sec.3(1)(5)) defines providers of services related to creation and provision of operation of a legal arrangement as REs without specifying the situations in which they obtain the said status. Latvian law does not recognize trusts as a distinct type of legal arrangement and is not a party to the Hague Convention on the Law Applicable to Trusts and on their Recognition. The SRS is the responsible authority for the supervision of Company Service Providers (including trustees).

Supervisory arrangements

83. The AML/CFT supervision framework appears to have been significantly enhanced since the last mutual evaluation, with a range of state authorities supervising all designated entities as follows:

Table 5: Financial institutions

Financial institutions	Licensing or registration	AML/CFT Supervisor
Banks[61]	Licensing by FCMC	FCMC
Currency Exchange Offices	Licensing by BoL	BoL
Latvian Post (for postal money transfers)	N/A	MoT
Securities investment companies	Licensing by FCMC	FCMC
Depository institutions	Licensing by FCMC	FCMC
Payment and electronic money institutions	Licensing/registration by FCMC	FCMC
Alternative investment funds managers	Registration/Licensing by FCMC	FCMC
Insurance companies and brokers	Licensing by FCMC	FCMC
Credit unions	Licensing by FCMC	FCMC
Financial Leasing Service Providers		SRS
Private pension funds	Licensing by FCMC	FCMC

[61] Banks are required to be authorised by the ECB.

84. Under the new AML/CFT Law, all DNFBPs are covered by specific AML/CFT supervision, under the below arrangements:

Table 6: DNFBPs

DNFBPs	Licensing, registration, appointment, regulation	AML/CFT Supervisor
Real estate agents	SRS	SRS
DPMS	SRS	SRS
Lawyers	Council of Sworn Lawyers	Council of Sworn Lawyers
Other independent legal professionals	SRS	SRS
Lawyers and other independent legal professionals	Council of Sworn Lawyers	Council of Sworn Lawyers
Notaries	Council of Sworn Notaries	Council of Sworn Notaries
Accountants	SRS	SRS
Auditors, audit firms	Latvian Council of Certified Auditors	Latvian Council of Certified Auditors
TCSPs	-	SRS
Casinos	LGSI	LGSI

International Cooperation

85. The Latvian CPL sets out a comprehensive legal framework for MLA, which enables the authorities to provide a broad range of assistance concerning ML/FT and associated predicate offences. Latvia is actively engaged in a variety of international initiatives in the areas of AML/CFT. In particular, all competent authorities of Latvia take part in the work of respective multilateral fora (both at the policy and operational level) such as MONEYVAL, the Egmont Group, Interpol, Europol or Eurojust. Latvia has signed and ratified the relevant international treaties regulating cooperation and taken steps to implement UNSCRs in areas relevant to AML/CFT. Bilateral cooperation, including MLA, is also based on a wide range of bilateral treaties and other arrangements.

Financing of Proliferation

86. Latvia's broader vulnerabilities have left it exposed to abuse by North Korean proliferators and their agents to evade international sanctions. Like other illicit actors, sanctions evaders seek to obscure their conduct behind opaque webs of foreign shell companies, and take advantage of regulatory and supervisory gaps and deficiencies. Latvia has taken steps following the detection of sanctions evasion schemes in 2017, taking enforcement action, and providing guidance to the regulated community. Still, serious deficiencies in the TFS legal framework, the dissuasiveness and proportionality of the penalties to date and the lack of resources of the authorities, including legal, are obstacles to mitigating those risks.

CHAPTER 2. NATIONAL AML/CFT POLICIES AND COORDINATION

Key Findings and Recommended Actions

Key Findings

- Latvia produced the report on its most recent full-scope national assessment of ML/FT risks in April 2017 demonstrating high-level commitment and support for making the national assessment of ML/FT risks a systemic exercise following a consistent process. National risk

assessments would benefit from substantial participation of competent authorities in all stages of the NRA process.

- Certain key authorities, such as the FIU and the FCMC, demonstrated rather broad understanding of the risks within the AML/CFT system. The FIU, as well as most of the supervisors and the LEAs agreed with the conclusions of the 2017 NRA Report.

- The understanding of threats and vulnerabilities within and beyond the NRA needs to be improved by achieving reliable estimates on the significance and volume of the proceeds of crime potentially laundered in and through Latvia, specifically considering the impact of large financial flows passing Latvia as a transit point in its capacity of a regional financial center. Also, the conclusion about the risk of FT in Latvia needs to account for certain factual circumstances in the country.

- While acknowledging the higher risk of ML identified with the banks involved in the non-resident clientele business, the authorities generally demonstrate tolerance towards shell company servicing products, which are the main conduit for that business[62].

- There are several documents defining nation-wide efforts aimed at effective implementation of AML/CFT measures; among them, the key document, i.e. the 2017-2019 Action Plan needs to be improved by articulating specific targeted measures to address the major ML threats emanating from, *inter alia*, the high concentration of the foreign customer base of the credit institutions and the related large cross-border movements of funds.

- Provisions of the AML/CFT Law and relevant regulations requiring application of enhanced measures for higher risk scenarios do not seem to be defined through giving due consideration to such scenarios as identified by any national and other risk assessments.

- Action plans produced by some key supervisors, such as the FCMC, to ensure consistency with the identified ML/FT risks would benefit from the establishment of measurable milestones and clear deadlines for their implementation, along with articulation of sensibly lessening tolerance of the supervisor to the formalistic compliance of the obliged entities with their AML/CFT obligations.

- The private sector provided input into the NRA process, and most of those met by the evaluation team were aware of the NRA results. There were opinions that the conclusions of the NRA could be more specific to be transformed into practicable actions taken by the obliged entities. Communication of the NRA results to the private sector needs improvement.

Recommended Actions

a) With regard to the proper understanding of its ML/FT risks, Latvia should take measures to:

- Ensure substantial participation of competent authorities in all stages of the NRA process;

- Improve the analysis and understanding of certain major ML threats[63] and vulnerabilities[64] in the country; as well as of FT threats and vulnerabilities inherent to regional financial centres in general and to Latvia's economy and society in particular[65].

[62] As indicated by the authorities, legislative amendments have been initiated to prohibit the FIs to establish or continue a business relationship or to perform casual business transactions with shell arrangements. These amendments to the AML/CFT Law came into force on 9 May 2018. However, these amendments have been initiated after the onsite visit to Latvia and have not been subjected to analysis.

b) With regard to the private sector's awareness of national ML/FT risks, Latvia should take measures to:

- Define an appropriate strategy for communicating the outcomes of risk assessments to the private sector;
- Ensure that conduction of national and any subsequent risk assessments is followed by issuance of specific guidance on identified risks and recommended mitigation measures;
- Motivate the private sector to use the results of the risk assessments for revisiting their relevant policies, procedures and controls.

c) With regard to national policies to address identified ML/FT risks, Latvia should take measures to:

- Among various national policies relevant for AML/CFT, substantively assess the effectiveness of implementation of the ones with expired term of fulfilment; and harmonize and synchronize the ones in the implementation phase;
- Ensure that the existing mechanisms and activities of the authorities enable timely identification of any undetected or newly emerging risks.

d) With regard to enhanced and simplified measures, Latvia should take measures to ensure that:

- Provisions requiring application of enhanced measures for higher risk scenarios are defined through giving due consideration to such scenarios as identified by national ML/FT risk assessments;
- Obliged entities draw from the relevant outcomes of national ML/FT risk assessments to support or supplement their own risk assessments.

e) With regard to the objectives and activities of competent authorities, Latvia should take measures to ensure that:

- Activities of the competent authorities are fine-tuned to provide for focused action consistent with identified ML/FT risks;
- Key nation-wide documents defining activities of the authorities in the field of AML/CFT provide targeted measures to address the major identified ML threats; and are sufficiently specific in defining measures aimed at improving effectiveness;
- Action plans of supervisors provide for consistency with the identified ML/FT risks; define forward looking and appropriately prioritized actions; establish clear deadlines and measurable milestones for implementation; and are implemented with sensibly lessening tolerance to the formalistic compliance by obliged entities.

---

[63] Including those emanating from undetected or latent criminality in the country; use of new technologies and delivery channels; illegal cross-border movements of funds, goods/ services/ cash, and humans; and illegal cash turnover in the country.

[64] Including those caused by insufficient quality of the constituent processes of detecting, deterring and prosecuting ML; Latvian legal persons and foreign legal entities; and contextual factors such as shadow economy and corruption.

[65] Particularly to the legislative and institutional frameworks, professional sectors of FIs and DNFBPs, relevant services and products, legal entities and NPOs, as well as applicable contextual factors.

f) With regard to national coordination and cooperation, Latvia should take measures to:

- Consider extending the mandate of the FSDB to cover consideration of global trends in ML/FT and their local implications; and to provide tailored guidance on implementation of and follow-up on the national AML/CFT/CPF policies and activities;
- Enable defined procedures and consistent practices for individual authorities to conduct strategic analyses with their outcomes feeding into the national policy development process; and to ensure horizontal exchange of information on risks/ trends and specific cases;
- Enable harmonisation of efforts of the FIU, supervisors and LEAs at policy-making and operational level.

87. 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 R1-2.

Immediate Outcome 1 (Risk, Policy and Coordination)

Country's understanding of its ML/FT risks

88. Latvia produced the report on its most recent full-scope national assessment of ML/FT risks in April 2017 presenting it as a key document that comprehensively articulates the understanding of ML/FT threats, vulnerabilities and residual risks in the country. In this regard, the fact that the authorities initiated two rounds of NRA in 2010 and 2014 demonstrates high-level commitment and support for making the national assessment of ML/FT risks a systemic exercise following a consistent process. Moreover, the development of action plans, which are aimed at mitigating the risks identified through the NRA, is indicative of the practicability of NRA outcomes.

89. Certain key authorities, such as the FIU and the FCMC, demonstrated rather broad understanding of the risks within the AML/CFT system. The FIU, as well as most of the supervisors and the LEAs agreed with the conclusions of the *2017 NRA Report* about the ML risk to be medium high and the FT risk to be low in Latvia, although such agreement was not always supported by sufficient analysis and argumentation either within or beyond the scope of the NRA. The FIU has had a pivotal role in the whole NRA process. In terms of the main ML/FT risks, it is well aware of the findings of the NRA, albeit the moderate number of disseminations on, for example, corruption-related crimes does not appear to be fully consistent with this good understanding. Among the LEAs, the Financial Police Department of the SRS (SRS FPD) and the SP have a reasonable understanding of the ML risk that the country is exposed to in their particular fields.

90. There are several regulators in Latvia assigned responsibility for supervising FI and DNFBP compliance with the AML/CFT requirements. Their views and knowledge about ML/FT risks significantly varies from advanced to moderate or even elementary levels.

91. Among them, the FCMC demonstrated a more advanced understanding of risks, in certain aspects going beyond what was articulated in the NRA, providing a comprehensive and detailed breakdown of the ML threats in the financial and capital markets that derive from the considerable shell company customer base in banks, correspondent relations with foreign higher risk credit institutions, provision of financial services to PI/EMIs and trust dealings that include the provision

of fiduciary credit services[66]. It also identified vulnerabilities associated with the deficiencies in the internal control systems of FIs, such as insufficient independence of the compliance function, formal enforcement of AML/CFT requirements, use of agent services for customer identification, and formal approach to reporting suspicious transactions.

92. Other supervisors referred to risks specific for their area of competence, such as widespread use of cash in gambling (LGSI), currency exchange operations below the identification threshold of EUR 8 thousand (BoL), use of proxies/frontmen in real estate transactions (LCSN) and non-regulated activities of certain professions such as legal advice, tax consultancy and similar services for onshore and offshore company formation, and real estate brokerage (SRS). Some of these supervisors referred to mitigation controls or non-compliance with preventative measures as a risk. Overall, the BoL displayed an acceptable level of understanding, while the others generally demonstrated a moderate or elementary level of understanding of ML/FT risks.

93. In the vast majority of the cases participation of competent authorities in the NRA process was limited to providing information with limited or no involvement in the analysis of collected data and input on relevant conclusions. In addition, some of the advanced (in terms of the understanding of risk) authorities were of the opinion that the information collected and analysis conducted for the assessment were not comprehensive enough to grasp the whole picture regarding the situation with ML/FT in the country. This means that the authorities might need to revise the NRA process to increase the stakeholders' participation in and contribution to all stages of the risk assessment.

94. As of the date of the onsite visit, the authorities have not implemented any sectorial or agency-level assessments of risks relevant for AML/CFT. As an exception to that, the FCMC provided a report of Compliance Control Department to the management of the FCMC summarising the results of AML/CTF compliance supervision for H1 2017, which includes certain analysis and assessment of the ML/FT risk exposure in sectors of financial service providers supervised by it.

95. According to the 2017 NRA Report, the most significant threats of ML are caused by the following predicate offences committed in large volume and/ or by organized groups: a) corruption and bribery; b) criminal offences in the tax area; c) fraud; and d) smuggling. At that, while concluding that 15% of the predicate offences are committed in Latvia, 28% – in foreign countries, and 6% – both in Latvia and abroad, the report states that the origin of the criminal proceeds and the respective predicate offence in the other 51% of cases is unknown and/or cannot be reliably identified.

96. The 2017 NRA Report does not provide any numeric/otherwise measureable estimates on the significance and volume of the proceeds of crime potentially laundered in and through Latvia. This appears to miss one of the main objectives of the NRA as far as reliable estimation of ML threats for the country is concerned.

97. In relation to the predicate crime environment, neither the 2017 NRA Report nor other analyses provide estimates of the significance and magnitude of undetected or latent criminality in the country. This means that the actual level of criminality in Latvia might be higher than the official

[66] Para. 14 of Sec.1 of the Credit Institutions Law defines fiduciary operations (trust) as transactions in which the relationship between a credit institution and a client is based on mutual trust, whereby the credit institution undertakes the responsibility for the management of property owned by the client for the benefit of the client, managing such property separately from its own property.

records, especially given the impact of the cross-border flows of potentially illicit funds for which a comprehensive analysis and reliable estimates are still to be achieved.

98. There is uneven and overall inadequate appreciation of the ML implications of the illegal cross-border movement of humans and, more importantly, potentially ML-related cross-border flows of funds, whereas the conclusions on the overall ML threat fail to encompass the all-embracing impact of the threats emanating from large financial flows passing Latvia as a transit point in its capacity of a regional financial center.

99. While acknowledging the higher risk of ML identified with the banks involved in the non-resident clientele business, the authorities generally demonstrate tolerance towards shell company servicing products, which are the main conduit for that business. This is important given that the risk appetite of the banks in the non-resident clientele business has not changed substantially at least within the comparable period of the last two years. There are no estimates on the significance and volume of illegal cash turnover in the country, and no analysis on ML threats emanating from the use of new technologies and delivery channels (e.g. virtual currencies, crowd funding).

100. The evaluation team generally agrees with the types of ML risks identified in the country. However, the overall level of risk (medium high) assigned is not substantiated by the findings of the NRA or understanding of the authorities, and does not correspond to the country-wide risks.

101. The conclusion of the *2017 NRA Report* about the low risk of FT in Latvia, which has been reaffirmed by the authorities in discussions during the onsite visit, does not account for certain factual circumstances in the country. FT threat inherent to regional financial centres in general and to specific financial and non-financial products/services offered in Latvia in particular has not been appropriately analysed. Major vulnerabilities in Latvia inherent to the country's legislative and institutional frameworks, professional sectors of FIs and DNFBPs, relevant services and products, legal entities and NPOs, as well as applicable contextual factors have not been duly analysed and assessed under the prism of their susceptibility to the threat of FT in the country.

National policies to address identified ML/TF risks

102. The key document defining nation-wide efforts aimed at effective implementation of AML/CFT measures is the 2017-2019 Action Plan. The plan defines seven courses of action to achieve its objectives, by means of: 1) enhancing the coordination in the development and introduction of the AML/CFT strategy and policy; 2) improving the statutory regulation on AML/CFT; 3) improving the effectiveness of investigation, indictment and adjudication; ensuring effective application of the preventive measures and penalties; 4) improving the effectiveness of FIU activities; 5) building the capacity of the subjects in the AML/CFT field; 6) building the capacity of the supervisory and control authorities in the AML/CFT field; and 7) improving data aggregation and analysis for ML/FT risk assessment and other AML/CFT purposes. Each course of action defines a set of specific measures to be implemented, their expected outcomes, the indicators against which implementation is measured, the agencies (co)responsible and the deadline established for implementation of such measures.

103. Overall, the 2017-2019 Action Plan seems to fall short of specific targeted measures to address the major ML threat emanating from, *inter alia*, the high concentration of the foreign customer base of the credit institutions and the related large cross-border movements of funds. It also appears to be somewhat general in defining measures aimed at improving the effectiveness of law enforcement action on the background of significant gaps in the investigation, indictment and

adjudication of ML cases. Defined activities of the competent authorities need fine-tuning to provide for focused action consistent with identified ML/FT risks.

104. The authorities advised that AML/CFT is set as a priority and integrated into the work plan of state institutions to restrain shadow economy for 2016-2020[67], the MoF strategy to reduce shadow economy for 2015-2020[68], the SP plan of activity priorities for 2016[69], the guidance on combating and preventing corruption for 2015-2020[70], the KNAB activity strategy for 2014-2016[71], and the plan on combating and preventing organised crime for 2014-2016[72]. Whereas the assessment team has not been provided English versions of the above-stated documents, it is critically important for Latvia to ensure that, among various national policies relevant for AML/CFT, those with expired term of fulfilment are substantively assessed for the effectiveness of implementation, and the ones in the implementation phase are harmonized and synchronized to coherently provide defined actions, measurable milestones and established deadlines for the measures aimed at combating ML/FT in the country.

Exemptions, enhanced and simplified measures

105. It does not appear that the provisions of the AML/CFT Law and relevant regulations requiring application of enhanced measures for higher risk scenarios have been based on due considerations to such scenarios – as identified by any national and other risk assessments – which are characteristic for the Latvian framework both in the financial sector (e.g. provision of financial services to PI/EMIs and trust dealings that include the provision of fiduciary credit services) and non-financial sector (e.g. widespread use of cash in gambling, currency exchange operations below the identification threshold of EUR 8,000, use of proxies/ frontmen in real estate transactions and non-regulated activities of certain professions such as legal advice, tax consultancy and similar services for onshore and offshore company formation, and real estate brokerage).

106. Provisions of the Latvian legislative framework permitting the REs to apply simplified CDD with regard to certain categories of customers whenever the identified lower risks do not contradict the national ML/FT risk assessment but rather simply represent a transposition of the relevant provisions of the former EU Directives 2005/60 and 2006/70, or of the non-exhaustive list of factors provided in Annex II of the Directive (EU) 2015/849. This does not amount to using the results of risk assessments to support simplified measures in case of lower risk scenarios.

Objectives and activities of competent authorities

107. The assessment team has not been provided information on the defined procedures and consistent practices for incorporation of NRA outcomes into the roles and priorities of competent authorities, adjustment of agency-level policies and updating of agency-level risk assessment procedures having regard to such outcomes, development of institutional and operational changes driven by focus on identified/emerging risks, as well as implementation of measures focused on identified higher risk factors and emerging/evolving risk patterns.

108. Whereas one of the key supervisors, the FCMC, produced plans of actions to ensure consistency with the identified ML/FT risks, the establishment of measurable milestones and clear

[67] Action plan of state authorities for limiting the shadow economy for 2016-2020 (adopted on June 10, 2016)
[68] MoF presentation "Strategy for limiting shadow economy for 2015-2020"
[69] Annex to the SP order No 4981 of December 29, 2015 "Work Plan for SP for 2016"
[70] Cabinet order No 393 of July 16, 2015 "Guidance for Corruption Prevention and Combating for 2015-2020"
[71] Operation strategy of CPCB for 2014-2016
[72] Cabinet order No 276 of June 5, 2014 "On Organized Crime Prevention and Combating plan for 2014-2016"

deadlines for the implementation of any such action plan, combined with sensibly lessening tolerance of the supervisor to the formalistic compliance of the obliged entities with their AML/CFT obligations, remains very important. Other supervisors met onsite did not produce similar plans of actions aimed at ensuring compliance with applicable AML/CFT requirements.

109. The Operational Strategy of the FIU for 2017-2019 refers to the outcomes of the 2017 NRA Report and the 2017-2019 Action Plan to determine its strategic priorities as the detection of major laundering schemes, freezing of laundered proceeds in large amounts, and drafting of materials with due quality to enhance effective pre-trial investigation. It establishes a number of measures aimed at implementing these priorities by means of, *inter alia*, regular conduction of ML/FT risk assessments, collection of statistics necessary for such assessments, enabling access to various databases, improving IT solutions available for operational and strategic analysis. Tackling complex ML schemes is one of the priorities for the FIU and freezing of funds is an instrument to achieve it. Nonetheless, the part of the strategy articulating the expected outcomes of its implementation mainly speaks about the measures that have been (or, in some cases, are being) taken by the FIU instead of providing a forward-looking plan of actions with specific implementation milestones and deadlines in order to realize the priorities of the FIU.

110. Activities by the KNAB are not fully consistent with Latvia's risk profile. In particular, there has been a limited number of ML-related domestic corruption cases investigated by the KNAB, even though it agrees that domestic corruption poses a significant ML risk in Latvia. Cross-border identification of cash is not adequately prioritised by customs authorities in light of the potentially significant cash-related ML/FT risks. While the SRS FPD and the SP have a reasonable understanding of the ML risk (as noted earlier), in practice a targeted approach founded on risk-based priorities is not fully applied.

National coordination and cooperation

111. The FSDB chaired by the Prime Minister and comprising high-level representatives of all key public sector (ministers, heads of agencies) and private sector (chairpersons of SROs, professional associations) stakeholders is the coordinating authority with the objective to improve the cooperation between state authorities and the private sector in the prevention of ML/FT. The FSDB holds regular and *ad hoc* meetings organising its work through the rules of procedure approved by the CoM. At the policy-making level, the FSDB defines high-level goals and objectives in the AML/CFT area, approves risk assessment methodologies, reports and mitigation actions plans, thus promoting cooperation and coordination in the field of combating ML/FT. The mandate of the FSDB could be beneficially extended by specifically articulating its function in considering global trends in ML/FT and their local implications, as well as in providing tailored guidance on implementation of and follow-up on the national policies and activities to combat ML/FT (and, where appropriate, PF).

112. At the operational level, all agencies represented in the FSDB provide relevant input, including statistical and other data, necessary for the development of national policies and activities. It would be beneficial to have defined procedures and consistent practices for individual authorities to conduct strategic analyses with their outcomes feeding into the national policy development process, as well as for horizontal exchange of information on risks/trends and specific cases.

113. The Advisory Board of the FIU (ABCS) chaired by the GP is tasked with, *inter alia*, facilitating the work of the FIU and coordinating its cooperation with pre-trial investigation agencies, the Prosecutor's Office, the judiciary and the subjects of the AML/CFT Law. Most of the government

agencies (except for the Ministry of Economy and the MFA) that are members of the FSDB also sit at the ABCS.

114. Limited information was provided on efforts made by the FIU, supervisors and LEAs to harmonize their activities, including through formal joint initiatives at policy-making and operational level (e.g. task forces), towards more effective cooperation and coordination in combating ML/FT (and, where appropriate, PF). It is therefore difficult for the assessment team to assess the effectiveness of such efforts. Based on meetings with representatives of LEAs during the onsite visit, it appears that the FIU does not have a coordinating role in LE joint actions. Provision of routine feedback on joint actions (if any) and specific cases between the FIU, supervisors and LEAs also seems to remain an area that needs significant improvement

Private sector's awareness of risks

115. The authorities have sought input from the private sector for the 2017 NRA through surveys conducted by means of thematic questionnaires. They have also held meetings and discussions with the private sector to enable fact-finding and collection of early views on risks prior to risk assessment. The 2017 NRA Report was produced in April 2017 as a strictly confidential document accessible for competent authorities only. Later on, however, it was declassified and published in November 2017 on the FIU website, as well as circulated to the private sector. Representatives of the private sector referred to meetings with some supervisors (e.g. the FCMC) and the FIU to discuss the findings of the 2017 NRA Report before its declassification and publication, which does not appear to amount to an appropriate strategy for communicating the outcomes of risk assessments to the private sector. An appropriate strategy would comprise a set of measures including, *inter alia*, various forms of outreach (e.g. face-to-face meetings, written guidance, references to websites) along with established frequency (e.g. upon updating risk assessments, emergence of new risks) and targeting (e.g. sector-specific communication) of outreach, as FIs and DNFBPs did not demonstrate sound understanding of the NRA conclusions.

116. Most representatives of FIs (except for an MVTS) and certain DNFBPs (such as casinos, auditors) were generally aware of the 2017 NRA Report, mainly due to their participation in the process in the stage of collection of information via predefined questionnaires. Within the private sector, there were opinions that the conclusions of the NRA were too general to be transformed into practicable actions taken by the obliged entities. Their impression was that most of the findings in the report relate to the legislative and institutional framework and have little to do with the preventive measures required from the private sector. Accordingly, they showed little if any interest in using the results of the risk assessment for revisiting their relevant policies, procedures and controls. This may be partly due to the lack of previously unidentified threats, vulnerabilities and residual risks articulated in the 2017 NRA Report, and partly for the disagreement with its analysis and conclusions.

Conclusion

117. Latvia produced the report on its most recent full-scope national assessment of ML/FT risks in April 2017 demonstrating high-level commitment and support for making the national assessment of ML/FT risks a systemic exercise following a consistent process. Certain key authorities, such as the FIU and the FCMC, demonstrated rather broad understanding of the risks within the AML/CFT system. However, there is uneven and overall inadequate appreciation of the potentially ML-related cross-border flows of funds, whereas the conclusions on the overall ML

threat fail to encompass the all-embracing impact of the threats emanating from large financial flows passing Latvia as a transit point in its capacity of a regional financial center.

118. The key document defining nation-wide efforts aimed at effective implementation of AML/CFT measures, i.e. the 2017-2019 Action Plan seems to fall short of specific targeted measures to address the major ML threat emanating from, *inter alia*, the high concentration of the foreign customer base of the credit institutions and the related large cross-border movements of funds. The conclusion of the 2017 NRA Report about the low risk of terrorism in Latvia, which has been reaffirmed by the authorities in discussions during the onsite visit, does not account for certain factual circumstances in the country. Latvia has a **moderate level of effectiveness for IO.1.**

CHAPTER 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

Key Findings and Recommended Actions

IO.6

- Competent authorities, including the FIU, have access to and make use of necessary sources of financial intelligence to support their analytical and investigative activities. The reliability of UBO information is limited, as also noted under IO.5.
- A well-built and regularly updated analytical software supports the FIU's analytical work. Some strategic analysis has been performed but resources allocated to that function are insufficient.
- The general quality of UTRs/STRs is modest, given the confusion between unusual transaction reports (UTRs) and suspicious transaction reports (STRs); the possible confusion with the parallel reporting system on tax suspicions; "defensive" reporting; insufficient documentation attached to STRs; inadequate UBO-related information; and limited FIU feedback to REs. The reports do not fully reflect the country's risk profile. A small part of the reports is disseminated to LEAs. Cross-border cash movement information is of limited use.
- The FIU requests additional information to REs in a limited number of cases. It sometimes asks REs to request additional information directly from the client, without taking steps to mitigate tipping-off risks.
- Although an important part of the FIU's disseminations lead to ML/FT investigations, the quality of FIU analysis is deemed unsatisfactory by some LEAs. However, FIU/SP coordination efforts since 2015 have resulted in FIU disseminations progressively becoming the main source of ML/FT prosecutions.
- The FIU pursues a very proactive freezing policy, in line with the FIU's priority objectives set by the FSDB. The FIU's freezing orders are the main source of non-conviction-based confiscation, as noted under IO.8. However, it was reported that in some instances a lack of coordination with LEAs in issuing freezing orders was detrimental to investigations.
- LEAs are empowered to request cooperation from the FIU, but only after approval by the GPO, which has resulted in some cases in delays in obtaining information.
- Coordination and cooperation efforts between the FIU and LEAs have increased since 2015, especially at the operational level, but no clear mechanisms have been established.

IO.7

- Latvia has a sound legal system and institutional framework for the investigation and prosecution of ML. Until recently, the judicial system of the country did not appear to consider ML as a priority and to approach ML in line with Latvia's risk profile as a regional financial centre. This appears to have lately changed to a certain extent, with some large-scale ML investigations underway, involving bank employees having actively facilitated the laundering of proceeds. While it is notable that the authorities now appear to take the investigation of ML which corresponds to Latvia's risk profile more seriously, the lack of ML investigations against legal persons in those cases suggests that major improvements are still required.

- While a great number of ML investigations are pending, a mere fraction of them eventually leads to a prosecution and subsequently a conviction. The country has achieved a certain number of ML convictions in the five years prior to the onsite visit, which however appears modest when compared with the high number of convictions for predicate offences during the same period. ML convictions for both domestic and foreign predicate offences have been achieved. Latvia also demonstrated one conviction for third-party laundering and one conviction for stand-alone ML, the latter however being possible only because the accused made a full confession. Otherwise, prosecutors still rely on the existence of a predicate offence to meet the prerequisite of proving that the accused had the knowledge of the illegal origin of the laundered property. Although legislative changes have addressed this issue, they have been too recent to produce tangible results.

- The large majority of custodial sentences are deferred. Sanctions for natural persons appear neither dissuasive nor proportionate due to the frequent reduction of sentences in light of the length of proceedings or the application of the legal possibility to suspend a custodial sentence of up to five years' imprisonment. Latvia demonstrated the application of coercive measures provided by the CL against legal persons. The country also uses a number of alternative criminal measures where a ML conviction is not possible for justifiable reasons.

IO.8

- Latvia has a broad legal and sound system for confiscation of criminal proceeds, which is based on two pillars (conviction-based and non-conviction-based confiscation). While results from conviction-based confiscation are hampered by previous evidentiary requirements to demonstrate the criminal origin of the property, the absence of routinely-performed parallel financial investigations and the modest number of ML-convictions achieved through the judicial system, non-conviction-based confiscation brought some encouraging results, enabling Latvian authorities to confiscate considerable amounts in both domestic and international cases. The large majority of cases of non-conviction-based confiscation are triggered by reports from the FIU.

- The authorities regard the pursuance of confiscation of criminal proceeds as a worthy and achievable goal in itself and have made it one of the priorities in the overall judicial ML system. With the assistance of the recently–established Asset Recovery Office (ARO), property can be identified in a more effective way and in a timely manner. Latvia does not have an asset management system with specialised staff trained on sophisticated assets. In individual cases, Latvia is able to demonstrate effective repatriation of large amounts of confiscated proceeds of crime to third states, as well as in a domestic context the restitution to victims of economic crime.

- Latvia has not been able to demonstrate an effective system of confiscation of undeclared or falsely declared cross-border movement of currency and bearer negotiable instruments. Given that

smuggling is identified as one of the main ML risks in Latvia, the lack of effectiveness raises concern. This is mostly due to the difficulty to meet the evidentiary standards to prove that the undeclared or falsely declared cash/ bearer negotiable instruments (BNIs) result from a criminal activity and to confiscate them as a consequence.

- The authorities are actively freezing and seizing illegal property, especially bank account assets, which resulted in some high-profile cases with considerable amounts of confiscated illegal property. In order to reach the characteristics of an effective system to a large extent, the evaluators would however have expected from Latvia to demonstrate even stronger confiscation results in line with the ML risks the country faces.

Recommended Actions

IO.6

- Latvia should revise the reporting obligations, as recommended under IO.4, and increase outreach, training and feedback for REs with regard to the differences between STRs and UTRs, the potential adverse effect of delayed/defensive reporting and develop further red flags indicators in order to enhance the quality of STRs.

- Efforts to improve coordination between the FIU and LEAs should continue, especially in relation to exchange of information and freezing orders. Clearer cooperation and coordination mechanisms should be established at the policy and operational levels.

- Adequate resources should be allocated to strategic analysis.

- The FIU should ensure that potential tipping-off risks are mitigated when requesting additional information to REs.

- The modalities of the oversight of the FIU by the GP should be reviewed in order to ensure that the FIU has the necessary operational capacity to engage in a timely way with partners.

IO.7

- Latvia should pursue ML as a priority and seek to systematically prosecute a wider range of ML offences, including third party and stand-alone/autonomous ML. ML investigations should be more streamlined and prioritised in order to accelerate their duration. Parallel financial investigations should be enhanced and performed systematically.

- Latvia should prioritise the investigation for ML in line with its profile as a regional financial centre.

- Prosecutors should test the recent legislative change in the ML definition to the effect that a ML conviction is possible on the basis of circumstantial evidence, as opposed to the previous reliance on the existence of a predicate offence. Latvia should develop law enforcement guidance, backed up by corresponding and comprehensive training for all stakeholders involved in the investigation and prosecution of proceeds-generating offences, including on the minimum levels of evidence which the courts may require to establish underlying predicate criminality in a ML prosecution under the recently-changed legislation.

- The impact of Sec.55 CL, which allows for the suspension of a sentence of up to five years, on the effectiveness of sanctions for ML convictions should be reviewed. Prosecutors should systematically appeal ML sentences which are too lenient.

IO.8

- The authorities should test the boundaries of the new legislation (Sec.70[11] CL) introducing a reversed burden of proof to recognise the property as illegally obtained.
- Latvia should develop a system which would enable it that relevant statistics are held for seizures and confiscations of property broken down by predicate offences, by amount of assets and by kind/nature of property confiscation.
- The country should pursue conviction-based confiscation systematically both with regard to ML and predicate offences.
- Latvia should take steps to ensure a more dissuasive system for seizing and confiscating falsely and non-declared cross-border movements of currency and BNIs and ensure that this includes the proper identification of ML/FT investigations in line with the country's risk profile.

119. 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.3, R.4 & R.29-32.

Immediate Outcome 6 (Financial intelligence ML/TF)

Use of financial intelligence and other information

120. LEAs report having access to a sufficient range of financial intelligence sources, but the information provided in that regard lacked specificity. The FIU's function is well understood by the other competent authorities and its resources and outputs are used by LEAs, although not as regularly as should be, as explained below. Cases were presented where financial intelligence generated and spontaneously shared by the FIU was used by LEAs to develop evidence for pre-trial investigations (see below).

121. The FIU exercises control over UTRs and STRs. It acquires, receives, registers, processes, compiles, stores, analyses and provides information to pre-trial investigative institutions, the Prosecutor's Office and the Court. The FIU can initiate investigations based on its own findings, foreign FIUs requests, or information from a third party (i.e., REs or other public authorities). The FIU is also a direct recipient of cross-border cash transportation reports.

122. The FIU has direct electronic access to a wide range of information and databases. Various State and Municipality databases (e.g., Procurement Monitoring Bureau, Register of Construction, etc.) are accessible upon written request. Electronic access to UBO information contained in the ER was granted to the FIU in November 2017. Until that date, UBO information was available to the FIU (or other authorities, such as KNAB)[73] upon written request. As noted below under IO.5, the availability and reliability of UBO information held by the ER (and REs), is however inadequate, especially given the specific risks associated with shell companies in Latvia.

Case 1 – FIU-initiated case on the laundering of funds of unclear origin, possibly derived from activities of a pyramid scheme

An STR indicated that Russian citizen F with a Latvian residence permit made large cash deposits into an account in Latvian bank A (EUR 82,500 in total in 2017), explaining that the funds originated from his businesses in Russia. The cash was brought by his relatives and colleagues and had not been declared at the customs as each amount transported did not exceed EUR 10,000. Upon further analysis, the FIU discovered

that F had opened other accounts in Latvian banks B and C, in which, in 2013-2017, he deposited EUR 253,435 and EUR 318,204 respectively in cash. F explained that funds originated from the sale of his real estate property in Russia.
F simultaneously provided identical sale agreements for a total value of EUR 203,360 as justifying documentation to all three banks. Two non-residential premises had been sold at a suspiciously high price to Russian citizen D in 2014.
F also simultaneously provided identical documentation on inherited assets amounting to EUR 64,400, as well documentation on income obtained from his self-owned enterprise in Russia (allegedly EUR 570 per month) to all three banks. Upon further inquiry, the FIU received intelligence that, in 2014 the savings accounts of both deceased family members in Russian banks had been credited with suspicious funds transfers for a total of EUR 221,010 after the date of their respective deaths.
Overall, those explanations could not account for the full amount of cash deposited in Latvian banks.
From 2013 to 2016, F purchased several real estate properties in Latvia that were worth EUR 217,250 in total. At the turn of 2012-2013, F transferred EUR 511,976 from his account in a Russian bank to accounts of Latvian citizen M (who later became his wife) at Latvian banks. Funds were then used by M to purchase EUR 162,000 worth of real estate in Latvia. Furthermore, from 2012 to 2017 M deposited EUR 119,000 of cash in her accounts in Latvian banks. The source of funds was never documented or explained to the banks.
Financial operations were also carried out in other EU countries. The FIU had intelligence that F established/purchased 9 companies owning luxury apartments in the Czech Republic. In 2016, those companies were merged under a single entity and the ownership of the real estate was entirely re-registered to that particular F's company. From 2016 to 2017 significant activity was registered on F's personal and business accounts in Czech banks. USD 2 million and EUR 8,481,939 were received from company O whose registered agent was from Seychelles and further circulated among the personal and business accounts of F.
Comparing publicly available information with information submitted to the Latvian banks it became evident that F was one of the key figures of Russian financial pyramid scheme MMM-2011 in which up to 40 million persons in the world may have lost USD 10 billion. The SP has initiated criminal proceedings against MMM-2011 for providing unlicensed financial services in Latvia. The FIU forwarded the case for review to the SP on the grounds of legalizing of large amounts of funds in without logical explanation of any legitimate origin. Currently a relatively small part of the assets has been frozen in F's account in Latvian bank A - no explanation was provided by the authorities about the reasons for which the amount frozen was limited.

123. LEAs have also regularly sought support from the FIU for their investigations (see statistics below). In many cases, this was limited to the freezing of funds, but information is also regularly requested and provided.

STRs received and requested by competent authorities

124. Reports to the FIU can be filed in an excel form, which represents the great majority of the cases; a paper form (5%); or an e-reporting platform (5%). The e-reporting tool (zinojumi.kd.gov.lv) has been available since April 2016, but it only became mandatory on 1 January 2018 (Cab. Reg. 768). It is aimed at facilitating the reporting and analysis of reports. "Methodical materials" were published on the FIU's website and training was provided to REs.

125. A number of factors have a negative impact on the quality of STRs as a source of intelligence.

126. It is not mandatory to provide all CDD-related information (e.g. supporting documents on the origin of the funds, UBO, etc.) jointly with the UTR/STR. According to the REs met onsite, those elements are regularly not provided.

127. As noted under IO.4, most REs met onsite - especially in the non-financial sector - did not see a significant difference between UTRs and STRs, given the overlap between their respective definitions. Their reporting activity often over-relies on identifying UTR indicators, most of them being threshold-based. Delayed reporting and defensive reporting are also part of reporting practices. In addition, the obligation to report local tax evasion-related suspicions to the SRS creates confusion, especially for REs that have more limited AML/CFT expertise.

128. Doubts remain concerning the reliability of statistics provided by the authorities in relation to UTR/STR obligations, since different data sets have been provided at the different stages of the assessment process. In addition, the number of STRs includes additional information provided by REs. Latvia is strongly encouraged to collect adequate statistics in this area (see the TC Annex on R.33). The latest information provided is as follows:

Table 7 – UTRs and STRs received by the FIU and dissemination to LEAs

	Unusual transactions		Suspicious transactions, activities, and relations, including additional information		Total		Cases disseminated to LEAs	
	Transactions	Reports	Transactions	Reports	Transactions	Reports	Transactions included	FIU cases sent to LEAs
2012	15,126	11,939	16,229	5,512	31.355	17,451	4,015	258
2013	12,225	9,856	13,131	3,525	25,356	13,381	4,009	259
2014	9,175	6,334	16,726	5,469	25,901	11,803	3,483	310
2015	10,830	7,216	17,525	7,267	28,355	14.483	6,409	340
2016	12,998	8,111	18,712	5,008	31,710	13,119	6,031	231
2017	16,785	8,725	25,517	7.722	42,302	16.447	14,177	225

129. The number of UTRs/STRs appears significant. This is at least partially explained by the defensive reporting approach followed by some banks. The ratio between UTRs/STRs received and disseminated by the FIU is an indicator of their moderate quality. In 2012-2016, only a minor part of the reports translated into cases disseminated to LEAs. STRs are the main source of these disseminations to LEAs, and UTRs are very rarely disseminated to LEAs.

Table 8 – Suspicious transactions, activities, and relations including additional information on the STRs/ SARs reports broken down by categories of reporting entities

	2011	2012	2013	2014	2015	2016	Total	
Banks	14,967	15,855	12,828	16,101	17,047	17,936	94,734	97,30 %
Insurances	15	1	5	-	4	-	25	0.02 %
Securities	-	-	-	-	-	-	0	0%
Investment firms	-	-	-	-	-	2	2	0%
Currency exchange	26	115	25	109	314	494	1,083	1,11 %
E-money services	-	5	64	98	17	28	212	0.21 %
Other FIs	10	139	108	364	129	215	965	0.99 %
Casinos	1	-	2	-	-	5	8	0%
Real estate	1	-	-	-	-	-	1	0%
DPMS	-	-	-	-	-	3	3	0%
Lawyers	7	60	79	44	11	8	209	0.21%
Notaries	7	4	3	4	3	15	36	0.03%
Accountants	-	-	-	-	-	-	0	0%
Auditors	-	4	-	-	-	5	9	0%
Tax consultants	-	46	17	6	-	1	70	0.07%
TCSPs	-	-	-	-	-	-	0	0%
Total	**15,034**	**16,229**	**13,131**	**16,726**	**17,525**	**18,712**	**97,357**	

130. The vast majority of reports are filed by banks, which is in line with the country risk profile, although reporting performance is very uneven across that sector. Overall, taking into account Latvia's risk profile, and in particular the use of shell companies in tax fraud schemes, DNFBPs seem to under-report suspicious transactions. Factors include a narrow definition (hence interpretation)

of UTR indicators for non-bank REs and under-regulation in the real estate, tax advice, accounting and company formation services sectors.

131. The consistency of the Latvian risk profile with the breakdown of STRs into main types of suspected ML/FT activity is difficult to assess. REs are not asked to specify the suspected underlying criminal activity when they report transactions, and the FIU does not systematically reclassify reports based on its own analysis. However, subject to available information, Latvia's reporting profile is not totally consistent with its risk profile. Fraud is reported on a regular basis. Tax crime reporting is limited in light of Latvia's risk profile. Corruption and smuggling-related crimes are not regularly reported, although they also feature among the four main ML threats highlighted in the NRA.

Table 9 - Breakdown of suspicious transactions, activities, and relations including additional information on the reports included in STRs into main types of suspected underlying activity

	2011	2012	2013	2014	2015	2016	Total	% of all transactions, activities, and relations in STRs filed in 2011-2016
ML	13,341	13,620	10,927	13,456	14,683	15,402	**81,429**	62.29 %
FT	3	1	2	-	4	15	**25**	0.02 %
Tax crimes	277	1,251	734	425	579	1,695	**4,961**	3.80 %
Fraud	1,413	1,357	1,468	2,845	2,255	1,600	**10,938**	8.37 %

132. In 2017 (until 31 October), the FIU sent 1,646 requests for additional information to REs, which is a modest number in comparison with the total number of the reports received, and considering that STRs do not contain all necessary information and that CDD measures are moderately effectively applied (see IO.4). The FIU sometimes requests REs to ask for additional information directly to their clients, which also reflects the lack of systematic CDD information joined to reports and limited effectiveness in CDD (particularly in relation to the UBO). Tipping-off risks posed by this practice do not seem considered – and mitigated – by the FIU.

133. To improve the quality of reports, the FIU organises meetings on an annual basis with banks to provide general feedback and discuss difficulties and best practices. The FIU also sent letters to some REs on drawbacks in specific reports. In practice, individual feedback is provided to REs only in relation to those cases that have been disseminated to LEAs and foreign FIUs, which the NRA notes is insufficient to improve the quality of reports. More risk indicators and guidelines would also be useful to improve the quality of reports.

134. The FIU has direct access to cross-border cash movement information (declarations and detected undeclared movements and false declarations). This potential source of financial intelligence is of limited use to support analysis of or investigations into ML or FT cases.

135. Detection and declaration mechanisms appear moderately effective and generate insufficient reports in light of the risks associated with cash couriers and the intensive use of cash in Latvia. Sanctions for non- or false declarations are not dissuasive, as mentioned under IO.8. In addition, Latvian banks are not required to ask (and do not do so when conducting CDD) their customers to present a duly completed customs declaration form for each deposit of EUR 10,000 or more when evidence suggests that the cash was introduced in Latvia through the border. In terms of detection, no indicators of ML/FT risk associated with cash cross-border transportation are at the disposal of

the Customs, which do not conduct targeted controls on cash cross-border movements. The number of detected undeclared/falsely declared cash movements is low in light of the country's risk profile.

136. The financial intelligence actually generated by the cash declaration system is of limited use, as recognised by the authorities met onsite. As noted under IO.8, an investigation is only initiated (and funds seized) by the Customs if the detected amount is over EUR 19,000 or in case of ML/FT suspicions; however, in practice the Customs have never had such suspicion. When an investigation is opened, approx. 95% of undeclared and falsely declared cash movements are associated with non-residents and funds coming from abroad. Challenges noted in cooperating with some neighbouring countries (see IO.2) are particularly critical in such investigations. Similarly, the FIU indicates that it would only open a case based on a false or non-declaration when a concrete link with a criminal offence is found, but the Customs have never reported any ML/FT suspicions to the FIU. No statistics on the final result of the investigations following a restraint of cash and BNI was provided.

Table 10 - Cross-border transportations of cash and BNI

	Incoming declarations		**Outgoing declarations**		**Undeclared and falsely declared**		
	No.	Amount (KEUR)	No.	Amount (KEUR)	No.	Restrained amount	Sanctions imposed
2011	232	19,740	101	57,890	3	213,993	NA
2012	403	20,680	94	60,736	22	1,317,391	NA
2013	472	28,805	101	30,903	33	817,961	NA
2014	600	41,955	95	12,685	19	68,349	NA
2015	529	74,468	188	335,874	8	277,424	NA
2016	566	96,044	188	216,263	41	1,209,699	NA
2017[74]	682	80,685	207	203,149	25	451,063	NA
Total	**3,484**	**362,377**	**974**	**917,500**	**151**	**4,355,880**	**NA**

Operational needs supported by FIU analysis and dissemination

137. Since 2016, the FIU has been staffed by 30 persons: Head, Deputy Head, 4 posts in the Systems Analysis Unit, 6 in the Data Processing Unit, 8 in the IAU, 3 in the Strategic Analysis Unit, 4 in the International Cooperation Unit, a secretary, a clerk and a housekeeper. In 2017, 5 additional posts were allocated to the FIU.

138. The FIU suffers from excessive staff turnover. For example, the Strategic Analysis Unit was created in 2015 to develop the NRA. However, all three posts were vacant at the moment of the onsite. Factors include the relatively low wages offered by the FIU in comparison with private sector salaries (which on average are twice as high as those of the FIU).

139. The FIU has designed - jointly with the Institute of Mathematics and Computer Science of the University of Latvia - a robust analytical software, which is placed in a secure network and updated annually. The software provides, *inter alia*, analytical tools, reports' data processing, risk scoring, enriching information with external sources, data mining, and visualisation tools. It is linked to other state databases, such as the SRS's database on cross-border cash declarations, but not yet electronically to the Bank Account Register. The software also serves as a case management system,

[74] Until 31 October 2017

containing comprehensive information on the evolution of the case and the amount of analysed/pending information, and monitoring deadlines. Cases are prioritised manually in the system, based on criteria such as the need for a freezing order or a link to FT or PF.

(a) Operational analysis & dissemination

140. The FSDB set three operational priorities for the FIU: detecting large ML schemes (20 or more participants); freezing proceeds of crime in large amounts; and preparing quality case materials to foster pre-trial investigations. The FIU thus gives high priority to complex cases, with a view to freezing potential proceeds as fast as possible and disseminating these cases to the LEAs.

141. 25 staff members are directly involved in operational analysis. The process follows an Instruction updated on September 2017. The extent of the updates is unclear and evaluators have been cautious in considering the document for assessing effectiveness. The Instruction describes in detail the registration, analysis and dissemination process. When reports are received, Initial Processing is performed by the FIU software tools (data validation, import, data mining, risk scoring, comparison with lists, etc.). When new targets or cases are detected, Preliminary Due Analysis starts. Cases are created and transferred to Examination based on two successive conditions: there is a reasonable suspicion of a criminal offence; then, the case appears "legally promising" in line with the priorities of the FIU. Examination Cases are assigned to transaction analysts, who gather additional information from databases (including the FIU's), REs and domestic or foreign institutions. If the reasonable suspicion is substantiated, the draft Material needs to be approved successively by the Head of the Information Analysis Unit (IAU), the Deputy Head of the FIU then the Head of the FIU, who also decides whether freezing orders need to be made. The analyst prepares the Material for dissemination. The criteria for approval are not explicit in the Instructions. In practice, considerations pertain to legality, prospect of successful proceeding and priorities of the FIU. No draft Material has been rejected, a thorough check of the robustness of cases being performed before starting an Examination. On average, cases are disseminated within 64 days following the receipt of the STR/UTR (2013-2016).

142. Most cases are disseminated to the SP Economic Crime Enforcement Department (74% in 2013-2016), followed by the SRS FPD (23%), which is in line with Latvia's risk profile.

Table 11 – Reports disseminated by the FIU and associated prosecutions and convictions

	FIU disseminated reports*	FIU disseminated reports regarding ML only*	ML/FT (and other criminal offences) criminal proceedings started on the basis of FIU reports		ML/FT (and other criminal offences) prosecutions based on FIU reports		Convictions based on FIU reports (number of cases)	
			No.	Ratio to FIU reports	No.	Ratio to FIU reports	No.	Ratio to FIU reports
2011	442	340	NA	NA	1 (6)	0.2% (1.4%)	3 (3)	0.8% (0.7%)
2012	258	212	NA	NA	2 (10)	0.9% (3.9%)	4 (1)	1.8% (0.4%)
2013	259	236	NA	NA	10 (5)	4.2% (1.9%)	1 (7)	0.4% (2.7%)
2014	310	281	65	23%	14 (13)	4.9% (4.2%)	5 (4)	1.7% (1.3%)
2015	340	316	184	58%	16 (11)	5.0% (3.2%)	4 (4)	1.2% (1.2%)
2016	231	210	89	42 %	18	8.5%	3	1.4%

					(13)	(5.6%)	(2)	(0.9%)
Total	**1,840**	**1,595**	**338****	**41%****	**61 (58)**	**3.8% (3.2%)**	**20 (21)**	**1.2% (1.1%)**

** Does not include additional information on previously disseminated cases nor replies to LEAs' requests*

*** For 2014-2016*

143. On average, 41% reports disseminated by the FIU translate into LEA criminal investigations. However, no criminal proceeding has been initiated by KNAB on the basis of information provided by the FIU (since 2013).

144. Some LEAs met onsite considered that FIU reports, including the analysis they contain, are of insufficient quality. They noted that FIU reports are sometimes incomplete and, critically, usually do not accurately identify UBOs. The FIU was mainly relying on UBO information collected by REs themselves, the low quality of which is described under IO.4. The SP also indicated that, in a number of cases, the link between the suspicious transaction and an offence is insufficiently substantiated or that key elements of information are missing. The SP then has to request additional information to the FIU, which however requires GPO approval (further developed ad infra). Some LEAs also stated that, given these difficulties, they sometimes prefer to obtain financial intelligence by themselves.

145. The SP and the FIU however noted that steps have been taken since 2015 to improve SP-FIU cooperation, including in relation to information sharing by the FIU and feedback from the SP. Table 12 shows that the proportion of prosecutions based on disseminations by the FIU has been steadily increasing since 2011.

Table 12 – Sources of ML prosecutions and convictions

	Prosecutions			**Convictions**		
	Based on FIU disseminations	Based on other sources	% based on FIU disseminations	Based on FIU disseminations	Based on other sources	% based on FIU disseminations
2011	1	25	3.8 %	3	7	30 %
2012	2	24	7.5 %	4	1	80 %
2013	10	16	38 %	1	7	12.5 %
2014	14	15	48 %	5	4	55 %
2015	16	15	51 %	4	8	33 %
2016	18	6	75 %	3	3	50 %
Total	**61**	**101**	**37.6 %**	**20**	**30**	**40 %**

146. A number of FT-related STRs were reported to the FIU during the period under evaluation (see Table 9), but no prosecutions or convictions have been initiated on that basis. These low numbers are not totally in line with the FT risk profile of Latvia (see IO.1 and IO.9). In 2016, the FIU sent 7 reports to LEAs on alleged FT cases. Criminal proceedings were initiated in two cases, the other 5 pertaining to TFS false matches (see IO.10).

147. In line with the priorities set by the FSDB, the FIU pursues a very proactive freezing policy. Freezing orders are issued in relation to most cases disseminated to the LEAs. In most cases, they continue a decision taken by an RE to refrain from executing a transaction related with or suspected to be related with ML or FT (as required by Sec.32 AML/CFT Law, unless there is a risk of tipping-off).

148. Although the FIU's freezing orders rarely result in convictions and conviction based confiscations, as noted under IO.8, the FIU is a key contributor to Latvia's encouraging results in non-conviction based confiscation. In 2016, 53 out of 57 criminal proceedings and parallel non-

conviction-based confiscation procedures were initiated upon the FIU's case materials, including several major cases.

Table 13 – FIU freezing orders

	Freezing orders issued by the FIU			Preliminary investigation and seizure order following FIU freezing		Preliminary investigation and freezing order following FIU freezing		Prosecutions following FIU freezing		Convictions and confiscations following FIU freezing	
	No. of cases prompting FIU freezing orders	Total amount (KEUR)	Average amount (EUR)	No. of cases	Total amount (KEUR)	No. of cases	Total amount (KEUR)	No. of cases	Total amount (KEUR)	No. of cases	Total amount (KEUR)
2011	97	5,096	46,752	11	2,133	12	NA	1	NA	-	-
2012	58	28,813	436,560	10	326	20	NA	4	NA	4	1,178.24
2013	81	21,450	170,238	8	1,312	17	NA	1	NA	-	-
2014	133	79,000	196,029	18	2,106	34	NA	9	NA	1	2.41
2015	139	21,614	88,946	21	25,398	32	NA	11	NA	4	201.25
2016	163	36,170	143,531	49	50,316	36	NA	14	NA	3	182.27
Total	**671**	**193,007**	**160, 252**	**117**	**81,593**	**151**	**NA**	**40**	**NA**	**12**	**1,564.17**

149. However, it was also reported that, in some instances, LEAs' investigations have been negatively affected by FIU freezing orders taken without prior coordination, especially since such orders are notified by the RE to the customer, in practice, immediately after they are implemented. The FIU informed that since 2015 the managements of the FIU and LEAs have agreed on common freezing policy and priorities, and the current practice is discussed monthly. The freezing policy and particular cases are also coordinated with foreign FIUs during in the margin of MONEYVAL meetings, by phone or by exchange of letters.

(b) Strategic analysis

150. At the time of the onsite, no strategic analysis was being conducted as all three relevant posts were vacant. Despite these difficulties, the FIU has conducted studies on ML/FT risk indicators, trends and typologies, and disseminated some of them in guidance, the NRA or as a part of the FIU's public annual reports. Nevertheless, this analysis appears limited and only partly covers FT. Strategic analysis has been used in updating the list of unusual transaction indicators, but these updates have been minor since 2013. In general, the FIU's Strategic Analysis Unit's staffing instability negatively affects the ability of the FIU to adequately identify ML/FT related trends and patterns.

Cooperation and exchange of information/financial intelligence

151. As noted under IO.1, limited information was provided on cooperation efforts between the FIU and LEAs at operational or policy level. The insufficient quality of FIU disseminations noted by some LEAs and instances of insufficient coordination in relation to freezing orders were noted above, as were efforts to improve exchange of information and coordination in these areas since 2015. Coordination and exchange of information between the FIU and the SRS is active in relation to tax crime-related reports filed to both.

152. The FIU must provide information to pre-trial investigative institutions, the GPO or the courts in cases of substantiated suspicions that a person has committed a criminal offence, including ML and TF. In practice, the FIU is required to qualify the crime that it believes has been committed to decide which authority it must report the case to (e.g. SRS FPD for tax crimes, KNAB for corruption, etc.).

153. The FIU has to provide information to them upon their request, which it has done in a significant number of cases (see table below). However, LEAs' requests for information have to be approved by the GPO before they can be submitted to the FIU (Sec.56 AML/CFT Law). The GPO indicates that requests are reviewed within 2-3 working days on average, unless further information is needed. 10% of the requests were refused in 2016-2017, for legal and practical reasons that appeared reasonable to the evaluation team. Some authorities met onsite however noted that requesting information to the FIU can be lengthy.

Table 14 – Requests received by the FIU from other domestic authorities

	2011	2012	2013	2014	2015	2016	Total
Number of requests received by the FIU	64	50	57	58	58	107	394
Number of responses including financial information	44	34	52	52	64	111	359

Conclusion

154. Sources of financial intelligence seem broadly adequate, accessible and actively used by competent authorities to support their analytical and investigative activities. Deficiencies in access to and reliability of UBO information however appear critical in light of Latvia's risk profile.

155. Main categories of reporters and underlying crimes are not fully in line with Latvia's risk profile and a small portion of reported transactions is disseminated to LEAs.

156. A number of factors also have a negative impact on the quality of reports, which call for clearer definitions of STRs and UTRs, as well as and further guidance, outreach and feedback. Cross-border cash-movement information is of limited use as a source of financial intelligence.

157. The FIU appears to have adequate IT and HR resources and processes to conduct operational analysis. Some strategic analysis has been performed, with positive results, but such activity could be enhanced. The FIU's power to request additional information is not used proactively, and its practice poses a risk of tipping-off.

158. Although the FIU disseminates an important number of cases to the LEAs, the quality of FIU analysis is also deemed unsatisfactory by some LEAs.

159. The FIU pursues a very proactive freezing policy, reflecting the objectives set by the FSDB. However, associated with early notification of the client, and without systematic coordination, the freezing of funds has jeopardised investigations in some instances.

160. LEAs are empowered to request information from the FIU, but only after approval by the GPO, which oversees the FIU. Cooperation between national authorities has improved since 2015, but mechanisms remain unclearly established, both at operational and policy levels. **Latvia has a moderate level of effectiveness for Immediate Outcome 6.**

Immediate Outcome 7 (ML investigation and prosecution)

ML identification and investigation

161. Latvia has a sound legal system and a designated institutional framework that has the capacity to investigate and prosecute ML. The country has a broad range of LEAs that have the responsibility to investigate ML and associated predicate offences, as defined in Sec.387 CPL. If not otherwise provided, the SP shall investigate any criminal offence (and does so in practice with regard to 95% of all criminal offences in Latvia). The SP consists of several entities which all investigate criminal offences related to ML. These entities include a national unit (Central Criminal Police Authority) and five regional units. The Central Criminal Police Authority has an Economic Crime Enforcement Department, which comprises a "Unit 1" which investigates criminal offences in credit institutions and ML. With the SP having increased its staff with regard to ML and ML-related offences since 2016, "Unit 1" is currently comprised of 23 staff members. According to the SP, the unit was strengthened in January 2017 to respond to the increasing exploitation of Latvia as a regional financial centre for ML by international criminal groups from various eastern European and CIS countries

162. Sec.387 CPL sets out a number of other LEAs with the responsibility to investigate criminal offences, including ML: the SRS FPD and the Customs Police Department of the SRS (SRS CPD) (regarding criminal offences in the field of State revenue and in the customs sector); the KNAB, regarding criminal offences related to violations of the provisions of the financing of political organisations and criminal offences related to corruption in the State Authority Service, including foreign corruption/bribery and related ML); and the State Border Guard (regarding criminal offences related to the illegal crossing of the State border).

163. LEAs have various special investigative measures at their disposal. In the case of acquisition of confidential information or documents from financial and credit institutions, a previous judicial approval is needed. A person directing the criminal proceedings may assign an auditor or other expert to conduct an expert-examination, but the investigators rarely make use of it in ML cases. Investigators are authorised to access a variety of databases (e.g. motor vehicles, land registry, enterprise registry), also via distance communication means. Latvian authorities do not keep statistics about the number of financial investigations, and only few LEAs representatives confirmed during the onsite visit that parallel financial investigations are regularly conducted in cases when there is a suspicion of ML, even where the predicate offence occurs outside of Latvia.

164. Although Latvia has adopted a number of (work or action) plans with regard to combatting or limiting organised crime, the shadow economy and ML/FT, none of them is specifically devoted for identifying or prioritising ML by the LEAs. Instead, authorities understand the general CPL provisions as the main guiding instrument for ML investigations and prosecutions. The SP prepared an (internal) administrative management task document focusing on the gathering of financial intelligence information and encouraging the investigators to look for assets, if an investigated crime is related to property. ML and all property-related issues are investigated separately. Investigators of predicate offences regularly seek advice from Unit 1 about ML-related issues. The priorities of the SP are set annually; while ML investigations did not figure prominently in previous years, they are set in 2017 as an explicit priority separately from organised crime investigations.

165. According to the principle of legality, LEAs have to investigate all the COs identified, regardless of the amount of laundered proceeds. Nevertheless, priorities are usually set on a case-by-case basis and senior investigators may be appointed to investigate complex ML cases.

166. The vast majority of ML investigations are performed by the SP at the regional and national level, where the most complex cases are investigated by Unit 1 of the Economic Crime Enforcement Department. Unit 1 investigators are considered to have the highest level of expertise in the field of ML investigations. Other LEAs may refer ML cases to the Unit 1 for further investigation and frequently avail themselves to that possibility. Investigations are carried out under the public prosecutor's supervision and instructions. The public prosecutor has to be informed of the initiation of the criminal proceeding within 24 hours.

167. Cooperation between LEAs is still predominantly informal and established on a case-by-case basis, despite a recent national criminal intelligence model, which regulates the cooperation among LEAs. FCMC employees are present during the search of bank premises to assist the investigators. The SP representatives informed the evaluators of a good cooperation practice with the SRS FPD throughout the investigations, avoiding any duplication of work between the two authorities with regard to predicate criminality and related (stand-alone) ML investigations.

168. During the period 2013–2017[75], the SP initiated a total of 466 ML investigations with a steady increase in the first three years (2013: 31; 2014: 61; 2015: 212; 2016: 95; 2017: 67). However, of these 466 investigations only 21 cases were eventually transferred to the GPO (2013: 2; 2014: 2; 2015: 4; 2016: 4; 2017: 9). 96 criminal proceedings were terminated by the SP during the period 2013-2016, which is a rather low number (around 20%). The authorities stated that the low number of cases sent to the GPO was due to the fact that many criminal cases are instead transferred to foreign countries, once the suspicion is confirmed by evidence, as they concern predicate criminality in those countries (cases in 2013: 3; 2014: 8; 2015: 14; 2016: 18; 2017: 5). This concerned in total 11 countries (both EU and CIS states) during the period under consideration. In total, around 80% of the ML investigations commenced by the SP since 2013 currently appear to be pending. As Sec.377 CPL provides for the termination of the investigation, *inter alia*[76], when it can be established that a criminal offence has not taken place or not all elements of a crime can be proven, this may leave a large majority of investigations, in which a criminal offence can neither be established nor excluded, in a limbo.

169. The ratio between ML investigations and cases referred to the GPO during the same period is more positive with regard to the SRS FPD, which initiated 56 ML investigations (2013: 26; 2014: 15; 2015: 8; 2016: 7) and sent the same number of cases to the GPO (2013: 20; 2014: 18; 2015: 13; 2016: 5), despite not having a specialised unit for ML. The evaluators note that the number of initiated ML investigations by the SRS FPD has steadily decreased during these years, a trend which may however have recently reversed: during the onsite visit the evaluators were informed that at least 15 cases (out of an overall total of 162 cases) investigated by the SRS FPD in 2017 are also related to ML. Despite of these rather encouraging results, the SRS FPD representatives informed the evaluators that staff shortage, a high personal turnover and lack of opportunities to properly train newcomers negatively affect the effectiveness of its ML investigations. Investigations of ML are regularly referred to the prosecution in connection with predicate criminality. If the latter is committed abroad, the SRS FPD is involved in respective Joint Investigation Teams (JIT) with foreign counterparts.

[75] References to the year 2017 only concern the period until the end of the onsite visit (i.e. November 2017).
[76] Sec.377 CPL contains a number of reasons for closing an investigation (e.g. death of the suspect, statute of limitation, amnesty, missing mandatory application by the victim).

170. The GPO received during the period 2013-2016 in total 95 cases (2013: 43; 2014: 27; 2015: 17; 2016: 8), while transferring 50 cases to the criminal courts (2013: 17; 2014: 14; 2015: 9; 2016: 10), three of which were transferred by entering into an agreement with the accused. Prosecutors informed the evaluators that cases are rarely sent back to the LEAs for additional evidence. The numbers indicate that around half of the incoming cases are prepared by the prosecution for indictments to the criminal courts. There is a notable tendency of decrease for both incoming and outgoing cases for the prosecution during the period under consideration. The ratio slightly improved in 2016, presumably due to the lower number of cases received. However, some of the judges met onsite informed the evaluators that, in some adjudicated cases of predicate offences, ML evidence was not of sufficient quality to achieve a conviction.

171. The extensive workload of the prosecutors with regard to other offences is considered as an obstacle for effective ML prosecutions, which is recognised by Latvia itself in its NRA. The 451 prosecutors who worked in Latvia at the end of 2016 receive job trainings before their appointment and undergo subsequent training which is organised either by the Judicial Training Centre or the GPO. They also attend joint trainings for LEAs, prosecutors and judges. The training also devotes time to ML, such as in 2017 when participants sought to reach common understanding of the ML offence, and to discuss the required level of evidence and the threshold for a ML conviction. The FIU also provides AML/CFT trainings on a regular basis (around 13-14 times per year) for all AML/CFT stakeholders.

172. The large majority of ML investigations (75%) by all ML-investigating authorities is initiated on the basis of FIU reports (some of which may be issued after the criminal proceedings were initiated by the LEAs at its own initiative), which does however not contribute to more prosecutions. Especially in cases of ML investigations carried out by the SP, only 2% of ML cases initiated on the basis of FIU reports were later prosecuted, with an even lower number being finally adjudicated. The evaluators were informed that this was due to the overreliance by the prosecution and courts on the mental element of ML. It should also be recalled that FIU information cannot be used as direct evidence. In practice, it is then the ML cases investigated by the LEAs without prior STR which are prosecuted (while those cases triggered by the FIU appear to mainly qualify for non-conviction-based confiscation, see IO.8). Amongst those, the SRS FPD's ML cases (i.e. with fiscal predicate offences) prevail amongst all ML-investigating authorities. Table 15 below demonstrates the numbers of investigations commenced without a previous STR, as well as subsequent prosecutions and (final) convictions achieved on the basis of these investigations.

Table 15

	2013 - 2017 (second half)											
	ML Investigations by law enforcement carried out independently without prior STR			Prosecutions commenced			Convictions (first instance)			Convictions (final)		
	Cases	Natural persons	Legal persons	Cases	Natural persons	Legal persons	Cases	Natural persons	Legal persons	Cases	Natural persons	Legal persons
ML	184	127	43	61	128	NA	19	40	NA	23	36	NA

173. The SRS CPD representatives informed the evaluators, that they did not initiate any ML investigation as to date. The KNAB has no specialised ML investigators, but it is authorised to

conduct ML investigations if they are related to corruption and fall within the KNAB's jurisdiction. It regularly delegates cases by decision of the GP (e.g. a recent foreign bribery case) to the SP, which is considered to be more specialised in ML investigations, especially if there is no link of the predicate offence with a Latvian citizen, resident or company. The KNAB also occasionally investigates ML itself (three such investigations were reported in the past five years, with one leading to a prosecution). The evaluators note in this regard concerns expressed by the OECD Working Group on Bribery with regard to public reports about alleged long-term human resources management problems and a high staff turnover which calls into question the capacity of the body to deal with the most complex cases[77], even though this has been recently addressed[78]. Although representatives of KNAB met during the onsite visit did not confirm such concerns, the evaluators note that they, if substantiated, may also have negatively impacted on KNAB's ML investigation activities.

174. During ML investigations, LEAs are regularly focusing on the collection of evidence against legal persons. In the period 2013-2017 (first half), investigations which commenced without prior STR (184 cases) concerned 126 natural and 42 legal persons against whom the authorities investigated. The number of cases against legal persons submitted to the courts for imposition of coercive measures has steadily increased from 10 cases in 2015 to 25 cases in 2016 and 16 cases in the first 8 months of 2017.

Consistency of ML investigations and prosecutions with threats and risk profile, and national AML policies

175. The NRA highlights corruption and bribery, tax evasion, fraud and smuggling as the main threats for ML. The evaluators were provided with the information that there is a relatively high number of ML investigations for these criminal offences, but a much lower number of prosecutions (especially in the cases of fraud and smuggling) and an even lower number of convictions (especially for tax offences, corruption and bribery). According to statistics broken down by the predicate offences with regard to the adjudicated ML cases, the main ML convictions achieved have predominantly fraud, tax evasion, and embezzlement as predicate offences. Comparison between the number of convictions for these predicate offences (see below) and convictions for ML reveals that not only few cases led to ML convictions, but also that the focus of the Latvian authorities is still predominantly on the predicate offences. Among the predicate offences, criminal offences related to illegal drugs prevail, but only a small number of cases with significant amounts are investigated.

176. Latvia is a regional financial centre, with a majority of its commercial banks focusing on servicing foreign customers, mainly from the CIS. The vulnerability of CIS countries to economic crime, especially corruption, remains one of Latvia's key ML risks. According to the NRA a significant part of laundered proceeds are generated abroad, while domestic ML mainly pertains to self-laundering.

177. During the onsite visit, the prosecutors designated tax evasion and tax fraud crimes as the prevalent domestic predicate offences; corruption, embezzlement of state funds and cybercrime fraud were identified as the prevalent foreign predicate offences. Investigations of cases with

[77] OECD, *Phase 2 Report on Implementing the Anti-Bribery Convention in Latvia*, October 2015, paras. 121-125.
[78] Latvia: Follow-up to Phase 2 Report and Recommendations, published on 7 December 2017 http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/WGB(2017)74/FINAL&docLanguage=En

predicate offences committed abroad are usually initiated on the basis of FIU reports, whereas investigations of cases with predicate offences committed in Latvia are predominantly a result of the LEAs' own intelligence and operational activities. Overall, the number of prosecutions of ML does not appear fully commensurate with the identified ML risks of the country.

178. The above-mentioned key risks for ML were illustrated in recent high-profile international scandals, as media reported that Latvian FIs are suspected to have knowingly engaged in – and even encouraged – ML by their customers, through the use of complex international transfer schemes relying on the use of shell companies. There appears to be a recent rethinking by the authorities to investigate cases which correspond better to the country's risk profile. To a certain extent, the SP has investigated, or is still in the course of investigating, cases with regard to large-scale ML schemes committed by organised groups. However, the criminal liability of FIs allegedly involved in these ML schemes has not been sufficiently considered with regard to convictions for ML. While there is no data on these particular type of investigations, the following cases were reported by the authorities as anecdotal evidence:

"Versobank" case

179. In 2016, the SP commenced criminal investigations against an organised group which had opened without licence an office of the Estonian bank "Versobank", where ten employees allegedly transferred money with fictitious purposes, using bank accounts for shell companies registered in Latvia, a CIS country and offshore jurisdictions. The money was estimated to originate from that CIS country and to be proceeds of crime. In the absence of a registration, the office was not controlled by the authorities and was suspected of having provided services to its customers which was considered as ML. Convictions of both natural persons and the bank itself under Sec.207 CL ("Entrepreneurial activity without the permission from the state authorities") followed. The authorities submitted that currently three (natural) persons are under investigation with regard to ML under Sec.195 CL.

"*Bank shareholder*" case

180. In 2013, a Latvian court convicted a person for fraud and ML. The convicted person was the shareholder of a bank, its Vice-President and the Head of Regional Development Department. Between 2003 and 2006, he had exploited his position to defraud and misappropriate the bank customers in the amount of USD 5.5 million. Afterwards the funds were transferred to other bank accounts in foreign countries with the purpose of ML. A part of the fraudulently obtained funds in the amount of around EUR 1 million was laundered, but not yet used as it was previously seized. The accused was sentenced to a custodial sentence of 4.5 years, with confiscation of property. The seized criminal proceeds were returned to the victims.

"Krājbanka" case

181. Five suspects were prosecuted, including the bank's owner (a CIS country citizen) and the management of the bank, for ML, appropriation of assets to the value of EUR 90 million, exceeding their authority and violating bookkeeping regulations. The case is currently pending before the criminal courts. As a result, the bank became insolvent. In relation to its insolvency proceedings, there are legal proceedings concerning an organised criminal group involved in the insolvency proceedings.

"*Winergy - Norvik banka*" case

182. The case concerned a defrauding case in the form of state co-financing for construction of wind power stations that was handled by officials of "Winergy", as well as creating obstacles in the process of "Winergy" insolvency. The criminal investigation has been ongoing since 2013. The GPO took over the criminal proceedings for further investigation as they have a sufficient amount of evidence to declare one of the largest "Norvik banka" shareholders as the suspect for the illegal acquisition of bank's shares. It appears that the investigations also include ML. The case has been meanwhile transmitted to the criminal courts.

"Trasta komercbanka" cases

183. The authorities reported about several investigations related to the bank "Trasta komercbanka" (which started in 2014, 2015 and 2017, respectively). In 2014, the SP started investigations against employees from the bank for ML on a large scale and by an organised group (Sec.195(3) CL) regarding criminal assets derived from, *inter alia*, tax fraud from a CIS country. The investigations are ongoing (in cooperation with an EU member state and two CIS countries) and concern three employees of the bank, including a member of the board. The SP received in 2015 further information concerning employees of the bank and their alleged involvement with ML. On the basis of this information, criminal proceedings were initiated, two of the bank's employees were arrested, and 7 real estate objects were confiscated (to the amount of almost EUR 1.8 million and USD 4.3 million). In the meantime, the bank was liquidated; in 2017 the SP initiated criminal proceedings against several persons (lawyers and insolvency administrators, including the head liquidator) for having misappropriated approximately 1 billion EUR in the course of the liquidation process from bank creditors. The money was allegedly laundered through shell companies in both Latvia and another EU member state[79].

"Baltic International Bank" case

184. The SP received in 2016 information concerning the involvement of several current and former employees of the "Baltic International Bank" with an organised criminal group. The group's activities with regard to ML had taken place since at least 2012, by performing money transfers in mutually related and complex transactions without any economic or obvious legal purpose. Based on this, criminal proceedings were initiated and several persons involved in the case were arrested. The authorities further reported about investigations (in cooperation with colleagues from Austria and Belarus) on the laundering of funds appropriated from the state budget of a CIS country through bank accounts of offshore companies held in "Baltic International Bank".

Types of ML cases pursued

185. During the period 2013-2017 (first half), Latvia achieved 33 ML convictions in respect of a total of 55 natural persons: 8 convictions in 2013; 5 convictions in 2014; 12 convictions in 2015; 6 convictions in 2016, and 2 convictions in the first half of 2017, respectively. In 13 cases, the courts acquitted the accused persons from the ML charges, which amount to almost one-third of a total of 46 cases in which ML charges reached the trial-stage. Table 16 gives an overview of the different types of ML convictions achieved by the Latvian courts during this period.

[79] The authorities reported that the Prosecutor brought charges against six persons in this case shortly after the onsite visit (December 2017).

Table 16

	Total number of ML convictions (persons)	Number of convictions for self-laundering (persons)	Number of convictions for third party laundering (persons)	Number of convictions for laundering proceeds of crime committed abroad (persons)	Number of convictions for fiscal predicate offences (persons)	Number of convictions for non-fiscal predicate offences (persons)
2013	15	15	0	1	11	4
2014	10	10	0	6	7	3
2015	17	17	0	3	9	8
2016	9	9	0	1	8	1
2017 (first half)	4	3	1	4	0	4

186. The number of 33 ML convictions appears modest, especially when compared to the overall number of convictions obtained for predicate offences. This is also conceded in the NRA (p. 43). During the period 2011-2016, Latvian courts achieved the following number of convictions for the predicate offences which are most relevant for Latvia with regard to ML: fraud (1,109 convictions), smuggling (165 convictions), tax crimes (286 convictions) and robbery/theft (13,776 convictions). The authorities stated that one reason for the modest number of ML convictions is the cross-border nature of many ML schemes and the consequent reliance on (often delayed or otherwise hampered) international cooperation when investigating ML. However, this aspect alone would not explain the discrepancy between the high numbers of convictions for predicate offences and the modest number of ML convictions by the Latvian courts. Even though not all predicate offences may necessarily have had a ML-aspect, such gap rather indicates that ML has not been a priority for the Latvian judicial system in the past.

187. Table 16 above demonstrates that Latvia has obtained ML convictions for both foreign and domestic predicate offences. About one quarter of the persons convicted for ML during the period 2013 – 2017 (first half) where convicted for ML in respect of predicate offences which were committed abroad. The large majority of ML convictions concerned self-laundering, with only one third-party laundering conviction handed out by the Latvian courts in the past five years. This case concerned a conviction for ML together with convictions of several other persons for fraud. The evaluators were told that Latvia achieved one stand-alone conviction for ML in 2017 concerning (unspecified) predicate criminality committed abroad, which was however only possible because the convicted person made a full confession and no further proof of the underlying predicate criminality was needed. This one case, described by the authorities as a "money mule"-case, does however not serve as evidence that an autonomous ML conviction would be possible in Latvia if the accused is not pleading guilty.

188. Latvian legislation does not require that a person be convicted of the predicate offence when proving during a ML trial that the property is the proceeds of crime. In practice, there is however a noticeable dependence of prosecutions on the identification of the underlying predicate offence, despite the fact that the ML offence follows an "all crimes"-approach. Since the prosecution was required until recently to prove that the accused person had knowledge of the criminal origin of the laundered proceeds, it relied heavily on a (simultaneous) conviction for the predicate offence which is the easiest possibility to meet this benchmark. There is uncertainty among LEAs what evidence is sufficient to prove that the person knew of the illegal origin of laundered property. The evaluators were informed that in some instances the prosecutions or the courts in practice had required the

exact circumstances (e.g. place and time) of a specified predicate offence committed abroad in order to go ahead with a ML-case. The fact that only a few investigated ML cases were subsequently prosecuted and went to court underlines this uncertainty. It also explains the practical absence of any systematic convictions for stand-alone or autonomous ML cases, as prosecutors tend to investigate ML by focusing on predicate activity.

189. The evaluators were informed of a legislative change in August 2017 in the ML definition of Sec.5 AML/CFT Law, which is used by the courts to fill the "blanket norm" of the ML offence in Sec.195 CL which does not contain its own ML definition. This change, reportedly heavily advocated by the LEAs, introduces a lower threshold for the proof of the mental element (replacing the requirement of "knowing" the illegal origin of the laundered property with "being aware of or assumed", thus possibly criminalising also "wilful blindness"). The evaluators recognise that this change may to a certain extent relieve the prosecution from having to prove that the accused had beyond reasonable doubt knowledge of the illegal origin of the laundered property. Nevertheless, it is not fully apparent that such a change would mark a departure from the dependence on the predicate offence for ML prosecutions and convictions, and that the courts would be willing to convict an accused for ML in cases where the exactly-defined predicate criminality is not given. Some of the judges at the time of the onsite visit considered this legislative change as a significant amendment which would allow for the conviction for ML on the basis of circumstantial evidence, while other judges remained more sceptical about its future impact. Much depends on the manner in which the judicial stakeholders will interpret this new legislation, for example whether (gross) negligence or wilful blindness with regard to the origin of the laundered property would suffice for a ML conviction. For the purposes of the present report, this legislative change has in any event been too recent to produce tangible results in practice[80].

Effectiveness, proportionality and dissuasiveness of sanctions

190. CL provides for sanctions which are potentially proportionate and dissuasive: the basic ML offence remains punishable for a term not exceeding three years, with the possibility of aggravated sanctions (up to five years' imprisonment for the commission of ML by a group of persons; three to twelve years' imprisonment for the commission of ML on a large scale, i.e. for amounts exceeding EUR 19,000, or by an organised group). The criminal code also provides for confiscation of legally-acquired property, fines or other forms of punishment (e.g. temporary deprivation of liberty, community service). Table 17 below shows information about penalties which have been applied with regard to ML during the period 2013-2016:

Table 17 - Penalties applied by final judgments (by aggregation of criminal offence of Sec.195 CL)

	2013	2014	2015	2016
Total number of convictions for ML in force	8	5	12	6
Number of convicted persons for ML	15	10	17	9
Basic penalties – deprivation of liberty				
Number of suspended penalties	12	10	12	6
Deprivation of liberty up to 1 year	0	0	1	0
Deprivation of liberty from 1 to 3 years	0	1	2	0
Deprivation of liberty from 3 to 5 years	4	0	1	0

[80] In this regard, the principle *nullum crimen sine lege* would prevent the authorities to use the newly-amended ML definition in Sec.5 AML/CFT Law retroactively with regard to investigations commenced prior to August 2017, when the amendments entered into force.

Deprivation of liberty from 5 to 10 years	0	0	0	0
Deprivation of liberty from 10 to 20 years	1	0	0	0
Other basic penalties				
Fine	0	2	2	3
The average amount of fine (EUR)	n/a	5600	2400	9328
Community service	0	1	0	0
Additional penalties				
Confiscation of property	3	0	1	2
Police control	2	0	3	0
Limitation of rights	1	0	4	5
Forfeiture of the rights to carry out business activities	1	0	4	5

191. As ML is almost exclusively prosecuted together with the predicate offence, and a conviction for both the predicate offence and ML leads to an amalgamated sentence, it is naturally difficult to assess the sanctions imposed for ML in isolation. In those cases where convictions were achieved, sanctions imposed on natural persons however do not appear to be dissuasive or proportionate enough. This view was widely shared by the relevant authorities met onsite. During the period 2013-2017 (first half), 33 convictions for ML were handed out, involving a total of 55 persons. In only one instance did courts hand out a sentence in the upper range provided by the CL, although the range of sanctions allows for up to twelve years' imprisonment (and even more, if the sentences are amalgamated with other criminal offences). The average amounts of fines applied by the courts to natural persons in the eight cases during the period 2014-2016 varied between EUR 2,400 and 9,328, with fines applied in actual individual cases ranging from EUR 1,600 to 21,300. While the evaluators were not provided with statistical data on fines for comparable predicate offences, these ML-fines do not appear very dissuasive. Despite the possibility to restrict business activities as a penalty (which the courts made use of in 10 cases during the period under consideration), some representatives of the LEAs reported anecdotal evidence of cases where convicted persons, who had abused their legal profession for ML-purposes, had been able to exercise their profession already after a short period of time.

192. CL provides for the possibility to suspend a sentence if its duration does not exceed five years (Sec.55 CL), with the courts having to take into consideration the nature of the offence and the harm caused, the personality of the offender and the unlikelihood that another offence could occur. Given that ML convictions were usually within the lower scale of the possible sanctions, they were eligible for such suspension. In the large majority of cases in which courts pronounced a custodial sentence, these sentences were indeed suspended. This concerned 45 out of a total of 55 convicted natural persons, which amounts to a share of 82%. Although it is not known to the evaluators whether the use of suspension for ML sentences equals the use for comparable (financial) crimes, they are concerned that this high rate of suspended sentences impacts negatively on the effectiveness of sanctions. The NRA also describes scenarios in which courts would avail themselves to the exceptional possibility in Sec.49 CL to impose less severe sanctions then provided by the law, without a systematic practice by the prosecutors to appeal any convictions where the sanctions appeared too lenient.

193. According to the authorities, sentences for ML convictions are often suspended because the courts are taking into account the length of criminal proceedings as a mitigating factor.

194. The evaluators note that the main influential issue appears to be the length of the investigations for ML, with the authorities stating that investigations of cases of predicate offences and ML usually take 2-3 years, with another period of 6 months at the prosecution stage and the

court proceedings taking 2-3 years. Not knowing whether the pre-trial investigations for comparable predicate offences likewise lead to suspended sentences because of their length, the evaluators consider that ML investigations could be much more accelerated if sufficiently prioritised. In any event, even if the length of proceedings were to be considered routinely as a mitigating circumstance in the majority of ML convictions, it is not evident that this factor weighs so heavily that it should have resulted in the suspension of the large majority of prison sentences. The evaluators note in this respect that the legal basis for lowering the sentence (Sec.49 CL) does not make the suspension of sentences mandatory for judges. Instead, the length-factor could have also been appropriately taken into account by the courts through reduced sentences without suspension, which would have significantly increased the dissuasiveness of such sanctions.

195. During the onsite meeting the prosecutors told the evaluators that they consider the sanctions not to be strict enough, and they conceded that sometimes they are not active enough to achieve the conviction and imprisonment of the accused person. In 2016, the GP issued guidance for the prosecutors, instructing them to appeal the sanctions imposed at the first instance court and to demand stricter sentences. However, it was not evident that such guidance had in practice led to a systematic policy by the prosecutors to appeal lenient sentences for ML handed out by the courts.

196. The CL provides for a wide variety of coercive measures which may be applied against legal persons, which are of a punitive nature and which are followed by an entry into the penal register. These include liquidation, restriction of rights, confiscation of property and fines. The table below sets out the number of cases and types of coercive measures applied with regard to legal persons in Latvia for ML during the period January 2015 – September 2017.

Table 18

Year	**Number of legal persons against which a coercive measure have been applied**					
	Liquidation	Restriction of Rights	Confiscation	Fine		**Total number**
	Nr.	Nr.	Nr.	Nr.	Amount in EUR (average)	
2015	2	0	1	4	55,440	**7**
2016	4	0	0	5	304,889	**9**
2017 (until Sept.)	3	0	0	5	29,060	**8**

197. Fines or liquidation of legal entities are the most commonly applied measures. Legal persons are held liable for all possible offences stipulated by the relevant provision of the CL (Sec.70[1] of CL), i.e. for criminal offences committed in the interests or for the benefit of the legal person, or as a result of a lack of supervision or control. As fines vary considerably during the period 2015-2017 (ranging on average from broadly 30,000 to 300,000 EUR), it is difficult to draw a conclusion as to their dissuasiveness.

Alternative measures

198. Where a ML investigation has been pursued but where it is not possible, for justifiable reasons, to secure a ML conviction Latvia applies a number of other (criminal) justice measures. Latvia has achieved a considerable number of convictions for "Acquisition and disposing of property obtained by way of crime" under Sec.314 CL[81]. Case examples were provided by the

[81] Note that Sec.314 CL was amended in June 2017 as "Acquisition, storage and disposal of property obtained by way of crime". In order to avoid any overlap of this newly-structured offence with the ML offence in Sec.195 CL (and as defined in

authorities where the perpetrators had resold stolen goods (e.g. cars or petrol). The authorities also make frequently use of non-conviction-based confiscation (see in more detail, IO.8), although the evaluators do not consider that this use would by itself constitute a justifiable reason for not securing ML convictions in those cases. Moreover, the authorities informed the evaluators of some successful extraditions of both Latvian and foreign citizens to other countries for the purposes of ML trials. Persons were notably extradited to Germany for ML-related trials involving fraud (in particular through "phishing", i.e. the fraudulent obtaining of sensitive information) as a predicate offence, or on the basis of a European arrest warrant issued by other EU member states. In other cases (see case-example No.2 under IO.8), Latvia has dropped ML investigations at the request of third states which took over the criminal investigations.

Conclusion

199. Latvia has a sound legal system and a designated institutional framework that has the capacity to investigate and prosecute ML. The country has achieved a certain number of ML convictions in the five years prior to the onsite visit, which however appears modest when compared with the high number of convictions for predicate offences during the same period. Until recently, the judicial system of the country did not appear to consider ML as a priority and to approach ML in line with Latvia's risk profile as a regional financial centre. This appears to have lately changed to a certain extent, with some large-scale ML investigations underway, involving bank employees having actively facilitated the laundering of proceeds. While it is notable that the authorities now appear to take the investigation of ML which corresponds to Latvia's risk profile more seriously, the lack of ML investigations against legal persons in those cases suggests that major improvements are still required. ML convictions for both domestic and foreign predicate offences have been achieved. Latvia also demonstrated one conviction for third-party laundering and one conviction for stand-alone ML, the latter however being possible only because the accused made a full confession. Otherwise, prosecutors still rely on the existence of a predicate offence to meet the prerequisite of proving that the accused had the knowledge of the illegal origin of the laundered property. Legislation introduced to bring about change in this respect was too recent to produce tangible results in practice.

200. A mere fraction of ML investigations eventually leads to a conviction, and if so, the large majority of custodial sentences are deferred. Sanctions for natural persons appear neither dissuasive nor proportionate due to the frequent application of the legal possibility to suspend a custodial sentence of up to five years' imprisonment. Latvia is able to apply coercive measures provided by the CL against legal persons. The country also uses a number of alternative criminal measures where a ML conviction is not possible for justifiable reasons. Overall, the evaluation team considered that Latvia achieves to some extent the characteristics of an effective and coherent system to investigate, prosecute and convict for ML. However, major improvements as indicated in the report are needed. **Latvia has a moderate level of effectiveness for IO.7.**

Immediate Outcome 8 (Confiscation)

201. Overall, Latvia has a broad and sound legal system for confiscation of criminal proceeds. The country has a two-tier confiscation system which involves both conviction-based and non-conviction based confiscation. Both confiscation regimes apply in principle to natural and legal

---

Sec.5 AML/CFT Law), the legislator decided that Sec.314 CL should only apply to minor cases (i.e. up to a threshold of approximately EUR 3,800) and thus be punishable by one year imprisonment as a maximum term.

persons. Sec.42 CL provides for confiscation of property as a penalty imposed upon a conviction – which relates only to legally-acquired property - if the particular criminal offence expressly provides for this (which is the case for the ML and FT offences in the CL). Other provisions (Sec. 355-369 CPL) deal with the confiscation of criminally-acquired property which is mandatory. With regard to the latter, a recent amendment in June 2017 to the CL (Sec.70[11] CL) has introduced a shift of the burden of proof for criminally-acquired property: if the value of a certain property is disproportionate to the person's income and the latter cannot give a legitimate explanation, that property can be considered criminally-acquired (and thus subject to confiscation) if the person has committed an economic crime, is member of an organised group or has links to terrorism. Prior to the change of legislation in cases of (most of) the economic crimes, the Latvian authorities had to prove that certain property is of criminal origin, except for cases prescribed by law (committed in an OCG etc.). The previous legislation had a negative impact on the confiscation of property in ML cases which were not committed in an organised group, as the prosecutors were obliged to prove the criminal origin of certain property.

202. Latvian law provides for the possibility of non-conviction-based confiscation. This is a procedure which can be separated from criminal proceedings if the transferal of a criminal case to a court is not possible in the near future or would cause substantial unjustified expenses (Sec.626 CPL), but there is sufficient evidence that assets previously seized amount to proceeds of crime. In this case, it is merely necessary to demonstrate that there are reasonable grounds to believe that the property concerned has been criminally-acquired or is related to a criminal offence. The Constitutional Court of the Republic of Latvia has confirmed the constitutionality of this CPL provision with regard to non-conviction-based confiscation[82]. Authorities stated during the onsite visit their opinion that non-conviction-based confiscation has an important preventive effect, clearly demonstrating that "crime does not pay off". If property is identified, in the vast majority of cases a decision to initiate separate non-conviction-based confiscation procedures is made.

203. Since in Latvia the length of criminal procedures, including at the pre-trial stage, usually extends to several years, and since according to Sec.389 CPL restrictions of rights of persons are limited to a maximum time period not exceeding 31 months for especially serious crimes, non-conviction based confiscation enables state authorities to settle the property issues in due time and confiscate it or return it to the owner or lawful possessor. The non-conviction-based confiscation procedure is a clear priority recognised by all LEAs. It is to a certain degree understood as an alternative measure to criminal proceedings, which can compensate for difficulties with the standard to prove the existence and defendants' knowledge of a (foreign) predicate offence.

204. Apart from the freezing and confiscation powers of the LEAs, the FIU has the right to issue binding orders regarding freezing of funds if there are substantiated suspicions that a criminal offence is being committed or has been committed, including ML and FT. In practice, the FIU is using these powers actively and on a regular basis. As its freezing orders have a certain time-limit (45 days), the FIU informs the LEAs on a regular basis to initiate criminal proceedings and apply the freezing measures on the basis of the CPL (requiring the decision by an investigative judge).

[82] Note however that, according to criminal procedural law (Sec.629(5) CPL), a person affected by a non-conviction based confiscation-decision to seize/freeze assets could not challenge before the courts the decision (taken by the person leading the proceedings) to not grant her/him access to the case-file. The Constitutional Court of Latvia recently ruled that this provision was not compatible with the fundamental rights as laid out in the Latvian constitution. In February 2018, the Latvian Parliament introduced into the CPL a right to appeal a decision to deny access to the case file, in order to implement the judgment of the constitutional court.

Confiscation of proceeds, instrumentalities and property of equivalent value as a policy objective

205. There is no nationwide-coordinated confiscation policy in Latvia[83]. Authorities usually see the applicable rules of the CPL as their guiding principles for seizure and confiscation. The SP prepared an (internal) administrative management task document focusing on the gathering of financial intelligence information and encouraging the investigators to look for assets, if an investigated crime is related to property. It appears that authorities regard the pursuance of confiscation of criminal proceeds as a worthy and achievable goal in itself, and as one of the main priorities for the fight against economic and organized crime. This is underlined through letters by the MoI, copies of which were made available to the evaluators, to the chiefs of the SP and the heads of the regional boards of the SP in June 2017, underlining the importance to take measures within the operational activities and the criminal proceedings to find property-related to crime. The country has been criticised in other contexts for unduly prioritising seizure and confiscation of proceeds of crime over pursuing ML as a criminal offence[84]. The vast majority of provisional measures relates to financial assets and is triggered by reports from the FIU.

206. Latvia has a sound legal asset-management system (i.e. general provisions of the CPL and Governmental Regulation No. 1025), but lacks specialised staff trained on sophisticated assets (such as, for example, company shares). The country has been able to order provisional measures in rather unusual cases and to provide practical arrangements on an individual basis, such as the seizures of dogs which were accommodated in a private shelter. It appears that the LEAs are looking for illegal property and prosecutors take respective decisions on a case-by-case basis, and that parallel financial investigations are not routinely performed.

207. The SP (which investigates 95% of all the COs) has an internal asset recovery program. By the end of 2016, an ARO was created as a separate unit in the SP's Criminal Intelligence Management Board. The ARO, whose basic function is the search for, identification and recovery of criminal proceeds, has currently 5 staff members, with more vacancies foreseen for the future. The ARO envisages a more active involvement in criminal investigations (subject to future amendments of the CPL). Representatives from the office considered their work as very effective due to highly-developed databases.

208. Until the onsite visit, the ARO had already provided support and assistance in 73 cases (22 domestic and 51 international cases). The low number of national cases may indicate that investigators are either still looking for property on their own or they are not sufficiently focusing on asset recovery. With the assistance of the ARO, property can be identified in a more effective way and in a timely manner. The SRS FPD uses the assistance of the ARO when looking for property in foreign countries. The ARO is seeking to identify all kinds of proceeds, including bank accounts, immovable property, legal entities, vehicles, ships, aircraft, tax payments, etc. Relatives of the suspected person are regularly included in the financial investigation. Around 90% of assets are however held by banks, in line with Latvia's position as a transit country for financial flows which requires rapid action. The ARO collaborates closely with the FIU with regard to financial

[83] The SP, in cooperation with GPO started developing in autumn 2017 special guidelines on ensuring confiscation of the illegally obtained assets during pre-trial investigation. The aim of the guidelines is to elaborate a common approach on ensuring identification, arrest and confiscation of the illegally obtained assets, foreseen in Sec.70.[11] CL, during pre-trial investigation.

[84] OECD, *Phase 2 Report on Implementing the Anti-Bribery Convention in Latvia*, October 2015, para. 240.

investigations. It sees its particular comparative advantage in the capability to carry out complex analytical work in a short period of time, has access to various national databases (motor vehicles, land register, company register etc.) and uses all kinds of available special investigative techniques in practice.

209. In general, the SP considers that so few cases result in prosecutions (and related confiscation-proceedings) is mostly due to the increasing international elements of ML-related cases. The office uses established links with the Camden Assets Recovery Interagency Network (CARIN), but ARO staff members met by the evaluators conceded that the cooperation could still be augmented due to the very recent establishment of the ARO. On the other hand, it reported very good cooperation with the prosecution; the latter however appeared to consider the ARO in the first place as a support for the police investigative work, which may leave some room to develop further synergies.

210. The SRS FPD freezes assets in about 80% of the cases in which it is notified by the FIU. It takes around 15 decisions per year on confiscating financial means, which are recognised as criminally obtained and transferred to the State budget. The amounts have varied in recent years between around EUR 435,000 and EUR 1 million. The evaluators were informed that adequate resources for the SRS to perform its functions are lacking (see IO.7).

211. Latvia is in the course of introducing a system according to which confiscated proceeds of crime are utilised in a "confiscation fund" to reinforce the fight against economic crime. Confiscated proceeds may thus be used to fund training, the purchase of technical equipment or other measures[85]. The recently-adopted "Law on Enforcement of Confiscation of Criminal Proceeds", which entered into force in August 2017, supplements Latvia's legal framework to avoid situations in which the courts order confiscation in amounts which exceed the actual confiscated amounts achieved later.

Confiscations of proceeds from foreign and domestic predicates, and proceeds located abroad

212. Non-conviction-based confiscation brought some remarkable results, enabling Latvian authorities to confiscate considerable amounts: almost EUR 2 million in 2013, more than EUR 16 million in 2014, more than EUR 25 million in 2015, almost EUR 60 million in 2016 and EUR 36 million in 2017. In contrast to this, ML convictions-based confiscations are rarely achieved and as a trend the number of cases and the amount of convictions-based confiscations are decreasing since 2013 (2013: 3; 2014: 1; 2015: 2; 2016: 2). As the table below demonstrates, the amount of confiscated assets through non-conviction-based confiscation (approximately EUR 137 million) exceeds by far the amounts achieved through conviction-based confiscation (approximately EUR 4.2 million) for ML cases.

Table 19 - Property frozen, seized and confiscated[86]

2013 - 2017 ½								
	Property frozen		Property seized		Property confiscated		Property recovered following conviction	
	Cases	Amount (EUR)	Cases	Amount (EUR)	Cases	Amount (EUR)	Cases	Amount (EUR)
ML – Conviction- based	NA	NA	NA	NA	NA	NA	28	4.234.038,16
ML-non-conviction-based	588	186.694.377,21	186	NA	162	105.409.791,82	NA	NA
Underlying predicate offences where applicable	142	Evasion of Taxes	NA	NA	NA	NA	18	Evasion of Taxes
ML Total	588	186.694.377,21	186	NA	162	105.409.791,82	28	4.234.038,16
FT – Conviction- based	NA	NA	NA	NA	NA	NA	0	0
FT-non-conviction-based	2	431,64	0	NA	0	0	NA	NA
FT Total	0	0	0	NA	0	0	0	0

were confiscated. The Latvian authorities later submitted that another EUR 34.66 million were confiscated in the second half of 2017.

213. Latvia also provided statistics for the period 2016-2017 for confiscation with regard to predicate offences. During that period, the overall amount of EUR 97,350 was confiscated in a total of 95 cases (including cases were property was returned to victims). With the shift of the burden of proof for criminally-acquired property only introduced to Sec.70[11] CL for all proceeds-generating crime in June 2017, these numbers suggest that conviction-based confiscation was previously hampered by evidentiary requirements to prove the criminal origin of the property. Compared with the high number of convictions for predicate offences (as referred to under IO.7), the above amount does not suggest that conviction-based confiscation was applied on a regular basis. The absence of routinely-performed parallel financial investigations (as likewise indicated under IO.7) to trace the proceeds of crime from an early stage of the investigations may also be a factor that weighs negatively on the effectiveness of conviction-based confiscation results

214. The precondition to initiate non-conviction-based confiscation is prior seizure of property or imposition of an attachment on property. As already indicated under IO.6, the FIU is very (pro)active in issuing freezing orders against assets (funds), and the majority of the decisions by the Prosecutor to confiscate were based on investigations commenced through FIU information and freezing orders. The FIU does not seize other kinds of property, for instance immovable property. But in these cases, the FIU recommends performance of additional actions to the SP. In almost all the cases criminal proceedings and parallel non-conviction-based confiscation procedures were initiated upon the FIU's case materials (53 out of 57 cases in 2016), including several major cases which were reported to the evaluators on the basis of anecdotal evidence. In these cases, the authorities managed to confiscate considerable amounts of criminal proceeds. These are described in the following paragraphs.

215. Case No. 1: The SP reported about a non-conviction-based confiscation in Latvia in 2015 concerning funds in the amount of around EUR 70 million owned by a high-level official from a CIS country and the use of Latvian bank accounts of companies registered in that country. The confiscation took place with the cooperation of the FIU which provided the financial information on which the measures were based. Despite difficulties in international cooperation (with regard to interviewing witnesses and other stakeholders resident abroad) and the political element of the case, a court ordered the non-conviction based confiscation. However, authorities informed the evaluators that the sharing of the confiscated assets was not possible for reasons beyond Latvia's control.

216. Case No. 2: In 2013 a group consisting of several persons from Lithuania defrauded the US-based company Google in the amount of more than USD 23 million by setting up a limited liability company with the same name as a popular Asian computer equipment producer and using it for "phishing purposes". The persons attempted to launder the financial assets through the banking sector of Latvia. The FIU issued a report (and initially issued a freezing order) on the basis of which the authorities managed to trace, freeze and confiscate the funds. The funds were subsequently returned to Google. The main actor of the organised group, a Lithuanian citizen, has been extradited by Lithuania to USA to await criminal prosecution. The US LEAs have submitted a request to take over the criminal proceedings which had initially been commenced in Latvia. The request appears to have been granted by the Latvian authorities.

217. Case No. 3: In 2015, the authorities received information about a bank (Trasta Kommercbanka) employee's collusion with money launderers. The bank employee being arrested,

the authorities confiscated seven real estate objects in the amounts of EUR 1.8 million and USD 4.3 million (see IO.7).

218. In general, Latvia's sharing of confiscated assets and/or restitution to victims in third countries depends on bilateral or multilateral agreements with third countries, with the MoJ being the competent authority. If the victim is a foreign citizen, the confiscated assets may be sent to the victim's country for repatriation. In practice, Latvia was on one hand able to demonstrate effective repatriation of large amounts of confiscated proceeds of crime (see above, case example No. 2). On the other hand, the authorities admitted that in other high-profile cases (see case example No. 1) repatriation or asset-sharing was in practice not possible (although this may sometimes be due to obstacles which are beyond the Latvian authorities' decision-making competencies). On the basis of anecdotal evidence, the evaluators were also provided with examples in which significant sums (e.g. EUR 4.5 million; see case example under IO.7) had been returned to the victims at national level.

219. Latvia also is capable to confiscate instrumentalities and property of equivalent value, although no separate statistics are kept which would allow an assessment on the effective confiscation in this regard. The investigators usually seize everything that is in the possession of the suspected person that can be useful as forensic evidence. Mobile phones and computer are returned to the possessors after examination. Items which may be used as evidence are seized and are not allowed to be sold prior to a court decision. If bigger items are seized, problems with storage space and costs of storage reportedly occurred. Latvian law provides for the possibility of selling seized property or instrumentalities before the finalisation of the criminal proceedings, e.g. if their value deteriorates with time and creates losses for the state. To a certain extent, the confiscated property of equivalent value is also repatriated to or shared with other countries.

Confiscation of falsely or undeclared cross-border transaction of currency/BNI

220. Latvia has borders with two EU member states (Estonia and Lithuania) as well as with Belarus and the Russian Federation. The country has currently two major international airports (Riga and Liepaja) and about nine sea harbours/ports. For the transportation of cash and bearer negotiable instruments (BNIs), Latvia has introduced a declaration system in line with the EU control system (see R.32 in the TC annex). The authorities met onsite were aware of the potential ML/FT risks of cash couriers, with smuggling being identified in the NRA as one of the prevailing predicate offences for ML. They use strategic analysis, trained dogs and other specialised measures (e.g. scanners). In practice, FT risks were not identified. With regard to ML, authorities suspect that professional launderers stay deliberately below the threshold for cash declarations and use individual "money mules" without previous criminal background.

221. The Customs Department of the SRS (SRS CD) receives approximately 700 cash declarations per year (incoming and outgoing). Until the onsite visit, 25 undeclared cash transactions had been detected in 2017 (with a total amount of 504,000 EUR). 41 undeclared transactions were detected in 2016 (total: EUR 1,337,000); 8 in 2015 (total: EUR 333,000); 19 in 2014 (total: EUR 422,000) and 33 in 2013 (total: EUR 817,000). If cross-border cash/BNI transactions concerning an amount exceeding 50 minimum wages (EUR 19,000 in 2017) are not or falsely declared, the SRS CD initiates administrative procedure and seizes the undeclared cash/BNIs. The cash is deposited into a special account of the State Treasury. The SRS CD then immediately transfers the case to the SRS CPD which is responsible for criminal offences related to the customs sector. If the amount exceeds EUR 10,000 but is below EUR 19,000, criminal proceedings are initiated only if the person cannot reasonably explain the legal origin of the cash/BNI.

222. On that basis, criminal proceedings were initiated in 48 cases in the past four years (2014: 3 cases; 2015: 4 cases; 2016: 33 cases; 2017: 8 cases), with a total of EUR 1,8 million seized. To a very large extent, currencies were seized (mostly USD and EUR) from predominantly foreigners importing cash from CIS countries. The small number of Latvian citizens concerned were further scrutinised by the SRS. In a case arising from a (later unconfirmed) FT suspicion due to the entry of a foreigner from a high-risk third country, the SeP was informed.

223. The authorities consider that the majority of illegal cash derives from smuggling, tax evasion and corruption[87]. The major obstacle to its confiscation is the need to demonstrate that the seized cash was derived from criminal activity. This is regardless of whether the investigations have the ML offence (Sec.195 CL) or the offence of "Avoidance of Declaring of Cash" (Sec.195[2] CL) as a basis, as the latter also requires the proof that the undeclared cash resulted from criminal activity. In all of the 48 cases of falsely or non-declared cross-border movements of cash and BNIs for which criminal proceedings were initiated, no confiscation of illegal property was ordered because the prosecutors were not able to prove the illegal origin of cash.

224. The evaluators note that new legislation (Sec.70[11] CL) has introduced in June 2017 a reversed burden of proof to recognise confiscated property as illegally acquired if it is disproportionate to the legitimate income of the person and the latter does not prove a legitimate source. However, the provision also requires full proof that the person concerned has either committed a financial criminal offence, is a member/abetter of an OCG or is connected to terrorism. The authorities met onsite consequently were doubtful whether this legislation (which was introduced too recently to produce tangible results) may bring any positive changes. The evaluators would encourage the authorities to test the new legislation with regard to its evidentiary threshold. Moreover, the possibility of fully reverting to non-conviction-based confiscation should be further explored in these cases. As non-conviction-based confiscation only requires demonstration that there are reasonable grounds to believe that the property concerned has been criminally-acquired or is related to a criminal offence, this lower evidentiary threshold could be overcome in at least some of the cases in which there appears to be a manifest inconsistency between the amount of undeclared cash and the legitimate income of the person concerned.

225. In the vast majority of the above-mentioned 48 cases, the necessity to demonstrate that a criminal offence had been committed still remained with the authorities, which have difficulties to meet this standard. In particular, no ML/FT offences were established. The only possibility to verify the origin of seized incoming cash is international cooperation, which is said by the authorities to be often hampered by inadequate responses from foreign counterparts (mostly CIS countries). Therefore, the initially-frozen assets in the amount of approximately EUR 1.8 million had to be returned to the original possessors. Consequently, only administrative sanctions were applied. Although in 2014 the maximum level of administrative sanctions for undeclared cash was raised from EUR 280 to 5% of the undeclared amount, the evaluators consider that this ceiling is still not dissuasive enough. The technical deficiency that Latvia, as a member of the EU, does not perform controls of cash on the inside borders with other member states, also weighs negatively on the effectiveness of the AML border-control system.

[87] The authorities are wary of potential collusion between criminals and customs officials. In the very few cases in which this was detected, criminal investigations by the Financial Police were commenced and disciplinary measures taken against the customs officers concerned.

226. Overall, even though Latvia has implemented the EU framework to register cross-border cash and BNI declarations for "non-EU borders", this has neither led to any cases of ML/FT investigations nor to corresponding confiscation. In this regard, the evaluators recall that a comprehensive analysis of potentially illicit cross-border flows has not yet been undertaken by Latvia (see above IO.1).

Consistency of confiscation results with ML/TF risks and national AML/CTF policies and priorities.

227. The authorities are actively freezing and seizing illegal property, especially bank account assets, which resulted in some high-profile cases with considerable amounts of confiscated illegal property. To a certain extent, the confiscation results appear to reflect the assessments of ML/FT risks. In particular, tax evasion offences (which are identified as a risk in the NRA) led frequently to a confiscation of property, both in ML-related cases of non-conviction-based confiscation and ML conviction-based confiscation. On the other hand, the statistics for seizure and confiscation do not appear to fully mirror the greatest risk for Latvia as a regional financial centre, whose banks reportedly have in the past been frequently used to launder proceeds of corruption and other economic crime from third countries. It appears that although the ML-related cases of non-conviction-based confiscation enables Latvian authorities to confiscate illegal property of foreign origin and without determining a certain predicate offence, tax evasion - as a typical domestic predicate offence in Latvia - still prevails. In order to reach the characteristics of an effective system to a large extent, the evaluators would have expected from Latvia to demonstrate even stronger confiscation results in line with the ML risks the country faces.

Conclusion

228. Overall, Latvia has a broad legal and sound system for confiscation of criminal proceeds, which is based on two pillars (conviction-based and non-conviction-based confiscation). Results from conviction-based confiscation are hampered by previous evidentiary requirements to demonstrate the criminal origin of the property, the absence of routinely-performed parallel financial investigations and the modest number of ML-convictions achieved through the judicial system. On the other hand, non-conviction-based confiscation brought some encouraging results, enabling Latvian authorities to confiscate considerable amounts in both domestic and international cases. The large majority of cases of non-conviction-based confiscation are triggered by reports from the FIU.

229. The authorities regard the pursuance of confiscation of criminal proceeds as a worthy and achievable goal in itself and have made it one of the priorities in the judicial ML system. With the assistance of the recently-established ARO, property can be identified in a more effective way and in a timely manner. Latvia does not have an asset management system with specialised staff trained on sophisticated assets. In individual cases, Latvia is able to demonstrate effective repatriation of large amounts of confiscated proceeds of crime to third states, as well as in a domestic context the restitution of victims of economic crime.

230. Latvia has not been able to demonstrate an effective system of confiscation of undeclared or falsely declared cross-border movement of currency and bearer negotiable instruments. Given that smuggling is identified as one of the main ML risks in Latvia, the lack of effectiveness raises concern. This is mostly due to the difficulty to meet the evidentiary threshold that the undeclared or falsely declared cash/BNIs result from a criminal activity. Consequently, no corresponding ML or FT investigations have resulted from the implementation of the respective EU framework to

register cross-border cash and BNI declarations, which in any event only applies to borders with non-EU member states.

231. The authorities are actively freezing and seizing illegal property, especially bank account assets, which resulted in some high-profile cases with considerable amounts of confiscated illegal property. In order to reach the characteristics of an effective system to a large extent, the evaluators would however have expected from Latvia to demonstrate even stronger confiscation results in line with the ML risks the country faces. **Latvia has a moderate level of effectiveness for IO.8.**

CHAPTER 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

Key Findings and Recommended Actions

Key Findings

IO.9

- Latvia has undertaken an assessment of its FT risks on two occasions, in 2010 and 2014, and has shown some awareness of key FT threats. However, the absence of a comprehensive FT risk assessment that accounts for Latvia's role as a financial hub presents a major deficiency in Latvia's effective implementation of IO.9. Without a thorough understanding of how its broader financial vulnerabilities expose Latvia to exploitation by terrorist actors, the country cannot provide a systematically effective response to FT risks.
- The SeP appears to be both empowered and enabled to identify potential terrorism and FT risks emanating from within Latvia.
- Latvia does not have a national counterterrorism or CFT strategy, instead incorporating CFT elements in other strategic policies. Latvian authorities are capable of cooperating to investigate cases of FT, but do not have a single platform for obtaining information on FT-related matters across all relevant agencies. Interagency awareness and cooperation has not been shown to suffer as a result, but could be enhanced. The Counterterrorist Centre Advisory Board does not include a representative from the MoF, potentially limiting opportunities to address FT threats and risks from a systemic financial perspective.
- Latvia has not yet achieved any prosecutions or convictions specifically for FT, while it has had a handful of terrorism-related investigations. This absence appears consistent with Latvia's internal threat level, if not necessarily its FT risk profile. The country is largely able to demonstrate the application of alternative measures to disrupt potential FT activities.

IO.10

TFS

- The legal basis for FT-related TFS is complex and exhibits serious uncertainties and gaps. Although there is no evidence they have allowed for evasion of FT-related TFS, these shortcomings could have an impact on the effectiveness of that regime, as they necessarily limit the authority to regulate, monitor and sanction breaches of TFS obligations. Critical elements of uncertainty include: the scope of the funds to be frozen, which may result in a restrictive interpretation of the freezing obligation by the authorities and the REs; the scope of the persons required to comply with the freezing obligation; and Latvia's ability to issue a permanent freezing order. The EU regime also does not allow the implementation of FT-related TFS "without delay".

- Some aspects of a TFS regime however appear to be in place, including domestically enforceable EU regulations; adequate list communication mechanisms; regular guidance and outreach to REs; some awareness demonstrated by most REs; and indirect evidence of effectiveness offered by cases of false positives, of freezing under other sanctions regimes, and the autonomous designation for TFS of an individual (although not related to FT).

- The FCMC cannot issue binding regulations pursuant to the Law on Sanctions, which prevents it from imposing enforceable requirements on FIs to take specific steps against evasion. The AML/CFT law does not allow the FCMC to issue binding specifically FT-related TFS compliance measures. Most supervisory bodies of DNFBPs do not conduct inspections for TFS. The BoL and the Chamber of Notaries appear to only verify the existence of screening tools, without looking into entities' efforts to identify potential involvement in sanctions evasion, such as transactional monitoring.

- The potential implications of these gaps are made more difficult to assess by Latvia's lack of a proper FT assessment. No evidence of exploitation by persons designated for terrorism was identified. However, cases of sanctions evasion in other areas, as well as large numbers of foreign shell companies and deficiencies in the effectiveness of CDD measures (IO.4) suggest a certain vulnerability to FT sanctions evasion.

NPOs

- There has been no specific assessment of the risks of FT abuse in the NPO sector, although there has been at least one organization linked to an FTF.

- Very limited targeted outreach has been conducted towards the NPO sector.

- However, the sector appears to be proactively monitored by a number of competent authorities, which seems to mitigate the potential risks of FT abuse. Latvia's tax authorities monitor the sector based on substantial registration/reporting requirements and scrutiny for tax objectives. The SeP also closely monitors the sector for threats to national security.

IO.11

- Large numbers of foreign shell companies, deficiencies in the effectiveness of CDD measures (IO.4) and limited penalties imposed to date, among other factors, create a permissive environment for sanctions evasion, as demonstrated by the exploitation of Latvian banks for the purposes of circumventing PF-related sanctions, as exposed in 2017.

- The significant uncertainties and deficiencies in the legal basis noted under IO.10 are valid for IO.11, and appear more acute in relation to PF, which is less clearly covered in the AML/CFT Law. These shortcomings may have an impact on the effectiveness of the PF-related TFS regime, as they necessarily limit the authority to regulate, monitor and sanction breaches of TFS obligations.

- The detection of sanctions evasion schemes resulted in enforcement actions in June-July 2017, an autonomous Latvian PF TFS designation, additional guidance to the financial sector and the implementation of improved internal control programmes by banks. Against a backdrop of considerable vulnerability, these efforts reflect progress at the very end of the period under assessment. At the same time, it must be considered that: (i) the requisite information in these cases was provided by a foreign partner; while acted upon, it is unclear whether such a scheme could have otherwise ever been detected; (ii) no form of sanctions were imposed for breaches of TFS obligations, although facts may have qualified for such under the FATF Standards; and (iii)

sanctions imposed for AML/CFT deficiencies were not proportionate or dissuasive such that evasion activity appeared to continue in at least one bank.

- The FCMC cannot issue binding regulations pursuant to the Law on Sanctions, precluding it from imposing enforceable requirements on banks to take specific steps against PF sanctions evasion. Accordingly, it cannot require FIs to adopt specific compliance measures against identified PF typologies. The AML/CFT law does not allow for specifically PF-related compliance measures.

- FIs and to a lesser extent DNFBPs have a general understanding of PF TFS. Banks' high level of awareness expressed during meetings may still be a recent consequence of the abovementioned FCMC's enforcement actions. The predominantly basic screening approach, which is followed by most REs, is insufficient in the context of the evasion schemes used by proliferant actors and agents. Limited transactional monitoring and deficiencies noted under IO.4, coupled with persistently high levels of shell companies, limit the ability to detect and report potential PF activity.

- Latvian supervisors other than the FCMC engage in limited to no supervision for PF-related TFS, which due to lack of resources and gaps in the legal basis.

- Latvia's export control committee is not directly connected to all main counter-PF authorities (the FIU and FCMC in particular).

Recommended Actions

IO.9

- Latvia should conduct a risk assessment focused on FT vulnerabilities inherent to its role as a regional financial centre, including with regard to specific financial products and services, and taking into account continued risks resulting from its high concentration of foreign shell company customers and related FT threats.

- Interagency awareness of pending FT investigations or reviews could be enhanced, which could be achieved by a common platform housing current information on terrorism-related investigations and information held by various Latvian authorities (including the SeP, FIU, FCMC and SRS). Moreover, expanding the Counterterrorist Centre Advisory Board to other key players with regard to FT considerations (e.g. the MoF) could lead to a more systematic recognition of FT risks.

IO.10

TFS

- Latvia should urgently conduct an in-depth review of the legal basis for the implementation of TFS in the country, with a view to ensuring consistency between the relevant pieces of legislation, a clear legal basis for the exercise of respective competent authorities' responsibilities, the capacity to impose permanent freezing orders, and the scope of the freezing obligations, with a view to ensuring full compliance with the FATF Standards.

- Latvia should ensure adequate coverage of TFS obligations in all supervisors' inspection programmes, with the necessary resources.

- The recommended assessment of FT risks in the country should include a specific component on FT TFS evasion risks.

- Outreach and the provision of training should be reinforced towards all REs, including with a view to promote transaction monitoring for TFS evasion risks.

NPOs

- Latvia should conduct specific assessment of the risk of FT abuse in the NPO sector, as informed by a broader FT risk assessment (see IOs 1 and 9), with a view to developing and implementing a FT risk-based approach to monitoring the sector.

IO.11

- As noted under IO.10, Latvia should review its legal basis for TFS, to correct the deficiencies identified in the TC Annex. As a priority, Latvia should amend the Law on Sanctions to allow the FCMC to issue binding regulations in relation to TFS.
- Supervisory authorities should allocate adequate resources and priority to PF related TFS compliance supervision.
- Latvia should increase outreach to and eventually regulation of REs to develop and institute internal control systems capable of detecting potential PF activity, taking into account developments in efforts at PF sanctions evasion and Latvia's PF vulnerabilities.
- Latvia should consider linking the export control committee to the FIU and financial supervisors.

232. 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.5-8.

Immediate Outcome 9 (TF investigation and prosecution)

Prosecution/conviction of types of TF activity consistent with the country's risk-profile

233. Latvia considers that its risk of terrorism and FT is low, based on its assessment of both a low threat level and a low level of vulnerability, despite the broader vulnerabilities in its financial sector. The most concrete type of threat Latvia faces is that posed by radicalised converts, who Latvia sees as more vulnerable to incitement and recruitment by foreign contacts. Between 2012 and 2016 there were at least four confirmed cases of such persons traveling to Iraq/Syria, with the SeP reporting and other sources documenting that some of these individuals trained in terrorist camps, engaged in fighting, and provided support to terrorist groups, as well as distributed terrorist propaganda in Latvian.

Case of Oleg Petrovs

In June 2014, Oleg Petrovs, a convert to Islam who studied in Saudi Arabia for several years, became head of the Latvian Islamic Cultural Center (LIKC), an association devoted to maintaining the Riga mosque and providing a community for Muslims. Petrovs paid considerable attention to promoting the faith and was an active organiser for the LIKC, his leadership burnished by his time spent abroad. During this time, he spoke out against terrorist acts.

Petrovs served as head of the LIKC for approximately one year before abruptly leaving for Syria. In early 2016, Petrovs appeared in a propaganda video calling on Latvian Muslims to join ISIS in Syria/Iraq and renouncing his previous condemnations of terrorism. Later that year he spread other ISIS propaganda materials translated into Latvian and allegedly retained influence among certain segments of Latvia's Muslim community. Petrovs has been referred for prosecution, but not apprehended, and his activities are under continued investigation. His current whereabouts are unknown.

234. Latvia has investigated the financing dimensions of these cases, but has not brought FT prosecutions or convictions. This is due to the absence of the relevant individuals from Latvia (aside from one case, discussed below), and the apparent "lone wolf" nature of their activities, which Latvian authorities found to be self-funded. Beyond these cases, Latvia observes that no terrorist groups or recruitment networks have been discovered, and no terrorist attacks have been committed, on its territory.

235. It cannot be concluded that Latvia's broader FT risks are low, or that its FT prosecutions and convictions are commensurate with its risk profile. This is because Latvia has not adequately considered the FT risks associated with the vulnerabilities in its financial system or its broader AML/CFT regime. Specifically, as discussed in IO.1, Latvia has not fully analysed its risk in the context of the vulnerability to FT threat inherent to regional financial centres in general. Nor has it conducted such analysis in relation to specific financial products or non-financial services known to be vulnerable to terrorist exploitation such as cash (e.g. cross-border cash movements, cash-intensive businesses and cash payments), money transfer and payment services, or services for onshore and offshore company formation.

FT identification and investigation

236. In Latvia's institutional model, the SeP has primary responsibility for counterterrorism (CT) and FT pre-trial investigations, which takes a targeted, intelligence-based approach. As in the abovementioned cases, the SeP investigates financial information as part of its underlying CT investigations, but it has not conducted independent FT investigations. It works cooperatively with the FIU as well as with other relevant bodies, including the FCMC and the SP, to obtain pertinent information. The SeP also reports good community contacts that help produce tips. The details of these cases remained confidential, but authorities stated that all relevant aspects, including financial elements, were actively investigated and considered.

237. Latvian law requires subjects to refrain from conducting FT-related transactions and report them to the FIU. Upon receipt of such a report the FIU can order funds that are suspected of being connected to terrorism frozen for six months. In one case (the "Martin Grinberg"-case), the FIU received a report independently of the SeP once news broke of his involvement with ISIS and froze his funds. The FIU can also order the freezing of assets pursuant to third-country requests, but has not done so for FT. Otherwise, the role of the FIU in identifying FT is chiefly to receive and disseminate FT-related STRs and UTRs, as well as related case materials, to the SeP and other relevant LEAs.

The FIU reports receiving few FT related STRs/UTRs, with less than handful until 2015, when it received four, referring two to law enforcement. Reports on FT rose to 15 in 2016, when the FIU referred seven reports filed for FT. These cases were all found false positives but suggest a system capable of identifying indicia of potential FT activity. **False Positive: Transfer of Funds to Spain**

In 2016, the FIU was notified by a foreign counterpart of a transfer from a Latvian bank to Spain with potential links to terrorism based on indicia of religious radicalism. The FIU requested information about the origin of the funds. Germany also requested additional information with a potential link to terrorism, but did not provide supporting information. The FIU did not freeze the funds because the transaction had already been executed, although it is unclear why it did not freeze any remaining amounts. The FIU immediately informed the SeP, which confirmed that the transfer had occurred and requested information from its German counterparts through a mutual legal assistance treaty mechanism. It was eventually concluded that the transfer was made by a Latvian national in Switzerland and that no links to terrorism were established. The FIU submitted a spontaneous report to Switzerland.

238. The FIU and SeP both report adequate resources to manage their caseloads with respect to terrorism, although the NRA notes that a potentially increasing threat environment may require additional resources. Precise figures on SeP investigators responsible for FT are classified, but approximately 40% have been specially-trained. As for the FIU, there are two staff members responsible for FT and counter-proliferation, one administrative position for managing and updating relevant sanctions lists and another for conducting substantive analysis and outreach with international counterparts and Latvian FIs.

239. Despite regular and efficient cooperation and the ability to exchange information freely across agencies, there is no single platform in Latvia for all relevant regulators and authorities to see and understand pending FT investigations and cases. While the FIU disseminates reports to the SeP on potential FT, for example, the SeP cannot see these reports as they are submitted in real time. The SeP, similarly, cannot view the status of an SRS review of an NPO with potential terrorism links. Although the absence of such real-time, comprehensive picture of all CFT activity occurring in Latvia at any one time has not been shown to impede appropriate investigation and enforcement, authorities believed they would benefit from a single database that would be accessible to appropriate agencies of all such investigations.

FT investigation integrated with -and supportive of- national strategies

240. Latvia's high-level strategy for countering ML and FT, the Plan of Measures for Mitigation of the ML/FT Risks for 2017–2019, is a broad set of measures to strengthen Latvia's AML/CFT regime, largely by addressing legal and institutional vulnerabilities. Reflecting Latvia's self-assessment of its FT risk as low, it does not contain dedicated measures to identify or designate individual terrorists, terrorist organisations or associated support networks specifically.

241. The SeP develops a periodically updated National Counterterrorism Plan, an operational document last revised in 2017. This plan is classified but is said to encompass certain financial elements. It is unclear how this plan contributes to Latvia's systemic FT measures, although insights gleaned from practical exercises conducted pursuant to the plan could in theory inform Latvia's broader counterterrorism strategy.

242. CoM Regulation No. 880 establishes a Counterterrorist Centre Advisory Board, which meets once a year. The FIU's presence on the Board helps ensure due inclusion of FT considerations in Latvia's investigative framework. However, the MoF is not a member of the Board, potentially leading to missed opportunities for more systemic recognition of FT threats and vulnerabilities.

243. The FIU's Operational Strategy for 2017-2019 includes initiatives to increase the efficiency and quality of STR and UTR reporting and analysis but does not speak of incorporation of lessons learned from FT investigations or other enforcement actions in Latvia to date.

Effectiveness, proportionality and dissuasiveness of sanctions

244. In the period under review, there have been no FT prosecutions and convictions. Therefore, the evaluators were unable to assess whether sanctions or measures applied against natural persons convicted of FT offences are effective, proportionate and dissuasive (but see "Martins Grinberg Case").

Alternative measures used where TF conviction is not possible (e.g. disruption)

245. Following the adoption of a number of new legal authorities, Latvia uses an adequate range of alternative means to disrupt terrorist or FT activities where it is not practicable to secure a FT

conviction. A 2015 amendment to the CL criminalised "unlawful participation in a foreign armed conflict" (Sec.77[1]) providing authorities with a firm basis to pursue charges against Latvians who had joined conflicts in, *inter alia*, Syria and Iraq. Most notably, the Grinberg case resulted in a conviction under Sec.77[1] CL as the authorities did not have sufficient evidence to demonstrate that the defendant had engaged in terrorism or supported a terrorist group. The prosecution also charged involvement in a criminal organisation committing war crimes (Sec.891 CL). Although a unique case, it is not clear that Grinberg's original sentence for a conviction under Sec.77[1] CL was a sufficiently proportionate and dissuasive sanction, although the sentence increased substantially on appeal shortly after the onsite visit (see box below).

Martins Grinberg Case

In 2014, after becoming radicalized online, including through contact with an individual in Finland, Latvian citizen Martins Grinberg travelled to Turkey and then to Syria, where he joined the ranks of ISIS. In summer 2015, the SeP obtained information that Grinberg had been detained by the Turkish authorities. According to Grinberg's testimony and public statements, he had escaped Syria to Turkey after becoming disillusioned with ISIS' conduct and being assigned to the front line against his will. Grinberg was extradited to Latvia, where in November 2015 the SeP launched a criminal investigation. Its investigation found that Martins had travelled to Syria using his own funds. Later, the FIU received an STR related to Martins and ordered that his account, containing over EUR 417, be frozen. The FIU prepared a formal set of case materials with analytical information regarding Grinberg's expenditure of funds on the way to Syria. Subsequent investigation found another relevant monetary connection that the Latvian authorities have kept confidential, but which was determined to be benign. Throughout its investigation, the SeP cooperated with Finnish counterparts.

On 29 October 2016, the investigation was referred to the GPO, which indicted Grinberg for unlawful participation in an armed conflict in violation of Sec.77[1] CL, a 2015-amendment to the law making such conduct illegal. He was also charged (but acquitted) on one count of participation in a criminal organisation for the purposes of committing war crimes, in violation of Sec.89[1] CL.

On 27 April 2017, the First Instance Court found Mr Grinberg guilty of unlawful participation in an armed conflict, but acquitted him of the war crimes-related charge. The court sentenced Mr Grinberg to 4 years imprisonment and probationary supervision of 2.5 years. Both Grinberg and the GPO appealed the judgment.

On 16 November 2017, the Riga District Court Criminal Court Council upheld the conviction for unlawful participation in an armed conflict, but also convicted Mr Grinberg for war crimes. As a consequence, Mr Grinberg received a sentence of 10 years and 3 months imprisonment (with probationary supervision of 3 years.) An appeal on points of law by Mr Grinberg is pending before the Supreme Court.

246. The authorities also reported the possibility of recourse to administrative measures such as asset confiscation, denial of welfare benefits, deportation, and passport and citizenship revocation, although none have yet been imposed for terrorism or related activity.

Conclusion

247. The absence of a robust FT risk assessment presents a major deficiency in Latvia's effective implementation of IO.9. Without a thorough understanding of how its broader financial vulnerabilities expose Latvia to exploitation by terrorist actors, the country cannot provide a systematically effective response to FT risks. The SeP appears empowered and enabled to identify potential terrorism and FT risks emanating from within Latvia. Its activities with respect to open investigations remain unavailable and difficult to judge. Overall, it appears to cooperate effectively with the FIU and other agencies as appropriate to investigate potential FT cases that arise.

248. Latvia has not yet achieved any prosecutions or convictions specifically for FT, although it has conducted a number of terrorism-related investigations. The lack of prosecutions/convictions appears consistent with Latvia's internal threat level, if not necessarily its FT risk profile. There is also no basis to consider whether penalties for TF are effective, proportionate, or dissuasive. Still,

the country is largely able to demonstrate the application of alternative measures to disrupt potential FT activities. **Latvia has a moderate level of effectiveness for IO.9.**

Immediate Outcome 10 (TF preventive measures and financial sanctions)

Implementation of targeted financial sanctions for TF without delay

249. In addition to the relevant EU Regulations, which are directly applicable in Latvia, FT-related TFS are implemented on the basis of the Law on Sanctions, Cab. Reg. 468, and the AML/CFT Law. As explained in the TC Annex (R.6), this legal basis gives rise to serious uncertainty with respect to the implementation of terrorism-related TFS. The exact articulation between these pieces of legislation, including in defining key elements of the TFS system such as the mechanisms for establishing permanent freezing obligations, the scope of funds to be frozen and the scope of persons obliged to freeze funds appear to feature significant gaps that designated parties might exploit, although to date there is no evidence this happened for terrorism-related TFS. Nevertheless, an in-depth review of the Latvian TFS legal basis with a view to ensuring compliance with the FATF Standards is strongly recommended.

250. UNSCR 1267 and successor resolutions are implemented on the basis of EU legislation, which raises important effectiveness issues: designations are not transposed into EU legislation "without delay", which, unlike some other EU states, Latvia does not remedy with domestic legislation at the national level. There is no clear authority to apply freezing measures to EU internals when they are not considered to threaten "international peace and security".

251. Latvia has never issued any proposals for designation through the EU's COMET Working Party, nor designated individuals or entities at the national level on the basis of UNSCR 1373, although it has the capacity to comply with the designation obligation under UNSCR 1373 obligations through EU Regulation 2580/2001 (EU designations), and the Law on Sanctions (national designations). Authorities appeared aware of these possibilities, which they considered in one case before deeming it an inappropriate response. As regards national designations, as described in IO.11, Latvia has designated an individual domestically using the same authorities as it would pursuant to UNSCR 1373, demonstrating in at least one case by the time of the onsite it was able to take such action (and took another subsequently).

252. Under the Law on Sanctions and its implementing regulation, both the FIU and the FCMC are charged with the "execution" of TFS, which they perform consistent with and as part of their broader institutional mandates. In practice this means that the FIU is responsible for receiving information from REs on sanctioned terrorists, disseminating it as appropriate to LEAs, ordering the freezing of their assets, issuing guidance, conducting trainings, and maintaining sanctions lists, among other responsibilities. The FCMC, for its part, is responsible for supervising FIs for their compliance with TFS obligations and making binding decisions on FIs.

253. Mechanisms for the communication of lists appear effective. Since July 2014, the FIU has maintained a searchable list of persons sanctioned under UN and EU sanctions regimes on its website, which is automatically updated daily. The FIU's database also includes information on select third-country sanctions lists, which the FSDB has directed the FIU to encourage REs, in particular banks, to monitor in addition to UN and EU lists.

254. The FCMC conducts TFS supervision through both onsite and offsite examinations of FIs for compliance with FT-related TFS, although resource constraints have limited the extent of supervision. To date, the FCMC has largely relied on the generic but TFS-relevant provisions of the

AML/CFT Law to regulate for TFS. FCMC Reg. 219, for example, requires FIs to maintain automatic screening systems and software that can automatically detect potential matches against relevant sanctions lists against customers, UBOs, representatives and others, as well as payment transactions. FIs must also have at least one specially trained sanctions compliance officer. These obligations are in addition to other relevant due diligence and ICS requirements.

255. Authorities explained that the Law on Sanctions does not provide an adequate legal basis to enable the FCMC to issue detailed, specific regulations on TFS. The FCMC considers this is a significant limitation that prevents it from issuing mandatory requirements for all FIs to take specified TFS compliance measures, for example to require banks to institute safeguards against sanctions evasion.

256. The powers and monitoring practice of the other supervisors in relation to TFS are unclear. The AML/CFT Law gives them general monitoring and sanctioning powers, including in relation to TFS-relevant obligations (refraining from executing a transaction; UTRs; internal controls). However, the Law on Sanctions and Cab. Reg. 468 do not mention any other supervisory authority than the FCMC. Most supervisory bodies of DNFBPs do not conduct inspections for TFS, except for limited instances of spot-checking of records against sanctions lists. The authorities mentioned resource issues and prioritisation of other areas of the AML/CFT Law, as the reasons for the limited coverage of TFS.

257. The FIU conducts regular outreach to increase the awareness of FIs and DNFBPs on TFS inviting REs for approximately monthly seminars. There the FIU conducts a detailed presentation describing the process to follow with respect to TFS matches. The FIU has also posted and distributed both FATF and other guidance on FT trends and methodologies on its website. It has also developed its own guidance in the form of both public and private advisories and typologies.

258. All REs showed at least a basic awareness of their obligations in relation to FT TFS, but FIs, especially banks, demonstrated the most advanced understanding. However, as noted under IO.4, most REs implement their TFS obligations by using screening tools to identify matches with the applicable sanctions lists; only a few banks expressed clear appreciation of the importance of transactional monitoring for TFS evasion. In the case of FT, for example, they generally did not account for how they integrated customer risk profiling, geographical indicators, and patterns of conduct to detect potential efforts at sanctions evasion. Banks and most FIs reported using built-in or internationally-recognized screening software, while DNFBPs reported relying on the FIU website.

259. Given the deficiencies in the identification of BO within Latvia's large numbers of non-resident shell customers, as discussed in IO.4, the limited use of transactional monitoring, and resource constraints noted above and in IO.3, which have limited the necessary pace and scope of supervision, it is unclear how effectively REs could detect evasion schemes hidden behind complex corporate structures or operations. In addition, given the weaknesses in the legal basis, there is a risk that only the most obvious breaches of TFS obligations could be sanctioned.

Targeted approach, outreach and oversight of at-risk non-profit organisations

260. Latvia has not specifically identified the types of NPOs at risk of FT abuse guided by the FATF definition[88]. Latvia has also not conducted a dedicated FT risk assessment of its NPO sector.

[88] Latvia identifies 22,890 "non-governmental organizations", which include trade unions and political parties, and 22,437 "associations and foundations", which includes organizations other than those described by the FATF. Latvia also

However, authorities believe the sector to be low risk. They base this conclusion on their understanding of Latvia's broader FT profile, the nature of Latvian NPOs' activities, the sector's regulatory and law enforcement scrutiny, and legal and institutional regulatory framework. Although as described in IO.1, Latvia has broadly failed to account for the FT risk posed by its pronounced vulnerabilities, this is somewhat mitigated with respect to its NPO sector by the close scrutiny the SeP, and to a lesser degree the FIU and SRS, give to risks of foreign influence in this sector more broadly.

261. The SeP began conducting an assessment of the NPO sector's vulnerabilities to "exploitation by foreign actors" in 2014 while reviewing regulatory and enforcement gaps that exposed Latvian civil society to destabilizing interference from abroad. The SeP identified funding ethnic "compatriot" organizations as a particular concern and identified ostensibly humanitarian organizations that provided backing to belligerents rather than aid to civilians. While FT was an ancillary issue, Latvian authorities saw that responding to this threat necessitated strengthening its ability to guard against FT abuse of the NPO sector. The SeP worked with the SRS and MoJ to develop proposed amendments to the Foundations and Associations Law in 2017 that would allow for imposing additional information requirements and dissolving organizations found to engage in a number of proscribed activities, including fomenting violence and hatred[89].

262. Among NPOs at risk of serving as FT threats or vectors, the authorities consider groups led by "radically oriented persons" as a unique threat, but do not believe such groups are currently operating in Latvia. This view is held despite having had an NPO that was led by a radicalized individual who later travelled to fight for ISIS. This individual served as the leader of the LIKC for over a year before departing for Syria (see Petrovs box in IO.9). As the investigation is open, the SeP did not provide details whether it looked at potential FT links as a result of his leadership, such as donors, foreign contacts, payments, or other such conduct. However, they assert that the LIKC itself was not compromised under Petrovs' leadership and that his affiliation with this group did not reflect on the group itself. In the view of the authorities, members of the LIKC, as well as the broader community, reject radical views.

263. Separate from the SeP's review, the FIU has performed two inspections of STRs involving Latvian NPOs to understand their financial activities and suspected links to criminal activity, as well as red flags for FT. No FT-related reports were identified.

264. As described under R.8, all NPOs are subject to a number of transparency and reporting requirements. Public benefit organizations (PBOs) are subject to additional scrutiny owing to their tax-preferential status. As the primary regulator for NPOs for tax purposes, the SRS conducts thematic audits of foundations and associations, including PBOs. PBOs are supervised by the SRS and subject to heightened disclosure requirements regarding donors, donations, expenditures, balance sheets, and other information.

---

reports 2,640 "public benefit organizations" (PBOs), a status allowing for tax exemptions and preferences for which only associations, foundations, and religious organizations are eligible, but that not all such organizations have obtained. A 2015 survey of this sector by activity, according to the NPO Civic Alliance found the greatest share of these organizations were of a type that could meet the FATF definition in that they performed "good works".

[89] These amendments became effective following the onsite. These laws provide Latvian authorities additional authorities to require information from NPOs and dissolve them if they engage in a number of proscribed activities, including fomenting violence, religious hatred. NPOs may be obliged to submit a balance sheet, income and expense reports, donations and donations reports, submit transaction documents or indicate sources of funding four times a year. Relevant documents received by the SRS will be sent to the state security agency.

265. There has been limited systematic outreach to the NPO sector on FT. NPOs engage with authorities in a forum called the Memorandum Council. This forum was used as the MOJ, the SeP, and the SRS were formulating the new amendments to the Associations and Foundations Law, at which there was no discussion of FT specifically. Authorities cited FT-related materials on the FIU website and interactions with auditors, accountants, and attorneys as possible means for NPOs to learn of FT risks. The SeP indicates that it has engaged on occasions with some NPOs to discuss FT-related trends.

Deprivation of TF assets and instrumentalities

266. *TFS:* Although Latvia has not identified any financial or other activities of designated terrorists, the FIU did receive reports regarding such persons that turned out to be false positives (see Case example below). In addition, four non-resident banks have frozen approximately EUR 12 million in relation to 109 legal persons and one natural person sanctioned by the EU in other sanctions programmes. Latvian banks have also reported (but not necessarily frozen) payments sent or received on behalf of dozens of customers, UBOs, or shareholders sanctioned or owned by sanctioned parties pursuant to certain third-country sanctions regimes. Those elements indicate a system that would also be capable of identifying and freezing assets under UNSCRs 1267 and 1373 or successor resolutions were they to be identified, at least in simple operations in which the designated person or entity are directly involved. In light of Latvian FIs' limited transactional monitoring, BO gaps and foreign shell company activity, far less confidence can be had that it would do so if funds were held indirectly by designated terrorist-related entities.

267. Other asset deprivation mechanisms: Latvia has consciously chosen not to pursue freezing actions, citing investigative reasons. This includes the case of Martin Grinberg, who the authorities sought to monitor instead, and who was not ultimately charged with a terrorist offense. Latvia has not received requests to investigate, seize or freeze such assets from foreign counterparts

"Bin Laden": Three False Positives

In 2015, the FIU received a STR from a bank referencing a payment in which the originator had entered "bin Laden" as the payer. The bank had refrained from executing the payment pending further investigation. The FIU referred the matter to the SeP, which located and questioned the payment originator, a Latvian national. In his account, the man explained that he owed money to a friend, and that his reference to himself as "bin Laden" had been a joke. The investigation confirmed his account and the man was warned against such "financial hooliganism" in the future.

In a similar instance in May 2016, the FIU received a report for a EUR 30 transaction in which the purpose of payment field stated "thanks for ak47 delivery, al qaeda and osama bin laden". The FIU froze the funds and referred the case to the SeP, which determined that the payment reference was a prank.

Likewise, an August 2016 report submitted to the FIU for a EUR 13.99 transfer had in its purpose field "obama terrorisms ben laden", which was similarly identified as unrelated to terrorism. Again the FIU froze the funds and referred the case to LEAs.

Consistency of measures with overall TF risk profile

268. Latvia's lack of a comprehensive understanding of its FT risk profile complicates assessing its efficacy. Broadly, the measures it has taken seem consistent with what an appropriate understanding of its risks would reveal in light of its domestic threat level, if not from threats emanating from outside its borders. Still, key authorities – primarily the FCMC, FIU, and SeP – recognize the risks that terrorists could exploit the vulnerabilities of Latvian FIs and have broadly made improvements to its CFT regime, including relating to TFS.

269. Latvia's general regime for monitoring and supervising NPOs, including through law enforcement means, appears to allow for an adequate mitigation of risks authorities identified in the sector, which is limited to a very small number of NPOs. Still, it is not clear to what extent Latvian authorities have developed "lessons learned" or protocols in response to the risks presented by the LIKC's previous leadership by a radicalized national who left Latvia to join Da'esh. Focused outreach to higher-risk NPOs and broader engagement with the wider NPO community could be a useful preventive measure to avoid any future abuse of the sector.

Conclusion

270. Despite a legal basis that calls for urgent clarifications and improvements, Latvia demonstrates elements of an effective system of terrorism TFS implementation. The vulnerabilities of its FIs remain a significant impediment to achieving a greater degree of preventive capability, as do gaps and uncertainties highlighted in the regime for freezing assets, and insufficient supervision in a number of sectors. The NPO sector appears to be effectively monitored, based on intelligence efforts and broad registration/reporting obligations applying to all NPOs, if mainly for non CFT-specific objectives (i.e. preventing foreign destabilization and tax offences). A FT-specific and comprehensive risk assessment of NPOs, perhaps as part of the broader NRA process, could allow for a better informed and targeted FT risk mitigation approach in the sector, which has seen at least one future terrorist lead a prominent organisation. In general, in the absence of a comprehensive FT risk understanding, the broader adequacy of FT prevention efforts remains to be demonstrated. **Latvia has a moderate level of effectiveness for IO.10**.

Immediate Outcome 11 (PF financial sanctions)

Implementation of targeted financial sanctions related to proliferation financing without delay

271. Latvia's legal basis for implementing TFS related to PF is governed by EU legislation, the Law on Sanctions and the AML/CFT Law, as well as subsidiary regulations. As noted under IO.10, the broader TFS legal framework presents a number of serious uncertainties and deficiencies. These shortcomings are somewhat more acute in relation to PF TFS, which are less clearly captured by the relevant obligations in the AML/CFT Law in that the Law does not clearly set up a reporting and freezing mechanism for PF TFS (see TC Annex, R.7).

Identification of assets and funds held by designated persons/entities and prohibitions

272. Altogether, proliferation-sensitive exports from Latvia to countries that are subject to PF-related sanctions at the UN do not seem material. The MFA and SeP coordinate an interagency committee that adjudicates license requests for export-controlled items, mostly for a handful of categories of dual use goods. The key Committee components are in daily contact to address PF issues as the need arises. However, the FIU does not sit on the Committee and there is no formal or routinized channel of information exchange and coordination with the FCMC. The interagency committee that adjudicates license requests for export-controlled items reported regular communication with banks, which will send informal requests for guidance on whether goods for which they are facilitating trade are sensitive or not.

273. Latvia's main vulnerabilities to exploitation for PF lie in its banking sector. In particular, weaknesses in establishing BO among its large stock of foreign shell company banking customers (see IO.1 and IO.4), coupled with an overreliance on list-based screening and rudimentary transactional analyses, all but preclude controls adequate to address PF-linked evasion activity.

This vulnerability was illustrated by at least six separate domestic and third country enforcement actions involving DPRK (see detail below).

274. Latvia has not identified (and accordingly has not frozen) assets of persons linked to relevant DPRK or Iran UNSCRs. Neither has the FIU received STRs or UTRs with links to PF. The SeP have been investigating potential criminal offenses relating to PF-related sanctions, upon FCMC referral of the DPRK sanctions evasion cases described below. Upon receipt of clear, actionable information provided by foreign counterparts, Latvia's authorities have acted to investigate and take remedial action.

275. Unique among most European states, Latvia had at the time of the onsite issued an autonomous designation under its new Law on Sanctions, targeting DPRK-linked proliferation agent Alex Tsai in 2017. The authorities have not taken steps to propose Tsai's designation at EU level on grounds it was not the originating country for the intelligence and evidence used to designate him.

Designation of Alex Tsai

In July 2017, the Cabinet issued Reg. 419, pursuant to the Law on Sanctions, providing for autonomous sanctions on persons related to the development of weapons of mass destruction by DPRK. Subsequent to this regulation Latvia imposed financial restrictions on Hsein Tai Tsai (Alex Tsai) for using two companies as intermediaries to provide financial and material aid to the UN- and EU-designated Korea Mining Development Trading Corporation (KOMID). The FCMC and other authorities had received information on Tsai's activity in Latvia from a foreign partner and, in investigating the matter, developed additional evidence indicating Tsai's role in moving money through Latvian FIs to evade international sanctions. The FCMC took action against five Latvian banks in connection with Tsai's scheme (see detail below). Tsai is currently in the custody of a separate jurisdiction. No assets of Tsai's have been identified in Latvia.

FIs and DNFBPs' understanding of and compliance with obligations

276. The FIU maintains regularly updated lists of entities subject to proliferation-related sanctions on its website and has discussed PF indicators in general training programmes. Both the FIU and FCMC have issued guidance and alerts to the regulated community reflecting developments in identifying and countering PF activity, both at the international level and in Latvia. Still, during the onsite REs showed an uneven level of understanding of their PF-related TFS obligations. FIs, in particular banks, demonstrated the highest level of awareness.

277. Banks were broadly aware of their TFS-relevant obligations under FCMC Reg.219 on AML/CFT internal controls, which requires them to maintain adequate sanctions compliance systems, including screening programs and a dedicated sanctions compliance officer, to identify transactions involving sanctioned persons. Banks met onsite reported that their systems update daily, allowing them to restrain transactions soon after the relevant authority designates them, even where this is not a legal requirement. Other FIs reported reliance on business partners' systems, e.g. credit card providers, for example. DNFBPs generally consult the lists on an as-needed basis and rely on the FIU, from which most said they received information on UN, EU, and Latvian obligations related to PF.

278. Latvian FIs' and DNFBPs' generally list-based approach to sanctions compliance, especially in light of the characteristics of non-resident banks' customer base, does not adequately account for the varieties and extent of sanctions evasion practiced by DPRK and the vulnerabilities of such Latvian FIs to such activity. Despite recent improvements, over the course of the assessment period such vulnerabilities were insufficiently accounted for and addressed. The importance of

transactional indicia of potential sanctions evasion, for example, seemed to be given secondary importance in banks' compliance programmes. Specific to PF-related TFS, banks generally did not display sophisticated understandings of PF-related evasion or indicate how they had developed screening tools to detect such activity, e.g. by integrating customer profiling, locational information, and sectoral characteristics into transactional screening criteria.

279. As a result of a number of factors, including an increased pace of FCMC enforcement actions, since 2016 banks have taken significant steps to enhance their compliance programmes. These steps include reviews by major global consulting firms of Latvia's non-resident deposit banks, hiring and training of new compliance personnel, enhancements to IT systems for sanctions and other screening, shedding higher risk clients and shell companies, and in keeping with regulatory requirements undertake improved due diligence criteria. Banks also reported employing at least one compliance officer dedicated to sanctions. The banking association has also issued voluntary guidance to Latvian banks on AML/CFT compliance, including sanction compliance. While such measures may ameliorate the lax control environment at Latvia's banks, residual exposure to evasion will continue to be significant until Latvian FIs maintain robust compliance with their BO and CDD obligations and implement effective transactional monitoring.

Competent authorities ensuring and monitoring compliance

280. The FCMC conducts supervision according to a schedule based on the general AML/CFT risks posed by particular FIs (e.g. number of non-resident deposits, turnover, business lines, etc.). As described in IO.4, there are broad AML/CFT vulnerabilities that provide avenues for sanctioned actors to exploit. Since these vulnerabilities remain substantial – DPRK-linked actors exploited at least six Latvian banks – the pace and level of supervision, resulting partly from resource constraints – does not appear adequate to adequately guard against evasion, a challenge that Latvian authorities described as significant. Despite this experience, the FCMC has not undertaken a concerted effort to conduct thematic inspections for PF TFS for other banks fitting the profile of those penalized for internal control violations as part of the FCMC's series of enforcement actions following receipt of information on the North Korea scheme. Moreover, little to no real thematic inspections have been conducted on PF TFS by the DNFBP supervisory bodies.

281. Under the AML/CFT law, FCMC Reg. 219 is relevant to TFS to the extent it regulates internal control systems, suspicious/unusual activity reporting, audits for quality assurance, staff training and testing, information technology, and CDD among other requirements. As discussed under IO.10, the FCMC indicates that its lack of authority to issue binding regulations specifically governing TFS obligations significantly inhibits its ability to promote compliance and conduct enforcement in that area. As noted under IO.10, the FCMC has used its general authorities under the AML/CFT Law as an alternative means when confronted with cases of sanctions evasion. Accordingly, while the FCMC can issue guidance to banks about the *modus operandi* of sanctions evasion, including identifying specific scenarios and risks, and has done so, it cannot issue binding regulations requiring adoption of specific preventive measures.

282. In October 2017, the FCMC issued internal procedures for supervising TFS compliance with Latvian national and international sanctions and conducted both on- and off-site inspections. These procedures lay out basic steps for how to process potential sanctions violations, engage and inform FIs, and exchange information with other authorities. It does not provide criteria with respect to how a violation will be determined.

283. As described below (see case study), in 2017, based on information received from a third country, the FCMC took enforcement actions against five banks for *"breaches of the AML/CTF Law and FCMC regulatory requirements: weaknesses in CDD and transaction monitoring that led to the situation that bank had been used to circumvent international sanctions requirements imposed against North Korea; and failure to ensure the effective functioning of the internal control system"*. It also settled with a sixth bank in an unpublicised administrative agreement, to which the evaluation team did not have proper access.

284. Despite this explanation, the FCMC ultimately decided that its findings did not identify direct evidence of sanctions violations, and no penalties in any case were imposed for breaches of UN or EU sanctions applicable during the time of the relevant transactions. The FCMC explained that its use of AML/CFT rather than sanctions authorities was based on its conclusion that given the complexity of the circumvention scheme, there was no obvious linkage to a designated customer, UBO, intermediary or affiliate. The scope of the freezing obligation under the FATF Standards (and EU Regulations applying in Latvia) is however broader, to include freezing funds or other assets that are wholly or jointly directly or indirectly owned or controlled by designated entities and funds or other assets of persons and entities acting on their behalf of, or at their direction.

285. Although FCMC staff members sought to obtain additional legal clarity from the EU on the question of whether such facts could give rise to a violation of EU sanctions, the fact that the FCMC did not ultimately consider these failures any sort of breach of the banks' TFS obligations – despite subsequently identifying a considerable set of red flags that it described in supervisory guidance – raises serious questions about whether the authorities are able to sanction only the most obvious TFS infringement cases or breaches of related AML/CFT obligations. The development by FCMC staff members of what was described as a robust record for referral to the SeP for criminal investigation of potential sanctions violations, moreover, underscores an apparent inability or unwillingness to take more meaningful TFS enforcement action in these cases (the FCMC's referral to the SeP was not provided to the evaluation team).

286. Perhaps at least partially for such reasons, the settlements with the banks included monetary fines and administrative injunctions that were far from dissuasive and proportionate. Although these penalties were higher than the historical norm given the dearth of enforcement actions prior to 2015, Latvian banks continued to engage in high-risk activity of the sort the FCMC identified as punishable violations. Partially explained as a function of the low statutory penalty structure at the time, these penalties were clearly not maximized given that two monetary penalties were just over EUR 35,000, and another little more than EUR 570,000. At the time the conduct occurred, the applicable penalty range went up to EUR 142,300 per violation.

287. In the unpublicized case, no penalty was imposed at all on a bank that had engaged in similar conduct as the others, on the grounds that a separate 2016 settlement for unrelated AML/CFT violations had already addressed the deficiencies that the FCMC had identified with respect to DPRK. Subsequently, as noted, the bank was the subject of an action by a foreign government, which found DPRK-linked activity occurring even after committing to prevent such activity[90]. Such ongoing conduct underscores the limited efficacy of the penalties levied. The FCMC has not yet used

[90] Financial Crimes Enforcement Network, *Proposal of Special Measure Against ABLV Bank, AS as a Financial Institution of Primary Money Laundering Concern*, 16 February 2018, 83 Federal Register, 6986, available at: https://www.fincen.gov/sites/default/files/federal_register_notices/2018-02-16/2018-03214.pdf

its new penalty authorities under amendments to the AML/CFT Law (in cases of PF TFS) or Law on Sanctions.

DPRK-Related Sanctions Evasion through Latvian Banks

Beginning in 2016, the FIU began receiving and referring to the FCMC and SeP information from a foreign counterpart relating to the evasion of international sanctions on North Korea through a number of Latvian banks. Following receipt of this information, the FCMC convened the heads of Latvia's banks, warned them of the seriousness of the situation, and carried out targeted inspections and onsite examinations of six banks operating in Latvia's non-resident deposit sector.

These inspections concluded that shell company accounts held by non-sanctioned foreign customers were used on behalf of UN- and EU-designated entities through a number of intermediaries. Underlying such transactions, the FCMC found that banks' AML/CFT internal controls were systematically unable to identify, assess, and manage sanctions risks. It also found numerous violations related to BO/CDD, transaction monitoring, and failure to detect or act upon inadequate and counterfeit business documentation; activities consistent with illegal "shell banks"; omission of material details from payment messages, and other evidence indicating possible operations on behalf of a UN-and EU-designated entities.

It also found that the bank customers were not designated persons themselves, but they acted on behalf of such persons through complex business and transactional chains. No funds were frozen, as no assets remained in the customer accounts at the time of the FCMC's investigation.

The FCMC imposed over EUR 3.5 million total in fines across the five banks, and required the banks to institute remedial measures. These measures included compliance audits, action plans to improve banks' compliance systems, a program of conducting and assessing banks' internal controls, and external testing. In publicly announcing the actions, repeated and elaborated in subsequent guidance to FIs, the FCMC also called attention to the red flags identified by UN and non-governmental bodies and that had been present in the scheme. These included offshore companies sharing the same officers and addresses paying the same beneficiary, dealings in areas or with businesses close to the DPRK border, DPRK -linked shipping companies, and transactions with companies in offshore jurisdictions linked to the North Korean government. The FCMC also stressed the inadequacy of list-based screening alone, risks involving the import and export of goods and the provision of transportation services.

288. As noted under IO.10, there is no clear basis for the monitoring and sanctioning powers of the other supervisory institutions with respect to TFS, since such powers are not mentioned specifically in the Law on Sanctions, Cab. Reg. 468, and since the legal basis for implementing PF TFS is unclear in the AML/CFT Law. Monitoring PF-related TFS compliance is also limited in light of the broader resource issues faced by supervisors

Conclusion

Latvia's legal basis for TFS, as already noted under IO.10, but with additional gaps under this IO, presents serious uncertainties and deficiencies. These shortcomings could have an impact on the effectiveness of its PF-related TFS regime, as they necessarily limit the authority to regulate, monitor and sanction breaches of TFS obligations. The country has not adequately implemented an effective regime to implement freezing obligations and guard against sanctions evasion, which in the case of proliferator states like DPRK is perpetrated through highly sophisticated means and which exploit opportunities offered in jurisdictions with inadequate financial controls. Large numbers of foreign shell companies with unreliable BO information and rudimentary transactional screening safeguards continue to create a permissive environment for sanctions evasion. REs' overly list-based approach is insufficient in that context. Latvia has not demonstrated the will or ability to require and institute the robust compliance programmes and active, dissuasive enforcement necessary to adequately mitigate its vulnerability to sanctions evasion. The FCMC was not provided the necessary regulatory powers to require FIs to take specific measures, and thus to conduct effective supervision, to implement TFS, and to prevent evasion activity. FCMC and FIU

guidance on evasion activity, while responsive to its recent experience, was issued only late in the assessment period. These serious vulnerabilities are illustrated by the six cases of exploitation of Latvian banks for the purposes of PF sanctions evasion detected in 2016 and the lack of a proportionate and dissuasive response, as illustrated by at least one bank continuing to process such transactions following these cases. Other supervisors' contribution to monitoring compliance with TFS appears very limited. In combination, these factors present a fundamental deficiency. **Latvia has a low level of effectiveness for IO.11**.

CHAPTER 5. PREVENTIVE MEASURES

Key Findings and Recommended Actions

Key Findings

- Among the representatives of the private sector, the understanding of ML/FT risks significantly varies both in terms of the knowledge on the subject matter and the comprehension of its significance.
- Some banks and most of the non-bank FIs appeared to confuse the enterprise-wide assessment of ML/FT risks with the customer risk classification and scoring systems/tools available for assessing certain risk factors. Moreover, their risk assessments did not provide any specific analysis of the FT threats and vulnerabilities and not always seemed to reflect the actual level of the overall ML/FT exposure of individual entities. The understanding of FT risks was largely confined to the use of what was generally referred to as "terrorist lists" – a combination of the UN and certain other lists, including the ones provided by the FIU.
- Non-bank FIs, with the exception of those that were part of larger international (financial) groups, did not demonstrate a clear understanding of the need to have consistent processes, practicable outcomes, appropriate documentation, as well as regular review and update practices for enterprise-wide assessment of their ML/FT risks appropriate to the nature and size of the business. The same is true for all DNFBPs, as well.
- All FIs mostly agreed with the risks identified in the NRA and recognised corruption, shadow economy and tax evasion as main threats. However, national risk assessments conducted by Latvia need to be improved to amount need to be improved to an exercise practicably facilitating better appreciation of sector specific ML/FT risks and relevant AML/CFT obligations in the private sector.
- Banks and, to a lesser extent, non-bank FIs met onsite were fluent in describing their policies and procedures providing for implementation of the risk mitigation framework, which were communicated to the management and staff on routine basis. Monitoring performance of the internal control system and taking remediation measures were told to be a part of the regular risk management practices.
- Effectiveness of the application of mitigating measures commensurate to the risks is in doubt, specifically with regard to the banks involved in the non-resident clientele business, due to major deficiencies related to the implementation of internal controls. DNFBPs met onsite did not demonstrate knowledge about or availability of the key constituents of an ML/FT risk mitigation framework.

- Banks and non-bank FIs demonstrated fair knowledge of the applicable requirements in the AML/CFT Law and relevant regulations regarding the pillars of the preventative regime, including those related to CDD and record keeping. Nevertheless, there are grounded concerns about the quality of the additional information/documents collected and maintained by banks in the CDD process for verifying the UBO, obtaining proof of the source of funds and source of wealth, as well as for monitoring transactions.

- Given the presence of a very sizeable base of non-resident customers, including shell companies in certain banks and PI/EMIs on one hand, and the well-known features of such clientele that complicate achieving a satisfactory level of compliance on some key issues, including BO and PEP identification, the effectiveness of implementation of relevant AML/CFT requirements remains in doubt.

- Poor implementation of the preventative measures by many DNFBPs is the presumed direct result of their insufficient knowledge in the area of AML/CFT. In addition, a non-estimated large number of individuals providing real estate brokerage services, legal advice, tax consultancy and company formation services without appropriate licensing and supervision aggravate the situation with the factual implementation of the AML/CFT requirements in the respective segments of professional activity.

- STR reporting performance of banks appears to be highly uneven, which is indicative of an uneven understanding and implementation of the reporting requirement among banks in general and among those exposed to comparable levels of the ML/FT risk in particular. Delayed reporting and defensive reporting also seem to be a part of the existing reporting practices.

- The overlap in the definitions of UTRs and STRs results in uncertainty as to the expected performance of the obliged entities, which often feel satisfied with the submission of a certain number of UTRs mostly comprised of over-threshold reporting.

- There are certain concerns about the insufficient independence of the compliance (as well as audit) function, the lack of appropriate access of the compliance staff to the CDD and other relevant information on non-resident customers/ shell companies, as well as formal enforcement of the AML/CTF requirements and relevant internal control measures.

- The lack of regulation in the fields of professional activity such as real estate brokerage, tax advice, accounting and company formation services, and the subsequent presence of a very significant unregulated market in these professions were reported to be a substantial impediment for the obliged entities to effectively implement their AML/CFT obligations.

Recommended Actions

a) With regard to the **understanding of ML/FT risks and AML/CTF obligations**, Latvia should take measures to ensure that:

- In conducting enterprise-wide assessment of the ML/FT risks appropriate to the nature and size of the business, the subjects of the AML/CFT Law have in place and apply consistent processes; practicable outcomes; appropriate documentation; and regular review and update practices;

- Such enterprise-wide risk assessments of the ML/FT risks provide specific analysis of the FT threats and vulnerabilities; and reflect the actual level of the overall ML/FT exposure;

- Among subjects of the AML/CFT Law the understanding of FT risk extends beyond the screening against "terrorist lists"; and the understanding of ML/FT risks is practicably facilitated by contributions to and feedback on national risk assessments;

b) With regard to the **application of risk mitigating measures**, Latvia should take measures to ensure that:

- The key constituents of an internal control system for ML/FT risk management are implemented in all FIs and DNFBPs;
- Effectiveness of the application of mitigating measures commensurate to the risks is enhanced, as ascertained through targeted supervisory action;

c) With regard to the **application of CDD and record keeping requirements**, Latvia should take measures to:

- enhance enforcement of the minimum requirements to the quality of additional information and documents collected and maintained by the subjects of the AML/CFT Law in the CDD process for verifying the UBOs; establishing the PEP status; obtaining proof of the source of funds and the source of wealth; and monitoring transactions in terms of legitimacy and economic rationale;

d) With regard to the **application of enhanced or specific measures**, Latvia should take measures to:

- Ensure that all subjects of the AML/CFT Law implement systems for risk-based application of CDD measures;
- Ensure that all subjects of the AML/CFT Law with high transactional activity (including payment gateway service providers) implement automated IT solutions for FT screening purposes; and that those with low transactional activity consistently use manual tools for FT screening purposes;
- Provide to the subjects of the AML/CFT Law systematized and specific communication on countries for which enhanced measures are called for by the FATF;
- Consider developing a centralized register or source to be consulted for checking the PEP status of Latvian residents;
- Consider banning customer introduction by entities other than those defined under Sec.29 of the AML/CFT Law;

e) With regard to the **reporting obligations and tipping off**, Latvia should take measures to:

- Enhance enforcement of the minimum requirements to the quality of the process for alert generation and STR reporting;
- Ensure the concepts of unusual transaction and suspicious transition avoid overlap in the relevant definitions, and introduce a system clearly delineating between STRs filed whenever the subjects of the AML/CFT Law have ML/FT suspicions; and over-threshold transaction reports filed in conformity with defined criteria relative to transaction methods and modalities, behavioural patterns etc.;
- Define indicators and "red flags" on suspicious transactions, both general ones applying to all subjects of the AML/CFT Law and specific ones applying to certain types of professional activity;

- Consider revising the "parallel" system of STR reporting to the SRS (within the framework of the broader revision of STR and UTR reporting system);

f) With regard to the **internal controls and procedures**, Latvia should take measures to:

- Consider introduction of additional (legislative) measures to ensure independence of the compliance (as well as audit) function;
- Ensure effective and substantial implementation of internal controls and procedures by all subjects of the AML/CFT Law, as ascertained through targeted supervisory action;
- Consider introducing regulation in the fields of professional activity such as real estate brokerage, tax advice, accounting and company formation services.

289. 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.

Immediate Outcome 4 (Preventive Measures)

Understanding of ML/TF risks and AML/CTF obligations

290. Among the representatives of the private sector, the understanding of ML/FT risks significantly varies both in terms of the knowledge on the subject matter and the comprehension of its significance.

291. With regard to risk assessment processes and practices, some banks and most of the non-bank FIs appeared to confuse the enterprise-wide assessment of ML/ FT risks[91] with the customer risk classification and scoring systems/ tools available for assessing certain risk factors such as the customer's state of residence (registration), economic or personal activity, or services used and transactions performed by the customer. Moreover, their risk assessments did not provide any specific analysis of the FT threats and vulnerabilities and not always seemed to reflect the actual level of the overall ML/FT exposure of individual entities. The understanding of FT risks was largely confined to the use of what was generally referred to as "terrorist lists" – a combination of the UN and certain other lists, including the ones provided by the FIU – sometimes setting forth details on fuzzy logic-based algorithms employed for identification of matches.

292. Non-bank FIs, with the exception of those that were part of larger international (financial) groups, did not demonstrate a clear understanding of the need to have consistent processes, practicable outcomes, appropriate documentation, as well as regular review and update practices for enterprise-wide assessment of their ML/FT risks appropriate to the nature and size of the business. None of them referred to such processes implemented or documents produced to enable identification and assessment of ML/FT risks. The same is also true for all DNFBPs.

293. Banks were fluent in articulating the risks associated with higher risk countries, transactions, products/services and delivery channels, as well as those emanating from contextual factors such as shadow economy and corruption. None of the banks, including those involved in the non-resident clientele business, were of the opinion that their residual ML/FT risks might be sensibly higher than medium. This kind of perception of risks, coupled with the analysis of the risk assessments mechanisms used by the banks and corroborated with the supervisor's vision on the

[91] Which should entail, *inter alia*, assessment of ML/FT risk inherent to the institution's customers, transactions, products/ services and delivery channels, examine the availability appropriate AML/CFT controls, and conclude on the level and magnitude of residual risks, as well as the necessary mitigation measures.

ML/FT risks in the financial sector indicates that the appreciation of risk is not commensurate with the factual exposure of the private sector in general and banks in particular to the risk of being misused specifically for ML, as well as for FT.

294. Almost all non-bank FIs were of the opinion that their exposure to ML/FT risk is low or, at the maximum, slightly higher than low. Some of them saw certain risks associated with their customers' behaviour such as, for example, the cases of making larger contributions than prescribed by the policy, early surrender and third-party payments in the life insurance business; mirror trading and market manipulation in the securities business; attempts of structured transactions not to exceed the identification threshold in the currency exchange business. Again, such understanding of risk does not appear to be commensurate with the factual risk exposure faced by, for example, PI/EMIs, most of which are not subject to a full-scope licensing procedure and are exposed to elevated ML/FT risks deriving from their high-risk customer base and complex, large volume transactions characterized by complicated monitoring and KYCC analysis, or by securities traders, some of which are very active in the Forex market.

295. None of the DNFBPs referred to mechanisms in place for identification and assessment of ML/FT risks pertinent to their activity. Many of them generally spoke about adverse phenomena related to their type of business, such as unfair gaming (casinos), reverse charge VAT fraud schemes (traders in high value goods), presence of a very significant unregulated market of real estate brokerage (realtors) and tax advise/accounting services (tax advisors and accountants), tax evasion both within and outside Latvia, shadow economy and envelope payments (auditors), transactions with participation of third parties/ offshore companies, fictitious agreements on non-existent debts (notaries). Such general understanding of risk virtually unrelated to the ML/FT implications relevant for individual businesses and professions does not amount to an appropriate perception and awareness of ML/FT risks.

296. As for the involvement in the NRA process, banks referred to questionnaires circulated for their input. Some of the non-bank FIs (securities traders, leasing companies, currency exchange offices) referred to the receipt of similar questionnaires, and others could not recall any contribution to the NRA process (representatives of Latvian Post met during the onsite visit).

297. Generally, both FIs and DNFBPs were involved in the NRA through questionnaires and industry association's input. None of the FIs received specific feedback on their contribution during or after the assessment process. Some of them were not even aware that the 2017 NRA Report was produced in the beginning of 2017 and made public later on in the same year.

298. All FIs mostly agreed with the risks identified in the NRA and recognised corruption, shadow economy and tax evasion as main threats. However, national risk assessments conducted by Latvia need to be improved to amount to an exercise practicably facilitating better appreciation of sector specific ML/FT risks and relevant AML/CFT obligations in the private sector.

Application of risk mitigating measures

299. The constituents of an internal control system for ML/FT risk management enabling a proper functioning risk mitigation framework are defined to comprise, inter alia: a) adoption of an ML/FT risk management strategy along with the methodology, policies and procedures for its implementation[92]; b) provision of IT system (including that for transaction monitoring) necessary

[92] Including the policies and procedures that define the structure and operational organization, division of responsibility and authorisation of management and staff with regard to ML/FT risk management, generation and submission of

for ML/FT risk management; c) establishment and regular review of ML/FT risk exposure indicators and their maximum admissible thresholds; d) conduction of ML/FT risk stress testing; f) regular review, efficiency assessment and improvement of the internal control system; and g) regular independent assessment of the internal control system.

300. Banks and, to a lesser extent, non-bank FIs were fluent in describing their policies and procedures providing for implementation of the above-stated components of the risk mitigation framework, which were communicated to the management and staff on routine basis. Monitoring performance of the internal control system and taking remediation measures[93] were told to be a part of the regular risk management practices.

301. Overall, effectiveness of the application of mitigating measures commensurate to the risks is in doubt, specifically with regard to the banks involved in the non-resident clientele business, due to major deficiencies related to the implementation of internal controls (as described under the analysis for below).

302. DNFBPs did not demonstrate knowledge about or availability of the key constituents of an ML/FT risk mitigation framework. The frequently mentioned objective factor mitigating the risk of ML/FT was the ban on any cash transactions above EUR 7,200 enacted since 1 January 2017, which indeed does not amount to an appropriate application of risk mitigating measures by the REs commensurate with their risks.

Application of enhanced or specific CDD and record keeping requirements

Application of CDD measures

303. Banks and non-bank FIs demonstrated fair knowledge of the applicable requirements in the AML/CFT Law and relevant regulations regarding the pillars of the preventative regime, including those related to CDD and record keeping. Most of the FIs confirmed using face-to-face identification only. Some banks, as well as securities traders offering certain types of services (e.g. Forex) referred to non-face-to-face identification practices using digital channels and methods such as on-line applications, recorded video calls etc. In such cases, certain risk mitigation techniques were used[94].

304. Nevertheless, there are grounded concerns about the quality of the additional information/documents collected and maintained by banks in the CDD process for verifying the UBO, obtaining proof of the source of funds and source of wealth, as well as for monitoring transactions in terms of legitimacy and economic rationale, where primary emphasis is made on self-identification and there is over reliance on internet data. Overall, given the presence of a very sizeable base of non-resident customers, including shell companies in certain banks and PI/EMIs on one hand, and the well-known features of such clientele that complicate achieving a satisfactory level of compliance on some key issues, including identification of beneficial ownership, the effectiveness of implementation of relevant AML/CFT requirements remains in doubt.

---

management reports by the compliance function, independence of the remuneration system of compliance staff from results of the institution's commercial activity, staff resources necessary for ML/FT risk management, and professional qualification requirements for compliance staff.

[93] For example, the risk assessment report provided by a bank for 2015 set out a plan of softly recommended, strongly recommended and immediate actions to be taken for mitigating the risk.

[94] E.g. requesting that the first payment was made from a bank account in the customer's name in Latvia or other equivalent country, establishing that the amount of transactions would be below a certain threshold (e.g. EUR 10,000), or that all back payments would be made to the same account.

305. Among DNFBPs, relevant knowledge of the preventative measures and AML/CFT obligations was demonstrated by auditors and (to a lesser extent) by casinos and notaries. Basic CDD practices varied among DNFBPs. Certain DNFBPs demonstrated remote understanding of their obligations and found the requirements hard to understand.

306. Poor implementation of the preventative measures by many DNFBPs is the presumed direct result of their insufficient knowledge in the area of AML/CFT as set forth above. In addition, a non-estimated large number of individuals providing real estate brokerage services, legal advice, tax consultancy and company formation services without appropriate licensing and supervision aggravate the situation with the factual implementation of the AML/CFT requirements in the respective segments of professional activity.

Establishing beneficial ownership

307. Banks were able to cite and interpret the definition of BO in the AML/CFT Law comprising the notions of ultimate effective ownership and control, by making reference to natural persons who have 25% direct or indirect ownership in a company's statutory capital, as well as to those who otherwise benefit from or have interest in a transaction or business relationship. Except for the cases when the BO was evident due to a person's holding company shares at or above the mentioned 25% or, in the case of foreign asset holding vehicles, the availability of trust declaration (which however might be long outdated), self-identification through a statement signed by the customer was used as a primary method for determining the BO of a transaction or a business relationship.

308. Information and documents from Latvian and foreign public registers, as well as from other sources such as internet and social networks was also used for the determination of beneficial owners. Some banks even referred to using services of detective agencies abroad to obtain reliable information about the BO of their foreign clients. Requiring recommendations from existing clients, scrutinizing transactions for the purpose of identifying apparent and hidden business ties and counterparties, looking at the identity of managers and authorized representatives were cited as supplementary measures to achieve a fair understanding about the UBOs. Some referred to a few cases of blocking customer accounts for checks on BO-related issues.

309. Some of the banks and most of non-bank FIs had a difficulty in explaining their understanding of BO in case of customers that were natural persons, i.e. the circumstances when the person who had come to the FI was not the person benefiting from or having interest in the transaction or business relationship. Also, there was a level of uncertainty about the methods and tools to be used for getting satisfactory assurance in cases when the individual – especially foreign high-profile persons – did not come to the FI in person, but was introduced by an authorized representative. Some banks referred to the practice of obtaining a self-identification statement with the signature of the UBO accompanied by the copy of the identity document of that person to enable verification of authenticity of the signature. However, this was not the common practice for all banks and for any non-bank FIs.

310. Discussions with the FCMC, as well as analysis of the breaches of AML/CFT requirements ascertained by the supervisor over the last years revealed certain problems with the quality of the process for identification of BOs. Particularly, there were cases when shell companies owned or controlled immediately by the shareholders and management of the banks in the non-resident clientele business comprised a significant part of the client base, while the respective documents were kept separately and not accessible for the internal control function. In certain cases the proof

obtained by banks on UBO of the customers was far lower the expectation, where primary emphasis was made on self-identification and over reliance on internet data, which was not always reliable.

311. Overall, given the presence of a very sizeable base[95] of non-resident customers, including shell companies in certain banks and PI/EMIs on one hand, and the well-known features of such clientele that complicate achieving a satisfactory level of compliance on some key issues, including identification of BO, the effectiveness of implementation of relevant AML/CFT requirements remains in doubt.

312. Except for the auditors, representatives of the DNFBPs had a vague or no understanding of BO, referred to the fact that they did not have any resources for doing relevant checks, often stating that asking questions within this notion would have a repellent effect on the customers and, in general, was something to be dealt with by the competent authorities.

Maintaining records and documents

313. Representatives of the financial sector were well aware of the requirement to maintain all transaction records, CDD data, customer files and business correspondence for at least 5 years. Some of them referred to the practice of maintaining such information and documents for significantly longer periods (e.g. 10 years for contracts or even 75 years for company staff and salary information). Notaries advised that notary deeds were kept for 75 years then handed over to the State Archive.

Refusing business for incomplete CDD

314. Legislation in force at the time of the onsite visit did not explicitly require the subjects of the AML/CFT Law to refuse customer on-boarding whenever they are unable to comply with all relevant CDD measures. There is a general prohibition to commence or continue a business relationship with the customer in cases, when identification and due diligence requirements set out in the law cannot be fulfilled. Banks and non-bank FIs referred to various standards and practices for deciding customer acceptability, varying from the lack of sufficient identification information to the matches with the names of designated persons. Internal policies of the banks define certain categories of customers unacceptable for them due to the type of activity (e.g. trade of arms, dual use goods), reputation (e.g. persons reported to be involved in illegal activities), country of residence (e.g. FATF-stated countries with deficient AML/CFT systems), designation under various international and national sanctioning regimes, or intra-company blacklisting for various reasons.

315. Unclear source of funds, inconsistent data on personal and business profile, publicly available adverse information, facts on refused on-boarding by other FIs were cited by banks and non-bank FIs as reasons for refusal of customer on boarding or termination of existing relationships. Some of them reported to have refused 10-15% of total attempts to establish business relationships or shrunk the customer base by almost 20% due to de-risking through the application of higher customer acceptance standards.

316. Failure to present the required identification documents, as well as some subjective judgment based on unusual/suspicious behaviour was cited by DNFBPs as the main, if not the only, reason for customer debarkment.

[95] Counting more than 25,000 shell companies and around 5,000 resident Latvian companies with at least one shareholder being a non-resident/shell company.

Application of EDD measures

Risk-based approach

317. Banks and other FIs presented risk-based application of CDD measures as an integral part of their internal control systems. All banks, as well as some non-bank FIs[96] reported to have implemented customer risk scoring systems for deciding the respective CDD measures to be applied. The total risk score represents the weighted sum of the scores assigned in various risk segments for factors characterizing the client, country/geography, services and products, and delivery channels. The level of risk is determined on the basis of the total risk score usually defined as low, medium or high with possible variations in between (e.g. medium low, medium high). Depending on the level of risk, simplified, standard or enhanced due diligence measures are applied. Some banks reported to be applying standard CDD measures even for low-risk customers. The initially determined risk category is subject to revision based on substantial changes in the factors within different risk segments.

318. Non-bank FIs other than licensed PI/EMIs presented a simpler framework for the risk-based application of CDD measures. Among them, the ones that were part of larger international (financial) groups (e.g. the company providing life insurance products) reported to have a risk scoring system consolidated within the group structure. The representatives of an MVTS reported to have no system for classification of clients based on risk.

319. DNFBPs did not report to have implemented any systems for risk-based application of CDD measures, including enhanced measures where applicable, for AML/CFT purposes.

Identification and verification of PEP status

320. All banks and, with a varying level of certainty, non-bank FIs[97] were aware of the PEP definition and related CDD measures. Senior management approval, establishment of the sources of wealth and funds and enhanced on-going monitoring were reported to be a part of the usual business practice in relationships with PEPs, their family members and close associates. To ascertain the PEP status of existing or potential foreign customers different databases are consulted. For local customers, some banks and non-bank FIs reported practical difficulties due to the lack of a centralized register or source to be consulted for checking the PEP status of Latvian residents conforming to the definition of PEP, including their family members and close associates.

321. There was a significant discrepancy in the number of PEP clients as presented by individual banks during onsite interviews compared to the same data provided by the authorities as ascertained through off-site reporting and onsite inspections. At that, this related to banks actively involved in the non-resident clientele business. This might be indicative of the banks' insufficient implementation of the PEP identification requirements or inadequate reporting of their PEP relationships. It should be noted that the supervisor identified significant deficiencies with regard to ascertaining PEP status of foreign clients due to insufficient information on their BOs within apparent or hidden groups of connected customers.

322. Overall, given the presence of the above-mentioned very sizeable base of non-resident customers, including shell companies in certain banks and PI/EMIs on one hand, and the well-

[96] Such as licensed PIs and EMIs.

[97] For example, representatives of an MVTS stated that whereas the PEP definition covers local PEPs only, they pay attention to foreign PEPs as well.

known features of such clientele that complicate achieving a satisfactory level of compliance on some key issues, including identification of PEPs, the effectiveness of implementation of relevant AML/CFT requirements remains in doubt.

323. DNFBPs (except for the auditors and, to a certain extent, casinos) demonstrated remote or no understanding of the PEP requirements and did not refer to any enhanced measures applied to this category of clients.

Opening and maintaining correspondent relations

324. Banks reported to have correspondent accounts with Latvian and, in some cases, with other European banks, including with the parent or sister company in case of the banks that were part of larger international (financial) groups. Internal control procedures of the banks did not contain provisions stipulating specific measures for correspondent relations with these banks.

325. The banks involved in the non-resident clientele business had a rather extensive correspondent account network with FIs – both banks and PI/EMIs – in CIS and some other[98] countries. It should be noted that the supervisor identified significant risks related to the business activities through these accounts due to the insufficient ability to monitor and assess the adequacy and compliance of the account holders' AML/CFT systems, as well as to the transactions conducted through these accounts often comprising complex transaction schemes, which did not constitute a clear economic and legal justification or purpose, but rather pointed out to intentions to hide the UBOs, to structure the transactions, as well as to enact other elements of the ML schemes.

Identification of ML/TF risks with new products, business practices, and technologies

326. There is no country-wide analysis on ML/FT risks that may arise from the use of new technologies and delivery channels (see the analysis for IO.1 for further details). Some of the banks and non-bank FIs referred to implemented or planned projects introducing new products (e.g. digital banking) or delivery channels (e.g. remote identification). However, the internal regulations of the banks submitted to the assessment team did not contain provisions defining procedures for the identification, assessment and mitigation of ML/FT risks related to the use of new products, practices (including delivery mechanisms) and technologies.

327. DNFBPs did not report any current or planned operations assuming significant use of new products, practices (including delivery mechanisms) and technologies, as well as any efforts aimed at identification, assessment and mitigation of relevant ML/FT risks.

Application of wire transfer rules

328. The assessment team was informed that all financial messaging systems used in Latvia, i.e. SWIFT for international transfers, SEPA for euro payments within EU, and TARGET2 for cross-border transfers in the Eurozone, had updated the structure of their standard messaging forms to require all originator FIs inclusion of the required beneficiary information in wire transfers. Representatives of payment service providers (i.e. banks and MVTSs) appeared to be aware of their obligations under the new Reg. (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds, which had come into effect on 26 June 2017 introducing new requirements regarding information on the beneficiary of a wire transfer and obligations on intermediary FIs involved in a wire transfer. They indicated that they would

[98] Such as China, Georgia and Turkey

refuse any transfer with incomplete accompanying information. The supervisor did not identify any breaches of the wire transfer rules both before and after enactment of the new EU regulation.

329. The assessment team was not provided information on the mechanisms and tools used by Latvian Post, in its capacity of the postal operator providing payment services using the postal network, to ensure compliance with wire transfer rules under the Regulation (EU) 2015/847.

Reliance on third-parties to perform CDD

330. Banks did not report to have practices of FATF-defined reliance on third parties[99] to perform certain elements of the CDD measures. On the other hand, the FCMC Reg. No. 196, which applies to banks, PIs and EMIs, provides, *inter alia*, the conditions and procedures for using third party agent services to perform CDD. At that, whereas the Regulation sets out a number of provisions pertinent to outsourcing/agency relations[100], it misses the key feature making them different from FATF-defined third party reliance insofar as it does not require that "the outsourced entity applies the CDD measures on behalf of the delegating FI, in accordance with its procedures" (INR 17, Paragraph 1) and that the agreement between the relying party and the agent includes a requirement for "the application of the bank's customer identification and CDD requirements" (BCBS Guidelines, Annex 1, Paragraph 14). Hence, agent relations of Latvian banks are considered in the context of the third party reliance under R.17.

331. According to information provided by the authorities (as of 30 June 2017), 5 credit institutions and 1 branch used 563 agents with authorization for customer identification in 35 different jurisdictions, 3 credit institutions used 170 agents with no authorization for customer identification in 21 jurisdiction; 1 credit institutions used 1 agent with authorization for both customer identification and collection of CDD information, and 1 credit institution was banned to use services of agents according to the FCMC decision. All of these were banks involved in the non-resident clientele business. The assessment team was not provided information on the factual use of agents by FIs other than banks.

332. The banks met onsite advised that over the last couple of years the use of agents with or without authorization for customer identification significantly decreased due to both economic and regulatory reasons. Among the agents used by these banks, some were legal companies offering company formation services, as well as accounting and tax advisory companies. Also, a number of agents were from countries with no or unknown level of compliance with the FATF Standards. This fails to conform to the definition of agent acceptability of the AML/CFT Law and does not provide for effective implementation of third-party reliance requirements. It should be noted that the supervisor identified significant deficiencies with regard to the reliance of the banks involved in the non-resident clientele business, which did not ensure adequate and regular control of the quality of customer identification performed by the agents thus exposing themselves to the risk of providing services to customers with an unacceptable level ML/FT risk.

333. Among DNFBPs, only company service providers advised of the practice to rely on third parties – mainly partner TCSPs from other countries – for customer introduction. Discussions with the private sector revealed that thousands of individuals with or without a legal status/registration

[99] That is the practice of relying on a third party (a FI or a DNFBP) that has an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the relying institution, and that applies its own procedures to perform the CDD measures (see FATF Recommendations, INR 17, paragraph 1).

[100] As set out in FATF Recommendations, INR 17 and in BCBS Guidelines for Sound Management of Risks Related to Money laundering and Financing of Terrorism (June 2017), Annex 1, "III. Outsourcing/ Agency".

in Latvia used to be engaged in this activity of finding and introducing customers to the banks involved in the non-resident clientele business. Representatives of the banks and the supervisor stated that with the tightening economic conditions and enhancing regulatory requirements, services offered by these individuals had become less popular.

334. However, as at the date of the onsite visit there were numerous references on the websites of companies registered and operating in or outside Latvia, as well as of business entities with an unknown place of registration/ operation, which, for a fee ranging between EUR 500-1,000, offered services related to the formation of Latvian companies along with opening of (offshore) bank accounts specifying the names of the Latvian banks they worked with, providing the details of the documents to be submitted on-line, guaranteeing short periods of processing the requests and high confidentiality regarding customer information.

335. In contrast, representatives of the company service providers met during the onsite visit had a very remote understanding of the AML/CFT requirements in general and of their role as providers or receivers of third-party services in particular.

Implementation of Targeted Financial Sanctions

336. All banks reported to have implemented automated IT solutions to screen customers and transactions for matches with designations under TFS related to FT. Sanctions monitoring was implemented as part of the business process in any interactions with the customers and for all types of the transactions. In case of false positives, manual analysis was done to allow the transaction.

337. Non-bank FIs reported to use the tool available on the FIU website (http://sankcijas.kd.gov.lv/) enabling searches in all relevant databases and lists of designated persons and entities. From an operational point of view it is not clear how FIs such as currency exchange offices, PI/EMIs (including the Latvian Post as a payment service provider) and securities traders (some of which are very active in the Forex market) would be technically able to screen the names of the parties and counterparties in transactions which take a time period from several seconds to several minutes to be completed. None of the banks and non-bank FIs reported to have had true positives with UN lists.

338. In relation to this, the assessment team was advised that for payment gateway services[101] there is no screening against any lists; such relationships are based on the principle of trust on the issuer of the card (which may be a Latvian or any other entity), and screening cannot be done technically due to the tight timeframes of processing the transactions, usually a matter of seconds. Given that PI/EMIs providing payment gateway services issue prepaid and postpaid payment cards, which are personalized only at an initial buyer level and can be reloaded from any bank account or even in cash[102], there is a possibility that such cards are used through merchants bypassing any sanctioning regime.

339. More importantly, the understanding and implementation of TFS appeared to be largely confined to the use of the built-in or external screening tools to identify matches with the applicable sanctions lists. There was limited display of the importance of ensuring that systems and processes

[101] That is services provided through e-commerce applications, which authorize processing of credit card or direct payments for e-businesses, on-line retailers and other "bricks and clicks" business models involving both offline and online operations.

[102] By making a cash payment at a bank desk and requesting a transfer to the IBAN account of the PI/EMI.

were in place to detect and prevent sanctions evasion through robust transactional monitoring and subsequent analysis, despite the recent sanctions-related enforcement actions and outreach by the FCMC. Whereas certain banks maintained advanced transaction screening software, FIs reported to have implemented little or no regular or *ad hoc* analyses of transactions, including credit card or direct payments, to and from locations neighbouring conflict zones in Eastern Europe or Middle East (despite the large network of correspondent accounts with FIs in such zones) or sanctioned countries. The deficiencies in the identification of UBO further obstruct substantial implementation of TFS for FT.

340. Auditors referred to the use of the tool available on the FIU website only for persons with "suspicious" names, and casinos advised about checking the names of their customers using the same tool but looking at exact matches only. Notaries informed that there was a dedicated information system developed by the Latvian Council of Sworn Notaries providing links to the Latvian registers and the FIU lists[103]. Other DNFBPs did not demonstrate any knowledge of the TFS and their implementation mechanisms.

Approach towards jurisdictions identified as high-risk

341. Banks reported to have implemented criteria of higher risk related to the customers' country of registration or operation (country risk classifier), most often referring to the lists approved by the CoM on equivalent countries[104] (the so called "white list") and low-tax or tax-free countries/territories[105] (the so called "black list"), sometimes also presenting the issue under the prism of the TFS. References were made to using various indexes issued by international organizations on corruption[106] and other criminality to determine the risk level of a country for the application of enhanced measures. Some banks and non-bank FIs referred their own lists of "unacceptably" high-risk countries.

342. The FCMC advised of providing monthly reports to the market participants on recent news from the websites of FATF, MONEYVAL and other international organizations, although not all non-bank FIs confirmed regular receipt of such communication. The FCMC website[107] contained a reference to the high-risk third countries defined by the FATF. Overall, FIs and especially non-bank FIs appeared to need more systematized and specific communication and guidance on countries for which enhanced measures are called for by the FATF, as well as on relevant concerns elaborated and countermeasures applied by the competent authorities.

343. DNFBPs demonstrated remote or no understanding of the requirements regarding high-risk countries and did not refer to any enhanced measures applied on the basis of country risk.

Reporting obligations and tipping off

344. In practice, reporting performance of banks appears to be highly uneven. Particularly, among smaller banks[108] actively involved in the non-resident clientele business, two banks with

[103] A notary advised about one case of having a positive hit, when she called the Police and got the person arrested; later on, however, the FIU informed that the hit was a false one.
[104] http://www.fktk.lv/en/law/general/laws/4265-regulation-on-the-list-of-the.html
[105] https://www.company-taxes.info/latvia-taxes-in-general/list-low-tax-no-tax-countries
[106] https://www.transparency.org/research/cpi/overview
[107] http://www.fktk.lv/en/law/general/high-risk-third-countries-identified-by-fatf/6552-high-risk-third-countries-identified-by-fatf.html
[108] I.e. the ones having less than 4 thousand active clients and EUR 500 million assets under management

comparable characteristics of client base[109] filed an STR on, respectively, every 550th and 9th customer. A similar picture is observed among bigger banks[110], again, actively involved in in the non-resident clientele business – the respective ratio of the number of clients to the number of STRs ranging between 48 and 205. This disparity is there when comparing STR reporting performance of the banks relative of other criteria of business activity such as the amount of the assets, the number of resident/ non-customers etc. This is indicative of an uneven understanding and implementation of the STR reporting requirement among banks in general and among those exposed to comparable levels of the ML/FT risk in particular.

345. Deeper analysis of the STR reporting process, i.e. the number of transactions processed by individual banks – especially those in the non-resident business – juxtaposed with the number of alerts generated by their internal control systems, the average time required for analysing each alert and the number of staff involved in the process indicates that in certain cases the alerts on potentially suspicious transactions are processed superficially without comprehensive analysis of all pertinent risk factors. Delayed reporting, i.e. the cases when STRs are filed on empty accounts after completing the relevant transactions along with defensive reporting, i.e. when the main purpose of filing STRs is to safeguard against possible future sanctions for the failure to report, also seemed to be a part of the existing reporting practices.

346. According to the statistics provided by the authorities, among around 4.7 thousand STRs filed by banks with the FIU less than 10% are made for suspicions related to potential tax evasion – both domestic and foreign. This ratio is even lower for 2015 and 2014 – 3% among around 6.8 and 5.1 thousand STRs, respectively. At that, some banks involved in the non-resident clientele business reported that they had never suspected foreign tax evasion. This was not commensurate with what the banks presented as the main hypotheses underlying their suspicions when filing STRs on one hand and to the ML threats identified by the 2017 NRA on the other hand. It might be indicative of, inter alia, the lack of specificity by banks in describing the potentially illicit activity, insufficient capacity of the FIU to classify the STRs as per the proposed hypotheses on ML or predicate offences to enable further operational and strategic analyses and, overall, of issues related to the quality and usefulness of STRs.

347. The FCMC was aware of the above-described issues with STR reporting. It advised of a significant number of cases when, in the course of onsite inspections in banks, the inspectors ascertained transactions and business relationships with characteristics of suspiciousness, whereas the bank failed to file an STR thus demonstrating a formal approach to its STR reporting obligation. In such cases, the FCMC filed STRs to the FIU on its behalf, also checking adequacy of the process through which the internal alert generation was escalated to suspicious transaction reporting to the FIU.

348. Among non-bank FIs, only PI/EMIs and currency exchange offices reported to have implemented transaction monitoring and alert generation systems based on regulator-developed and own scenarios. The reporting figures were low, e.g. in 2016 PI/EMIs filed 77 STRs, the MVTS – 160 STRs, currency exchange offices – 494 STRs, and other non-bank FIs did not file any STRs, which may be partly due to the nature of their business and partly due to the lack of proper systems and capacities to identify and report suspicious activity.

[109] I.e. with almost 100% of the total credit turnover on accounts held by high-risk customers including, respectively, 71% and 54%– by shell companies

[110] I.e. the ones having more than 25 thousand customers and EUR 2.7 billion in assets under management

349. Among DNFBPs, auditors and (to a lesser extent) notaries demonstrated some knowledge of the STR reporting obligation. Other DNFBPs understood this obligation as the reporting of UTRs only. They sometimes confused it with the reporting to the SRS for local tax evasion-related suspicions, and had rarely, if ever, filed STRs as required

Factors impeding efficient STR reporting

350. Discussions with the obliged entities showed a certain extent of confusion caused by the current system of reporting what the legal framework defines as "unusual transactions" and "suspicious transactions". Particularly, UTRs are to be filed whenever the amount of cash transactions exceeds certain thresholds, as well as in relation to any customers suspected for committing or participating in acts of terrorism or characterized by publicly accessible adverse information pointing out to a potential relation of the customer to proceeds of crime, ML or FT[111]. STRs, in turn, are to be filed in the presence of any suspicions that "funds involved therein are directly or indirectly obtained in the result of a criminal offence or are related with terrorism financing, or an attempt to carry out such actions"[112]. This overlap in the definition of UTRs and STRs results in uncertainty as to the expected performance of the obliged entities, which often feel satisfied with the submission of a certain number of UTRs mostly comprised of over-threshold reporting.

351. Legislation in force at the time of the onsite visit does not define any indicators for suspicious transactions[113]. The CoM Reg. 1071 (22 December 2008) establishes the indicators for unusual transactions, as well as the procedure and form[114] for reporting unusual and suspicious transactions to the FIU. These indicators for unusual transactions provide various – mainly upper threshold-based and cash-related – descriptions of types and patterns of transactions in relation to different categories of the subjects of the AML/CFT Law. The only indicator that applies to all REs, refers to situations whereby the customer is "suspected of committing an act of terrorism or participation therein and is included in the list of such persons regarding which the FIU has informed the REs and their supervisory and control authorities". This means that any suspicions about a customer to be a potential terrorist would trigger filing an unusual – but not necessarily a suspicious – transaction report.

352. Then, for banks, in addition to the indicator referring to situations where publicly accessible information points out to the customer's potential involvement in ML/FT[115], transacting in cash at or above various amounts is the only criterion to determine whether the transaction is unusual or not, thus leaving aside many other key characteristics of unusualness/suspiciousness related to the personality, transactional behaviour and other profile-specific features of the customer.

353. Moreover, for all other categories of the REs, the indicators for unusual transactions are too narrowly defined and would unavoidably result in a very limited interpretation (and implementation) of the reporting obligation or, in some cases, reasonably be confused with other

[111] Art.8.2 of the CoM Reg. No. 1071 of 22 December 2008.
[112] Sec.1(17) AML/CFT Law.
[113] On 25 September 2017 the FCMC issued non-binding Recommendation No. 152 setting forth the "red flags" for banks to identify suspicious transactions.
[114] According to the CoM Reg. 765, a new on-line reporting system currently tested in the FIU (since April 2016) will be *de jure* implemented starting from 1 January 2018.
[115] At that, this indicator does not apply to the subjects of the AML/CFT Law other than banks.

responsibilities under the AML/CFT Law[116], eventually failing to provide a solid reference base facilitating implementation of the reporting requirement.

354. Finally, both the authorities and the obliged entities referred to the Law on Taxes and Fees providing for the obligation of every subject of the AML/CFT Law to file reports to the SRS (as per indictors for determining suspiciousness of transactions from the standpoint of tax compliance) on transactions concerning taxes which are suspicious for the purposes of the AML/CFT Law. The assessment teams considers that such a "parallel" system of STR reporting, whereas having no relevance for the compliance of the obliged entities with STR reporting obligation to the FIU, might potentially create confusion as to the appropriate authority to deal with the ML/FT suspicions of the subjects of the AML/CFT Law. This issue is especially topical for the DNFBPs with insufficient knowledge in the area of AML/CFT.

Practical measures to prevent tipping off

355. Representatives of the private sector were aware of the prohibition to tip-off the customers and the permission to inform them about enacting the refraining mechanism, which was reported to be used from time to time. There were references to cases when customers refused by the bank to transact due to the application of the refraining mechanism already knew about the referral of the case to the FIU because of their involvement in scandals widely known to the public.

Internal controls and legal/regulatory requirements impending implementation

356. In addition to the mechanisms available for identification and assessment of ML/FT risks (as described above) and in the context of the ML/FT risk mitigation framework (as described above), FIs were fluent in describing their internal control systems to comprise all three lines of defense, i.e. the front office/ customer servicing function in charge of identifying and communicating the ML/FT alerts, the compliance function in charge of implementing AML/CFT measures, and the internal audit function in charge of independently testing overall implementation of the AML/CFT requirements.

357. References were made to the availability of internal regulations, procedures, instructions and other guidance providing details of the business processes with clear description of the relevant AML/CFT obligations of the staff. Banks reported to have policies and processes for screening the staff so that appropriate ethical and professional standards were ensured, and to have ongoing employee training programs so that the staff was adequately trained to implement their AML/CFT obligations. In a number of cases external certification (such as ACAMS) was made a requirement for compliance officers.

358. The AML/CFT compliance function was reported to be installed within or outside the broader compliance setup, in the form of a separate structural unit or, at smaller institutions, of a responsible staff member. To implement the requirement of the AML/CFT Law, banks appointed a member of the Board responsible for AML/CFT matters. The chief compliance officer had the responsibility for ongoing monitoring of the fulfilment of the AML/CFT duties and was the contact point regarding AML/CFT issues both for internal parties and external authorities (such as the FCMC and the FIU). Consideration of ML/FT concerns at the highest level was provided for through dedicated AML/CFT or similar compliance-focused committees adjunct or subordinated to the

[116] For example, DPMS are required to file a UTR whenever the customer settles the payment in cash at or above EUR 15,000, which means that in all instances of acting as a subject of the AML/CFT Law (i.e. dealing a cash transaction at or above EUR 15,000 as defined in Clause 9 of Sec.3(1) of the Law) these DNFBPs would not file anything but UTRs.

Board. Staffing of the AML/CFT function increased significantly over the last two years, with some banks having up to 20% of the total staff dedicated to AML/CFT tasks.

359. Nevertheless, there are certain concerns about the insufficient independence of the compliance (as well as audit) function particularly regarding the decision-making on termination of business relationships and reporting of STRs, and concentrated ownership structure of the banks is among the reasons for that. Another concern is about the lack of appropriate access of the compliance staff to the CDD and other relevant information on non-resident customers/shell companies owned or controlled by the shareholders and management of the bank (as described above). Formal enforcement of the AML/CFT requirements and relevant internal control measures (including applicable policies and procedures) is a further concern disabling substantial determination of the ML/FT risk exposure of the customer base and implementation of adequate mitigation measures. In relation to this, none of the banks involved in the non-resident clientele business reported about significant AML/CFT breaches identified and remedied by their internal control systems, even in cases when the presence of major deficiencies in the AML/CFT internal control systems with the deliberate involvement of some bank staff was widely reported in mass media.

360. Non-bank FIs that were part of larger international or local (financial) groups reported to be availing the relevant AML/CFT structures and resources of the parent company by way of, for example, applying group-wide policies and procedures, using the group's data processing and analysis systems, and employing services of the group AML/CFT function. In relation to this, there are concerns about staff resources and capacity of the Latvian Post (7 staff members responsible for AML/CFT, of which 2 responsible for transaction monitoring throughout a total number of 620 locations, of which 450 provide financial services) to provide for an appropriate AML/CFT function.

361. Some of the DNFBPs (such as auditors and casinos) reported to have installed a position responsible for AML/CFT, others (such as notaries) informed that they implement the respective function themselves, whereas the rest did not see the need and relevance for having a dedicated function in their business for any reason.

362. On the background of the sanctions imposed by the FCMC for breaches of the AML/CTF Law and regulatory requirements over the last two years due to major weaknesses in CDD, transaction monitoring and other internal control systems of the banks, it does not seem that the apparent knowledge of the relevant requirements demonstrated by the banks to the assessment team necessarily transforms into their appropriate implementation in practice. Given the fundamental nature of the compliance issues identified at least with regard to some banks involved in the non-resident business, it would not be realistic to assume that within the relatively short time period after the supervisor ascertained those issues the banks have been able to remedy them to a significant extent.

363. With regard to the sanctioning practices of the FCMC, the banks were of the opinion that regulatory requirements were growing too fast, and that they were not charged for a specific (intentional) breach of the existing rules but for the opinion of the supervisor that much more could have been done in terms of improving their internal control systems. On the other hand, 80% and more implementation of the respective remediation plans reported by individual banks do not seem to reflect the real situation if counted not by the number of the supervisory recommendations, but by their essentiality as well as the investment factually made for the improvement of compliance.

364. The lack of regulation in the fields of professional activity such as real estate brokerage, tax advice, accounting and company formation services, and the subsequent presence of a very significant unregulated market in these professions were reported to be a substantial impediment for the obliged entities to effectively implement their AML/CFT obligations.

Conclusion

365. Among the representatives of the private sector, the understanding of ML/FT risks significantly varies both in terms of the knowledge on the subject matter and the comprehension of its significance. Risk assessments conducted by the banks did not provide any specific analysis of the FT threats and vulnerabilities and not always seemed to reflect the actual level of the overall ML/FT exposure. The understanding of FT risks was largely confined to the use of what was generally referred to as "terrorist lists" – a combination of the UN and certain other lists, including the ones provided by the FIU. Effectiveness of the application of mitigating measures commensurate to the risks is in doubt, specifically with regard to the banks involved in the non-resident clientele business, due to major deficiencies related to the implementation of internal controls.

366. Banks and non-bank FIs demonstrated fair knowledge of the applicable requirements in the AML/CFT Law and relevant regulations regarding the pillars of the preventative regime, including those related to CDD and record keeping. Nevertheless, there are grounded concerns about the quality of the additional information/documents collected and maintained by banks in the CDD process for verifying the UBO, obtaining proof of the source of funds and source of wealth, as well as for monitoring transactions. Given the presence of a very sizeable base of non-resident customers, including shell companies in certain banks and PI/EMIs on one hand, and the well-known features of such clientele that complicate achieving a satisfactory level of compliance on some key issues, including BO and PEP identification, the effectiveness of implementation of relevant AML/CFT requirements remains in doubt.

367. STR reporting performance of banks appears to be highly uneven, which is indicative of an uneven understanding and implementation of the reporting requirement among banks in general and among those exposed to comparable levels of the ML/FT risk in particular. Delayed reporting and defensive reporting also seem to be a part of the existing reporting practices. There are certain concerns about the insufficient independence of the compliance (as well as audit) function, the lack of appropriate access of the compliance staff to the CDD and other relevant information on non-resident customers/ shell companies, as well as formal enforcement of the AML/CTF requirements and relevant internal control measures. **Latvia has achieved a moderate level of effectiveness for IO.4**.

CHAPTER 6. SUPERVISION

Key Findings and Recommended Actions

Key Findings

IO.3

- There is a large number of sector regulators in Latvia who are each assigned responsibility for supervising FI and DNFBP sectorial compliance with the AML/CFT law. This approach, while in theory ensuring that there is supervision applied to all sectors, creates potential for execution risk

when ensuring all sectors are covered by AML/CFT supervisors. A recent example: changes to AML legislation in the recent past mistakenly left a gap in coverage. In addition, given the uneven level of understanding of risk, the potential for inconsistent interpretation of obligations, and application of supervisory measures are also issues. Finally, most regulators (particularly the SRS) appear to lack adequate resources to supervise their obliged entities populations.

- There is a broad range of market entry measures in the FI sector, most of which seems adequate, especially those operated by the FCMC, the BoL and the Consumer Protection Rights Agency (CRPC), which seem quite robust. However, it is not clear that during the monitoring process the FCMC's measures for monitoring on-going compliance with fit and proper requirements are always effective. The same is true of the LGSI in the casino sector. The Sworn Lawyers, Notaries, and Auditors operate systems aimed principally at professional standards but with adequate criminal checks. The DPMS operate professional entry requirements that do not include criminal checks. There are no entry requirements in the tax consultant, accounting, legal services provider, real estate, car dealer/intermediaries, and other high value providers sectors. This is a concern given that company service providers and real estate agents are among the medium to high risk-ranked groups in the NRA.

- The supervisors demonstrate widely varying views and knowledge about ML/FT risks. The authorities are aware of this issue, as noted in the FSDB strategic plan. The FCMC displays the highest level of risk understanding demonstrated through multiple examples. Other supervisors often referred to mitigation as risks, and non-compliance with preventative measures as a risk. Overall, the BoL displays an acceptable level of understanding. All other supervisors generally displayed a moderate to low level of understanding of ML/FT risks, even in some cases where their supervised sector was medium or high risk – for example the company service providers supervised by the SRS.

- All FI and DNFBP supervisors appear to understand the theory of paying more supervisory attention to their higher risk market segments; however, in practice, issues such as understanding the nature or significance of ML/FT risk, or a lack of knowledgeable resources, prevented them from fully implementing such programs. For example, the FCMC has inspected a relatively low number of high risk banks in the foreign deposit sector, despite understanding its high risk characteristics, because it had to divert attention and resources to PF sanctions evasion issues. Resources are also a particular issue in the sectors supervised by the SRS where onsite supervision is in its early stages in some higher risk sectors.

- Effective, proportionate and dissuasive sanctions are relatively new in Latvia as the increased sanctions for AML/CFT related breaches entered into force between (in the banking sector) July 2016 and the date of the onsite visit; the assessors believe that it is therefore too early to determine the overall effect the sanctions are having on the obliged sectors.

- The FCMC has used its powers to some effect in the non-resident deposits banking sector by applying significant penalties for failing to identify BOs and implement adequate controls, and this has improved the focus of banks providing services in this sector. Other regulators have either not applied such penalties or have been granted authority too recently to have effective sanctions already applied.

- Despite the knowledgeable and persistent approach taken by FCMC to the non-resident banking sector, the rate of change of risk appetite in this sector is slow. Some banks in the non-resident account market have actively de-risked their portfolios over the past few year, and the

authorities anticipate this will likely continue but the rate of de-risking is not known. The MoF is for the time being content to let the FCMC deal with the risks presented by the non-resident bank accounts. This is on the basis of the reduction in the size of this account group over the past year, along with the assessment that the prudential risks presented by these accounts is lower than calculated a year ago. The other FI regulators have provided guidance on risks and are considered to be a source of help by FIs interviewed. The impact of supervisors in the DNFBP sector, with the exception of the LGSI, is not really noticeable.

Recommended Actions

- The authorities should review the FSDB strategic plan as it relates to supervision, with a view to:

a. Setting up a mechanism under the auspices of the FSDB to ensure that all supervisors (including SROs) come to a common understanding of ML/FT risks and the adequacy of preventive measures to be applied to address these risks; and

b. sharing knowledge of ML/FT risks, addressing adequacy and consistency of supervisory resources (including market entry criminal background checks for all sectors), identification of high risk FIs/DNFBPs, and the risk- based approach to supervision.

- The FCMC should substantially increase the frequency of AML/CFT supervisory visits to the foreign deposits banking sector.
- All financial and DNFBP supervisors should review their criteria for the application of available sanctions to ensure that the full range of sanctions is applied by the authorities to address violations of AML/CFT obligations, both with regard to institutions and their management, and analyse the dissuasiveness of the sanctions applied.
- The supervisory authorities should continue systematic outreach to FIs and DNFBPs to promote understanding of ML/FT risks and preventive measures.
- The numbers of staff and resources for the supervisory authorities should be reviewed to ensure that these authorities can adequately deal with identified risks and monitor how their subject entities respond to them.
- The SRS should apply more resources to its AML/CFT supervisory programme and ensure adequate, risk- based, coverage over the wide variety of obliged entities subject to its supervision.
- The supervisory authorities should further enhance consistent policy in monitoring on-going compliance with fit and proper requirements in case of failure of AML/CFT requirements.
- Authorities should take measure in a reasonable timeframe to undertake assessment of non-resident deposit base and related cross-border flows in the context of identified and potential ML/FT risks.

368. 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 R26-28 & R.34 & 35.

Immediate Outcome 3 (Supervision)

369. In Latvia AML/CFT supervision is the responsibility of the sectorial supervisors in the FI and Casino sectors, and the SROs that supervise the legal, auditing and notaries professions. The SRS is

the designated AML/CFT supervisor for other sectors, notably the real estate, DPMS and large value sectors, and the TCSP sector (which includes the accounting sector). Cash collectors and financial leasing companies are subject to the AML/CFT Law but at the time of the onsite visit were not supervised for compliance with AML/CFT preventive measures (although in practice many of these providers are indirectly supervised by their parent FIs, notably banks, which in turn are subject to supervision by the FCMC). Under amendments to the AML/CFT Law that entered into force during the onsite visit, the CRPC (previously unsupervised for AML requirements) became their sector supervisor.

370. The FCMC has demonstrated a proactive supervisory stance in respect of the vulnerabilities of the banks that provide deposit services to non-residents; however, despite these efforts, the rate of change of risk appetite in this sector is slow. The other FI supervisors and LGSI displayed a more passive approach but with a general awareness of some higher risks. In the DNFBP sector, the professional SROs have done some preliminary work on identifying higher risk elements of their population but have not yet completed supervisory programs based on these elements. The SRS programs are in their early stages (started 1 September 2017), notwithstanding that the AML/CFT Law has been in place for some time in some sectors. Accordingly, the assessors' ability to assess effectiveness was limited in these sectors.

371. The FI sector is dominated by the banking sector, which is supervised by the FCMC. The NRA notes that about 80% of the capital in this sector is foreign controlled, with shareholders in Scandinavia being the single largest group, followed by investors in Russia, Ukraine, UK and USA. The overall size of the banking sector has shrunk over the past several years and stood at EUR 29.5 billion as of the end of 2016.

372. Non-residents hold a significant portion of deposits in the banking sector. Foreign controlled deposits amount to more than 50% of all deposits, although this percentage has been declining over the past several years. A number of banks specialize in these foreign deposits services, which historically developed to meet the demand for Western banking services in Eastern Europe following the collapse of communism and the need for a stable and safe place for deposits. Latvia's strong IT infrastructure and Russian- language facilities were additional attractions.

373. These non-resident accounts present the highest ML and other risks to the financial sector in Latvia. Due to the transitory nature of Latvian non-resident business, the FCMC considers that the best measure of ML/FT risk exposure, used for supervisory purposes, is actual volumes of non-resident customers' payment turnover rather than by their deposit amounts, because low account balances on high payment turnover accounts may represent the same risk level, as those of higher balances. Non-resident customer transaction volumes made through NOSTRO correspondent accounts (incl. accounts held with the Bank of Latvia) accounted for EUR 118.5 billion in the first nine months of 2017 or 50.36% of the total customer transaction turnover processed via NOSTRO account networks by Latvian banks.

374. Holders of record of many of these foreign deposits are in a number of offshore financial centres, with no access by Latvian authorities to their UBO due to the presence of foreign legal structures and lack of access to BO information in such centres. The authorities report that there are more than 25,000 "shell" entities involved in opaque ownership structures. About 5,000 of these are Latvian entities. This structure is discussed in more detail below.

375. The measures taken by the authorities over the years to address the risks posed by opaquely-owned foreign deposits are limited. Until the time of the onsite there were two BO definitions in

place, one in the Companies Law and the other in the AML/CFT Law; this issue is more fully discussed under IO.5. The divergent definitions were addressed whilst the assessors were onsite, and for this reason effective BO measures cannot yet be assessed. In addition, the risks (including ML risks) presented by these accounts were the subject of a World Bank report to the authorities in 2016 but, as noted below, by the time of the onsite visit the authorities had not taken any action, outside of supervisory action.

376. The number of banks offering services to non-residents has declined significantly over the past 10 years. The remaining aggregated foreign deposits held in Latvian banks pose stability and supervisory issues for the authorities. In 2016 following de-risking of a number of Latvian banks by western banks due to ML/FT concerns, the World Bank report (noted above) made a number of recommendations, both prudential and structural, to address the ML/FT risks, which as of the date of the onsite visit had not been acted upon by the authorities. However, the FCMC is very conscious of the ML/FT risks to the Latvian banking sector presented by these deposits, and agrees with the concerns of the WB. Overall, it is not clear whether the ML/FT risks in the sector are yet being adequately mitigated.

Licensing, registration and controls preventing criminals and associates from entering the market

Financial Institutions

377. Fit and proper decisions are made through the EU Single Supervisory Mechanism (SSM) for members of the management board and supervisory board of the three significant banks in Latvia, and for qualifying shareholders of all banks[117].

378. As described by the authorities, entry to the banking sector is subject to a robust and comprehensive set of controls administered by the FCMC, which includes criminal background checks on the BOs, supervisory boards, and management boards of all banks. The FCMC assesses not only the direct acquirer of qualifying holding but also the influence and close links with relatives and joint business partners. When assessing the integrity of the proposed acquirer, the supervisor may take into consideration the integrity and reputation of any person linked to the proposed acquirer, meaning any person who has, or appears to have, a close family or business relationship with the proposed acquirer.

379. Similar controls apply to newly appointed persons in existing board positions, and new BOs. The FCMC monitors compliance through an annual information process exercise, monitoring major transactions in which banks are involved, and criminal checks.

380. However, it is not clear that during the monitoring process the FCMC's measures for monitoring on-going compliance with fit and proper requirements are effective; for example the PF sanctions evasion measures taken by managers at some banks suggest that some managers should not have been considered "fit and proper". As indicated by the authorities the FCMC does not have more statistics on official rejections because of the pre-notification process, meaning that potential shareholders are pre-assessed before an official application is filed and therefore many are rejected due to several reasons - incapacity of financial resources, state of origin, reputation issues, membership or ownership of questionable groups or companies.

[117] The ECB has the power to make fit and proper decision only for the banks which are considered as significant. National authorities are responsible for fit and proper decisions in relation to less significant banks.

381. The FCMC also applies similar fit & proper standards to the payment provider, insurance, investment broker and investment management sectors, except for alternative investment funds, which in certain cases provided in the legislation (please see R.26) are subject only to registration.

382. Similar controls apply to the bureaux de change supervised by the BoL. The Latvian Post is a state-owned monopoly on financial services (deposits and remittances) offered through post offices.

383. Consumer lending companies must be licensed by the CRPC. Background checks are applied to the members of capital company councils (if such have been formed) and boards. Funds which are invested into the equity capital of the capital company are checked, but no checks are applied to the BOs. No licensing or entry controls are applied to financial leasing companies, except those that also provide consumer lending (leasing).

384. To identify unlicensed service providers, the FCMC experts examine applications and information about the unlicensed service providers pursuant to the Commission procedure No. 04.07.03.PRC.72.1 and if in addition to direct everyday duties suspicious advertisements or offers are identified, this information is submitted to the FCMC expert directly responsible for monitoring the activities of unlicensed service provider.

385. Information about possible unlicensed service providers has been also reported to the FCMC by existing market participants, notifying of suspicious service providers, as well as the FCMC calls on natural and legal persons to communicate with the FCMC to make certain about the right of individual service providers to offer financial services before starting business relations with them and report about unlicensed service providers if any breaches ascertained. In the cases when unlicensed activities are confirmed, the FCMC sends a written request to the relevant FI suspending the provision of unlicensed services and requiring an explanation of its activities. If the breach is not remedied, the FCMC places a warning about the unlicensed service provider on its website (20 warnings have been published since 2016) and forwards aggregated information about the breach to the SRS (Sec.166.2 and 215.1 of the Latvian AVC) and the SP (Sec.207 CL), the authorities responsible for examining the breaches of business activity according to the severity of crime (including the provision of financial services without relevant licence).

386. According to information provided by the authorities, several criminal proceedings related to unlicensed service providers' activities have been initiated by the SP. The SRS had refused in one case to initiate an administrative case because of the lack of evidence; on 15 December 2016, the SRS (decision NK.031199) imposed a EUR 280 fine on a natural person; on 10 August 2015, the SRS (decision NK.025112/479p) applied a EUR 280 penalty to the board member of the company (natural person). In cases where unlicensed service providers are from other EU States the FCMC communicates with those supervisory authorities to inform them about unlicensed service providers and requests the regulators of those countries to take relevant measures to suspend the provision of unlicensed services in Latvia.

387. In 2016 the FCMC decided to prohibit a bank in another EU State from providing financial services in Latvia: including a prohibition on attracting new customers in Latvia and a requirement to terminate existing contractual relationships with current customers in Latvia. The decision to impose the ban was adopted because the bank had substantially violated applicable procedures laid down in the Credit Institution Law. The bank had continuously provided financial services through a permanent and unauthorised physical presence in Latvia.

DNFBPs

388. Entry to the Casino sector is subject to a robust and comprehensive set of controls applied by the LGSI, which includes criminal background checks on staff and owners of casinos (lotteries are a State monopoly). However, as noted in the TC Annex, the check does not cover the associates of criminals. The Council of Sworn Notaries is an SRO which controls entry to the notarial profession on behalf of the MoJ. There are fit & proper controls in place. Similar processes are applied by the Council of Sworn Lawyers in respect of the legal profession, and the Association of Sworn Auditors for the auditing profession. The DPMS operate professional entry requirements that do not include criminal checks.

389. There are no entry controls in place in the real estate agent, accountant, and trust/company service providers sectors.

Supervisors' understanding and identification of ML/TF risks

FCMC

390. The FCMC's breadth and depth of understanding of ML/FT risks in the financial sector is high, and they have developed their own risk matrices applicable to the sectors they supervise. This is more fully discussed below. Generally, they do not agree with the risk ranking conclusions of the NRA, although they agree that the NRA analysis is broadly acceptable. They demonstrate a high level of understanding of risks compared to the other financial regulators. The FCMC has a broad understanding of ML risks of each bank, including information on the client base, provided services and internal control systems. Given the size of the banking sector and its domination of the financial sector in Latvia, the assessors assigned a somewhat higher than average weighting to the impact of the FCMC in the Latvian AML/CFT regime.

391. BoL: The BoL demonstrated an adequate level of knowledge of ML/FT risk. The foreign exchange sector is at a lower risk level than the banks and other FIs, and the BoL's level of knowledge is adequate to supervise this sector.

392. MoT: The MoT demonstrated a low level of knowledge of ML/FT risks compared to the other financial regulators and considered cash as the main ML threat for the post offices. Although they seemed to understand ML, they had not considered any FT risk factors.

393. CRPC: the CRPC demonstrated an adequate level of knowledge of ML/FT risk. The consumer lending sectors are at a lower risk level than the banks and other FIs, and the CRPC's level of knowledge is adequate to supervise this sector.

394. SRS: The SRS demonstrated a basic knowledge of ML/FT risks in their sectors (financial leasing companies, accountants and DPMS). The financial leasing sector is at a lower risk level than the banks and other FIs.

395. LGSI: The LGSI demonstrated a basic knowledge of ML/FT risks but have not developed a risk matrix applicable to the casino and lottery sectors. Their supervisory process seems to be mostly aligned to compliance with the gambling legislation.

396. Association of Sworn Lawyers: The Association participated in the NRA process by way of supplying information and interviews. The Association views Sworn Lawyers as lower risk overall than those practicing as trust or company services providers outside the supervision of the Association.

397. Association of Sworn Auditors: demonstrated a basic knowledge of ML/FT risks. The Association's representatives considered that auditors working in the financial, construction and pharmaceutical sectors were at highest ML/FT risk. The Association partly agrees with the conclusions of the NRA.

398. Association of Sworn Notaries: The Association demonstrated a fairly good knowledge of how funds can be laundered in transactions supervised by them, mostly through the real estate market. It is not mandatory in Latvia to use a notary to formalize a real estate contract; only about 10% of the market is subject to notarial scrutiny. The Association generally agrees with the conclusions of the NRA.

Risk-based supervision of compliance with AML/CTF requirements

399. FCMC: The FCMC has 15 staff members in the AML/CFT unit devoted to AML/CFT supervision (onsite and offsite). This comprises six staff members from the bank supervision section, three from the transaction monitoring division, three from the non-banking supervision division, and three from the sanctions and compliance division. The FCMC has a well-developed supervisory programme that is risk-based using their knowledge of risks in the financial sector. They have divided their FI population into four risk groups using client, product, geographic and other risk criteria. The banks that specialise in foreign deposits are the highest risk group and these are usually subject to more frequent and deeper on- and off- site supervisory programmes. These programmes also address compliance with TFS. In order to assess overall inherent ML/FT risk-weight a set of risk factors has been developed that is used to evaluate comprehensively and in greater detail the inherent ML/FT risks of banking activities, their provided services and client-base. According to the risk categories of each bank, the FCMC plans the schedule of examinations of each bank (types, frequency and scope of examinations).

400. The FCMC regularly assesses and analyses the overall risk exposure indicators of banks, who are obliged under the FCMC Regulations to submit a quarterly report to the FCMC on the characteristics of their ML/FT risk exposure.

401. Banks are assessed using a suite of financial and ML/FT risk criteria: which includes the ML/FT risk profile of the financial services sector, AML/CFT priorities, processes and quality control, bank-specific ML/FT risk exposure, the scope of the information subject to analysis, and corporate governance. This information is obtained from the quarterly AML/CFT reports filed by the banks with the FCMC.

402. Offsite examinations are targeted at a specific element of or related to the bank depending on the purpose of the examination (e.g. clients or their BOs, indicating possible involvement in ML/FT). In 2014 the FCMC conducted 10 targeted off-site examinations and assessed bank internal regulations (procedures) on 10 thematic topics[118]. In 2015 the FCMC conducted 4 targeted off-site examinations and assessed bank internal regulations (procedures) on 8 thematic topics. In 2016 8 targeted off-site examinations, on 25 thematic topics in regard of internal regulations (procedures) of the banks where assessed; in 2017: 6 targeted off-site examinations, on 63 thematic topics in regard of internal regulations (procedures) of the banks where assessed. The institutions

[118] Thematic topics usually involve review or assessment of particular subject within financial institution's AML/CFT framework and internal control system. Such cases have involved e.g. assessment of procedures governing the cooperation with bank agents, assessment of bank's AML/CFT risk management strategy, review of ML/TF risk assessment methodology, sanctions risk assessment methodology, assessment of internal documents related to expansion of e-commerce operations within the organization, and other issues.

representing the highest risk in the market were selected for targeted inspections. In 2016-2017 the FCMC Compliance Department analysed ML/FT risk management strategies elaborated by all credit institutions in order to assess compliance with the legal requirements including assessment with regards to established ML/FT risk exposure indicators, measures and tools to mitigate the identified ML/FT risks and existence of criteria for allocating sufficient level of resources. The FCMC has provided supervisory interventions on the shortcomings in strategies to all banks.

403. This approach thus enables the FCMC to test the effectiveness of these controls during the schedule of onsite visits.

Onsite visits to banks

404. Onsite inspection visits are prioritized for the highest risk FIs as assessed by the FCMC. The following table sets out the numbers of onsite visits made to banks by the FCMC in the years indicated.

Table 20

Banks	Banks oriented towards the provision of services to local customers	Banks oriented towards the provision of services to foreign customers	Number of visits to banks in each risk category			
			2014	2015	2016	2017 (January-June)
Critical ML/FT risk banks	0	0	0	0	1	1
High ML/FT risk banks[119]	0	10	7	5	3	4
Medium ML/FT risk banks	1	3	0	1	0	0
Low ML/FT risk banks[120]	9	0	1	0	1	1

405. The FCMC also conducts thematic work (for example, work arising from the US audit in 2016). Typically, a FCMC team can spend 6 weeks to two months on the onsite portion of the supervisory work at a high risk bank. Findings result in a letter to the bank, and a two-week period is allowed for receipt of a response. Most findings across the sector require "essential" remediation measures. The priority of FCMC in planning the supervisory actions is to ensure the systematic supervision of the banks oriented towards the provision of services to foreign customers. Generally, the number of onsite visits conducted to such banks in the period under consideration is low. The reasons for this are noted below.

406. In addition to the onsite and off-site inspections mentioned above, the FCMC uses a variety of other supervisory tools such as regular reports on risk exposure, payment flows, *ad hoc* inquiries, etc. to monitor the activities and risks relating to FIs.

407. PIs and EMIs, as well as other FIs under FCMC's supervision are also subject to onsite examinations and off-site examinations (in the form of review of technical compliance of internal regulations (e.g. procedures)), which are carried out according to the examination plan. The length of the examinations vary depending upon the business model of the institution, the scope of the inspection, the severity of violations identified during on-going supervision, the risks the FIs face and other factors. The number of inspections of PI/EMIs has been as follows: three in 2014 (three high risk institutions), two in 2015 (two medium risk institutions), two in 2016 (two high risk

[119] Bank poses high ML/FT risk and its risk management is weak.
[120] Bank poses low ML/FT risk and its risk management is adequate.

institutions) and one in the first half of 2017 (one high risk institutions). The FCMC has conducted a limited number of inspections of PIs and EMIs.

408. As for the other FIs supervised by the FCMC, two onsite inspections of participants of financial instruments market, which were classified as high risk institutions, were conducted in 2015 and 2016.

409. Based on the number of inspections conducted, it can be concluded that the FCMC does not have sufficient resources to improve full risk-based supervision of FIs it supervises. The FCMC advised the assessors that the primary measures considered by FCMC to increase the efficiency of the supervision processes are related to the improvement and expansion of the usage of IT tools, not increases in the numbers of staff. However, the assessors consider that given the range of issues facing the foreign deposits banking sector (and notably the resources diverted to the sanctions evasion matter referenced below which negatively impacted the number of onsite inspections in the banking sector in 2016 and 2017), the FCMC should address whether it has sufficient staff to apply an appropriate frequency of onsite inspections in this sector.

410. BoL: The BoL has a standard inspection methodology for all foreign exchange dealers, which is not particularly geared to higher risk FIs, but which does include an assessment of compliance with TFS. The number of inspections has been as follows: 44 in 2014, 35 in 2015, 27 in 2016 and 13 in the first half of 2017. Most of the onsite work is oriented to reviewing reported STRs and the systems designed to support these filings. The BoL also reviews hiring processes, as well as records designed to detect structuring of transactions. More frequent inspections are reserved for FIs with high turnover or those demonstrating non-compliance with legal requirements, rather than high risks.

411. The BoL drew attention to Reg. 158 which entered into force during the onsite visit; however, the representatives interviewed by the assessors seemed unfamiliar with the concept of enhanced due diligence as defined in this Regulation.

412. MoT: The MoT inspection of Latvian Post is essentially confined to an examination of systems and processes at the headquarters of Latvian Post in Riga: there are no inspections of individual post offices and thus no assessment of higher risk post offices based on ML/FT risk. The inspection process is questionnaire- driven, gathering data from post offices around the country. The resulting data is used to manually assess the ability of Latvian post to detect structuring; Latvian post is upgrading the system to an automated process. The MoT also reviews STR transaction printouts to assess the timeliness of filing STRs with the FIU. The inspection process does not seem to focus on CDD obligations, and representatives interviewed had no information on why the STRs filed by Latvian Post with the FIU were considered suspicious.

413. CRPC: At the time of the onsite visit the CRPC did not have a supervisory program in place as the legislation only came into force during the visit. Representatives of the CRPC interviewed indicate that the AML unit staff complement would be increased from two to eight and the first step in the process would be an information gathering exercise on the size and extent of the consumer lending sector. There was no information available, for example, on the extent to which this sector is tied to ownership interests in the CIS countries, or other foreign countries.

414. LGSI: As noted above the LGSI's supervisory model seems to be primarily aligned to ensuring compliance with the casino governing legislation, with a secondary set of AML/CFT elements. Onsite inspections focus mostly on accounting for cash purchases and redemption of chips, and

winnings/losses at tables. They do inspect customer entry records, including identification records, once per month. The number of inspections has been as follows: 620 in 2014, 669 in 2015, 650 in 2016 and 390 in the first half of 2017. The LGSI representatives interviewed considered high rollers and PEPs to be high risk customers of casinos.

415. Association of Sworn Lawyers: AML/CFT supervision is the responsibility of the Association's Disciplinary Committee (DC), which is an elected body but whose decisions cannot be overridden by the Association. The DC supervises the Monitory and Control Commission (MCC), an 11-member body which can hire additional resources where needed. The MCC has undertaken a risk assessment of sworn attorneys and grouped them into three categories as follows: (1) Attorneys who represent clients in court: these activities are not covered by the reporting obligation (AML/CFT Law, Sec.30(3)) when they defend or represent their customers in a pre-trial criminal proceeding or judicial proceedings or advise on instituting or avoiding judicial proceedings. About a third of all sworn lawyers in Latvia fall into this category; (2) Attorneys who appear in court but who mostly prepare "deals", i.e. transaction documents. Their clients are mostly natural persons. About 50% of all sworn lawyers in Latvia fall into this category; and (3) large law firms working mostly with foreign individuals, who also represent these clients in court. This group constitutes about 20% of all sworn lawyers in Latvia. At the time of the onsite the Association had not yet considered what impact this analysis would have on its AML/CFT inspection programme and no onsite inspections had actually been carried out; however, some off-site inspection processes had begun, mostly involving the collection of sworn attorneys' AML/CFT policies and procedures. The Association's representatives confirmed that there is full authority to see customer files pursuant to regulations passed by the Association's Council.

416. Association of Sworn Auditors: The Association's quality control inspection methodology is used for the supervision of AML/CFT obligations. This contains elements to assess CDD and other obligations and includes inspection of client files onsite. There is a focus on high risk customers (as designated by the auditor). The number of inspections has been as follows: 31 in 2014, 32 in 2015, 41 in 2016 and none in the first half of 2017. It should be noted that sworn auditors are not subject to the reporting obligation under the same measures as sworn lawyers noted above – however, the Association did not mention this as a risk factor. The Association has a 16- person unit used for all quality control work (including AML inspections), all of which are sworn auditors with at least three years' experience and no disciplinary or negative regulatory records in their files. Training for this group mainly consists of anti- fraud courses, with no AML-specific training. Findings are documented and the auditor is required to prepare and file a corrective plan. In more severe findings the inspection process is repeated at the auditor's expense. The most common findings are issues around use of cash and inadequate risk management practices.

417. Association of Sworn Notaries: The Association's supervisory process consists of ensuring that all clients of notaries have been properly identified, and inspecting the deeds signed by clients including the CDD conducted on the client by the notary. The Association has grouped Latvian notaries into three risk groups based largely on disciplinary criteria or complaints – no ML/FT risk factors. Extra supervisory resources are applied to the high-risk group, which is small in number (seven notaries). These extra measures include financial checks on the notaries' records. It should be noted that sworn notaries are not subject to reporting obligation under the same measures as sworn lawyers noted above – however, the Association did not mention this as a risk factor. The Association has a staff of 27 to conduct examinations. The number of inspections has been as follows: 90 in 2014, 51 in 2015, 25 in 2016 and two in the first half of 2017. After an onsite

inspection a written report is prepared and issued by the Notarial Board. Corrective measures are applied, and the notary is expected to respond with a confirmation.

418. SRS (General): Up until the time of the onsite visit the SRS was responsible for the supervision of DPMS, accountants, and company service providers. During the onsite visit, legislation entered into force giving SRS the additional responsibility of supervising Financial Leasing Companies. The SRS AML supervisory unit was created after the previous MER and at the time of the onsite visit had 13 employees, with authority to hire an additional eight employees by January 2018. The SRS onsite inspection process began in September 2017 and by the time of the onsite visit the AML unit had started what it called "spot checks" by way of onsite inspections, completed 11 standalone AML/CFT inspections (two car dealers, two legal services providers, two real estate dealers, two accountants, two tax consultants and Altum[121]), and 10 inspections as part of tax audits. These last were triggered by previously identified tax issues of a suspicious nature. The SRS has not completed a comprehensive risk analysis of the diverse population of firms for which it has AML/CFT supervisory responsibility.

419. SRS (DPMS, accountants): Generally, higher risk subjects were noted to be high turnover or high-volume businesses, length of time in the business, ownership by non-residents of Latvia and/or by PEPs. Regarding accountants, the SRS noted that higher risk accountants are generally identified by the amount of their sales turnover, volumes of services and whether the accountant provides company incorporation services. Higher risk factors for DPMS include sale of high value products, type of target market, and whether the dealer is involved in smelting operations.

420. SRS (company service providers; financial leasing companies): As noted above, SRS only became responsible for supervising financial leasing companies (except companies which also provide consumer lending) during the onsite visit and so no supervisory information is available (previously this group was not supervised for AML). Only four supervisory visits (noted above) had been completed for company service providers at the time of the onsite visit.

421. SRS (real estate dealers): Essentially, the SRS applies the same type of analysis in this sector as the others it supervises. There is no ML/FT risk matrix and higher risks are selected on the basis of tax issues, transactions with non-residents, transactions which are fully or partially performed in cash and transactions where the property value significantly differs from the market value, and volumes of business. The SRS had completed six onsite supervisory visits in 2017 up to the time of the onsite visit.

Remedial actions and effective, proportionate, and dissuasive sanctions

422. Only the FCMC had authority to apply financial penalties to its supervised entities at the time of the onsite visit. The other supervisors all have processes that enable them to identify control weaknesses and enforce the application of remedial measures. However, due to the general low level of knowledge of ML/FT risk, the lack of a RBA to supervision in some sectors, and the lack of any onsite supervision in others, the remedial actions applied in these sectors are very low.

423. In 2016 significant changes were introduced to improve the Latvian AML/CFT system in both legislation and supervisory approaches; which largely contributed to the successful accession to the

[121] A state-owned development finance institution, which offers state aid to various target groups with the help of financial tools (such as loans, credit guarantees, investing in venture capital funds, etc.).

OECD. Monetary fines placed on banks for poor internal controls in AML/CFT have been raised substantially. As of 2014 the FCMC publishes information on the persons that have been sanctioned for AML/CFT related breaches. The publicly available information includes the name of the bank, the nature of the offence, the sanctions imposed and information on appeal status and the decision of the regulator, as well as additional obligations imposed on the bank.

424. Number of banks sanctioned, and the amounts of fines imposed (banks, which have been sanctioned multiple times during one year, are indicated only once):

Table 21

Year	2013	2014	2015	2016	2017 (January-June)
Number of banks sanctioned (incl. issuance of warning) [122]	5	2	4	5	3 (2 administrative agreements were signed in July 2017; however the corresponding examinations were completed and the decision on conclusion of the agreements with these 2 banks were taken in the 1st half of the year.
Total amount of fines imposed.	Banks: EUR 327,000.00	Banks: EUR 70,000.00	Banks: EUR 2,211,830.00; Staff: EUR 135,336.00	Banks: EUR 5,933,636.00; Staff: EUR 25,000.00	Banks: EUR 641,514.00 (+ 2,891,271[123])

425. In some cases, banks are also required (by the regulator, e.g. part of the administrative agreement) to invest substantial resources in the development of Internal Control System in order to improve the efficiency of AML/CFT function.

Table 22

Period	Sanctioned institutions for violations of AML/CFT requirements	Number of institutions sanctioned	Sanctions imposed
2017 (January-June)	Banks	3 (+2)	Financial and administrative sanctions have been imposed on banks, including 3 (+2*) monetary fines and administrative requirements to improve bank Internal control system, undergo independent audit, revise the customer base and assess the adequacy of IT resources[124].
2016	Banks	5	Financial and administrative sanctions have been imposed to FIs (EUR 5.93 million and various administrative requirements have been set) and their responsible staff members (EUR 25,000.00) and various administrative requirements have been set. The license of one bank was revoked[125].
	Payment institutions	1	Suspension of operations, disqualification of the manager responsible for AML/CFT.

[122] If a bank has been sanctioned several times within the reporting year, it is considered as one case.

[124] These two examinations have been performed by the FCMC before June 2017, with decisions on administrative cases taken in after June 2017. Administrative agreements have been signed in July 2017.

[125] The European Central Bank took a decision to revoke the license based on the information provided by the FCMC.

2015	Banks	4	Financial and administrative sanctions (EUR 2.2 million) have been imposed on banking institutions and their responsible staff members (to staff members fines totalling EUR 145,336.00 and administrative requirements have been set including withdrawal of the board).
	Payment institutions	1	Removal from the register
2014	Banks	2	Financial sanctions set in the amount of EUR 70,000.00 and 1 warnings issued to banking institution.
	Payment institutions	3	Fine in the amount of EUR 7000.00 and additional administrative sanctions have been imposed. Removal from the register and suspension of activities.

426. To intensify supervisory follow-up on the implementation of remediation measures, the FCMC has used Administrative agreements to apply mandatory external audits of certain banks' internal control systems. The agreements are based on the scope, type and impact of the particular AML/CFT sanctions and non-compliance issues. The scope and the specifics of these audits are determined by the FCMC, as well as the auditing company (only the "big Four" audit firms are used) and paid for by the banks. The FCMC monitors supervision of the execution of the remediation measures on a monthly basis. Any delays or deviations from remediation plans are a violation of the relevant Administrative agreement and are subject to further supervisory measures. However, in the instance discussed in the next paragraph, the assessors did not have proper access to the relevant Administrative Agreement and thus were unable to confirm the appropriateness of measures applied for non-compliance with the Agreement. The fact that the bank engaged in similar transactions subsequent to the Agreement being in place strongly suggests that the measures applied were not proportionate or dissuasive (see IO.11). Applicable statistics on such audits in the non-resident deposit banking sector comprise: 2 audits during Q2 2017, 2 audits in Q3 2017 and 1 audit in Q4 2017.

427. Overall in 2016 the FCMC initiated eight ML- related off-site examinations and five onsite inspections in the banks, which resulted in one revoked license and sanctions (increased volumes compared to previous years) in 4 cases. However, in one instance where the FCMC became aware of the likely evasion of PF sanctions by a bank in 2017, the FCMC did not apply sanctions as it considered that certain sanctions, applied in the previous year to the bank, were for similar control issues. However, the assessors believe that there should have been more dissuasive sanctions applied in 2017 given that the element of evasion was present, and not in 2016 (see Conclusion to analysis under IO.11)

428. Overall, it is too early to conclude on the overall effectiveness, proportionality and dissuasiveness of sanctions in the FI/DNFBP sectors, as the AML/CFT Law provisions on sanctions (aside from the banking sector) entered into force recently.

Impact of supervisory actions on compliance

429. The impact of the actions of supervisors on the FI and DNFBP sectors ranges from negligible (some DNFBP sectors) to fairly good (FCMC). At the time of the onsite visit some FIs were not subject to supervision. The FCMC's approach (the only supervisor to have authority to apply sanctions before the onsite visit) has resulted in a modest reduction in the vulnerability of this sector, a trend which the authorities believe will continue for several years as the banks de-risk out of this market. Notwithstanding these results, the FCMC will need to continue effective supervision

of this sector to ensure that the high risks associated with this sector are adequately addressed by banks.

430. An example of innovation by the FCMC is the requirement for all banks to define "reportable schemes" which are required to be tied in to their risk assessments. Information reported to the FCMC on "reportable schemes" enables the FCMC to identify potential laundering in the sector, which in turn helps it apply appropriate supervisory measures and report suspicious transactions to FIU. The "Moldovan Scheme" was an example of this approach shared with the assessors.

431. The other financial and DNFBP supervisors have only had a moderate impact on their sectors' compliance as their programs are not yet fully risk- based and in some cases have yet to begin or fully roll out the programs. They are mostly focused on limited thematic reviews (such as reporting STRs) or base their work on required professional standards. For example, the SRS suggested that there had been an increase in STR reporting in the DPMS and car dealership sectors in 2017.

Promoting a clear understanding of AML/CTF obligations and ML/TF risks

432. The FCMC has developed and updated guidance to the banking and investment sector on typologies and the implementation of preventive measures. It regularly organizes AML/CFT seminars and is represented on the Compliance Control Committee of the Latvian Bankers Association. At the time of the onsite visit it was planning to publish in 2018 a public report on its work. Finally, it plays a role in assisting the Government to draft AML/CFT laws and regulations.

433. The BoL organises bi-annual seminars for the foreign exchange sector and notifies the sector of AML/CFT legislative changes. It provides feedback and comments to foreign exchange companies as part of its supervisory program, and also operates a "hot line" which can be used by the sector to submit questions on compliance.

434. The CRPC has not issued written guidance to the consumer lending sector as it only become responsible for supervising this sector during the onsite visit.

435. The MoT does not have the resources to support an active AML/CFT guidance program, which is one of the reasons why AML/CFT supervision will be transferred to the FCMC in the future.

436. The LGSI has issued guidance to the casino sector addressing AML/CFT risks and typologies, along with expected internal controls to ensure measures are in place. The SRS has issued some guidance in the DPMS and accountant sectors; guidance applicable to the AML/CFT Law amendments, which took place during the onsite visit, had not yet been addressed.

437. The Association of Sworn Lawyers does not have written guidance or training on AML/CFT matters; however, it does have professional training programs in place and at the time of the onsite visit was working on a plan to introduce an obligation for sworn lawyers to allocate a set number of hours for AML/CFT training.

438. The Association of Sworn Notaries has periodically issued guidance letters on some AML issues, mostly having to do with the use of cash in various types of transactions.

Conclusion

439. Latvia has achieved a reasonably good level of effective supervision in the banking sector, having resulted in identification of failures to implement AML/CFT requirements. Due to the dominance of the financial sector by the banks and other FIs supervised by the FCMC, and its leadership role in the FI sector, the assessors have weighted the impact of the FCMC accordingly.

The other FI supervisors' effectiveness varies in strength but is generally adequate, and in the DNFBP sector is generally inadequate (due in several cases to supervision either not having begun, or only recently begun) and mostly not yet risk- based. It was not possible to review effectiveness of sanctions outside the financial sector as available sanctions only came into effect at the time of the onsite visit. **Latvia has achieved a moderate level of effectiveness for IO.3.**

CHAPTER 7. LEGAL PERSONS AND ARRANGEMENTS

Key Findings and Recommended Actions

Key Findings

IO.5

- The NRA acknowledges that a significant number of Latvian legal persons and foreign legal entities are very likely involved in ML/FT schemes; nevertheless, the NRA does not consider them to be a vulnerability in the Latvian AML/CFT system of the country.
- As mentioned under IO.4 the interviews with the DNFBP sector have highlighted the involvement of company service providers to incorporate companies in Latvia. However, there is insufficient understanding of AML/CFT risks and measures in the company service providers sector.
- The definition of BO in the AML/CFT Law conforms to the FATF definition, and this legislation, which entered into force at the time of the onsite visit is now incorporated by reference into the Commercial Law; thus, no information was available to the assessors on the effectiveness impact this change has had on BO information gathered through the incorporation process.
- BO information gathered by REs must conform to the AML/CFT Law but self-identification through a statement signed by the customer was used as a primary method for determining the BO of a transaction or a business relationship.
- The ER (a subset of the Commercial Register) will be populated by BO information obtained from all legal entities following the application of the BO definition in the AML/CFT Law to the Companies Law. However, this functionality was not up and running as of the time of the visit. When fully implemented, BO information contained in the ER will be publicly accessible.
- About 5,000 LLCs have one or more legal person as a registered shareholder and are classified as high risk by the authorities, of which the BO of less than 300 of them is known to the authorities.
- The administrative sanctions imposed on legal persons for non-compliance with information requirements did not apply to BO information until legislation took effect during the onsite visit. While criminal penalties apply for providing false information, only one case (not related to BO) was provided to the evaluators on whether these have been applied in practice.
- The FIU, LEAs and control authorities in the field of tax administration, public procurement or public-private partnership have direct electronic access to a wide range of information and

databases and indirect access to other databases. At the time of the onsite visit BO related information was accessible following a written request to the ER or the corresponding FI[126].

Recommended Actions

- Latvia should continue improving the new measures enacted during the onsite visit to ensure that the authorities collect the relevant BO information as defined in the AML/CFT Law at the time of incorporation and throughout the lifetime of all legal persons. Priority should be given to the LLC sector as this is the most prevalent and also at the highest risk of ML/FT according to the NRA.
- To ensure that law enforcement has full access to BO records, Latvia should expedite arrangements to ensure the new ER is fully operational as soon as possible. Latvia should also implement measures to ensure that the BO information on the current population of LLC legal persons (the highest risk group according to the NRA) is gathered and input into the ER at an early date. Priority should be given to preventing the misuse of Latvian companies with at least one shareholder that is a non-resident/shell company.
- ML/FT risks present in the formation and administration of companies by company service providers should be assessed and addressed as part of the NRA process.
- Latvia should establish a mechanism to compel FIs/DNFBPs to take reasonable measures to determine the BO of their customers who are legal persons and actively verify such information.

440. 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 and 25.

Immediate Outcome 5 (Legal Persons and Arrangements)

441. Latvian residents can incorporate a wide variety of commercial and non-profit legal persons with relative ease. Information on how to incorporate is widely available to the general public (gate keepers are not needed). It is not possible to create legal arrangements under Latvian law. However, foreign trusts can be created by any person with knowledge of the process where this is not prohibited by foreign law. In practice, it seems that the presence of trusts in the ownership of Latvian entities' BO chains was rare to non-existent; the NRA highlights the risks related to services provided to foreign trusts, however there is no information on estimate of presence of foreign trusts in the country.

Public availability of information on the creation and types of legal persons and arrangements

442. As noted in more detail in the TC Annex (R.24), a variety of legal persons may be incorporated in Latvia for commercial or social reasons. It is not mandatory for the incorporators to use intermediaries to form legal persons, and information on the incorporation process is widely available in Latvian, Russian and English.

443. The most commonly used form of legal person for commercial purposes is the LLC, of which there were approximately 164,000 as of March 2017, or about 98% of all commercial enterprises incorporated in Latvia.

444. The company formation requirements require incorporators to file basic information on legal persons, including registered shareholders, and the natural persons who are incorporating the

[126] Legislation enacted at the time of the onsite visit is analysed under R.24.

entity. These requirements are set out in more detail in the TC Annex. All the basic, and other, information on commercial enterprises is publicly accessible.

Identification, assessment and understanding of ML/TF risks and vulnerabilities of legal entities

445. The authorities acknowledge that Latvian legal entities have been misused for ML/FT purposes. According to the NRA LLCs are the most frequently implicated type of legal person in ML schemes in Latvia. The authorities estimated that as of 30 June 2017 there were approximately 5,000 Latvian companies that exhibited the features of shell companies.

446. The NRA indicates that of all legal persons implicated in ML schemes, 52% are estimated to be Latvian and the balance from various low- tax or tax- free countries (off-shore companies).

447. The NRA highlights that legal persons are often involved in ML/FT schemes and therefore are vulnerable to ML/FT risks. Both fictitious and real business operators are involved in ML/FT schemes. The NRA highlights the use of fictitious companies registered in Latvia to commit tax evasion on a large scale and launder criminal proceeds. The NRA nevertheless does not consider them to be vulnerable in the AML/CFT system of the country and the authorities have not taken sufficient measures to address this issue.

Mitigating measures to prevent the misuse of legal persons and arrangements

448. The legislative provisions which were in force prior the amendments to the AML/CFT law contained requirements merely for shareholders/ stockholders of companies (member of partnerships) to provide to the ER information regarding the UBO, if a shareholder acquired at least 25% of the shares of a LLC or JSC on behalf of another person and if no other person is deemed to be a BO under the AML/CFT Law (there were no explicit obligations on other legal persons). The authorities considered that registered owners of companies were also the BOs, unless other information was submitted. Sec.18.[1] and 18.[2] AML/CFT Law which were enacted during the onsite visit obligate all legal persons in Latvia to collect and submit information about BO to the ER. It was thus not possible for the assessors to gather information about the effectiveness of these measures.

449. Companies were prohibited from issuing bearer shares in 2008 (bearer warrants are unknown in Latvia). The companies that had issued bearer shares in paper form were obliged to either convert these shares into registered shares or register bearer shares in the Latvian Central Depositary (dematerialise the shares). This obligation had to be met by not later than 31 December 2009. The Commercial Law provides that the competent authorities are entitled to request information on the holders of dematerialised shares from the Latvian Central Depository.

450. The ER and SRS have implemented a risk management system which prevents legal persons from being misused for criminal purposes and specially to restrict the creation of fictitious legal persons, paying particular attention to LLCs. The Risk system addresses all stages of formation and includes, for example, refusal of registration if potential shareholders are registered on the SRS list of risk persons (publicly available) or who are prevented by criminal proceedings from carrying out all types of commercial activities. The system also includes the pre-check of applications submitted to the ER (if the application is identified as suspicious), which is carried out by the SRS; and striking off a company on a basis of SRS decision for various violations such as non- submission of information or submission of false declarations. Additionally, the SRS has made an internal risk management system which also analyses information received from the ER in the online data transmission mode.

451. Many REs rely on self-declarations submitted by the customer when meeting their obligation to determine the BOs of their clients. Some REs also rely on information and documents from the register, as well as Internet sources for the determination of BOs. Gaps in the application of preventative measures are described under IO.4.

452. There is a large number of individuals providing company formation services (the exact figures are not known). As noted under analysis of IO.4, problems have been identified in the implementation of preventive measures in this sector. It is stated in the NRA that the ability to provide non-face-to-face services and services for anonymous clients creates a significant risk for the operation of these types of DNFBPs.

453. The interviews during the onsite visit highlighted the significant use of company service providers to incorporate companies in Latvia. The representatives of the company service providers interviewed did not demonstrate sufficient understanding of AML/CFT requirements. Whereas the NRA assesses the risk of the tax advisers, external accountants and providers of legal services as medium high, the authorities did not demonstrate sufficient understanding of risks related to this sector. This is a vulnerability that has not been sufficiently considered.

Timely access to adequate, accurate and current basic and beneficial ownership information on legal persons

454. Basic information on the legal entity is available online. As noted under the analysis of R.24 in the technical annex, the Commercial Law and the Law on the Enterprise Register provide for a number of measures for the registrar to verify basic information on legal entities.

455. As for the information on BOs, 64% of all registered legal entities in registers are private LLCs. Approximately 92% of them (150,613) have one or more shareholder natural persons acquiring at least 25% of shares. Additionally the ER has received 289 notifications from BOs who stand behind registered shareholders. As noted above the authorities previously considered that the registered owners of companies were also the BOs, unless other information was submitted. Based on the statistics of known BOs, the assessors conclude that potentially BOs of approximately 4,700 LLCs are unknown.

456. As noted above, as of the onsite visit the authorities had received 289 statements of actual BOs in companies. However, this information was not included in the information system of the ER and was stored separately with limited access. It was only available to LEAs and control authorities in the field of tax administration, public procurement or public-private partnership. At the time of the onsite visit BO related information was available following a written request to ER[127]. As indicated by the authorities, usually information was provided in response to a written request no later than the next working day; however, the number of requests made to, or received, by the competent authorities has not been provided.

457. As mentioned by the LEAs met onsite the BO information included in bank records is not always accurate. This is consistent with the two different BO definitions in place up until the time of the onsite and is also consistent with the findings of the assessors relating to the effectiveness of establishing BO by the FI and DNFBP sectors, discussed in more detail under IO.4 above.

458. More detailed information on the accuracy of the BO information provided by the REs to the competent authorities is described under IO.4.

[127] Legislation enacted at the time of the onsite visit is analysed under R.24.

459. Timely access to adequate, accurate and current basic and BO information on legal arrangements appears to be non-existent, as the authorities have no information on whether Latvian- based trustees hold information on foreign trusts.

460. As noted in the TC Annex, legal arrangements in the form specified by the FATF cannot be formed in Latvia. However, it is possible that Latvian DNFBPs act as trustees of foreign trusts, although no information is available on the extent to which this is the case in practice.

461. The AML/CFT law applies to trustees but does not require trustees to identify themselves to FIs. It is the responsibility of the FIs to determine if they are dealing with trustees when performing CDD. Although the banks interviewed appeared to be knowledgeable about foreign trusts, they indicated that these form only a small percentage of their client base; but they indicated that they are able to ascertain if a client is acting on behalf of a trust.

Effectiveness, proportionality and dissuasiveness of sanctions

462. The authorities have an active approach to ensuring that information in the ER is accurate and is kept up to date. Statistics were submitted showing a significant number of penalties had been applied, or LLCs dissolved, over the previous 3 years for various failures to provide information. In addition, criminal penalties apply for providing false information. However, the authorities did not provide statistics indicating whether these actions applied to situations relating to BO information or the lack of it. As indicated by the authorities the RE does not keep track of directly what kind of information person who was punished failed to submit, but it can be presumed that no sanction has been imposed for failure to submit information about BOs.

463. The administrative sanctions imposed on legal persons for non-compliance with information requirements did not apply to BO information until legislation took effect during the onsite visit. For this reason, the effectiveness of these measures is not considered for the purposes of this assessment.

464. The REs are responsible for non-compliance with BO identification and record-keeping requirements under the AML/CFT legislation. The analysis of the breaches of AML/CFT requirements ascertained by the supervisor over the last years revealed significant problems with the quality of the process for identification of BOs as more fully discussed under IO.4.

Conclusion

465. Latvia only updated its BO requirements during the time of the onsite visit and thus the effectiveness of these measures cannot be considered. Previous legislation applicable to the ER did not fully meet the FATF standard. As of the onsite visit and despite the AML/CFT Law then containing a satisfactory definition of BO, Latvian authorities only had access to a very small number (less than 300) of BO data files on Latvian LLCs (which according to the NRA are the most frequently used in laundering schemes) exhibiting characteristics of shell companies, out of approximately 5,000 that have one or more legal person as a registered shareholder and are classified as high risk by the authorities, and out of 164,000 LLCs in existence. This is a very low rate of success. **Latvia has achieved a low level of effectiveness for IO.5.**

CHAPTER 8. INTERNATIONAL COOPERATION

Key Findings and Recommended Actions

Key Findings

- Latvia is frequently confronted with ML cases where the predicate offences are committed abroad. International cooperation thus constitutes a critical component of the country's AML/CFT system.
- The CPL sets out a reasonably adequate legal framework for MLA, which enables the authorities to provide and seek a broad range of assistance. International cooperation is also facilitated by a clear division of responsibilities and clear communication channels at the domestic level, an important number of international agreements, as well as by active engagement in networks such as EUROJUST, INTERPOL and EUROPOL.
- Most LEAs regularly provide and seek informal cooperation, especially with other Baltic and EU Member States, although MLA appears to be the most common form of cooperation. MLA is proactively sought by the Latvian authorities. Latvia also regularly engages in JITs in relation to transnational OC schemes.
- The good quality and timeliness of MLA provided by Latvia has in general been noted by its partners, including critical partners in light of its risk profile.
- Latvia's capacity to provide timely assistance would however be improved by reinforcing judicial authorities' and LEAs' human resources; and establishing clear prioritisation and case management arrangements.
- Extradition requests are generally executed in a timely manner, although some difficulties exist in relation to refugee status abuse or rules applying to the extradition of EU nationals to non-EU Member States.
- Latvia faces important difficulties in cooperating with a number of CIS countries, which do not always provide timely and/or useful assistance. Some Latvian authorities have taken steps to address what constitutes a major obstacle to ML investigations and prosecutions, but positive results from these efforts are however yet to be demonstrated.
- Except for the FCMC, supervisors do not seem to be involved in international cooperation. The legal framework does not clearly allow supervisors to conduct inquiries on behalf of foreign partners and no such inquiries have been conducted in practice.
- International cooperation of the FIU is satisfactory and in line with the country's risk profile.
- Latvia's capacity to provide assistance in relation to UBO information is hindered by general issues at national level highlighted under IO.4 and IO.5.

Recommended action

- The remaining technical shortcomings related to international cooperation should be remedied.
- Latvian authorities, including the FCMC, should step up efforts to engage with key partners to address cooperation issues.

- International cooperation in supervisory matters should be enhanced, including in relation to lawyers and other legal professions, taking into account the Latvian risk profile. Supervisors' authority to conduct inquiries on behalf of foreign partners should be clearly established.
- Additional resources should be allocated to international cooperation in judicial authorities and LEAs, considering the country's risk profile.
- Clear criteria on prioritisation and case management systems should be established by each authority involved in international cooperation (incl. for the purpose of maintaining more comprehensive and consistent statistics).
- The development of clear and expeditious mechanisms to deal with extraditions of non-Latvian EU citizens to non-EU Member States should be pursued.

466. 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.

Immediate Outcome 2 (International Cooperation)

467. ML cases in Latvia are frequently related to predicate crimes committed abroad. International cooperation is therefore critical to the effectiveness of the Latvian AML/CFT system.

Providing constructive and timely MLA and extradition

468. The CPL sets out a reasonably adequate legal framework for MLA, which enables the authorities to provide a broad range of assistance in relation to investigations, prosecutions and related proceedings concerning ML, associated predicate offences and FT. International cooperation in Latvia is executed, depending on the stage of the criminal proceedings, through three central competent authorities - the SP, the GPO and the MoJ. The SP and the GPO are more frequently involved in international cooperation than the MoJ, given their respective responsibilities (investigation; prosecution; and trial stage). The FPD, the KNAB, the SP (including the ARO), the SeP and all other LEAs can also send and receive MLA requests through the central authorities. Respective responsibilities are clearly established, and communication channels are well-known by all stakeholders and effective.

469. Although international cooperation through direct communication is permitted by the CPL, its use is limited to some foreign partners -such as the Czech Republic, Finland, Lithuania or Estonia. Formal international cooperation remains the most usual cooperation method.

470. Although no statistics were provided on the type of assistance requested, the authorities indicated that most incoming MLA requests are aimed at obtaining documentary evidence (financial and banking information, e.g. financial statements or CDD information) and statements from witnesses. Foreign partners also seek UBO identification (especially in relation to shell companies) and asset freezing or seizing.

471. According to the authorities, incoming MLA and extradition requests are related most frequently to fraud, ML, robbery or theft, corruption and bribery and organised crime. The authorities also indicate that incoming requests also frequently pertain to tax crime.

Table 23 - Incoming MLA and extraditions requests regarding the most frequent crimes (2014-2016)

	MLA requests	Extradition requests	Total
ML	438	29	467
FT	-	-	-
Organised criminal group related crimes	70	7	77
Terrorism	7	-	7
Drug trafficking	38	13	51
Corruption and bribery	77	2	79
Fraud	896	54	950
Murder and grievous bodily injury	41	12	53
Robbery or theft	151	52	203
Smuggling	20	2	22
Forgery	59	6	65
Tax crime	220	8	228

472. The number of terrorism-related incoming requests is not negligible, despite the assessment by the Latvian authorities in the NRA that the FT risk is low (see discussion on FT risk in IO.1).

473. Latvia engages in effective international cooperation with key partners such as Estonia and Lithuania and other EU countries (e.g. Finland, Poland, Czech Republic, Italy, Germany, the UK, etc.), as well as the USA and Switzerland. Although this is broadly in line with the Latvian ML/FT risk profile, cooperation is challenging with some other relevant countries (see below).

474. In general terms, Latvia cooperates with foreign counterparts in a constructive and positive manner as confirmed by the feedback received from the global community, which highlighted the good quality and timeliness of assistance provided by Latvia. In a limited number of cases, Latvia did not execute foreign MLA requests due to the lack of dual criminality[128] (e.g., "violation of crediting rules" is not a crime in Latvia) and insufficient information supporting the MLA requests. Nevertheless, the authorities informed that, when incoming requests do not contain all necessary information under the CPL, a complement of information is usually requested, especially in relation to those countries where direct communication has been established.

475. Consistent with the fact that a great number of cases investigated by Latvian LEAs involve predicate offences committed abroad, the creation of working-groups and JITs for carrying out diverse joint investigation activities is a common practice. The JITs are most often built up with EU countries, leaving aside important countries of commission of predicate offences, illustrating difficulties faced by Latvia in cooperating with a number of them (see infra).

JIT with support from Eurojust

In late 2011, Estonia started to investigate an Estonian-Latvian OCG, operating out of Estonia and Latvia but using Estonian and Latvian couriers, and involved in the trafficking of liquid cocaine from the Dominican Republic to Europe and the Russian Federation.
In January 2012, the SP initiated a criminal proceeding in Latvia. In February 2012, a first coordination meeting with the Estonian partners was held. In March 2012, during the first coordination meetings held at Eurojust on this case, the Latvian and Estonian police and judicial authorities recognised the need to join forces. A JIT agreement between Estonia and Latvia was signed in July 2012, allowing parallel investigations.

128 Dual criminality is requested only in case of special investigative actions (Sec.853 CPL).

The goals of the JIT were to coordinate efforts to seize drugs, confiscate profits, disrupt the OCG and arrest the suspects.
From September 2012 to March 2013, the quantity of drugs handled by the OCG was estimated to amount to at least 8,086 litres of liquid cocaine, which, when converted back into powdered form, would yield 16,172 kg, with an approximate street value of EUR 55,600 to 1,552,000.
One courier was arrested in Tallinn airport in possession of 1,456 kg of liquid cocaine.
As the result of the investigation 18 members of the OCG were identified in Latvia and Estonia and prosecuted. According to the Latvian authorities, 8,086 litres of liquid cocaine and 109.7 kg of hashish were seized in Latvia; two drug trafficking routes were dismantled; and another OCG was identified and dismantled.
Latvia, Estonia, the Dominican Republic, Germany and the Russian Federation were involved in these operations, although Latvia did not provide detail in that regard.

476. The authorities listed other JIT experiences on offences such as ML, fraud, tax evasion, participation in a criminal organization, and involving the Latvian GPO and counterparts from other countries, such as Estonia, Lithuania, Finland and Sweden over the period 2014-2017. Two JIT agreements were still in place at the time of the onsite visit.

477. Beyond JITs, Latvia also presented several successful cases of international cooperation based on the information provided by Latvia in the execution of foreign MLA requests (e.g. from France, the UK, Germany, Belarus, Ukraine, Estonia, etc.).

MLA request from France

The SP received a MLA request from France in relation to a case of fraud, ML and tax evasion committed by an OCG, which had caused losses of more than EUR 100,000,000. French LEAs conducted an investigation against several natural and legal entities (in total, more than 586), including, company A which was managed by individual B. In the course of the investigation, it was established that B was acting in the capacity of the manager of company A and was its representative in foreign counties, including Latvia. Company A was used in the aforementioned criminal fraud, ML and tax evasion case.
These criminal offences were committed by an OCG (VAT carousel). Since 2007, B's activities had been aimed at funding fictive companies with bank accounts opened at Latvian Bank R in Latvia. The French MLA request was responded by the SP, which provided information obtained from Bank R about 349 bank accounts through which the proceeds of criminal activity were laundered. Later, as a result of the MLA request, the chairman of this bank was recognized as a suspect and was interrogated in the form of a video conference.

478. Latvia also presented a number of cases of asset identification and seizure on behalf of foreign partners, as well as cases of asset repatriation, e.g. to the UK and the US. For example, in 2015, the Riga District Court ruled that USD 23.26 million held by a Latvian company in a Latvian bank account were to be considered as illegally obtained and the funds were transferred back to the rightful owners of the assets – a US company, in a US bank account.

479. As noted under other IOs, Latvia has not maintained comprehensive and consistent statistics on MLA for the period under review. Nevertheless, in general, the statistics provided tend to show a substantial level of activity in providing MLA.

Table 24 – Number of incoming MLA requests

	Incoming MLA requests			
	Received during the year	**Of which pending at the end of the year**[129]	**Of which refused**	**Of which executed during the year**
2014	590	154	6	430

[129] All request(s) were executed during the following year.

2015	643	106	0	537
2016	609	125	2	482

480. The average time of execution of MLA requests appears satisfactory, although incomplete statistics were provided in that respect. Authorities indicated that, on average, incoming MLA requests are processed within 1 to 2 months, unless a shorter time-frame is specified in the request. The vast majority of the jurisdictions who provided feedback indicated that Latvian responses are usually provided in a reasonably timely manner.

481. Some authorities, especially the SP, but also the ARO and the SRS, however noted that, given the volume of requests they receive, the human and technical resources are not sufficient to respond in a timely and effective manner to all MLA requests. Having to translate foreign requests also contributes to slowing down the processing of such requests. The GPO is the most active central authority receiving MLA request from foreign partners and, given Latvia's risk profile and the fact that one of the main goals of requests is obtaining financial information, granting the GPO legal power to directly access this type of information could improve the timeliness of responses.

482. Extradition requests are executed in a timely way, as confirmed by foreign counterparts' positive feedback in that respect. In some cases, extradition was not executed because the request was withdrawn by the requesting country before Latvia took action. In other cases, extradition could not be granted until a final decision on granting refugee status to the person whose extradition had been requested was taken. This administrative procedure usually takes over a year and is sometimes abused to delay the extradition process or even to try to influence the administrative decision in order to obtain the refugee condition irregularly.

Table 25 – Incoming extradition requests

	Incoming extradition requests			
	Received during the year	**Of which pending at the end of the year[130]**	**Of which refused**	**Of which executed during the year**
2014	50	24	4	22
2015	72	45	3	24
2016	73	41	12	20

483. Latvia is able to rapidly execute European Arrest Warrants (EAWs) from other EU Members.

Case example - Extradition: the Petruhhin case

In October 2014, the Russian Federation requested the extradition of an Estonian national to the Latvian authorities based on criminal proceedings on a drug trafficking offence. The Estonian national had been the subject of a priority Red Notice on Interpol's website since 2010 and had been arrested by the Latvian authorities in September 2014.

The Latvian GPO authorised the extradition to Russia. Following an appeal of the Estonian citizen, the competent Latvian court observed that neither Latvian national law nor any of the international agreements signed by Latvia, including with the Russian Federation or the other Baltic countries, would restrict the extradition of an Estonian national to Russia. Latvia can only refuse the extradition of a Latvian national.

However, according to the same court, the lack of protection of EU citizens against extradition, when they have moved to a Member State other than the one of which they are nationals, is contrary to the essence of EU citizenship, which includes the right to receive the same protection as that of a Member State's own nationals.

For that reason, on 26 March 2015 the Supreme Court of Latvia annulled the decision to detain the Estonian

[130] All request(s) were executed during the following year.

person, decided to suspend proceedings and referred the question to the Grand Chamber of the Court of Justice of the European Union (CJEU) for a preliminary ruling.
On 6 September 2016, the CJEU concluded that, when a Member State to which a national of another EU Member State has moved, is subject to an extradition request from a third State with which the first EU Member State has concluded an extradition agreement, it must inform the Member State of the citizen and, should that second Member State so request, surrender that citizen to it, provided that it has jurisdiction, pursuant to its national law, to prosecute that person for offences committed outside its national territory.

484. This judgment requires EU Member States that receive an extradition request from a third State about an EU citizen from another EU Member State to inform the authorities of the latter State so as to enable it to issue an EAW. It is unclear if this requirement would also apply to simplified extradition procedures where the person concerned consents to his/her extradition or when the extradition request concerns EU citizens from countries that allow extradition of their nationals. In any case, the Petruhhin requirement might entail the application of the reciprocity principle and, in such a case the application of the European Convention on Extradition would be weakened.

Seeking timely legal assistance to pursue domestic ML, associated predicate and TF cases with transnational elements

485. Due to the international dimension of many Latvian ML cases, the authorities are proactively seeking international cooperation and, as noted above, regularly engage in JITs to deal with transnational ML schemes.

Table 26 – Outgoing MLA requests

	Outgoing MLA requests			
	Sent during the year	Of which pending at the end of the year	Of which refused	Of which executed during the year
2014	224	87	1	136
2015	222	108	2	113
2016	270	144	-	126

486. Latvia has more incoming MLA requests than outgoing MLA requests (e.g. 609 incoming v. 270 outgoing requests in 2016), which seems in line with the risk profile of the country, where ML is often linked to predicate offences committed abroad.

487. Outgoing MLA requests are mostly used to monitor financial flows, obtain banking and financial information, gather evidences and identify UBOs and IP addresses of persons connecting to bank accounts from foreign countries.

488. The offences that most commonly prompt outgoing MLA requests are ML, fraud and tax crime. Based on the statistics provided, the number of MLA requests sent by the KNAB in relation to ML does not appear to be in line with Latvia's risk profile, where corruption is one of the main predicate offences, often committed abroad.

Table 27 – KNAB: international cooperation related to ML cases

	KNAB: ML-related cooperation	
	Incoming requests	Outgoing requests
2011	5	3
2012	1	2
2013	4	2
2014	-	2

2015	6	-
2016	-	-
Total	16	9

489. Outgoing extradition requests most often pertain to robbery or theft and drug trafficking. Imprisonment, provisional or definitive, is rarely applied in relation to ML (see IO.7), which may explain the limited requests for extradition related to ML.

Table 28 – Outgoing MLA and extradition requests regarding the most frequent crimes (2014-2016)

	MLA requests	Extradition requests	Total
ML	233	4	237
TF	1	-	1
OCG	1	-	1
Terrorism	-	-	-
Drug trafficking	7	132	139
Corruption and bribery	48	7	55
Fraud	206	50	256
Murder and grievous bodily injury	12	41	53
Robbery or theft	19	337	356
Smuggling	73	4	77
Forgery	59	16	75
Tax crime	271	6	277

490. In general, Latvia's MLA requests are duly executed by its partners. A very small number of requests were formally rejected on the grounds that they would contravene the dual criminality condition, or the assets involved were of insufficient value for the partner country to take action.

491. However, the authorities indicate that obtaining effective and timely assistance from and cooperating with the Russian Federation, Ukraine and other CIS countries has been challenging. This is reflected to an extent in the growing backlog of pending outgoing MLA requests. This also results in Latvia not seeking cooperation with those countries as proactively as it should, in light of the origin of illicit flows affecting Latvia, as highlighted in the NRA. Difficulties often take the form of very lengthy response delays or poor quality of responses (sometimes no response). More specific challenges mentioned by the Latvian authorities have been an excessive interpretation of the humanitarian clause to refuse extradition; or the refusal to conduct procedural steps on behalf of Latvia, on the grounds that the proceeding should be transferred to the requested party's authorities, since it involves a national of the requested party.

492. The Latvian authorities have provided little information on steps taken to address cooperation problems with those key partners. Bilateral meetings or contacts have taken place, especially with the SP and KNAB, to facilitate or encourage the execution of Latvia's outgoing requests with some of the relevant countries. However, no improvement has yet been noted.

Other forms of international cooperation

493. Based on a reasonably adequate legal framework for providing other forms of international cooperation, Latvia is actively engaged in non-MLA cooperation, which is regulated by international treaties, multilateral or bilateral agreements and MoU or take place on an ad hoc basis. Direct and

informal international cooperation is a usual practice, especially with other Baltic countries and EU jurisdictions (e.g. Czech Republic, Estonia, Finland, and Lithuania).

494. A significant number of MoUs have been signed between the GPO and foreign partners to enhance non-MLA relationships and promote fluent international cooperation. EUROJUST, INTERPOL and EUROPOL networks are regularly used and Latvia has liaison officers at these networks (e.g., 3 liaison officers in EUROPOL from SRS, SeP and SP) and also in third countries. Latvia is a regular member of EUROJUST and the authorities indicated that they have participated in EUROJUST's coordination and cooperation meetings a number of times which led to successful international operations against crime. There is limited information on the promptness of informal cooperation provided by Latvia, except for the FIU and the FCMC.

FIU

495. The FIU is able to share information with its foreign counterparts, regardless of the existence of a cooperation agreement or a MoU. Nevertheless, the FIU has signed agreements with a number of foreign FIUs[131]. The FIU usually cooperates with foreign counterparts via the Egmont Secure Web. Incoming and outgoing assistance covers a broad range of information (e.g. origin of funds, UBOs, bank account statements, bank account opening and closing dates, copies of CDD documents and contract correspondence, IP addresses used to access the bank account, existence of (other) bank accounts opened by the subject…).

496. Most requests are received from Moldova, the Russian Federation, Ukraine and Lithuania, which is in line with Latvia's risk profile. The cooperation provided by the FIU to foreign counterparts is considered constructive and useful by the foreign partners who provided feedback, although some delays and incomplete information were noted in a few instances (not by major partners). In general, the FIU should be commended for the fast execution of the foreign requests, with responses provided within an average of 12 to 24 days, and which has steadily decreased over time. The most common reasons for refusing to execute a foreign request are related to lack of information and dual criminality (in cases of FIU to LEAs or courts cooperation). The FIU also indicated that, in some cases, there had been reasonable grounds to believe that the subject of the request would be prosecuted or punished because of his/her political opinions; such requests are not executed either.

Table 29 – FIU: incoming foreign requests

	Incoming requests			
	Received	**Executed**	**Spontaneous sharing of information**	**Refused**
2011	478	545	55	4
2012	447	457	30	4
2013	691	691	26	3
2014	672	637	65	3
2015	731	828	138	2
2016	642	683	190	4
Total	3,661	3,541	504	20

[131] Armenia, Aruba, Australia, Belarus, Belgium, Bulgaria, Canada, Czech Republic, Cyprus, Estonia, Finland, "the former Yugoslav Republic of Macedonia", Guernsey, the Holy See, Hungary, Israel, Italy, Japan, Kazakhstan, Liechtenstein, Lithuania, Malta, Moldova, the Netherlands, the Netherlands Antilles, Norway, Panama, Poland, Romania, the Russian Federation, San Marino, Singapore Slovenia, Taiwan and Ukraine.

497. The FIU is proactive in sharing information spontaneously with foreign FIUs, which is considered a good practice, as well as in requesting foreign FIUs' cooperation. The FIU sends an average of 250 requests per year, mainly to the Russian Federation, Estonia, Lithuania and Poland, which appears to be in line with the country's risk profile.

Supervisory authorities

498. The FCMC directly cooperates with foreign counterparts and has MoUs in place with relevant foreign prudential supervisors (direct or through the IOSCO MMoU) in order to exercise consolidated supervision[132]. Its cooperation covers sharing information regarding the authorisation and licensing process, supervision and sanction procedures. Incoming requests mostly concern banks, although most recent requests have dealt with e-money and payment institutions and investment brokerage firms. Foreign partners usually require bank/customer related information, account statements, information of BOs of customers, to support their investigations.

499. In 2016, the FCMC's main partners were the National Bank of Moldova, the Central Bank of Russian Federation, the US Securities and Exchange Commission and the National Bank of Ukraine. The FCMC indicates that the number of days for executing requests depends on the amount of information requested and takes 7 to 30 calendar days in general. Key partners in consolidated supervision have praised the quality of cooperation with the FCMC.

FCMC international cooperation

The FCMC inspected several banks upon the request of assistance received from the Bank of Moldova, indicating the involvement of Latvian registered bank customers in transactions funnelling large amounts of funds from Moldovan banks. Mutual cooperation, with the involvement of Kroll, exchange of information and targeted investigations led to identification of complex transaction schemes and led to sanctioning of the three banks involved in the scheme (three banks were fined in total for EUR 5,488,512 and additional sanctions were imposed on the management members of those institutions (fines totaling EUR 143,336 and a warning), and banks were required to substantially improve their internal control system functionalities, providing substantial financial resources to finance this requirement set by the regulator.

Table 30 – FCMC: international cooperation requests

	FCMC international cooperation on ML		
	Requests received	Requests executed	Requests sent
2011	12	12	5
2012	16	16	10
2013	26	26	12
2014	8	8	1
2015	19	19	6
2016	2	2	23

500. The FCMC has the possibility to conduct joint supervision with foreign supervisory authorities and indicated that it has a permanent representative in the US. However, as noted in the TC Annex, it is unclear whether the FCMC, as the other supervisors, can conduct inquiries on behalf of foreign partners, if not related to intra-EU consolidated supervision.

[132] Latvia is involved in consolidated supervision in relation to the 4 branches of Latvian credit institutions located abroad and 7 foreign banks' branches and 3 foreign banks' subsidiaries located in Latvia. All these foreign branches and banks are located in the EU.

501. The FCMC noted that concerns in cooperation with some neighbouring countries mentioned above have also been an obstacle in performing its function, noting excessive delays and poor quality of responses. It is unclear what steps the FCMC has taken to overcome these challenges.

502. Active international cooperation was not observed in relation to the other supervisors, not being involved in any kind of international cooperation for AML/CFT purposes, which is an issue given the risk profile of Latvia (e.g., use of shell companies and complex legal structures).

State Police

503. The SP explained onsite that it cooperates closely with foreign counterparts and a number of successful cases were presented to the assessment team.

State Police (2014-2017)

Between 2014 and 2017, the Latvian authorities cooperated with the USA concerning a case of fraud committed through an automated data processing system, unlawful entrepreneurship and tax evasion. A Latvian national together with other persons maintained a network platform to support those activities, which also included the illegal sale of pharmaceutical products. An illegal internet website was partly maintained on the basis of 7 IP addresses located in Latvia.
Since 2014, continuous special investigatory operations had been conducted in Latvia (interception of IP addresses and their control) with the aim to identify the natural and legal persons who maintained this unlawful internet website.
As a result of these activities, several persons and their role in the commission of the criminal offences were identified and detected.
In 2017, 4 searches were conducted, and 2 suspects were detained. These 2 persons have already been extradited to the USA and, in the framework of the referred searches, a large amount of evidence and criminally acquired cash (USD 30,000) was seized. The evidence obtained permitted to complete the investigation and to bring charges.

504. Despite those fruitful examples, as with MLA, the SP highlighted the need for additional human resources and the optimization of its case management system in order to continue to successfully engage in informal cooperation.

ARO

505. The ARO was only established in 2016 and its effectiveness can only be assessed to a limited extent. Latvian ARO is member of CARIN and uses the CAMDEN network. The ARO also uses SIENA. The Agency has already been involved in international cooperation for the purposes of tracing assets. From 1 January 2017 to 31 October 2017, the ARO provided support and assistance in 73 cases with an international dimension, identifying the following assets: funds on bank accounts (EUR 7001.64 and USD 262.21), 14 vehicles, company shares for a value of EUR 432,892 and 13 real estate properties for a total cadastral value of EUR 335,118. The limited human resources of the Agency (5 agents at the time of the onsite visit) may however limit its capacity to provide such help.

SRS FPD

506. Considering the complexity of the case and its cross-border dimension, the SRS makes case-by-case decisions on the priority of the cases and organises and takes part in some JITs. It has participated in five JITs with Lithuania and Estonia between 2014 and 2016. The SRS also cooperated with EUROPOL (where the SRS has a liaison officer) network and has signed several bilateral cooperation agreements (e.g. Lithuania, Estonia, Georgia).

SRS CPD

507. Latvia has been a member of the World Customs Organisation since 1992, participates in periodic meetings of the Execution Committee and has access to its databases. The Customs Police also cooperates with other counterparts through the SRS.

Exchange of basic and beneficial ownership information of legal persons and arrangements

508. As noted above, requests for UBO information, especially in relation to shell companies, are one of the main types of MLA requests received by Latvia. Although limited information has been provided in that respect, the FIU reports that 70% of requests received include requests for UBO information, including concerning TFS.

509. The country has the legal capacity to provide basic and UBO information on legal persons and arrangements, through MLA, but also, for example, via FIU channels. Although very limited feedback has been provided to the authorities on the quality of the UBO information provided, it seems that the reliability of UBO information available in Latvia, as highlighted under IO.5, is very limited. Information on UBO held by REs and the ER is not always accurate (see IO.4 and IO.5) and access to the information of the ER concerning the UBO required a written procedure at the time of the onsite visit.

Conclusion

510. Latvia has many of the characteristics of an effective system in the area of international cooperation. Overall, the Latvian authorities proactively cooperate with foreign counterparts, effectively not only providing and seeking MLA, but also exchanging financial intelligence, and engaging in joint investigations and cooperation meetings with positive results. However, with the exception of the FCMC, the supervisory authorities do not seem to take an active part in international cooperation.

511. The main difficulty appears to be connected to difficulties to obtain assistance from CIS countries, which should be critical partners given the transnational nature of the ML cases that the Latvian authorities are faced with. Another area for improvement is the lack of prioritisation and case management systems and the lack of human resources dedicated to international cooperation. Limitations noted under IO.4 and IO.5 in relation to the availability and reliability of UBO information in Latvia have an impact on exchanges of this type of information. **Latvia has a substantial level of effectiveness with Immediate Outcome 2.**

TECHNICAL COMPLIANCE ANNEX

1. This annex provides detailed analysis of the level of compliance with the FATF 40 Recommendations in their numerological 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 (MER).

Recommendation 1 - Assessing Risks and applying a Risk-Based Approach

2. The requirements on assessment of risk and application of the risk-based approach (RBA) were added to the *FATF Recommendations* with the last revision in 2012 and, therefore, were not assessed during the previous mutual evaluation of Latvia.

3. *Criterion 1.1* – Using the FATF guidance, Latvia performed the first assessment of the money laundering and terrorism financing (ML/FT) risks in 2010-2011. The second round of national ML/FT risk assessment was launched by the decision of the Cabinet of Ministers (CoM) of 16 September 2014. The World Bank national risk assessment (NRA) methodology was used to conduct the assessment. The report on the second national ML/FT risk assessment covering the period of 2013-2016 was adopted on 27 April 2017 providing an overview of the ML threats; ML national vulnerability; vulnerabilities of the banking, securities, insurance and other financial institutions (FIs) sectors and designated non-financial business and professions (DNFBPs), as well as FT risk assessment, and risk assessment of financial inclusion products.

4. *Criterion 1.2* – The meeting of the CoM held on 16 September 2014 decided, *inter alia*, to create a mechanism for ML/FT risk assessment led by the national financial intelligence unit (FIU) and designated the Ministry of Finance (MoF) and the Ministry of Justice (MoJ) as the institutions responsible for developing the policy of ML/FT risk prevention according to their areas of competency. According to Sec.61 of the Law on the Prevention of Money Laundering and Terrorism Financing (AML/CFT Law), the Financial Sector Development Board (FSDB) chaired by the Prime Minister and composed of the key stakeholder public agencies (as well as representatives of the private sector) is the coordinating authority in the field of combating ML/FT.

5. *Criterion 1.3* – It is noted in the introduction of the Latvian ML/FT risk assessment, that it will be carried out repeatedly and regularly by following current ML/FT trends and tendencies and effectively addressing new and emerging risks. Implementation of two consecutive rounds of national ML/FT risk assessments is indicative of Latvia's commitment to keep these assessments up-to-date.

6. *Criterion 1.4* – The FSDB chaired by the Prime Minister and composed of the key stakeholder public agencies and representatives of the private sector[133], as well as the Advisory Board of the FIU (ABCS) chaired by the General Prosecutor (GP) and composed of public agencies and self-regulatory organisations (SROs) of DNFBPs[134] constitute the necessary mechanism to provide information on the results of the risk assessments to all relevant competent authorities and SROs, as well as to the FIs and DNFBPs. The 2017 NRA Report was produced in the beginning of 2017 as a strictly confidential document accessible for competent authorities only. Later on, however, it was

[133] Such as the Association of Latvian Commercial Banks, the Latvian Insurers Association, the Association of Professional Members of Latvian Securities' Market, and the Association of Latvian Private Banks Society

[134] Such as the Latvian Association of Certified Auditors, the Latvian Sworn Notaries Council and the Latvian Council of Sworn Advocates

declassified, and the NRA was published on the FIU website in November 2017, as well as circulated to the private sector.

7. *Criterion 1.5* – Based on the findings of the second national ML/FT risk assessment covering the period of 2013-2016, the Government approved the Plan of Measures for Mitigation of ML/FT Risks for 2017-2019 on May 3, 2017. The plan sets out seven courses of action which provide for measures aimed at enhancing the coordination in the development and introduction of the AML/CFT strategy and policy; enhancing the statutory regulation on AML/CFT; improving the effectiveness of investigation, indictment and adjudication, and ensuring effective application of the preventive measures and penalties; improving the effectiveness of the FIU operation; building the capacity of the subjects in the field of AML/CFT; building the capacity of the supervisory and control authorities in the field of AML/CFT; and improving data aggregation and analysis for ML/FT risk assessment and other AML/CFT purposes. Certain measures under these courses of action also provide for (re)allocation of resources to higher risk areas[135].

8. *Criterion 1.6* – Applicable Latvian legislation does not provide for disapplication of any FATF Recommendations requiring FIs or DNFBPs to take certain actions.

9. *Criterion 1.7* – Reporting entities (REs) are required to apply enhanced customer due diligence (CDD) when establishing and maintaining a business relationship or conducting individual transaction with the customer, if the higher ML or FT risk is present (Sec.22(2)(5) AML/CFT Law)). Paragraphs (1) and (1.1) in Sec.6 AML/CFT Law require the REs to perform and document the assessment of their ML/FT risks by taking into account, inter alia, the risks identified by the national ML/FT risk assessment report. Also, Paragraph 10 of the Financial and Capital Market Commission (FCMC) Regulation 234, which is applicable to banks, as well as licensed payment and electronic money institutions, defines that, while performing assessment of the risks inherent for their customers, these FIs must take into account also the risks identified in the risk assessments done by Latvia and by the European Commission.

10. *Criterion 1.8* – Sec.26 AML/CFT Law defines the scope of simplified measures allowed in the presence of low risk as that of carrying out identification of natural and legal persons prescribed in Sec.12-14 of the Law and other CDD measures prescribed in Sec.11.[1] of the Law to the extent "corresponding to the nature of the business relationship or occasional transaction and the level of ML and FT risks". It permits the subjects to apply simplified CDD – whenever the identified lower risks do not contradict the national ML/FT risk assessment report – with regard to certain categories of customers representing a transposition of the relevant provisions of the former EU Directives 2005/60 and 2006/70, or of the non-exhaustive list of factors provided in Annex II of the Directive (EU) 2015/849 (as described under the analysis for c.10.18).

11. *Criterion 1.9* – The legislation sets forth requirements for FIs and DNFBPs to assess and manage their ML/FT risks, as described under the analysis for c.1.10 and c.1.11 below. On the other hand, Sec.45 AML/CFT Law defines the supervisory and control authorities, including SROs, tasked with ensuring compliance of the REs with the requirements of the applicable legislative framework.

[135] For example, introducing changes to the SRS structure, establishing a structural unit with 21 positions (including 10 new positions), increasing the number of onsite inspections; establishing a new position with the Lottery and Gambling Supervision Inspection with a profile in the AML/CFT issues etc.

Reference is made to the analysis of relevant criteria[136] in R.26 and R.28 for further details on the structural and substantial elements of the AML/CFT supervisory and control regime in Latvia.

12. *Criterion 1.10* – Sec.6(1) AML/CFT Law defines that the REs, in conformity with their type of activity, should perform assessment of ML/FT risks in order to identify, assess, understand and manage the risks inherent for their own activities and customers. Such assessment is considered to be a constituent part of the obliged entities' internal control systems.

a) Document risk assessments – The provision in Paragraph 1 of Sec.6 AML/CFT Law requires the REs to document their assessments ML/FT risks.

b) Consider all relevant risk factors – Paragraph 1.2 of Sec.6 AML/CFT Law requires that, in performing risk assessment, the REs take into account at least risk factors relevant for customers, countries and geographical areas, services and products, as well as delivery channels and establish an AML/CFT internal control system. In addition, the FCMC Regulations 234[137] and 125[138], as well as the BoL Regulation 158[139] define the obligation of FIs to assess the inherent ML/FT risk vis-à-vis various segments of risk[140] and to use the outcomes of the assessment in their customer risk scoring systems for deciding the respective mitigation measures to be applied[141]. FCMC Regulation 154[142] specifically requires banks to take into account all relevant factors that may affect the ML/FT risk.

c) Keep assessments up to date – Sec.8 AML/CFT Law provides that the subject of the Law shall, on a regular basis and in accordance with the inherent risks, but at least once per each three years review and update the ML/FT risk assessment.

d) Mechanism for communicating risk assessment information to competent authorities – Sec.47(1) AML/CFT Law entitles supervisory and control authorities (including SROs) to request information from the REs that is related to compliance with the requirements of the Law. The REs, in turn, may use the mechanisms for their regular communication with the supervisory and control authorities for communicating risk assessment information.

13. *Criterion 1.11* – Latvian legislation sets forth the following provisions with regard to risk mitigation measures to be taken by FIs and DNFBPs:

a) Have policies, controls and procedures – The general requirement for the subjects of the AML/CFT Law to have policies and procedures enabling management and mitigation of identified risks is laid down in Sec.6(1) of the Law. Such policies and procedures are to be to be approved by the Board of Directors, if any, or by the senior management body of the subject of the Law.

b) Monitor implementation of controls – Sec.8(2) AML/CFT Law requires the REs to assess on a regular basis, but at least once per each 18 months, the effectiveness of the internal control system,

[136] I.e. c.26.1 and c.28.1-3
[137] Which is applicable to banks, as well as licensed PIs and EMIs
[138] Which is applicable to registered PIs and EMIs, private pension funds, investment brokerage companies (investment firms), investment management companies
[139] Which is applicable to currency exchange offices
[140] The segments of risk are defined in relation to customers, countries and geographic areas, products/ services and, in the FCMC Reg. 234, also to delivery channels.
[141] Further details on the application of the RBA are provided under the analysis for c.10.17. Currency exchange companies are not required to have a customer risk scoring system.
[142] Which is applicable to banks

and to take measures for its improvement by means of, inter alia, reviewing and adjusting the AML/CFT policies and procedures.

c) Take enhanced measures – Sec.22(2)(5) AML/CFT Law requires the REs to take enhanced measures where higher risks are identified.

14. *Criterion 1.12* – Reference is made to the analysis for c.1.8 and c.10.18 for the application of simplified measures, as well as to the analysis for c.1.10 and c.1.11 for the implementation of risk management and mitigation measures. Sec.26(8) AML/CFT Law defines that simplified measures may be applied in the presence of low risk only and cannot be applied if the subject of the Law suspects or knows about committed or attempted ML/FT.

Weighting and Conclusion

R.1 is rated compliant.

Recommendation 2 - National Cooperation and Coordination

15. In 2012 MER, Latvia was rated largely compliant with former R.31. The assessment identified technical deficiencies related to the absence of a cooperation mechanism to involve DNFBP's supervisory authorities or respective SROs, and to the lack of regular reviews of the AML/CFT system effectiveness at policy level.

16. *Criterion 2.1* – Latvia has several national policies which contain essential elements of coordinated action to mitigate ML/FT risks. To implement the declaration on the actions intended by the CoM, on 28 February 2017 the Government approved the *Financial Sector Development Plan 2017-2019*, which recognizes elevated exposure of the Latvian financial sector to ML/FT risks and provides a range of measures for their mitigation. Moreover, based on the findings of the second national ML/FT risk assessment covering the period of 2013-2016, on 3 May 2017 the Government approved the *Plan of Measures for Mitigation of Money Laundering and Terrorism Financing Risks for 2017-2019* setting out specific actions to ensure the country's compliance with the international commitments and standards in the field of ML/FT by means of addressing threats and vulnerabilities identified in the financial and non-financial sectors due to the national assessment of ML/FT risks in 2017. Other national policies relevant for AML/CFT efforts include the action plan to implement recommendations of the *Phase 2 evaluation by OECD Working Group on Bribery in International Business Transactions* approved by the CoM on 21 June 2016 and the *Action Plan to Combat Organized Crime for 2014-2016* approved by the CoM on 5 June 2014.

17. *Criterion 2.2* – On 16 September 2014 the CoM designated the MoF and the MoJ (members of both the FSDB and the ABCS) as the institutions responsible for the ML/FT risk prevention policy according to their areas of competency. The MoF together with the FIU is also responsible for developing action plans on mitigation of ML/FT risks.

18. *Criterion 2.3* – Sec.61 AML/CFT Law defines the FSDB chaired by the Prime Minister as the coordinating authority with the objective to improve the cooperation between state authorities and the private sector in the prevention of ML/FT. Sec.59 of the Law establishes the ABCS chaired by the GP with the task of, *inter alia*, facilitating the work of the FIU and coordinating its cooperation with pre-trial investigation agencies, the Prosecutor's Office, the judiciary and the REs in the implementation of the requirements of the AML/CFT framework. All policy makers, including the national FIU, law enforcement and judicial authorities, supervisors (including SROs) and other competent authorities are represented in the FSDB and the ABCS. Relevant provisions of the AML/CFT Law and the CoM' decisions provide for the exchange of information and other interaction between these stakeholders both at policymaking and operational levels.

19. *Criterion 2.4* – The AML/CFT Law establishing the national coordination and cooperation mechanisms for fighting ML/FT does not contain any references to the subject matter of combating the financing of proliferation of weapons of mass destruction (WMD). Nonetheless, Sec.3(4) of the *Law on International Sanctions and National Sanctions of the Republic of Latvia* (15 February 2016) defines the authority of the CoM to impose national sanctions if that is necessary to achieve, *inter alia*, the objective of combating international terrorism or manufacture, storage, movement, use, or proliferation of WMD. Whereas, under Sec.12(1) of the Law, the Ministry of Foreign Affairs is tasked to inform the CoM and the competent authorities regarding imposition of international and national sanctions and to provide the information necessary for their execution, it also sits at the FSDB, which is a key cooperation and coordination mechanism in the AML/CFT framework of Latvia.

Weighting and Conclusion

20. The cooperation and, where applicable, coordination mechanisms to combat the financing of proliferation of WMD are not clearly defined in the Latvian institutional system. **R.2 is rated largely compliant.**

Recommendation 3 - Money laundering offence

21. Latvia was rated largely compliant in the 4th round MER with the requirement to criminalise ML. As far as technical compliance is concerned, this rating was based on the fact that the FT offence was not fully in line with requirements of the TF Convention; this in return impacted on that offence not being fully covered as a predicate offence for ML.

22. *Criterion 3.1* – The ML offence is laid down in Sec.195 Latvian Criminal Law (CL), but the provision does not contain a definition of ML and is considered as a blanket norm under Latvian law. Such definition is laid down instead in Sec.5 AML/CFT Law. Although there is no clear reference in neither of the two laws that this definition is authoritative for the purposes of the CL where the criminal sanctions for the ML offence are prescribed, in practice Latvian criminal courts make reference to this definition in their judgments. The 2012 MER concluded that the definition in Sec.5 AML/CFT Law was in line with the Vienna and Palermo conventions. The wording of that provision was amended since then, without however having any impact on the criminalisation of ML on the basis of these two international treaties.

23. *Criterion 3.2* – Latvia has an "all crimes" approach which means that all criminal offences which generate proceeds can be predicate offences to ML. The CL includes all designated categories of offences, except participation in an organised criminal group (OCG) as an offence in its own right, which is only criminalised for the commission of especially serious crimes (such as genocide, war crimes and crimes against humanity)[143]. The criminalisation of the FT offence does not cover all the aspects of the FT offence (as required by the international standards) as a predicate (see c.5.2 with regard to the lack of criminalisation of the collection of funds for the generic FT offence, which was deleted during the transfer of the FT definition from the CL to the AML/CFT Law in 2014).

24. *Criterion 3.3* – This criterion is not applicable as Latvia is not applying a threshold approach.

[143] Latvia's CL provides in Sec.21(2) for a definition of the participation of an organised group, which may be an aggravated circumstance if a criminal offence expressly provides for this. However, this requires the commission of a certain criminal offence, whereas the mere participation in an OCG is an offence in its own right only in the limited circumstances of Sec.89 CL.

25. *Criterion 3.4* – Sec.5 AML/CFT Law defines "proceeds of crime" as funds which have come into the ownership or possession of a person as a direct or indirect result of a criminal offence. The term "funds" is defined in Sec.1 AML/CFT Law as encompassing financial resources or other corporeal or incorporeal, movable or immovable property. This definition does strictly speaking not refer to "tangible or intangible" property, which is however widely mitigated by reference to "corporeal or incorporeal" property. The term "financial resources" encompasses legal documents or instruments evidencing title or interest in such assets (Sec.1 AML/CFT Law). Overall, the ML offence (in relation to which the Latvian courts make use of the definition in Sec.5 AML/CFT Law) extends to any type of property that directly or indirectly represents the proceeds of crime, regardless of its value.

26. *Criterion 3.5* – When proving that the property is the proceeds of crime, it is in principle not necessary that a person be convicted of the predicate offence. According to Sec.5(2) AML/CFT Law, a person will be found guilty of ML if he/she is aware (until a legislative change in August 2017, full knowledge was required) that the funds in question are proceeds of crime and if the conduct in question is carried out with the purpose of assisting "any person who is involved in committing a criminal offence in evading legal liability". Hence there is no legislative requirement of a criminal conviction for the predicate offence.

27. *Criterion 3.6* – Sec.5(2) AML/CFT Law establishes jurisdiction to prosecute ML if the predicate offence has occurred in another country, and if it constitutes an offence in that country.

28. *Criterion 3.7* – The criminalisation of ML is not restricted to crimes committed by other persons. The wording of Sec.195 CL does not distinguish between laundering by the person who committed the predicate offence and a third person. On that basis, prosecutions for self-laundering are possible under Latvian law.

29. *Criterion 3.8* – It is possible for the intent and knowledge required to prove the ML offence to be inferred from objective factual circumstances. In the absence of a specific legislative rule on this issue, the general rule of evidence applies that the mental element of criminal offences may be proved based on objective factual circumstances. To that effect, the authorities have provided examples of case-law by the Supreme Court according to which the nature of the intent could be based on the circumstances of the crime committed (Supreme Court of Latvia, SKK - 683/2007, criminal case No 11390091505).

30. *Criterion 3.9* – Since the last evaluation, Sec.195 CL has been amended in 2013. The basic ML offence remains punishable for a term not exceeding three years (Sec.195(1)). If the ML offence is committed by a group of persons, Sec.195(2) provides for a term of imprisonment not exceeding five years (previously: three to eight years, and with the possibility by an individual to commit this offence - without being part of a group - in case of repeated commission). If the ML offence is committed on a large scale or by an organised group (Sec.195(3)), the term of imprisonment ranges from three (previously: five years) to twelve years. Confiscation of also legally-acquired property as a separate criminal sanction is possible as an additional penalty in all cases ("with or without confiscation of property"). Sec.195 (paras. 1 and 2) provides for the possibility to impose fines or other forms of punishment (e.g. temporary deprivation of liberty, community service).

31. The maximum sentences for ML appear equivalent when compared with other jurisdictions and other equivalent financial offences under the CL. A possible negative factor on the proportionality and dissuasiveness of sanctions could be the scenario that a person is found guilty of the aggravated ML offence under Sec.195(2) (ML committed by a group of persons) and could potentially receive a mere term of community service as a penalty, although courts take into

account various factors (including the nature and the harm caused by the offence) when determining the sentence.

32. *Criterion 3.10* – There is no express criminal liability for legal persons in Latvia. Sec.12 and 70 of the CL provide that a legal person may be subject to "coercive measures" under its provisions. However, the CL appears to differentiate between criminal liability for natural persons, on the one hand, and simply being subject to measures that are specified in the CL ("a natural person…shall be held criminally liable, but the legal person may be applied the coercive measures provided for in the CL"). The authorities informed the evaluation team that the difference was introduced because a legal person cannot possess the requisite mental state, although no fundamental principle of domestic law was cited to that effect. However, this does however not alter the fact that the "coercive measures" against legal persons have their basis in criminal law, are of a punitive nature, have as a consequence an entry into the penal register and thus can be considered as achieving a quasi-criminal liability. While Sec.70.[1] CL states that the criminal action of a natural person is generally necessary for coercive measures to apply to a legal person, Sec.439 of the Latvian Criminal Procedure Law (CPL) provides for the initiation of proceedings to apply coercive measures absent any finding that a natural person is culpable, for example when "circumstances have been established that prevent clarifying whether a particular natural person should be held criminally liable" (Sec.439(3)(2)). In any event, the above liability of legal persons is without prejudice to the criminal liability of natural persons and does not preclude any possible parallel civil or administrative proceedings.

33. With respect to Latvia's ability to impose proportionate and dissuasive sanctions, authorities can avail themselves of a wide range of options for coercive measures: 1) liquidation of the legal person; 2) restrictions of its rights (e.g. prohibit specific permits, state assistance, procurement eligibility, or perform a specific activity for up to ten years); 3) confiscation of property; and 4) monetary levy. Fines range from ten to hundred thousand minimum monthly wages in Latvia (Sec.70.[6] CL). As the minimum monthly wage was EUR 380 per month in Latvia in 2017, this equalled a range of fines from EUR 3,800 to EUR 38 million at the time of the onsite visit. This range, together with the other available coercive measures (in particular the possible liquidation of the legal person), allows for proportionate and dissuasive penalties.

34. *Criterion 3.11* – There are appropriate ancillary offences to the ML offence which are covered by Sec.15 to 21 CL. These are notably: attempt (Sec.15); participation in (Sec.18-19); aiding and abetting/facilitating (Sec.20); counselling the commission (Sec.20); and commission of an offence within an organised group (Sec.21). However, the definition of the latter requires a previous agreement with divided responsibilities, which appears more restrictive than forming "an association with or conspiracy to commit" an offence, as required by c.3.11 (see in more detail the related discussion under: c.5.10).

Weighting and Conclusion

35. Participation in an OCG as an offence in its own right is not fully criminalised, but only with regard particularly serious offence (e.g. genocide, war crimes). **R.3 is rated LC.**

Recommendation 4 - Confiscation and provisional measures

36. In the 4th round MER of 2012, Latvia was rated largely compliant in relation to confiscation and provisional measures under R.3 of the 2003 FATF Recommendations. As far as technical

compliance is concerned, the rating was based on deficiencies in the criminalisation of FT which eventually limited the power to confiscate.

37. *Criterion 4.1* – Latvia has a broad set of legal powers to deprive criminals of their proceeds or instrumentalities. On 1 August 2017 amendments to the CPL and CL and a new Law on Execution of Confiscation of Criminally Acquired Property entered into force. Provisions of the CL (Sec.70.[10] et seq.) provide for measures to confiscate all proceeds, laundered property, instrumentalities of crime, as well as property related to any criminal activities committed within the context of a criminal or terrorist organisation. This includes income or other benefits derived from such proceeds (Sec.70.[11](4) CL) and applies regardless of whether the property is held by criminal defendants or third parties. Sec.70.[14] CL allows for the confiscation of corresponding value. Sec.358.[1] CPL states that criminally acquired property shall be confiscated and acquired financial resources shall be transferred to the State budget.

38. Sec.4(1) AML/CFT Law defines (also for the purposes of the CL and the CPL) "proceeds of crime" as property laundered owned or possessed by a person as a result of a direct or indirect criminal offence. Additionally, unless the opposite is proven, such property is recognised as "criminally acquired" if there is a discrepancy with the income of the possessor who belongs to a group of specifically defined persons (among others, members and supporters of organised criminal groups, persons engaged in terrorist activities or maintaining permanent relations with a person who is involved in terrorist activities, Sec.70.[11] CL).

39. *Criterion 4.2* – a) Investigation institutions have investigative powers and are able to identify and trace property that is subject to confiscation (Sec.190 CPL), as well as to evaluate it (if need be by a specialist, Sec.364 CPL).

b) In order to prevent any transfer or disposal of such property, law enforcement authorities (LEAs) are empowered to carry out provisional measures, such as the freezing and seizure of property. The freezing/seizure procedure in criminal cases is governed by Sec.361–366 CPL. A decision to freeze property taken by an investigative judge should be disclosed to the person whose property is concerned only upon execution such decision (Sec.361 CPL). This means that initially the application to freeze or seize property subject to confiscation may be made *ex-parte* or without prior notice.

c) As a general rule Sec.1415 of the Civil Law provides that an impermissible or indecent action, the purpose of which is contrary to laws or moral principles, or which is intended to circumvent the law, may not be the subject-matter of a lawful transaction. As a consequence, such a transaction is void. In cases of freezing/seizure such or actions cannot take place as the freezed/seized property/proceeds are accordingly secured (in a public registry). A property which is at the disposal of a person who maintains permanent family, economic or other kind of property relationships with a person who has committed a crime which in its nature is focused on the gaining of financial or other kind of benefit or is a member of an organised group or abets such group or is connected with terrorism, can also be recognised as a criminally acquired property, if the value of the property is not proportionate to the legitimate income of the person and the person does not prove that the property is acquired in a legitimate way (Sec.70.[11] CL). And if criminally acquired property has been found on a third person, such property shall be returned, on the basis of ownership, to the owner or lawful possessor thereof (Sec.360(1) CPL).

d) According to Sec.179 CPL, a search shall be conducted for the purpose of finding objects or documents that are significant in criminal proceedings. Sec.215 provides for special investigative measures in this respect, subject to a decision by the investigative judge.

40. *Criterion 4.3* – The CPL provides protection for the rights of bona fide third parties. Third parties who possessed criminally-acquired property in good faith are provided with a civil remedy for compensation when such property is returned to the lawful owner/possessor (Sec.360 CPL). Such protection is consistent with the requirements of the Palermo Convention.

41. *Criterion 4.4* – Latvia has mechanisms for managing seized, frozen or confiscated property. Since the CPL provisions are limited to the storage of property, the Law on Execution of Confiscation of Criminally Acquired Property was adopted in 2017, which regulates in detail different forms of executing confiscated property. The government has further determined the procedures for the storage and disposing of criminally acquired property through Cab. Reg. 1025 "on actions with material evidence and arrested property".

Weighting and Conclusion

42. **R.4 is rated C.**

Recommendation 5 - Terrorist financing offence

43. In 2012 MER, Latvia was rated "largely compliant" with former SR.II. The assessors found that some of the financing of the offences covered in the Annex to the TF Convention had an additional mental element. In addition, the implementation of the applicable standard was challenged by various views expressed by practitioners as to whether the then applicable CL provision referred to acts of terrorism against all the international community or only against the Latvian State. In 2014, the FT offence was amended and the definition of financing of terrorism was included in the AML/CFT Law.

44. *Criterion 5.1* – Latvia criminalises FT in Sec.88.[1] CL, a provision which reads in paragraph 1 that "For financing of terrorism, the applicable punishment is…". The CL itself does not contain a definition of FT, which is instead set out in Sec.5(3) AML/CFT Law. In defining FT, this provision does not contain a direct reference or link to the CL. From the text itself, it is thus not clear whether a criminal court would apply the FT definition in Sec.5(3) AML/CFT Law when deliberating a case under Sec.881 CL. However, the authorities explained that the CL's criminalisation of FT is lex generalis that implicitly references the lex specialis-definition of FT in Sec.5 AML/CFT Law. Such an interpretational method is common practice according to the Latvian authorities, which cite a 2008 Latvian Constitutional Court decision to that effect. Although there is no FT case confirming this, a November 2011 Riga City Latgale Suburb Court case references the AML/CFT Law definition of ML in a conviction for a ML offence under Sec.195 CL. The interrelation between the two laws with regard to FT is supported by the fact that before 2014, when Sec.881 CL was amended and the definition of FT was moved from the CL to the AML/CFT Law, the CL contained the relevant definition of FF.

45. The definition of FT refers to the "direct or indirect collection or transfer of financial funds or other property acquired by any form with a view to use them or by knowing that they will be fully or partly used in order to carry out" a list of acts (Sec.5(3) AML/CFT Law). This list includes terrorism and the nine offences referred to in the UN TF Convention. FT also includes the transfer of funds at the disposal of a terrorist group or an individual terrorist (Sec.5(4)). The previous assessment concluded that the FT offence did not cover all of the relevant acts annexed to the UN

TF Convention. In particular, acts against civil aviation, airports, and crimes against diplomats and other protected persons were not covered by the FT offence. However, all treaties referenced in Art.2(1) of the UN TF Convention are now listed in the FT definition under Sec.5(3) AML/CFT Law.

46. Latvia's previous assessment raised concerns that the FT offence in Sec.881 CL did not expressly contain the term "wilfully" and thus did not conform with Art.2(1) of the TF Convention. Although Sec.5(3) AML/CFT Law does not contain this term, the FATF Guidance on Criminalising Terrorist Financing makes clear that prohibiting deliberate conduct with an unlawful intention meets the R.5 standard. Moreover, the language of Sec.5(3) AML/CFT Law contains a clear act and knowledge requirement, from which wilfulness, if not also lesser degrees of intent, can be inferred.

47. *Criterion 5.2* – Sec.5 AML/CFT Law defines FT as: i) the "direct or indirect collection or transfer of financial funds or other property acquired by any form" knowing they will be used to commit a listed offence (Sec.5(3)), or ii) the "transfer of financial funds or property acquired by any form at the disposal of a terrorist group or a separate terrorist" (Sec.5(4)). This latter provision does not clearly apply to the collection of funds, or to their indirect transfer, which falls short of the requirement under c.5.2. The Latvian authorities pointed out that, before the definition of the FT offence was transferred from the CL to the AML/CFT Law in 2014, the text clearly covered both the transfer and collection of funds (both direct and indirectly) to a terrorist group or individual. As currently drafted, the collection of funds for terrorist groups or individuals is not clearly criminalised with regard to the generic FT offence. The authorities have acknowledged this gap and indicated their intent to seek amendments.

48. *Criterion 5.2bis* – Pursuant to amendments enacted on 9 November 2017 implementing the Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism, Sec.5(3)(11) AML/CFT Law criminalises the financing of the travel of individuals "for the purpose of terrorism". In addition, Sec.5(4) AML/CFT Law covers the transfer of funds put at the disposal of an individual terrorist, which means that the regular FT offence may also apply, although this has not yet been tested in practice. These amendments also prohibit funding for engagement, organisation, or management of a terrorist group. However, the criminalisation of the financing of the travel for the purpose of terrorism does not explicitly cover the provision or receipt of terrorist training. In this respect, it should also be noted that Sec.883 CL criminalises the provision of terrorist training, but its financing would merely be punishable as aiding and abetting of that offence. CL amendments to implement the Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism (which entered into force for Latvia on 1 November 2017) which would specifically criminalise travel for terrorist training purposes were under consideration in the Saeima at the time of the onsite visit.

49. *Criterion 5.3* – The AML/CFT Law covers "funds or other property acquired in any manner" and does not differentiate between legitimate and illegitimately sourced funds. "Funds" is defined in Sec.1(1) AML/CFT Law as "financial resources or other corporeal or incorporeal, movable or immovable property." The definition of "financial resources" at Sec.1(2) includes documents evidencing possession of such resources, consistent with the FATF glossary. According to the Commentaries to the CL "funds or other property" can be money or any type of material value of any nature, a definition that appears to encompass "assets of every kind" per the FATF glossary.

50. *Criterion 5.4* – None of the FT offences require that funds or property be used for or linked to a specific terrorist act. According to Sec.5(4) AML/CFT Law, FT includes "the transfer of financial funds or property acquired by any form at the disposal of a terrorist group or a separate terrorist".

51. *Criterion 5.5* – It is possible for the intent and knowledge required to prove the ML offence to be inferred from objective factual circumstances. In requiring a mens rea element, Sec.8 CL provides that the "mental state of the person in relation to objective elements of the criminal offence must be established". The authorities have provided examples of case-law by the Supreme Court according to which the nature of the intent could be based on the circumstances of the crime committed (Supreme Court of Latvia, SKK - 683/2007, criminal case No 11390091505).

52. *Criterion 5.6* – FT is punishable by 8-20 years of deprivation of liberty or life imprisonment (Sec.88.[1] CL). If committed by a group on the basis of an agreement, or on a large scale, the sanction ranges from 15-20 years' to life imprisonment (Sec.88.[2] CL). In both cases, the deprivation of liberty is possible "with or without confiscation". These sanctions are both proportionate and dissuasive when compared to the penalties for comparable serious crimes in the CL and to the sanctions for FT in the criminal codes of other countries.

53. *Criterion 5.7* – Sec.12 CL provides that a legal person may be subject to "coercive measures" under its provisions. However, Sec.12 appears to differentiate between criminal liability for natural persons, on the one hand, and simply being subject to measures that are specified in the CL ("a natural person…shall be held criminally liable, but the legal person may be applied the coercive measures provided for in the Criminal Law"). The authorities informed the evaluation team that the difference was introduced because a legal person cannot possess the requisite mental state, which does however not alter the fact that the "coercive measures" against legal persons have their basis in criminal law. While Sec.70.[1] CL states that the criminal action of a natural person is generally necessary for coercive measures to apply to a legal person, Sec.439 CPL provides for the initiation of proceedings to apply coercive measures absent any finding that a natural person is culpable, for example when "circumstances have been established that prevent clarifying whether a particular natural person should be held criminally liable" (Sec.439(3)(2)). In any event, the above liability of legal persons is without prejudice to the criminal liability of natural persons and does not preclude any possible parallel civil or administrative proceedings.

54. With respect to Latvia's ability to impose proportionate and dissuasive criminal sanctions, authorities can avail themselves of a wide range of options, namely: 1) liquidation of the legal person; 2) restrictions of its rights (e.g. prohibit specific permits, state assistance, procurement eligibility, or perform a specific activity for up to ten years); 3) confiscation of property; and 4) monetary levy. Fines range from ten to hundred thousand minimum monthly wages in Latvia (Sec.70.[6] CL). As the minimum monthly wage was EUR 380 per month in Latvia in 2017, this equalled a range of fines from EUR 3,800 to EUR 38 million at the time of the onsite visit. This range, together with the other available coercive measures (in particular the possible liquidation of the legal person), allows for proportionate and dissuasive penalties.

55. *Criterion 5.8* – There are appropriate ancillary offences to the FT offence (including attempted FT offences) which are covered by Sec.15 to 21 CL. These are notably: attempt (Sec.15); participation (Sec.18-19); and organising and directing others (Sec.20). Concerning the contribution to the commission of FT offences by a group of persons acting with a common purpose (c.5.8(d)), Sec.21 CL establishes liability for persons who commit an offence within an "organised group". The definition of the latter requires a previous agreement with divided responsibilities, which appears more restrictive than the mere acting with a common purpose as required by c.5.8(d). This deficiency is not resolved by Sec.88[1](2) CL, which provides for an aggravated offence if FT was committed by a group, as the provision also stipulates a "prior agreement". Sec.20 CPL,

moreover, states that "[i]f a joint participant has not had the knowledge of a criminal offence committed by a perpetrator or other joint participants, he or she shall not be held criminally liable for such." Such language further suggests the need for a "prior agreement" such that a joint participant must have knowledge of the criminal offense. This possible deficiency is not addressed by the Supreme Court's decision in case No. SKK 01-0020/06 (criminal case No 1814002803), which concluded that "a previous agreement with divided responsibilities" can be proved by concrete actions showing concerted actions of the accused. The court's conclusion in this case may instead have turned on the question of proving a "previous agreement" by objective circumstantial evidence rather than direct evidence. Acting with a "common purpose" as described in c.5.8 – implying a shared objective rather than an intention to cooperate as the CL seemingly requires - could thus potentially not suffice for liability under Sec.21 CL.

56. *Criterion 5.9* – Latvia has adopted an "all crimes" approach in (Sec.195 CL and Sec.5(1) AML/CFT Law) to defining predicate offenses for ML, such that FT offences are predicate offenses for ML.

57. *Criterion 5.10* – Although FT is defined in Sec.5(3) AML/CFT Law, there is no respective FT provision as in Sec.5(2) AML/CFT Law which expressly establishes jurisdiction for ML in case of predicate offences committed abroad. On the other hand, the wording of Sec.5(3) AML/CFT Law is sufficiently broad to establish jurisdiction for the FT activity in cases with such a third-state element and there is no provision in the relevant Latvian laws that the FT offences cannot apply in cases where the alleged offender is in a different country from the one in which the terrorist(s) or terrorist organisation(s) is located or where the terrorist act will occur. Moreover, Sec.4 CL explicitly provides for extraterritorial jurisdiction for both Latvian citizens and foreigners.

Weighting and Conclusion

58. The generic FT offence does not cover indirect transfer as well as the direct and indirect provision or collection of funds. **R.5 is rated LC.**

Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing

59. In the 2012 MER, Latvia was rated PC with previous SR.III. Assessors identified the following deficiencies: under UNSCR 1373, Latvia did not have a national mechanism to consider foreign freezing requests (outside the EU mechanisms) or to freeze the funds of EU internals (citizens or residents); the scope of EU Regulation 881/2002 did not extend to all required categories of funds or other assets; there were concerns over the effectiveness of the freezing system at the request of another party that relies on judicial proceedings; there was not any clear and publicly known procedure for de-listing and unfreezing; the lack of awareness in a part of DNFBP sector of the UN and EU lists raised effectiveness concerns; there was no specific national legislation allowing access to frozen funds for basic expenses and other purposes; and the national TFS system, which had not yet been tested in practice, relied only on judicial mechanisms.

60. In general, the legal basis for implementing R.6 is complex, and presents serious ambiguities and gaps. UNSCRs 1267/1989, 1988 and 1373 are implemented in the EU by a number of EU regulations[144], which are directly applicable in Latvia, as per general EU law principles, and as also made explicit in the context of TFS by Sec.11 Law on Sanctions. However, under Cab. Reg. 468,

[144] Regulations 881/2002 (UNSCR 1267/1989), 753/2011 (UNSCR 1988) and 2580/2001 (UNSCR 1373).

issued to implement the Law on Sanctions, the FIU is assigned the task of "executing" TFS "in accordance with" the UTRs/STRs provisions of the AML/CFT Law, which are not specific to TFS. The provisions of the AML/CFT Law differ from those of the EU Regulations (and from the Law on Sanctions) on a number of points (see detail in criteria below), and it is unclear how the interplay between the EU Regulations, the AML/CFT and the Law on Sanctions regimes works in practice.

61. *Criterion 6.1* – (a) Under the Law on Sanctions, the Ministry of Foreign Affairs (MFA) is the competent authority for proposing persons for designation to the 1267/1989 and 1988 Committees. To date, no such persons have been nominated or considered by Latvia. As per Cab. Reg. 468 (Clause 18), if the CoM has imposed sanctions, the MFA shall request the UN, the EU, or, where necessary, to another international organisation, to assess the necessity to include the sanctions in international lists. No such request has been made by Latvia to date.

(b) Although no explicitly defined mechanism has been established, Latvia states that the process for identifying designation targets encompasses identification and evidence-gathering actions that involves several agencies. The MFA (relevant country desk and international law counsel) serves as the focal point for requests from other countries and as an organizer of Latvian agencies to present proposals for CoM approval. Information collected in the course of agencies' work can be nominated by the MFA or National Security Committee of the Saeima (NSC) to the CoM for consideration of sanctions through ordinary interagency decision-making procedures. The proposal, which requires CoM approval for adoption, comes in the form of a draft regulation citing the need and basis for the measure chosen. An order is then attached specifying the designated persons and/or entities and the basis for their designation.

(c), (d), (e) – For these sub-criteria, Latvia says it would abide by the relevant UN 1267/1989 Sanctions Committee evidentiary standards, as well as follow the appropriate procedures, forms, and requests for information. These would include the EU Best Practices. There appear to be no dedicated procedures already in place, and these recommendations have not been tested in practice.

62. *Criterion 6.2* – (a) At EU level, under Reg. 2580/2001, the EU Council is responsible for designating persons or entities meeting the criteria set forth in the resolution. The Council takes decisions on the basis of proposals submitted by EU member states or third states and reviewed by the Council's COMET Working Party. At the national level, as per Sec.3 Law on Sanctions, the Cabinet may, upon its initiative or on the basis of an MFA proposal or an NSC recommendation, impose national sanctions to combat, *inter alia* "international terrorism". It is unclear whether the UNSCR 1373 criteria for designation would be fully met. There is no formal domestic process to consider requests from third countries. However, authorities indicate that, in practice, those could trigger a proposal from the MFA or a recommendation of the NSC to the CoM.

(b) There is no explicitly defined mechanism for the identification of targets for designation in line with UNSCR 1373. In practice authorities explain that the MFA would receive and consider the information in consultation with other departments, which could also suggest targets to the MFA. See discussion at c.6.1(b).

(c) At EU level, the COMET WP examines the requests received at the European level to determine whether they are supported by reasonable grounds and meet the criteria set forth in CP 2001/931/CFSP, which are compliant with those stipulated in UNSCR 1373. All governments of Member States are represented at the Working Party. No clear time limit has been set for the WP's

review. At national level there is no mechanism to consider foreign requests and no set timeline, but authorities indicated they would work expeditiously and in keeping with the EU Best Practices.

(d) As with (c), at EU level, the COMET WP's assessment of EU proposals applies an evidentiary standard of proof of 'reasonable basis' and the decision is not conditional on the existence of criminal proceedings (Art.1(4) CP 2001/931/CFSP)). At the national level, authorities reported abiding by the EU Best Practices for targeted financial sanctions (TFS).

(e) At EU level, there is no specific mechanism for asking non-EU member countries to give effect to EU restrictive measures. At the national level, the authorities indicate that requests made by Latvia would go through diplomatic channels, but Latvia has not issued any such requests.

63. *Criterion 6.3* – (a) At EU level, under EU Reg. 881/2002 (UNSCR 1267/1989) and 2580/2001 (UNSCR 1373) all Member States must provide each other with the widest possible range of police and judicial assistance. At national level, Latvia does not cite specific legal provisions on robust information-sharing which would allow authorities involved in the identification of targets to collect or solicit all necessary information. The Law on Sanctions provides that competent authorities for the execution of sanctions shall have the authority to "perform any activities, which are necessary to ensure execution of international and national sanctions". The FIU is charged under Cab. Reg. 468 with "executing" financial sanctions "in accordance with" the AML/CFT Law. The FCMC is charged under the Law on Sanctions of executing the sanctions in relation to the participants of the financial and capital market. The authorities indicate that legislation would allow for information collection and exchange within those mandates. LEAs, such as the Security Police (SeP) and the State Police (SP), including the Economic Crime Enforcement Department, have the authority to employ the range of investigative tools and methods.

(b) At EU level, as for the UNSCRs 1267/1989 and 1988 regime, EU Reg. 1286/2009 provides for *ex parte* proceedings against a person or entity whose designation is considered. 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 designation. At national level, no provision of the AML/CFT or other law requires that notice should be given to a party prior to a designation.

64. *Criterion 6.4* – UNSCRs 1267/1989 and 1988 regime – At EU level, UN lists are given effect through amendments to the relevant EU Regulations. In 2017, transposition times exceeded the FATF definition of "without delay". On the basis of Sec.3(3) Law of Sanctions, the Latvia may impose national TFS but this provision has not been used to accelerate the transposition of UN designations at national level. Sec.4(4) AML/CFT Law requires the FIU to make available information on designated persons, so that obliged entities can act before the lists are transposed, although they are not required to do so. According to Cab. Reg. 468, only international sanctions published in the EU Official Journal and domestic sanctions published in the official Latvian gazette are legally binding. UNSCR 1373 regime – At EU level, listings pursuant to Reg. 2580/2001 are immediately applicable in the EU. Under the Law on Sanctions, it is unclear whether the executing authorities are required to take actions "without delay" to implement national sanctions.

65. *Criterion 6.5* – (a) As noted above, the legal basis for the implementation of the freezing obligations has serious uncertainties and gaps. Under the EU Regulations, all natural and legal persons must comply with the freezing obligations upon publication in the Official Journal of the EU, and refrain from giving prior notice to targeted persons. However, delays in transposing the UN designations into EU law raise the question of whether freezing, in practice, takes place without prior notice. The AML/CFT Law or the Law on Sanctions contain no obligation to give prior notice

to designated persons or entities. Under Reg. 2580/2001 asset freezing measures may apply to EU persons or entities insofar as they threaten international peace and security. "EU internal terrorists" can only be subject to enhanced measures related to police and judicial cooperation in criminal matters. There is a significant issue in the scope of persons subject to TFS obligations, which is different, and narrower in the AML/CFT Law and the Law on Sanctions than in the EU Regulations. Under the AML/CFT Law, all REs must refrain from conducting transactions with listed persons. The Law on Sanctions, meanwhile, applies in relevant part to "participants of the financial and capital market", a category that covers FIs supervised by the FCMC. Not all Latvian persons are encompassed under these definitions. Another important deficiency is that the AML/CFT Law does not allow for the permanent freezing of funds. Beyond 40 days (possibly extended for 40 additional days) plus 6 months (Sec.32^2), a court must find that the funds belong to a designated person pursuant to provisions of the CPL. There is no such time limitation or need of a judicial finding in the EU Regulations.

(b) UNSCRs 1267/1989 and 1988 regime – EU Reg. 881/2002, as amended by EU Reg. 363/2016, fulfils the sub-criterion. UNSCR 1373 regime – The freezing obligation under EU Reg. 2580/2001 does not cover all elements of the subcriterion. In national law, the scope of funds covered by the freezing obligations is unclear. Sec.5 Law on Sanctions imposes the obligation to freeze all "financial resources and financial instruments" under the ownership, possession or control of the subject of sanctions. While not defined in the Law on Sanctions, the authorities explain that "financial resources" is defined by Sec.1(2) AML/CFT Law as "financial instruments or means of payment", a definition that does not include corporeal or incorporeal, movable or immovable property. In contrast, the definition of "funds" in Sec.1 AML/CFT Law, as used in Sec.32^1 of that law describing the object of the freezing order issued by the FIU, is broader, encompassing "financial resources or other corporeal or incorporeal, movable or immovable property". Under Sec.32 AML/CFT Law, REs must refrain from executing a transaction if it is related with or there are reasonable suspicions that it is related with or obtained as a result of ML or TF, or their attempt. This language raises serious issues in that it does not refer to the sanctions lists. The authorities have explained in guidance that the property of a designated terrorist is considered to be "proceeds of crime" under Sec.4(3) AML/CFT Law and thus required to be frozen under Sec.32, but this is not clearly provided for in law or regulation. As a consequence, it is unclear whether all elements of c.6.5.b are covered.

(c) EU Reg. 752/2011, 2580/2001 and 881/2002 prohibit EU nationals and all other persons or entities present in the EU from making funds or other economic resources available to designated persons or entities. Provisions in national law are narrower and inconsistent. In Sec.5 Law on Sanctions, access to "financial resources" should be denied "for the subject of sanctions". Again, "financial resources" have a narrow definition. In the AML/CFT Law, Sec.32 should be understood as covering the prohibition to make funds available, and the definition of "freezing of funds" in the AML/CFT Law covers access to or use of funds.

(d) At EU level, designations are published in the EU Official Journal and website and included in a consolidated financial sanctions database maintained by the European Commission, with an RSS feed. The relevant data are produced using an application called FSD ("Financial Sanctions Database"). At national level, the MFA has launched a sanctions webpage, consistent with its responsibility in Cab. Reg. 468 to publish information on international and national sanctions in force. Additionally, pursuant to Sec.4(4) AML/CFT Law and Cab. Reg. 468, the FIU maintains current lists of persons subject to national and international sanctions. Both the FIU and FCMC have provided guidance on sanctions to the REs on multiple occasions.

(e) At EU level, Reg. 881/2002 (Art. 5(1)), 753/2011 (Art.8) and 2580/2001 (Art. 4) require persons and entities to report any information which would facilitate compliance with the Regulations, such as accounts and amounts frozen. Under Sec.32 AML/CFT Law, REs must notify the FIU "without delay, but no later than the following working day" that they have refrained from executing a transaction. There is no such obligation in the Law on Sanctions or Cab. Reg. 468 implementing the Law.

(f) At EU level, EU Reg. 881/2002 (Art. 6), 753/2011 (Art. 7), and 258/2001 (Art. 4) contain protections for bona fide third parties acting in good faith. Under Sec.40(3) AML/CFT Law, RE, its management and employees having in good faith refrained from executing a transaction in accordance with Sec.32 this Law, shall not be subject to legal liability.

66. *Criterion 6.6* – (a) At EU level, procedures to submit de-listing requests to the 1267/1989 and 1988 UN sanctions Committee are applicable to Latvia through EU Reg. 881/2002 and 753/2011, which meet the relevant UN procedures and criteria. Latvia has not, however, decided that, as a rule, its citizens or residents should address their de-listing requests directly to the Focal Point through a declaration addressed to the Chairman of the Committee (footnote 1 of UNSCR 1730(2006).

(b) At EU level, modifications to the list under Reg. 2580/2001, introduced by the Council, are self-executing. De-listing may occur ad-hoc (as requested by listed persons, groups and entities, by a member state or by the third state which had originally proposed the listing) or as a result of the mandatory six-monthly review of all listings. The procedure is accessible on the Council's website and described in the working method document. At national level, Sec.14(2) Law on Sanctions provides that the Cabinet may, upon its initiative, upon proposal of the MFA or of the subject of sanctions, or upon recommendation of the NSC, amend or revoke national sanctions. As per Sec.15(2), the Cabinet must revise the national sanctions list at least annually and, if necessary, amend or partially or completely revoke it. No formal criteria for de-listing have been established.

(c) At EU level, a listed individual or entity can write to the Council to have the designation reviewed or can challenge the relevant Council Regulation, a Commission Implementing Regulation, or a Council Implementing Regulation in Court (Art.263(4) TFEU). Art.275 TFEU also allows legal challenges of a relevant CFSP Decision. At national level, as per Sec.15(1) Law on Sanctions, sanctions, including those imposed pursuant to UNSCR 1373, may be appealed to the District Administrative Court.

(d) and (e) Latvia refers to the EU Best Practices paper as basis for fulfilling c.6.6(d) and (e). However, the paper is not binding, is not on the MFA sanctions webpage, and does not provide procedures that private or other holders of blocked assets should follow.

(f) and (g) At EU level, de-listing and unfreezing decisions taken in accordance with European regulations are published in the EU Official Journal and the updated list of designated persons and entities is published on a dedicated site. At national level, under Clause 19 of Cab. Reg. 468 the MFA must publish relevant information on international and national sanctions in force, although not necessarily explicitly notify such revocations "immediately" after they are delisted.

67. *Criterion 6.7* – EU Reg. 881/2002, 753/2011 and 2580/2001 contain procedures for allowing access to funds and other assets in the conditions described under c.6.7. These exemptions are reflected in Sec.10 Law on Sanctions and Cab. Reg. 468, Chapter III. There is no reference to those provisions in the AML/CFT Law.

Weighting and Conclusion

68. The legal basis for implementing FT-related TFS presents major uncertainties and gaps. Obligations imposed by the EU Regulations, the AML/CFT Law and the Law on Sanctions are not fully consistent, including on a number of critical points. Main gaps pertain to delays in transposing UN designations, the limited scope of the freezing obligation and limited scope of persons obligated to comply with the freezing obligation, and the inability of the FIU to indefinitely order the freezing of assets without a court order. **R.6 is rated PC.**

Recommendation 7 – Targeted financial sanctions related to proliferation

69. Latvia's previous ME was conducted prior to FATF's 2012 adoption of R.7.

70. The legal basis for implementing R.7 includes relevant EU legislation, the AML/CFT Law and the Law on Sanctions, which contain inconsistent provisions on a number of points. The complexity, uncertainties and gaps described under R.6 are also relevant to R.7. The issues noted in relation to the AML/CFT Law under R.6 are however more acute under R.7, since the link with PF is more tenuous in that piece of legislation (see in particular c.7.2(b)).

71. *Criterion 7.1* – The relevant UNSCRs are implemented in the EU by Council Regulations 2017/1509 (DPRK) and 267/2012 (Iran), as amended[145]. In the EU legal framework, Regulations are directly applicable in Member States. In relation to TFS, Latvia makes this principle explicit in Sec.11 Law on Sanctions. In practice, delays taken at EU level to transpose UN lists are not consistent with the FATF definition of 'without delay'. On the basis of Sec.3(3) Law of Sanctions, the Cabinet may impose TFS to combat "the manufacture, storage, movement, use, or proliferation of WMD". However, this national framework is not used to supplement the EU framework in that respect. According to Sec.19 Law on Sanctions EU sanctions are binding in Latvia only upon publication in the Official Journal of the EU.

72. *Criterion 7.2* – At the national level, Cab. Reg. 468 makes the FIU the competent authority for the execution of financial sanctions relating to WMD proliferation. Similarly, Sec.13(4) and Sec.5 Law on Sanctions together make the FCMC the competent authority for supervising the provision of restrictions provided for in international or national sanctions in relation to the participants of the financial and capital markets. See c.6.3(a).

(a) EU regulations implementing proliferation-related UNSCRs are directly binding on Latvian natural and legal persons, and require them to freeze designated persons' assets, upon publication in the Official Journal of the EU, and to refrain from giving prior notice to targeted persons. However, there are delays in transposing the UN designations into EU law, as described in c.6.4, which also raises the question of whether freezing can take place without prior notice. There is also a major uncertainty in the scope of persons obligated to comply with TFS obligations, which is different, and narrower in the AML/CFT Law and the Law on Sanctions than in the EU Regulations (see c.6.5(a)). Additionally, the AML/CFT Law does not itself provide for the permanent freezing of funds absent a judicial order (see c.6.5(a)). The basis for the freezing obligation for PF differs from FT in that Sec.32 AML/CFT Law contains no mention of proliferation or WMD. Instead it provides

[145] As regards the DPRK, UNSCRs 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 and 2321 (2016) have been transposed by Council Decision 2016/849/CFSP and Council Regulation 2017/1509, both as amended. As regards Iran, TFS imposed by the UN are mainly established by Council Decision 2012/35 and Regulation 267/2012. With the adoption of UNSCR 2231 (2015), which terminated UNSCR 1737 and its successor resolutions, a number of targeted restrictive measures contained in EU Regulation 267/2012 have been lifted.

that REs must refrain from executing a transaction if "there are substantiated suspicions that the funds are directly or indirectly obtained in [sic] the result of a criminal offense." As the authorities have explained, such funds are considered "proceeds of crime" under Sec.4 AML/CFT Law, which is defined to include funds of persons on all relevant sanctions lists. As a consequence, the AML/CFT Law does not provide a clear legal basis for the freezing obligation for PF-related TFS.

(b) In the relevant EU Regulations, all types of funds or other assets mentioned in c.7.2(c) must be frozen. As described in c.6.5(b), the scope of funds required to be frozen is limited in Latvian law and do not cover the categories defined under c.7.2(b).

(c) EU Reg. 267/2012 and 2017/1509 prohibit making available assets to designated persons, or for their benefit. See discussion on the Law on Sanctions and the AML/CFT Law in c.6.5(c). The uncertainty noted in c.7.2(b) on whether PF-related sanctions are clearly captured by the AML/CFT Law also applies.

(d) See discussion for c.6.5(d). The FIU maintains a list of PF-designated persons on its website and hosts regular trainings, while both the FIU and FCMC issue PF-relevant guidance and indicators.

(e) FIs and DNFBPs must immediately provide to the competent authorities all information that will facilitate observance of the EU Regulations, including information about the frozen accounts and amounts (Reg. 2017/1509, Art. 50 and Reg. 267/2012, Art. 40). Under Sec.32 AML/CFT Law, REs must notify the FIU "without delay, but no later than the following working day" that they have refrained from executing a transaction. There is no such obligation in the Law on Sanctions or Cab. Reg. 468.

(f) The rights of bona fide third parties are protected by EU Reg. 2017/1509, Art.54 and Reg. 267/2012, Art.42. Under Sec.40(3) AML/CFT Law, a RE, its management and employees having in good faith refrained from executing a transaction in accordance with Sec.32 the Law, shall not be subject to legal liability.

73. *Criterion 7.3* – EU Reg. 267/2012 (Art. 47) and 2017/1509 (Art. 55), Member States must take all necessary measures to implement EU regulations, as well as develop a regime to adopt and administer effective, proportionate and dissuasive sanctions.

74. *Monitoring:* Sec.45 AML/CFT Law defines the authorities in charge of supervising REs' compliance with the AML/CFT Law. Sec.5 Law on Sanctions makes the FCMC the competent authority for supervising the provision of restrictions provided for in international or national sanctions in relation to the "participants of the financial and capital market". The other supervisors are not charged with monitoring or supervision for sanctions under that Law.

75. *Sanctions:* Criminal penalties, include incarceration and monetary fines, can apply for violations of international of national sanctions (Sec.84 CL). Under transitional provision 30 of the AML/CFT Law, the FCMC is entitled to impose sanctions on "participants of the financial and capital market" also for the violations of the requirements of the laws and regulations in relation to the financial restrictions specified in the Law on Sanctions. Sec.78 AML/CFT Law establishes penalties for violations of the requirements under the AML/CFT Law to the extent the AML/CFT Law in fact imposes obligations on persons with respect to PF-related TFS. Given the uncertainties in the legal basis for implementing R.7, the actual scope of sanctions and monitoring described above is unclear.

76. *Criterion 7.4* – (a) If designated persons or entities comment on their inclusion in the sanctions list or if new substantial proof is presented, the EU Council must reconsider its designation decision. Individual de-listing requests must be processed upon receipt, in compliance with the applicable legal instrument and EU Best Practices for the effective implementation of restrictive measures. The Best Practices mention resolution 1730(2006) and the de-listing focal point, and the possibility to submit de-listing requests either through the focal point or through their State of residence or citizenship. Latvia has not, however, decided that, as a rule, its citizens or residents should address their de-listing requests directly to the Focal Point through a declaration addressed to the Chairman of the relevant UN Committee (footnote 1 of UNSCR 1730(2006)).

(b) See c.6.6(f).

(c) EU Reg. 2017/1509 (Art.36 and 37) and 267/2012 (Art.24, 26, and 27) authorize access to funds where countries have found an applicable exemption. Clause 9 of Cab. Reg. 468 provides that the exceptions provided for in the EU regulations shall be complied with. There is no reference to those provisions in the AML/CFT Law.

(d) See c.6.6(g).

77. Criterion 7.5 – The criterion is met under the EU Regulations, Sec.9 of Cab. Reg. 468 repeats the "exceptions and conditions" of the EU Regulations. There is no reference to those provisions in the AML/CFT Law.

(a) The addition of interests or other earnings to frozen accounts is permitted pursuant to EU Reg. 267/2012 (Art. 29) and 2017/1509 (Art. 36).

(b) Payments under a contract entered into prior to designation are possible under the necessary conditions, as per EU Reg. 2015/1861 (Art. 25), which amends Reg. 267/2012.

Weighting and Conclusion

78. In general, as with R.6, Latvia's compliance with R.7 is limited by uncertainties and gaps in its legal basis. The AML/CFT Law does not explicitly impose obligations to implement PF-related TFS despite its references to PF-related sanctions in its definition of funds subject to freezing orders. Technical deficiencies also relate to delays in implementing sanctions; uncertainties in the scope of persons required to implement the freezing obligations and the scope of funds to be frozen; and the incapacity of the FIU to issue a permanent freezing order. Appropriate measures for monitoring and ensuring compliance such as supervisory inspections are not commensurate with identified deficiencies pertaining to PF TFS compliance. **R.7 is rated PC**.

Recommendation 8 – Non-profit organisations

79. Latvia was rated Compliant with previous SR.VIII in the 2006 MER and this rating was maintained in the 2012 report.

80. *Criterion 8.1* – (a) Non-profit organisations (NPOs) as defined in the FATF Glossary can assume a number of different legal forms under Latvian law, primarily associations, foundations, and religious organizations. No subset of organizations that fall within the FATF definition of NPOs has been identified. Latvia's NPOs definition is over-inclusive, encompassing trade unions and political parties. "Public benefit organizations" (PBOs), which receive certain favourable tax treatment, do not cover all NPOs meeting the FATF definition. Latvian authorities consider that NPOs at FT risk are those led by "radically-oriented persons" and that no specific FT risks exist in

the sector. However, other than citing general trends and one specific example, the authorities do not show this conclusion was reached upon a systematic assessment.

(b) Because Latvia has not identified any at-risk NPOs, it has not identified the nature of FT threats to the sector. The FIU has conducted two separate reviews of suspicious transaction reports (STRs) and unusual transaction reports (UTRs) connected with NPOs filed between 2007-2015 and considered potential linkages to FT. No reports indicating FT were identified. The State Revenue Service (SRS) is the primary regulator of NPOs, and along with the SeP and FIU, can obtain timely information on the sector as a whole or specific NPOs. NPOs are required to file annual reports containing information about their directors, members, operations, and expenses, and the SRS can also conduct more in-depth reviews. These are performed for supervising compliance with applicable regulations pertaining to tax and commercial activity, but also allow the SRS to observe other conduct of potential concern.

(c) In 2014, the SeP started reviewing NPO legislation out of concern that they may be exploited by foreign actors to undermine the Latvian state. The SeP prepared amendments to CoM Reg. 808 (03.10.2006) "Regulation on Annual Accounts of Associations, Foundations and Trade Unions", which provides for detailed information on the use of donations. They also recommended statutory amendments to the Law on Associations and Foundations to increase the transparency of NPOs and provide authorities with increased flexibility to monitor their operations and dissolve them as appropriate. That ongoing process indicates that the adequacy of the general legal framework governing this category of NPOs has been assessed, not specifically, but in a manner that is also relevant, to CFT.

(d) Latvia does not have provision for the periodic and regular assessment of the adequacy of its laws and regulations that relate to NPOs in light of new or emerging TF risks. It also does not appear to have specifically addressed how other vulnerabilities in its AML/CFT regime, such as those it identifies as ML risks, could also be exploited by foreign terrorists, although it has identified and addressed gaps in its laws related to the transparency of donations of associations. There is no systematic requirement for ongoing evaluation other than for religious organizations. The latter are subject to an annual re-registration for 10 years, involving a review by the MoJ, the State Police and municipal police, in which it is however unclear to what extent TF risks are considered.

81. *Criterion 8.2* – (a) The obligations and requirements imposed on associations and foundations can be said to reflect policies intended to promote accountability, integrity, and public confidence in the administration and management of NPOs (see c.8.3). The Activity and Development Strategy of the SRS for 2017-2019 includes a strategic action direction on "More Efficient Monitoring of PBOs", which is to improve the risk analysis for conducting inspections. One of the strategic goals is "Open and proactive cooperation with public, non-governmental and private partners."

(b) Latvia does not describe specific outreach initiative to NPOs or the donor community on FT. The "Memorandum Council" established by Cab. Reg. 14 (2014) consists of government officials and the heads of certain NPOs, and provides a forum for NPOs to consult with the heads of relevant government agencies. No description of engagement on FT issues in this format has been provided. However, the SeP reports meeting with NPOs on occasion to discuss FT-related trends.

(c) Latvia does not describe specific initiatives on best practices relating to FT risks in the sector.

(d) The Law on Associations and Foundations requires the submission of annual accounts on income and expenditures to the SRS, which may encourage the use of formal financial channels, as

may the PBO status, since upon being audited or otherwise reviewed NPOs that are PBOs may need to provide documentary evidence of their financial dealings. However, these requirements do not constitute explicit guidance or encouragement to use formal financial channels.

82. *Criterion 8.3* – Most measures detailed in sub-paragraph 6(b) of INR.8 apply to Latvian associations, foundations and religious organisations, without having regard to the specific level of TF risks they face, as noted above. NPOs must register to obtain legal personality and open a bank account. Upon registration, they should submit information to the Enterprise Register (ER). Associations and foundations should provide to the ER information on their objectives. Associations should also notify the identity of the members of the executive board; and maintain a membership register containing identity information, which is available to LEAs upon request. Religious organisations should provide the Register with information of their objectives and the identity of members of the governing institution, as well as officials entitled to represent the organisation. Before registration, the MoJ verifies that objectives are in line with relevant legislation, and whether there the organization poses a threat to human rights, the democratic structure of the State, public safety, welfare and morals.

83. All information provided to the ER must be updated as appropriate, is publicly available online and is kept for an unlimited period of time. CoM Reg. 808 requires annual financial reports, including incomes and expenditures for NPOs. Reports should mention sources and use of donations and gifts. NPOs are subject to the Law on Accounting, under which information provided in accounting registers and annual accounts must be truthful, comparable, timely, significant, understandable and complete. NPOs must submit annual activity reports, allowing for controls on the use of funds. Donors to a foundation may at any time verify the activities of the foundation, as well as have access to all documents, except for accounting records and information regarding other donors. Information to be provided upon registration does not cover the full range of persons who could control or own NPOs. In addition, no obligation to maintain records of domestic and informational transactions has been reported.

84. *Criterion 8.4* – (a) As the tax authority, the SRS monitors the financial assets and donations to NPOs, including for compliance with conditions relevant to their non-profit status. Under the Law on Associations and Foundations (Sec.52(3)), and Cab. Reg. 808 (2006) associations must submit annual reports to the SRS detailing donations, gifts, expenditures and income. Additional details are required from associations granted the status of a PBO, which allows for certain tax advantages and which are supervised more closely by the SRS, primarily for tax purposes. Associations and foundations must submit information to the ER, which maintains it and makes it available to SRS and law enforcement (Associations and Foundations Law Sec.13(1)). The ER grants registration or re-registration upon receipt and "examination" of required information. The nature of the checks conducted by the ER remain however unclear. If the ER receives information on the possible submission of false information, it refers the case to the SP. The authorities further indicate that the SeP is continuously monitoring activities of NPOs. Sec.272 CL provides criminal liability for submission of false information to state institution, including to the ER. If the ER receives any information about the fact, that someone has given false information to the ER, the ER notifies the relevant authorities (SP) regarding possible violations of laws and regulations (Sec.4(4) of the ER Law).

(b) A court may terminate an association or foundation on a number of grounds, upon application by a prosecutor or SRS, including if their activities are in contradiction with the Constitution, laws

or other regulatory enactments; or if profit-making has become their primary activity (Associations and Foundations Law, Sec.57). The activities of a religious organization may be terminated by a court on various grounds: if it is in conflict with the Constitution, regulatory enactments or articles of association; invites others not to observe the law; or threatens the democratic structure of the State, public peace and order as well as the health and morals of other persons with its activities. (Law on Religious Organizations, Sec.18(2))

85. *Criterion 8.5* – (a) Latvian authorities responsible for overseeing NPOs and FT are broadly empowered to share relevant information with one another. The ER can provide information to relevant authorities (Sec.4(4) of the ER Law), who are mandated to cooperate with one another, and which are generally authorized to do so according to their internal procedures and governing statutes. Pursuant to Sec.3(4) AML/CFT Law, the Register is obliged to report unusual and suspicious transactions, including suspicions of FT. The FIU can share information on suspected FT transactions of which it becomes aware, and the SRS can report suspicious transactions to the FIU. Similarly, the SeP are empowered to share information as appropriate with the FIU and SRS, as well as the SP.

(b) The SeP as the lead agency for FT matters can work with the SRS and FIU to investigate suspicious NPOs. Each agency brings with it its own specific expertise that together allow for an appropriate investigation of NPOs of concern.

(c) Competent authorities can request information on particular NPOs' administration and management, including financial and programmatic information from the information required to be submitted to the ER (ER Law 4.[10]). Latvian LEAs can also obtain information on administration and management through standard investigative competencies.

(d) Between the information-sharing mechanisms available to the FIU, MoJ, ER, and LEAs, Latvia can share information on FT activity involving NPOs and take action as necessary and appropriate.

86. *Criterion 8.6* – Latvia's FIU and LEAs maintain both formal and informal channels to share information on FT threats, including through Egmont channels. Latvia's LEAs can share information with foreign counterparts if requested in MLA requests (see also discussion in R.40).

Weighting and Conclusion

87. Laws are in place that require transparency of NPOs. Relevant authorities can share information on NPOs potentially involved in FT activities. The SeP and SRS scrutinize the sector more broadly for other concerns and NPOs can be dissolved for engaging in illicit activity. However, Latvia has not defined or conducted an assessment of those NPOs that might be susceptible to or engage in FT according to the FATF definition. Latvia does not describe specific outreach to the NPO sector on FT. **R.8 is rated PC.**

Recommendation 9 – Financial institution secrecy laws

88. In 2012 MER, Latvia was rated compliant with former R.4.

89. *Criterion 9.1* – Financial institution secrecy laws do not inhibit the implementation of AML/CFT measures in Latvia.

a) Access to information by competent authorities: Pursuant to Sec.63 of the Credit Institution Law, confidential information may be provided to a wide range of authorities, including the FCMC, the FIU, courts, investigation authorities, the Prosecutor's Office, the SRS, the BoL, etc. In addition,

Sec.37.1 and 37.2 AML/CFT Law define that the REs shall submit to the FIU, as well as to supervisory and control authorities information obtained due to application of CDD measures and about transactions executed by a customer, as well as other information related to management of ML/FT risks. Similar requirements enabling access to information by request of supervisors, LEAs and courts are provided in other sectorial laws[146].

b) Sharing of information between competent authorities domestically: Sec.54 AML/CFT Law defines that all state and local government authorities have an obligation, pursuant to the procedure specified by the CoM, to provide information requested by the FIU for the implementation of its functions. Sec.55 of the Law specifies that the FIU shall provide information to pre-trial investigative institutions, the Prosecutor's Office and the court, if such information allows for substantiated suspicions that the relevant person has committed or attempted to commit a criminal offence, including ML/FT.

c) Sharing of information between competent authorities internationally: Paragraph 1(10) of Sec.46 AML/CFT Law enables supervisory and control authorities to conduct information exchange with foreign supervisory and control authorities for the purpose of tackling ML/FT. Sec.62 of the Law defines that the FIU may, on its own initiative or pursuant to a request, conduct information exchange with foreign authorized institutions with essentially similar obligations and is entitled to enter into agreements for that purpose. Then, Paragraph 5 of Sec.63 of the Credit Institution Law establishes that FIUs for the prevention of ML/FT of a Member State and a foreign country relevant to a bank supervisory authority shall provide information on the basis of mutual cooperation or other agreements. Similar provisions enabling exchange of information with foreign counterparts are contained in other sectorial laws[147].

d) Sharing of information between financial institutions: Paragraph 6 of Sec.63 of the Credit Institution Law defines that a bank shall submit confidential information to another bank registered in a Member State or a foreign country in accordance with the procedures specified by the AML/CFT Law. Sec.44 AML/CFT Law, in turn, specifies that for the purpose of implementing the objectives of the Law a bank shall provide, at the request of a correspondent bank, information and documents obtained in the process of identification and due diligence of its customers (as well as their beneficial owners (BO) or authorized persons) and their transactions executed with the intermediation of the relevant correspondent bank. Credit institutions shall not be subject to legal, including civil, liability for the provision of such data.

Weighting and Conclusion

90. **Latvia is compliant with R.9.**

Recommendation 10 – Customer due diligence

91. In 2012 MER, Latvia was rated partially compliant with former R.5. The assessment identified technical deficiencies related to the lack of explicit prohibition of accounts opened in fictitious names; insufficient process for establishing equivalency of jurisdictions for CDD purposes; the failure of the BoL regulations to provide clear requirements for ongoing due diligence in certain important areas; and the availability of exemptions from CDD in some cases of simplified CDD.

[146] E.g. Part 2 of Art.61 of the Law on Payment Services and Electronic Money Institutions, Part 7 of Art.131 of the Law on Financial Instruments Market.
[147] E.g. Art.107.1 of the Law on Insurance and Reinsurance, Art.143 of the Law on the Financial Instruments Market, Art.88 of the Law on Investment Management Companies.

92. *Criterion 10.1* – Sec.15 AML/CFT Law defines that a bank and a FI shall be prohibited to open and maintain anonymous accounts or accounts in fictitious names (non-conforming to personal identification documents).

When CDD is required

93. *Criterion 10.2* – Sec.11 AML/CFT Law requires the REs to apply CDD in, *inter alia*, the following circumstances: 1) before establishing a business relationship; 2) before conducting an occasional transaction, if: a) the amount of the transaction or the total amount of several seemingly linked transactions is equal to or above EUR 15,000; b) when performing remittance of funds[148] above EUR 1,000; c) when carrying out foreign cash currency purchase or sale, if the amount of the transaction or the total amount of several seemingly linked transactions is above EUR 1,500; 5) when a transaction conforms to any of the indications within the list of unusual transactions, or there is a suspicion of committed or attempted ML/FT; and 6) when there are doubts about the veracity of the previously obtained CDD data. The assessors were advised that, with regard to multiple operations, the notion of "seemingly linked" is applied in the meaning of the FATF-defined "appear to be linked". Hence, the AML/CFT Law does not require the REs to undertake CDD measures when there are doubts about the adequacy of the previously obtained CDD data.

Required CDD measures for all customers

94. *Criterion 10.3* – The obligation to identify customers is set out in Sec.11[1](1) AML/CFT Law. According to Sec.12 of the Law, natural persons are identified by means of verifying their identity based on a personal identification document[149] issued in or valid for entering Latvia. Sec.13 of the Law defines that legal persons and legal arrangements are identified by means of, *inter alia*, checking their incorporation documents and obtaining information on their registered office. The law permits to identify a legal person or a legal arrangement by obtaining relevant information from publicly-available, reliable and independent sources.

95. *Criterion 10.4* – Sec.12(5) and 13(1) AML/CFT Law stipulate that in cases when a person purports to act on behalf of customer, the subject of the Law shall identify and verify the identity of the such person, obtaining (the copy of) the relevant document confirming the right to represent, respectively, the natural or legal person.

96. *Criterion 10.5* – Sec.18 of the Law defines that, in cases when CDD is to be applied, the REs should determine the BO of the customer and, based on assessment of risk, should take the necessary measures to verify their identity. The possible methods for identifying and verifying the identity of BOs include obtaining a written statement approved by the customer, and consulting information systems of Latvia and foreign states. Relevant measures are taken to verify the identity of BOs by obtaining a specified set of data on them[150].

---

[148] Including a credit remittance, direct debt remittance, non-account holder money remittance or remittance performed by payment card, electronic money instrument, mobile telephone, digital or another information technology device

[149] Personal identification document is defined by the Law on Personal Identification Documents (Sec4(1)) settuing out that there are two types of valid personal identification documents – passport and ID card. Such identification documents should comprise the following data: 1) residents – the given name, surname, personal identity number; 2) non-residents – the given name, surname, date of birth, photograph, serial number and date of issue of the personal identification document, as well as issuing state and authority.

[150] Such as the given name, surname, date, month and year of birth, serial number and date of issue of the personal identification document, the country and institution issuing the document, citizenship, country of permanent residence, as well as the amount of the capital shares or stock of the customer owned and also directly or indirectly controlled by such

97. The definition of BO is provided in Sec.1(5) of the Law making reference to natural persons who own or control the customer, or on whose behalf, for whose benefit or in whose interests the business relationship is being established or the occasional transaction is being executed. In case of legal persons, these are the natural persons, who own, in the form of direct or indirect shareholding, more than 25 per cent of the capital shares or the voting stock of the legal person, or who directly or indirectly control it. In case of legal arrangements, these are the natural persons, who own or in whose interests the legal arrangement has been established or operates, or who directly or indirectly exercise control over it, including the founder, proxy or supervisor (manager) of the legal arrangement.

98. While the above-stated definition does not specifically refer to situations in which ownership or control is exercised through a chain of ownership, this can be reasonably inferred from the notion of "indirect ownership or control". Hence, the definition of BO appears to encompass the notions of ultimate effective ownership and control, thus being broadly compliant with the FATF definition.

99. *Criterion 10.6* – Gathering information on the purpose and intended nature of the business relationship is part of the CDD measures set out in Sec.11[1](1) AML/CFT Law. Moreover, Paragraph 6 of the same Section defines that, when establishing a business relationship, the REs shall obtain and document information on the purpose and intended nature of the business relationship, including the services that the customer intends to use, the planned number and amount of transactions, the customer's economic or personal activity within the framework of which the customer will use the relevant services.

100. *Criterion 10.7* – Clause 4 in Paragraph 1 of Sec.11[1] AML/CFT Law defines that, as part of the CDD measures taken by the REs, after establishment of the business relationship they should monitor it for ascertaining that, *inter alia*, transactions executed in the course of the business relationship comply with their knowledge of the customer, its economic activities, risk profile and origin of funds. In addition, Clause 5 in the same paragraph requires the subjects to maintain, regularly assess and update the documents, personal data and information obtained in the process of CDD. Finally, Sec.20(1 AML/CFT Law further details that the REs should, on an on-going basis, update information on economic or personal activity of the customer (presumably also that on higher risk categories of clients).

101. *Criterion 10.8* – Obtaining information on the economic activity, i.e. the nature of business of the customers is part of the CDD measures set out in Sec.11[1](1) AML/CFT Law. At that, with regard to legal persons and legal arrangements, the REs are required to determine the customer's ownership and control structure. Sec.28 of the Law further defines that the REs are entitled to request their customers and the customers are obliged to provide true information and documents necessary for CDD.

<u>Specific CDD measures for legal persons and legal arrangements</u>

102. *Criterion 10.9* – Paragraph 1 of Sec.13 AML/CFT Law defines that for the identification of a legal person the following shall be requested: 1) the documents attesting to the firm name, legal form and incorporation or legal registration; 2) information on the registered address and the actual place of economic activity, if different from the registered address; and 3) the incorporation

person, including the direct and indirect shareholding, in the total capital, as well as the type of directly or indirectly exercised control over the customer.

document (memorandum of incorporation, articles of association), as well as the name and surname of the relevant persons holding positions in the management body of the legal person. Paragraph 1.[1] of the same section establishes that for the identification of a legal arrangement the following shall be requested: 1) the documents attesting to the status of the legal arrangement, the purpose of its creation and the firm name; 2) information on the registered address and the actual place of economic activity, if different from the registered address; and 3) the structure and mechanisms of governance, including the BO or the person, in whose interests the legal arrangement has been created or operates. Hence, for legal arrangements there is no requirement to obtain the names of the relevant persons holding senior management positions in the arrangement.

103. *Criterion 10.10* – Reference is made to the analysis for c.10.5 regarding the definition of BOs of legal persons and the general requirement to identify them and take reasonable measures for verifying their identity.

104. Sec.1(5) AML/CFT Law defines that, in respect of legal persons, the BO is the natural person, who owns, in the form of direct or indirect shareholding, more than 25 per cent of the capital shares or the voting stock of the legal person, or who directly or indirectly controls it. Also, the identity of the relevant natural persons holding senior management positions is to be established under Sec.13(1) AML/CFT Law. The procedure for determining the BOs as set out in Sec.18 of the Law stipulates that, in implementing the obligation to duly justify and document the actions taken for the identification of the BO, the REs may consider a person holding a senior management position in a legal person or legal arrangement to be the BO, if they have exhausted all possible means for determining the BO as defined by the Law, and there are no doubts that the legal person or the legal arrangement has another BO.

105. *Criterion 10.11* – Reference is made to the analysis for c.10.5 regarding the definition of BOs of legal arrangements and the general requirement to identify them and take reasonable measures for verifying their identity.

106. Sec.1(5) of the AML/CFT Law defines that, in respect of legal arrangements, the BO is the natural person, who owns or in whose interests the legal arrangement has been established and operates, or who directly or indirectly exercises control over it, including the founder, proxy or supervisor (manager) of the legal arrangement. Paragraph 11 of Sec.11.[1] of the Law establishes that, where the BO of a legal arrangement is determined within the scope of the governance of a legal arrangement according to special features, the subject of the Law shall obtain information about the BO to an extent allowing determination of the identity of the BO during the payout of funds (benefits) or when the BO intends to exercise the vested rights.

107. The language of these provisions seems to be somewhat ambiguous in the use of the terms "proxy" and "supervisor (manager)" (as opposed to the FATF-defined "trustee" and "protector").

CDD for beneficiaries of life insurance policies

108. *Criterion 10.12* – Clauses 1 and 2 in Paragraph 9 of Sec.11[1] AML/CFT Law define that the subject of the Law, insofar as it provides life insurance or other insurance services related to the accumulation of funds should, in addition to CDD measures, take the following measures with respect to the beneficiary of the insurance indemnity, as soon as it is identified or determined: 1) if the beneficiary is a particular natural or legal person – take the name and surname or the natural person or the firm name of the legal person; 2) if the beneficiary is determined according to specific

features – obtain information on the beneficiary to an extent allowing determination of the beneficiary's identity at the time of payout of the insurance indemnity. Sec.11.[1](10) further establishes that in both cases the said measures should be carried prior to the payout of the insurance indemnity[151].

109. Criterion 10.13 – Clause 3 in Paragraph 9 of Sec.11.[1] AML/CFT Law defines that the subject of the Law, insofar as it provides life insurance or other insurance services related to the accumulation of funds should, in addition to CDD measures and as soon as the beneficiary of the insurance indemnity is identified or determined to be a legal person or a legal arrangement, carry out enhanced due diligence in order to determine the BO of such beneficiary at the time of payout of the insurance indemnity.

Timing of verification

110. *Criterion 10.14* – Reference is made to the analysis for c.10.3 regarding the procedure for identification of customers (in view of the fact that such identification[152] is done by verifying the identity of natural persons[153] and obtaining identification information on legal entities[154]) and for c.10.5 regarding the procedure for identification and the measures taken for verification of the identity of BOs.

111. According to Sec.11(1) AML/CFT Law, identification of the customers and BOs – while performed through verification of their identity – is required before establishing a business relationship or conducting an occasional transaction. Sec.11(3) of the Law defines that, where there is a documented low risk of ML/FT and enhanced CDD is not required, in order not to interrupt the usual procedure of a transaction, verification of identity of the customer and the BO may be carried out at the time of establishing the business relationship, as soon as it is possible after the initial contact with the customer, but prior to carrying out the transaction. Sec.11(4) of the Law further establishes that, in similar circumstances, life insurance service providers and intermediaries may carry out verification of identity of the customer and the BO after the establishment of the business relationship but before the payout or the exercise of vested rights.

112. *Criterion 10.15* – With regard to the timing of verification of the identity of customers and BOs, Sec.11(5) AML/CFT Law defines that the REs should document relevant assessments of risk and should establish policies and procedures setting out ML/FT risk mitigation measures through, *inter alia*, defining limitations on the amount, number or type of transactions.

Existing customers

113. *Criterion 10.16* – Clause 5 in Paragraph 1 of Sec.11[1] AML/CFT Law defines that, within the scope of risk-based CDD measures, the REs should regularly assess and update the documents, personal data and information obtained in the course of the customer due diligence according to the inherent risks, but at least once per each five years. Such periodicity established for applying CDD measures to existing customers does not take into account, for example, the major impact of the significant changes in the national legislation on, *inter alia*, CDD and related requirements adopted by the Latvian National Assembly on 26 October 2017 and signed by the President of

[151] See the analysis for c.10.3 on the specifics of verification of identity of the customers (including the beneficiaries of life insurance products).
[152] As set out in Sec.11.[1]
[153] As further detailed in Sec.12
[154] As further detailed in Sec.13

Latvia into law on 9 November 2017. Accordingly, the AML/CFT Law fails to require CDD of existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

Risk-based approach

114. *Criterion 10.17* – Sec.22(2) of the Law requires the REs to apply enhanced CDD in case of establishing business relationships or conducting occasional transactions: 1) with non-face-to-face customers; 2) with customers or BOs that are politically exposed persons (PEPs), their family members or close associates; and 3) with respondent banks or other FIs in the framework of correspondent relationships; and 4) in other cases, whenever higher ML/FT risk is present.

115. Sec.22(1) AML/CFT Law defines enhanced CDD as a set of risk-based measures carried out in addition to standard CDD in order to: 1) additionally ascertain that the person determined as the BO is the customer's BO; and 2) ensure enhanced monitoring of the transactions executed by the customer. Hence, bearing in mind that ascertaining the identity of the BO is part of the standard CDD as defined under Sec.11.[1] of the Law, the only measure making enhanced CDD different from standard CDD is the enhanced monitoring of the customer's transactions.

116. Sec.20(2) AML/CFT Law defines the process of monitoring the activities and transactions of the customer for the purpose of ascertaining that the transactions are not considered unusual or suspicious. Within the framework of monitoring, the REs are required to pay special attention to: 1) unusually large, complex transactions or mutually linked transactions with no apparent economic or visible lawful purpose; and transactions involving a person from high-risk third countries.

117. Whereas the constituents of enhanced monitoring are not defined anywhere in the applicable legislation to comprise, for example, increasing the number and timing of controls applied, or selecting patterns of transactions that need further examination, the monitoring of customer activities and transactions as set out in Sec.20(2) – even if applied in the undefined "enhanced" mode as required under Sec.22(1) – does not amount to applying enhanced CDD measures such as, *inter alia*, obtaining additional information on the customer and updating more regularly the identification data of the customer and the BO, obtaining additional information on the intended nature of the business relationship, obtaining information on the source of funds or source of wealth of the customer, and obtaining the approval of senior management to commence or continue the business relationship for customers other than PEPs.

118. Paragraph 2 of Sec.11.[1] of the Law stipulates that, when determining the amount of and the procedures for CDD, as well as the regularity of the assessment of the documents, personal data and information obtained in the course of CDD, the subject of the Law shall take into consideration ML/FT risks posed by the customer, its state of residence (registration), type of economic or personal activity, services, products and delivery channels used and transactions conducted by the customer. Paragraph 3 of the same section requires the REs to take into account certain risk-increasing factors in relation to customers[155], countries[156], transactions/ business relationships[157]

[155] Private asset management companies, companies with bearer shares or nominal shareholders, companies with complex ownership structure

[156] EU-defined high risk jurisdictions, those with high level of corruption and other criminal activity, subject to sanctions imposed by the UN, US or EU

[157] Unusual business relationships, large cash transactions, payments received from unrelated third parties

and products, services or delivery channels[158] articulated in similarity of the non-exhaustive list of factors provided in Annex III of the Directive (EU) 2015/849.

119. Paragraph 4 of Sec.22 of the Law stipulates that the FCMC may additionally determine for the banks and FIs under its supervision the categories of customers subject to enhanced CDD, the minimum scope of the enhanced CDD measures for different customer categories, as well as the factors increasing the ML/FT risks. This is achieved by means of certain FCMC regulations on enhanced CDD such as Reg. 234 (23 December 2015)[159] and Reg. 125 (27 August 2008)[160]. The first one provides rigidly defined combinations of the characteristics to establish fixed categories of customers in terms of their ML/FT risk exposure. It also contains technical overlaps in the definition of the types of customers and the circumstances in which enhanced CDD is required. The second one seems to be rather outdated and does not amount to an explicit requirement to the respective FIs to perform the FATF-defined enhanced CDD where the ML/FT risks are higher.

120. *Criterion 10.18* – Sec.26 AML/CFT Law defines the scope of simplified measures allowed in the presence of low risk as that of carrying out identification of natural and legal persons prescribed in Sec.12-14 of the Law and other CDD measures prescribed in Sec.11.[1] of the Law to the extent "corresponding to the nature of the business relationship or occasional transaction and the level of ML and FT risks". It permits the subjects to apply simplified CDD – whenever the identified lower risks do not contradict the national ML/FT risk assessment report – with regard to customers that are Latvian public authorities and companies listed in one or more Member States, to transactions that comply with specific characteristics, as well as to certain insurance and pension investment products. It also recommends certain risk reducing factors that the REs may take into account when assessing the ML/FT risk. All of these are articulated in similarity of either the relevant provisions of the former EU Directives 2005/60 and 2006/70, or the non-exhaustive list of factors provided in Annex II of the Directive (EU) 2015/849.

121. Sec.26(8) establishes that simplified CDD cannot be applied if, based on the assessment of risk, the subject of the Law detects high risk of ML/FT or has information regarding committed or attempted ML/FT, including when there are any indicators of risk-increasing factors referred to in Sec.11[1] of the Law. Sec.26(9) further defines that simplified CDD shall not be applied in respect of natural persons or legal entities, which carry out economic activity in high-risk third countries.

Failure to satisfactorily complete CDD

122. *Criterion 10.19* – Sec.28(2) AML/CFT Law defines a general requirement that in cases, when the REs do not receive information and documents necessary to comply with customer due diligence requirements as set out in Sec.11 and 11.[1] of the Law, they should terminate the business relationship with the customer. Then, Sec.11(7) of the Law establishes that, whenever the subject of the Law is unable to identify and verify the identity of the customer and the BO, as well as to obtain information on the purpose and intended nature of the business relationship[161], it is prohibited to establish or continue a business relationship or to execute an occasional transaction with the

[158] New products, services or delivery channels, those favouring anonymity, restricting the possibility to identify the customer, using new technologies, private banking

[159] Which is applicable to banks, as well as licensed payment and electronic money institutions

[160] Which is applicable to registered PIs and EMIs, private pension funds, investment brokerage companies (investment firms), investment management companies

[161] As set out in Clauses 1-3 in Paragraph 1 of Sec.11.[1] of the Law

respective customer. In such circumstances the subject of the Law should document and assess the situation and, in case of having ML/FT suspicions, file a report with the FIU.

123. Hence, the above provisions do not require explicitly the REs to refrain from opening accounts whenever they are unable to comply with the CDD measures set out under Sec.11 and 11.[1] of the Law, as well as to refrain from opening accounts, commencing business relationships, performing transactions, and to terminate business relationships whenever they are unable to comply with all relevant CDD measures (and not only with those set out under Sec.11 and 11.[1] of the Law). Also, the provision on filing a STR with the FIU is contingent on the circumstance of suspecting ML/FT as opposed to the FATF requirement to consider making a STR whenever the subject of the Law is unable to comply with relevant CDD measures.

CDD and tipping-off

124. *Criterion 10.20* – Sec.11(6) of the AML/CFT Law establishes that, should the subject of the Law have, on one hand, ML/FT suspicions and, on the other hand, grounds to believe that the application of further CDD measures may disclose these suspicions to the customer, it is entitled not to continue the CDD, but to file a report to the FIU.

Weighting and Conclusion

125. The AML/CFT Law does not require the REs to undertake CDD measures when there are doubts about the adequacy of the previously obtained customer due diligence data. It also does not require CDD of existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained. The only measure making enhanced CDD different from standard CDD is the enhanced monitoring of the customer's transactions, which is not defined anywhere in the applicable legislation to comprise certain key elements of enhanced CDD. The subjects of the AML/CFT Law are not required to refrain from opening accounts, commencing business relationships, performing transactions, and to terminate business relationships whenever they are unable to comply with all relevant CDD measures. **R.10 is rated PC.**

Recommendation 11 – Record-keeping

126. In 2012 MER, Latvia was rated largely compliant with former R.10. The assessment identified technical deficiencies related to the limited ability for authorities to ask obligors to keep records beyond five years.

127. *Criterion 11.1* – Sec.37(2) AML/ CFT Law defines that the REs shall maintain information on all payments performed by the customers for five years following the conclusion of an occasional transaction. Hence, the AML/CFT Law does not require maintaining records on a vast variety of transactions other than payments.

128. Nonetheless, in a broader context, Sec.2 of the Law on Accounting, which applies to all natural and legal persons performing economic activities, establishes that any undertaking has to organize the accounting so as to clearly reflect all economic transactions and to preserve all originals, copies or representation of data of all documents substantiating such transactions.

129. With regard to the term of maintaining information and data relevant for the analysis of C.10.1 and C.10.2, Sec.37(3) AML/CFT Law defines that the FIU, supervisory and control authorities, as well as LEAs and courts may extend the five-year term for another period not exceeding five

years based on the necessity, commensurability and justification of such further storage in order to prevent, discover or investigate ML/FT cases.

130. *Criterion 11.2* – Sec.37(2) AML/CFT Law provides for the maintenance of the following data and information for a period of five years following the end of business relationships: 1) all information obtained within the scope of the CDD, including information on the customer and its accounts, copies of the documents attesting to the customer identification data, CDD outcomes; and 2) correspondence with the customer, including electronic correspondence. As this list is very specific, it cannot be presumed that it necessarily encompasses the FATF requirement to maintain the results of analyses undertaken by the REs.

131. *Criterion 11.3* – The AML/CFT Law does not require transaction records to be sufficient to permit reconstruction of occasional transactions so as to provide, if necessary, evidence for prosecution of criminal activity.

132. Nonetheless, in a broader context, Sec.7 of the Law on Accounting requires that transaction records are backed by "source documents" comprising, *inter alia*, title, number and date of the document, description and basis of the transaction, data on the participants and quantifiers (volumes, amounts) of the transaction, Such source documents, along with accounting registers and other relevant data are to be systematically arranged and kept in the archives of the undertaking.

133. Sec.127 and 130 CPL provide the notions of evidence and its admissibility in criminal proceedings. According to the Latvian authorities, transaction records kept by REs are considered to be sufficient to permit reconstruction of individual transactions so as to provide evidence as defined by the CPL.

134. *Criterion 11.4* – Sec.37[2] AML/CFT Law requires the REs to document the CDD measures, as well as information on all payments performed and received (and also, as described in the analysis for c.11.1, on other transactions conducted) by the customer and, upon request of supervisory and control authorities or the FIU, present such documents to the supervisory and control authorities or copies of such documents to the FIU within the term specified in the request.

135. Sec.37[1] AML/CFT Law further requires that the REs supervised by the FCMC[162] provide to it information obtained as a result of customer identification and due diligence, as well as information regarding transactions carried out by the customer and other information related to the ML/FT risk management.

Weighting and Conclusion

136. The record-keeping provision is defined too specifically to presume that it necessarily encompasses the FATF requirement to maintain the results of analyses undertaken by the REs. **R.11 is rated LC.**

Recommendation 12 – Politically exposed persons

137. In 2012 MER, Latvia was rated largely compliant with former R.6. The assessment identified technical deficiencies related to the definition of PEP, which did not cover all PEP categories specified in FATF standards.

[162] I.e. banks, EMIs, insurance companies carrying out life insurance, private pension funds, insurance intermediaries providing life insurance services, investment brokerage companies, managers of alternative investment funds, investment management companies, savings and loans associations, and providers of re-insurance services and PIs.

138. *Criterion 12.1* – The definition of PEP is provided in Sec.1(18) AML/CFT Law and appears to be in line with the FATF definition of politically exposed persons. Sec.25(5) of the Law establishes that, when the PEP passes away or ceases to perform functions related to being PEP, enhanced measures continue to be applied for at least 12 months and until the business relationship with the person causes higher ML risks. This timeframe of 12 months does not meet the definition of PEP in the FATF Glossary, which includes individuals "who are or have been" in the prescribed roles.

139. Sec.1(181) and 1(182) of the Law provide, respectively, the definitions of family members and close associates of PEP, which appear to be broadly in line with those provided in the FATF guidance.

140. Latvian legislation does not differentiate between foreign and domestic PEPs.

141. The AML/CFT Law contains the following provisions in relation to PEPs:

a) Risk management systems – According to Sec.25(1) of the Law, when establishing a business relationship with a customer, the subject of the Law shall determine, by means of taking risk-based assessment measures, whether the customer or the BO is PEP or a family member or close associate of PEP. Sec.25(2) of the Law further requires having internal control systems that enable to determine whether a customer becomes PEP or a family member or close associate of PEP, after the establishment of the business relationship.

b) Senior management approval – Clause 1 of Sec.25(3) of the Law defines that approval of the senior management should be obtained if, before the establishment or in the course of a business relationship, it is detected that the customer or the BO is PEP or a family member or close associate of PEP.

c) Source of wealth and funds – Clause 2 of Sec.25(3) of the Law requires implementing and documenting risk-based assessment measures to determine the source of wealth and source of funds of the customer or the BO who is PEP or a family member or close associate of PEP.

d) Enhanced ongoing monitoring – According to Sec.25(4) of the Law, when establishing and maintaining a business relationship with PEP or a family member or close associate of PEP, the REs shall carry out ongoing monitoring of the customer's transactions. Although this provision does not make reference to enhanced monitoring of relationships with PEPs, Sec.22 of the Law which specifically requires application of enhanced CDD with regard to a customer who is PEP or a family member or close associate of PEP, defines enhanced monitoring of the business relationship and the transactions as part of the enhanced CDD.

142. *Criterion 12.2* – The measures provided by the AML/ CFT Law with regard to PEPs are equally applicable to domestic and foreign PEPs, as well as to the persons entrusted with a prominent function by an international organization, since all these categories of persons are covered by the PEP definition in Sec.1 of the Law. Hence, determination of a customer's or a BO's PEP status is done as described under the analysis for c.12.1, and the measures specified in c.12.1 (b) to (d) are implemented in all (including higher risk) business relationships with PEPs.

143. *Criterion 12.3* – All additional measures stipulated in the AML/CFT Law are equally applicable to the customers who have the status of a family member or close associate of PEP.

144. *Criterion 12.4* – According to Sec.25(21) AML/CFT Law, life insurance service providers and intermediaries shall ascertain that the beneficiary of the insurance agreement or, in relevant cases, the BO of the beneficiary is PEP or a family member or close associate of PEP. This should be

carried out not later than before the payout or transfer of the contract to another insurer. If higher risks are identified, life insurance service providers and intermediaries shall, in addition to CDD measures laid down in Sec.11.[1] of the Law, obtain approval of the senior management, determine the source of wealth and source of funds of the customer and the BO, and apply enhanced CDD (which comprises application of enhanced monitoring of the business relationship), as well as consider filing a STR with the FIU.

Weighting and Conclusion

145. The timeframe of 12 months established for derecognizing PEP status does not meet the definition of PEP in the FATF Glossary. **Latvia is largely compliant with R.12.**

Recommendation 13 – Correspondent banking

146. In 2012 MER, Latvia was rated compliant with former R.7.

147. The amendments adopted by the Latvian National Assembly on 26 October 2017 and signed by the President of Latvia into law on 9 November 2017 introduced changes to provide for compliance with all criteria under R.13.

148. *Criterion 13.1* – Sec.24(1) AML/CFT Law defines that, when establishing a correspondent relationship with a bank or other FI (respondent), Latvian banks and other FIs shall take the following measures in addition to CDD: 1) gather information on the respondent in order to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the respondent and the quality of supervision; 2) assess the measures related to the prevention of ML/FT taken by the respondent; 3) obtain approval from the board or the specially authorized member of the board prior to establishing new correspondent relationships; 4) document the respective responsibility of the respondent in the field of prevention of ML/FT, and 6) obtain information about possible involvement of the respondent in ML/FT - related activities and offences, and about the respective sanctions imposed on the respondent.

149. *Criterion 13.2* – Clause 5 of Sec.24(1) defines that, when establishing a correspondent banking relationship with a bank or other FI (respondent), Latvian banks and other financial institutions shall ascertain that the respondent, which provides services that enable direct access to accounts of the correspondent, has verified the identity of and applied enhanced CDD to the customers having such direct access and, upon request, is able to provide relevant CDD data.

150. *Criterion 13.3* – Sec.1(15) defines shell bank as a bank or any other (financial) institution performing similar activities, or a person providing similar services by carrying out non-cash remittance on behalf of a third party, which has no physical presence (including the presence of its actual management) in the country in which it is registered, and which is unaffiliated with any regulated and supervised group. This appears to overlook certain elements of the FATF definition of a shell bank, i.e. the lack of physical presence in the country in which the bank is licensed (as opposed to being registered only) and, more importantly, the lack of affiliation with a regulated financial group that is subject to effective consolidated supervision (as opposed to being subject to non-effective and/or non-consolidated supervision).

151. Sec.21(1) of the Law prohibits the REs to carry out transactions of any kind with shell banks. According to Sec.24(2) of the Law, a bank shall not enter into a correspondent relationship with a bank or other FI which is known to be engaged in business relationships with shell banks.

Weighting and Conclusion

152. The definition of a shell bank appears to overlook certain elements of the FATF definition. **Latvia is largely compliant with R.13.**

Recommendation 14 – Money or value transfer services

153. In 2012 MER, Latvia was rated partially compliant with former SR.VI. The assessment identified technical deficiencies related to the lack of a consolidated list of agents; the failure of the Latvian Post to conduct complete customer verification and ensure appropriate record keeping; and the lack of effective supervisory powers, authorities and resources for the Ministry of Transport (MoT) to supervise the Latvian Post.

154. *Criterion 14.1* – According to Art.4, 5 and 51 of the Law on Payment Services and Electronic Money (LPSEM), any provider of money and value transfer services shall be licensed by the FCMC or registered with the Commercial Register (upon due notification of the FCMC in writing) prior to the launch of such services.

155. Money or value transfer services (MVTS) in Latvia can be provided by banks, payment institutions (PI), electronic money institutions (EMI) and the Latvian Post. Among these, banks[163] that operate MVTS do so as one of the financial services stipulated in their license issued by the FCMC. PIs and EMIs[164] are either registered with or licensed by the FCMC[165]. Latvian Post is registered as a postal operator in the register of the Public Utilities Commission[166] and acts as "other provider of payment services"[167] offering services through two systems – the Western Union (which is covered by the LPSEM) and the Universal Postal Union (which is covered by bilateral agreements with UPU member postal administrations under the Postal Law).

156. *Criterion 14.2* – Art.1662 of the Latvian Administrative Violations Code defines that in the case of commencing commercial activities without registration or without a special permit (license), statement or permit, if the necessity thereof is specified by the Law or by CoM's regulations, a fine shall be imposed on natural persons or on a legal person's member of the board in an amount from LVL 200 (approximately EUR 285) up to LVL 500 (approximately EUR 711), with or without confiscation of the objects and tools of committing the administrative violation, or with or without the suspension of the right for the member of the board to hold certain offices in commercial companies. It does not appear that the amount of fine determined for unregistered/unlicensed MVTS activities is either proportionate or dissuasive in the Latvian context.

157. The FCMC advised that upon identifying natural and legal persons that carry out MVTS without obtaining permission (license or registration) it requires these persons to cease their illegal activity. The FCMC also informs the Customers Protection Center, the SRS and the SP on the illegal activity. Information about persons that carry out MVTS without a license or registration is obtained either from customers or market participants or in the course of supervision (inspections) performed by the FCMC.

---

[163] As defined in Sec.1(6) AML/ CFT Law
[164] As defined in Sec.1(7), letters "f" and "g" AML/CFT Law
[165] Registered PI/EMI, which do not obtain a license from the FCMC, are entitled to operate in the territory of Latvia only, and certain monetary thresholds apply to the volumes of their activity.
[166] The Commission is the regulator for postal services, whose competencies are defined in Sec.6 of the Postal Law.
[167] As defined Sec.1(7), letter "i" AML/CFT Law

158. *Criterion 14.3* – According to Sec.45(1) AML/CFT Law, the supervisory authorities tasked with controlling compliance of the REs are the FCMC for banks, electronic money institutions and PIs, and the MoT for the Latvian Post. Paragraph 28 of the Transitional Provisions of the AML/CFT Law defines that on 25 June 2019 the MoT shall cease to be the supervisor for the Latvian Post in terms of its compliance with the amendments to the AML/CFT Law adopted by the Latvian National Assembly on 26 October 2017 and signed by the President of Latvia into law on 9 November 2017, passing the relevant function to the FCMC.

159. *Criterion 14.4* – Art.27 and 28 of the LPSEM define that an MVTS provider may offer services directly or through an agent, upon due notification of and non-objection by the FCMC. Art.31 and 32 establish the rules, respectively, for institutions registered in another Member State to open branches and operate through agents in Latvia, and for institutions registered in Latvia to the same in another Member State, provided that the FCMC has agreed to such activity and has informed the MVTS provider and the supervision institution of the Member State about its positive decision. Information on agents is published on the FCMC website (separately for PIs and EMIs).

160. *Criterion 14.5* – According to Art.27 of the LPSEM, an institution intending to operate through an agent shall submit a written application to the FCMC providing, inter alia, a description of the internal control mechanism that the agent will use to comply with the regulatory provisions on the prevention of ML/FT. Art.28 of the Law establishes that the FCMC shall prohibit an institution from providing payment services through an agent where it is not able to ensure compliance with the regulatory provisions for the prevention of ML/FT. However, the Law does not provide for the obligation of the institution to monitor agents for compliance with AML/CFT programs. The authorities advised that amendments were undergoing consultations with stakeholders to provide that the authorisation contract between institution and agent shall include the institution's rights to monitor on an ongoing basis the agent's compliance with the provisions of AML/CFT regulations.

Weighting and Conclusion

161. The amount of fine determined for unregistered/unlicensed MVTS activities is neither proportionate nor dissuasive in the Latvian context. The AML/CFT Law does not provide for the obligation of MVTS providers to monitor agents for compliance with AML/CFT programs. **R.14 is rated LC.**

Recommendation 15 – New technologies

162. In 2012 MER, Latvia was rated largely compliant with former R.8. The assessment identified technical deficiencies related to the insufficiently stringent levels of CDD given the significant size of non-face-to-face customer base.

163. *Criterion 15.1* – Neither the most recent national ML/FT risk assessment[168] nor other analyses provided to the assessment team contained references to the work done by the authorities for the purpose of identifying and assessing ML/FT risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

164. Sec.8(3) AML/CFT Law requires the REs to carry out assessment of ML/FT risk whenever they intend to introduce changes in their operational processes, governance structure, provided services, products and their delivery channels, including introduction of new technologies or

[168] Adopted on 27 April 2017

services. The authorities presented that the notion of "introducing changes" in the mentioned items is interpreted to cover the element of developing new ones.

165. *Criterion 15.2* – According to Sec.8(3), subsequent to the assessment of ML/FT risk before introducing changes in the products, practices and technologies, the REs have to take measures for improving their internal control systems, which is done by means of, inter alia, reviewing and adjusting the AML/CFT policies and procedures.

Weighting and Conclusion

166. National ML/FT risk assessments and other analyses do not reflect the work done by the authorities for the purpose of identifying and assessing ML/FT risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. **R.15 is rated LC.**

Recommendation 16 – Wire transfers

167. In 2012 MER, Latvia was rated compliant with former FATF SR.VII due to direct applicability of the relevant requirements at the EU level as set out in the Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006. Certain changes have been made to the FATF requirements in this area due to the revision of the FATF Standards in 2012 , which have been incorporated into the new Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006, having come into effect on 26 June 2017. Hence, national implementation is limited to establishing an appropriate monitoring, enforcement, and penalties regime, and applying certain derogations allowed for in EU Regulations.

168. For consistency reasons, the analysis below uses the terminology of the FATF Recommendations interchangeably with that of the Regulation (EU) 2015/847 .

169. *Criterion 16.1* – Art.4 of Regulation (EU) 2015/847 implements the FATF requirement regarding all cross-border wire transfers of EUR 1,000 or more to be always accompanied by required and accurate originator information, as well as by required beneficiary information.

170. *Criterion 16.2* – The FATF requirements regarding batch files are implemented through Art.6 of Regulation (EU) 2015/847 with relevant references to Art.4 for required and accurate originator information, as well as for required beneficiary information.

171. Criterion 16.3 – Art.6 of Regulation (EU) 2015/847 implements the FATF requirement regarding cross-border wire transfers below EUR 1,000 to be always accompanied by required originator and required beneficiary information.

172. *Criterion 16.4* – According to Art.6 of Regulation (EU) 2015/847, financial institutions need not verify the information on the originator unless, inter alia, they have reasonable grounds for suspecting ML/FT.

173. *Criterion 16.5* and *16.6* – Wire transfers with all participants in the payment chain established within the EU are considered domestic transfers for the purposes of R.16, which is consistent with the FATF Standard. Art.5 of Regulation (EU) 2015/847 defines 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. At that, 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. Art.14 of the Regulation requires FIs to respond fully and without delay to enquiries from appropriate AML/CFT authorities.

174. *Criterion 16.7* – Art.16 of Regulation (EU) 2015/847 establishes a 5-year period for ordering and beneficiary FIs to retain the records of originator and beneficiary information. Upon expiry of this retention period, personal data is to be deleted, unless provided for otherwise by national law. The Regulation defines that Member States may allow or require further retention only after they have carried out a thorough assessment of the necessity and proportionality of such further retention, and where they consider it to be justified as necessary for the ML/FT purposes. That further retention period shall not exceed five years.

175. *Criterion 16.8* – Art.4 of Regulation (EU) 2015/847 prohibits the ordering FI to execute any transfer of funds before ensuring full compliance with its obligations concerning the information accompanying transfers of funds.

176. *Criterion 16.9* – Art.10 of Regulation (EU) 2015/847 requires intermediary FIs to ensure that all the information received on the originator and the beneficiary, that accompanies a transfer of funds, is retained with the transfer.

177. *Criterion 16.10* – Regulation (EU) 2015/847 does not provide for the exemption specified in this criterion regarding technical limitations preventing appropriate implementation of the requirements on domestic wire transfers.

178. *Criterion 16.11* – Art.11 of Regulation (EU) 2015/847 stipulates the obligation of the intermediary FI to implement effective procedures including, where appropriate, ex-post or real-time monitoring, in order to detect whether required originator or required beneficiary information in a transfer of funds is missing.

179. *Criterion 16.12* – Art.12 of Regulation (EU) 2015/847 stipulates the obligation of the intermediary FI to establish effective risk-based procedures for determining whether to execute, reject or suspend a transfer of funds lacking the required originator and required beneficiary information and for taking the appropriate follow up action.

180. *Criterion 16.13* (Met) – Art.7 of Regulation (EU) 2015/847 stipulates the obligation of the beneficiary FI to implement effective procedures including, where appropriate, ex-post or real-time monitoring, in order to detect whether required originator or required beneficiary information in a transfer of funds is missing.

181. *Criterion 16.14* – Art.7 of Regulation (EU) 2015/ 847 defines 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. Provisions of Art.16 of the Regulation on retention of the records of beneficiary information apply, as described under the analysis for c.16.7.

182. *Criterion 16.15* (Met) – Art.8 of Regulation (EU) 2015/847 stipulates the obligation of 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.

183. *Criterion 16.16* – The Regulation (EU) 2015/847 is binding for all MVTS providers and, according to Art.2, applies to the transfers of funds, in any currency, which are sent or received by an ordering, intermediary or beneficiary FI established in the EU. Credit and FIs in Latvia, as

defined in Sec.1, Parts 6 and 7 AML/CFT Law, which are authorized to provide MVTS, are REs and, according to Sec.3(2) of the Law, shall ensure that their structural units (including agents), branches and subsidiaries providing financial services in Member States and third countries comply with the requirements for prevention of ML/FT at least to the extent provided for by applicable Latvian legislation.

184. *Criterion 16.17* – The Regulation (EU) 2015/847 does not specifically address situations where both the ordering and beneficiary institutions are controlled by the same MVTS provider.

185. Articles 9 and 13 of the Regulation require beneficiary and intermediary FIs to take into account missing or incomplete information on the originator or the beneficiary 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. Art.4 of the Regulation, in turn, prohibits ordering FIs to execute any transfer of funds before ensuring full compliance with the obligations on accompanying information. Overall, this appears to fall short of the FATF requirement for an MVTS provider to take into account all information from both the ordering and beneficiary sides (as opposed to missing or incomplete information on the originator or the beneficiary).

186. The Regulation (EU) 2015/847 does not require to file a STR in the country affected by the suspicious wire transfer and to make relevant transaction information available to the FIU.

187. Criterion 16.18 – FIs conducting wire transfers are subject to the requirements of the EU Regulations and domestic measures that give effect to UNSCRs 1267, 1373, and successor Resolutions. Reference is made to the analysis for R.6 for further details.

Weighting and Conclusion

188. Regulation (EU) 2015/847 appears to fall short of the FATF requirement for an MVTS provider to take into account all information from both the ordering and beneficiary sides (as opposed to missing or incomplete information on the originator or the beneficiary). It does not require to file a STR in the country affected by the suspicious wire transfer and to make relevant transaction information available to the FIU. **R.16 is rated LC.**

Recommendation 17 – Reliance on third parties

189. In 2012 MER, Latvia was rated partially compliant with former R.9. The assessment identified technical deficiencies related to the failure of the AML/CFT Law to provide unconditional and immediate access to the necessary information from the third party related to the CDD process; the lack of provisions to obtain upon request, without delay, from third parties, the CDD documentation; and the absence of direct referral to the list of equivalent countries.

190. *Criterion 17.1* – According to Sec.29(1) AML/CFT Law, a credit or financial institution is entitled to recognize and accept outcomes of certain CDD measures[169] carried out by acceptable third parties[170], if it: 1) is able to immediately receive from the third party all copies of documents and other necessary information with respect to CDD; and 2) ascertains that the third party applies CDD and record keeping requirements similar to the ones set out in the Latvian AML/CFT Law, and that it is supervised and controlled at least to the same extent as laid down in the Law. Hence, the relying parties are requested to be able to immediately receive – but are not required to

[169] Particularly, identification and verification of the identity of the customer and the BO, as well as understanding the purpose and intended nature of the business relationship

[170] Which are defined as credit and financial institutions in Member States or in third countries

immediately obtain – the necessary information concerning the mentioned CDD measures. In addition, compliance with the Latvian AML/CFT Law does not necessarily amount to compliance with the requirements set out in the R.10 and R.11.

191. Sec.29(3) of the Law defines that the REs are responsible for the compliance with the requirements of the Law whenever they rely on third parties and are required to conduct ongoing monitoring of the business relationship with the customer.

192. *Criterion 17.2* – Sec.29(1) AML/CFT Law defines that a credit or financial institution is entitled to recognize and accept outcomes of certain CDD measures carried out by acceptable third parties, if it has assessed the risk related to the third party or to the country of its operation and has taken the respective risk mitigating measures. The assessment of country risk has to take into consideration the definition of high risk third countries provided in Sec.1(12[1]) AML/CFT Law, which includes the countries or territories determined by the European Commission as having strategic deficiencies in the AML/CFT regimes and posing significant threats to the financial system of the European Union.

193. *Criterion 17.3* – According to Art.29(4) AML/CFT Law, a competent authority shall assume that a credit or financial institution complies with the provisions on third party reliance through its group AML/CFT policies and procedures, provided that: 1) the credit or financial institution relies on information provided by a third party, which is part of the same group; 2) CDD, record-keeping and ML/FT prevention requirements applied within the group comply with the requirements of the Latvian AML/CFT Law; 3) effective implementation of these requirements is supervised at group level by a competent authority of the home Member State or of the third country. It should be noted that compliance with the Latvian AML/CFT Law does not necessarily amount to compliance with the requirements set out in R.10 to R.12 and R.18.

194. Sec.29(1) of the Law further defines that a credit or financial institution is entitled to recognize and accept outcomes of certain CDD measures carried out by acceptable third parties, if it will not accept the outcomes of such CDD measures carried out by a third party, whose operations or country of operation is characterized by higher ML/FT risk.

Weighting and Conclusion

195. The relying parties are requested to be able to immediately receive – but are not required to immediately obtain – the necessary information concerning CDD measures. Compliance with the AML/CFT Law aimed to meet the requirements under c.17.1 and c.17.3 does not necessarily amount to compliance with the requirements set out in R.10-R.12 and R.18. **R.17 is rated LC.**

Recommendation 18 – Internal controls and foreign branches and subsidiaries

196. In 2012 MER, Latvia was rated largely compliant with former R.15 and R.22. The assessment identified technical deficiencies related to lack of legal or regulatory requirements to establish an adequately resourced and independent audit function for certain FIs; no explicit requirement to appoint compliance officers at management level and to introduce screening procedures to ensure high standards when hiring employees. There were also limited requirements to ensure that foreign branches and subsidiaries observe AML/CFT measures, and no requirement to apply the higher standard.

197. *Criterion 18.1* – Sec.6(1) AML/CFT Law defines that the REs, in conformity with their type of activity, shall perform and document the assessment of the ML/FT risks and, on the basis of such

assessment, shall establish an internal control system for AML/CTF, including by developing and documenting the relevant policies and procedures.

a) Compliance management arrangements – Sec.10(1) AML/CFT Law defines that the REs, which are legal persons, shall appoint one or several employees directly responsible for compliance with the requirements of the Law. Sec.10(2) further establishes that the REs shall, in addition to appointing compliance staff, also appoint a member of the Board responsible for monitoring the field of AML/CFT in the respective legal person. Nonetheless, it does not appear that, in terms of the relevant powers and responsibilities, the position of the Board member qualifies for that of the compliance officer appointed at the management level as required by the FATF Standard.

b) Employee screening – According to Sec.10(21) AML/CFT Law, banks, PIs and EMIs are obliged to develop a policy for suitability of the compliance officers and the responsible Board member. Hence, this requirement does not apply to the FIs other than the ones specified in Sec.10(21) of the Law.

c) On-going training – Sec.9 AML/CFT Law requires the REs to ensure that relevant employees are aware of the ML/FT risks and the regulatory enactments governing the prevention of ML/FT, and to conduct regular training of employees on these matters.

d) Independent audit function – Sec.7(1) AML/CFT Law defining the constituents of the internal control system requires the REs to have an independent internal audit function in order to ensure the conformity of the internal control system to the AML/CFT requirements and to assess its effectiveness "if such function is possible considering the number of the employees of the subject of the Law". Hence, availability of an independent audit function is made contingent on an undefined number of employees of the subject of the Law.

198. *Criterion 18.2* – The definition of a group is provided in Sec.1(2^1) AML/CFT Law as a group of legal persons or legal arrangements: a) consisting of the parent undertaking and its subsidiary undertaking, as well as the arrangements, where the parent undertaking or the subsidiary undertaking holds a participatory interest; and b) being a group of companies, within the meaning of Law on the Annual Financial Statements and Consolidated Financial Statements.

199. Information sharing policies and procedures – Sec.3(2) of the AML/CFT Law defines that the REs belonging to a certain group shall implement the information exchange policy and procedures established within the group for the purposes of AML/CFT. The authorities presented that the formulation "for the purposes of AML/CFT" is interpreted to include CDD and ML/FT risk management, as well. Such group-wide policy and procedures shall be effectively implemented in the Member States and third countries also at the level of branches and majority-owned subsidiary undertakings.

200. Provision of information from branches and subsidiaries – Sec.3(2.1) AML/CFT Law defines that the REs belonging to a certain group at the group level shall ensure that the structural units in charge of compliance, audit or AML/CFT functions have access to information from the branches and subsidiary undertakings necessary for the fulfilment of the said functions, including information regarding customers, accounts and payments.

201. Safeguards on confidentiality and use of information – Sec.3(2) AML/CFT Law defines that the REs belonging to a certain group shall implement, inter alia, the group-wide personal data protection policy established within the group for AML/CFT purposes.

202. *Criterion 18.3* – According to Sec.3(3) AML/CFT Law, the REs, whose branches or legal representatives operate (offer services) in another Member State, shall ensure that those branches and legal representatives comply with the requirements of the legal framework of the relevant Member State in the field of AML/CFT.

203. Sec.3(3^1) of the Law defines that where the REs have branches or majority-owned subsidiary undertakings in Member States or third countries, where the minimum legislative requirements with respect to AML/CFT are less strict as those in Latvia, then the requirements laid down in Latvian legislation shall be implemented insofar as they do not contradict to the respective requirements of the host country. Finally, Sec.3(3^2) of the Law provides that the host country does not permit proper implementation of AML/CFT measures consistent with those applied in Latvia, the REs shall ensure that their branches and majority-owned subsidiary undertakings in Member States or third countries take additional measures to effectively restrict the ML/FT risk and inform their supervisory and control authority in Latvia.

Weighting and Conclusion

204. In terms of the relevant powers and responsibilities, the position of the Board member does not appear to qualify for that of the compliance officer appointed at the management level as required by the FATF Standard. The requirement for employee screening applies to banks and PI/ EMIs only. Availability of an independent audit function is made contingent on an undefined number of employees of the subject of the Law. **R.18 is rated LC.**

Recommendation 19 – Higher-risk countries

205. In 2012 MER, Latvia was rated partially compliant with former R.21. The assessment identified technical deficiencies related to lack of supervision on the implementation of the sanctioning mechanism for the Latvian Post; with regard to FIs other than those subject to FCMC supervision, the absence of any requirements for special attention to transactions without an apparent economic or lawful purpose and for enhanced CDD requirements with respect to customers from countries that do not sufficiently apply FATF Recommendations.

206. *Criterion 19.1* – As described in the analysis for c.10.17, Sec.22(2) of the Law requires the REs to apply enhanced CDD in case of establishing business relationships or conducting occasional transactions whenever, inter alia, higher ML/FT risk is present.

207. Sec.11.1(3) of the Law stipulates that the REs should take into account at least certain risk-increasing factors, among which there is the one on affiliation of customers or BOs with higher risk jurisdictions, including the ones that have "refused to cooperate with international organisations in the field of AML and CFT". The authorities presented that this formulation encompasses the countries for which certain actions are called for by the FATF.

208. *Criterion 19.2* – Paragraphs 11 and 12 of Sec.46 AML/CFT Law define the broader obligation of supervisory and control authorities to take supervisory measures based on regularly conducted and revised risk assessments. Sec.47(1) of the Law entitles supervisory and control authorities to issue proposals to the REs for the performance of their AML/CFT obligations, and Sec.78(1) provides for the sanctioning measure of, inter alia, imposing a duty to perform, or to refrain from performing, certain actions in the context of ensuring compliance of the subjects of the AML/CFT Law. These empowerments and instruments enable the application of countermeasures when called upon to do so by the FATF or when decided so by the state authorities.

209. *Criterion 19.3* – The FCMC website provides links to the FATF website. The FCMC advised that it provides monthly reports to the market participants on recent news (including the ones from websites of FATF, MONEYVAL, Basel Committee etc.). The assessment team considers that there is room for improvement in taking proactive action (such as providing up-to-date information on revised lists, publishing notifications etc.) to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries.

Weighting and Conclusion

210. There is room for improvement in taking proactive action to ensure that FIs are advised of concerns about weaknesses in the AML/CFT systems of other countries. **R.19 is rated LC.**

Recommendation 20 – Reporting of suspicious transaction

211. In 2012 MER, Latvia was rated partially compliant with former R.13 and SR.IV. The assessment identified the following technical deficiencies: the failure of the reporting obligation to refer to funds that are proceeds of crime and to cover funds suspected to be linked or related to or to be used for terrorism, terrorist acts or by terrorist organizations; the application of a restrictive list of indicators for suspicion; and the deficiencies in the incrimination of FT potentially limiting the reporting obligations. Since 2012, amendments to the AML/CFT Law have modified the reporting regime.

212. *Criterion 20.1* – Sec.30 AML/CFT Law defines the obligation of the REs to notify the FIU without delay[171] regarding each unusual or suspicious transaction. At that, the reporting obligation also applies to the funds creating suspicions of being directly or indirectly obtained as a result of crime or related to FT or an attempt to carry out such actions, but not yet involved in a committed or attempted transaction. According to Sec.1(16) and 1(17) of the Law, an unusual transaction is defined as "a transaction complying with at least one indication included in the list of unusual transaction indications", and a suspicious transaction is defined as "a transaction creating suspicions that the funds involved therein are directly or indirectly obtained in the result of a criminal offence or are related with FT, or an attempt to carry out such actions".

213. Sec.4(1) AML/CFT Law stipulates that funds owned or possessed by a person in the result of a direct or indirect criminal offence are considered proceeds of crime; i.e. all crimes are predicate offenses. Moreover, Sec.4(3) of the Law stipulates that funds owned by or being under direct or indirect control of the persons included in the lists[172] of persons related to terrorism or proliferation are considered to be proceeds of crime regardless of their legitimate origin. Finally, Sec.5(2) of the Law prescribes to recognize a crime as ML even in cases when the predicate offense has been committed outside Latvia[173], and Sec.5(2.1) recognizes ML as such irrespective of whether or not the exact criminal offence, from which the proceeds have originated, has been identified.

214. While addressing the element of reporting in the presence of suspicions ("a suspicious transaction" or "funds creating suspicions"), the AML/CFT Law does not appear to cover the element of carelessness (failure to give sufficient attention to avoiding harm or errors) or

[171] Latvian authorities advised that the term "without delay" is interpreted as notifying the FIU within 24 hours or on the next working day the latest.
[172] As decided by the CoM or by investigation and judiciary bodies.
[173] ML is defined in Sec.5(1) AML/CFT Law and criminalized by Sec.195 of the CL. The definition of FT is provided in Sec.5(3) and 5(4) AML/CFT Law; terrorism is criminalized by the Sec.88 and FT is criminalized by Sec.88[1] CL. Reference is made to the analysis for c.3.1 and c.5.1 for the compliance of these definitions with the FATF requirements.

negligence (breach of duty of care, which results in damage)[174], i.e. the situations where there are reasonable grounds for suspicions, which are nevertheless neglected.

215. CoM Reg. 1071 (22 December 2008) establishes the indicators for unusual transactions, as well as the procedure and the form[175] for reporting unusual and suspicious transactions to the FIU. While certainly expanding the scope of the transactions to be reported to the FIU, these indicators of unusual transactions do not appear to facilitate or enhance the STR reporting obligation towards "compensating" the deficiency in relation to the lack of obligation to report suspicious also on the basis of reasonable grounds, as set forth in the above analysis. Recommendation No. 152 issued by the FCMC on 25 September 2017 define "red flags" for credit institutions to identify suspicious transactions.

216. *Criterion 20.2* – The obligation to report covers all suspicious transactions, included the attempted ones, regardless of the amount of the transaction. Moreover, Paragraph 2 of CoM Reg. 1071 requires providing a report to the FIU with regard to any consulted, planned, proposed, commenced, deferred, executed or approved unusual or suspicious transaction.

Weighting and Conclusion

217. While addressing the element of reporting in the presence of suspicions, the AML/CFT Law does not appear to cover the element of carelessness or negligence, i.e. the situations where there are reasonable grounds for suspicions, which are nevertheless neglected. **R.20 is rated LC.**

Recommendation 21 – Tipping-off and confidentiality

218. In 2012 MER, Latvia was rated compliant with former R.14.

219. *Criterion 21.1* – According to Sec.40 AML/CFT Law, if the subject of the Law has reported in good faith to the FIU in compliance with the requirements of the Law, irrespective of whether or not the committed or attempted ML/FT or another associated criminal offence is proved during the pre-trial criminal proceedings or on trial (i.e. whether or not it actually occurred), as well as irrespective of the provisions of the contract between the customer and the subject of the Law, such reporting shall not be deemed as disclosure of confidential information and, therefore, the subject of the Law – including its management and employees – shall not be subject to legal or civil liability (which the authorities define to cover any type of liability, including criminal liability).

220. Moreover, actions of the REs in compliance with the requirements of the Law may not be qualified as a violation of the norms regulating the professional activity or the requirements of the supervisory and control authorities.

221. *Criterion 21.2* – Sec.38 AML/CFT Law prohibits the REs – including its management and employees – to notify the customer, BO, as well as other persons (except for supervisory and control authorities) regarding the fact that the data concerning the customer or his/her transactions have been provided to the FIU, and that the analysis of such data may be or is being performed, or that pre-trial criminal proceedings are or may be commenced in relation to a criminal offence, including committed or attempted ML/FT.

[174] The terms "carelessness" and "negligence" are also defined as the failure to act with the prudence that a reasonable person would exercise under the same circumstances.
[175] According to the CoM Reg. 765, a new on-line reporting system currently tested in the FIU (since April 2016) will be de jure implemented starting from 1 January 2018.

222. Sec.32(1) of the Law entitles the subjects to refrain from executing a transaction if it is – or if there are substantiated suspicions that it is – related with ML/FT, or that the funds are directly or indirectly obtained in the result of a committed or attempted criminal offence, including FT. In such cases the subjects should without delay notify the FIU. As a remedy to situations where refraining from executing a transaction would tip-off the involved customer, Sec.36(1) goes on requiring that, whenever refraining from executing such transactions might give a hint assisting the potential offenders to escape liability, the REs are entitled to execute the transaction and report it to the FIU.

Weighting and Conclusion

223. **Latvia is compliant with R.21.**

Recommendation 22 – DNFBPs: Customer due diligence

224. In 2012 MER, Latvia was rated partially compliant with former R.12. The assessment identified technical deficiencies – in addition to those vis-à-vis former R.5 and R.10 – related to uneven application of relevant AML/CFT requirements across the entire field of organizers of lotteries and gambling houses, real estate agents etc.

225. In the analysis presented below, the deficiencies identified in relation to the compliance of FIs with the FATF requirements under respective Recommendations are also relevant, where applicable, for the DNFBPs, unless specified otherwise.

226. *Criterion 22.1* – Reference is made to the analysis for R.10 on the general coverage of CDD requirements within Latvian legislation. The assessors were advised that, with regard to multiple operations, the notion of "mutually linked" is applied in the meaning of the FATF-defined "appear to be linked".

a) Casinos – Clause 7 of Sec.3(1) defines organizers of lotteries and gambling as REs. Sec.11 AML/CFT Law defines specific situations for these types of DNFBP to comply with the CDD requirements, particularly when they engage in transactions[176] with customers equal to or above EUR 2,000 regardless of whether the transaction is carried out in a single operation or several mutually related operations. This provision appears to be in line with the FATF-defined situations for the said categories of DNFBP to comply with the requirements set out in R.10[177].

b) Real estate agents – Sec.3(1)(6) defines persons acting as real estate agents or intermediaries in immovable property transactions as REs without specifying the situations in which they obtain the said status. There is no provision for real estate agents to comply with the requirements set out in R.10 with respect to both the purchasers and the vendors of the property. Except for the AML/CFT Law, the assessors have not been provided legislation setting out additional specific provisions relevant for their compliance with AML/CFT requirements under R.10.

c) Dealers in precious metals and stones (DPMS) – Sec.3(1)(9) define other legal or natural persons trading in precious metals, precious stones and articles thereof as REs. Sec.11 AML/CFT Law defines specific situations for these types of DNFBP to comply with the CDD requirements, particularly when they engage in a cash transaction, or a transaction settled by paying cash into the seller's account with a bank, equal to or above EUR 10,000 regardless of whether the transaction is

[176] Including the cases when the customer wins, buys the means for participation in the game or lottery tickets, or exchanges currency for such purpose

[177] Also, the Gambling and Lotteries Law contains certain provisions relevant for customer identification and verification of identity by operators of land-based casinos, and customer identification (with no verification of identity) by operators of interactive gambling.

carried out in a single operation or in several mutually related operations. This provision appears to be in line with the FATF-defined situations for the said categories of DNFBP to comply with the requirements set out in R.10.

d) Sworn lawyers, notaries, other independent legal professionals and accountants (tax advisors) – Clause 4 of Sec.3(1) defines these categories of DNFBP as REs when they, acting on behalf and for their customer, assist or participate in the planning or execution of transactions, or carry out other professional activities related to the transactions for their customer concerning the following: a) buying and selling of immovable property, shares of a commercial company; b) managing of the customer's money, financial instruments and other funds; c) opening or managing of all kinds of accounts in banks or financial institutions; d) creating, managing or providing operation of legal arrangements, as well as organizing contributions necessary for the creation, operation or management of a legal arrangement. With the exception that the FATF-defined buying and selling of business entities not always is done through buying or selling shares of a commercial company, this provision appears to be in line with the FATF-defined situations for the said categories of DNFBP to comply with the requirements set out in R.10[178].

Nonetheless, according to Sec.11(8) AML/CFT Law these categories of DNFBP are not covered by the requirement of Sec.28(2) and Sec.11(7) to terminate the business relationship where they are unable to obtain the necessary CDD information and documents (as set out under c.10.19), in cases when they defend or represent their customers in pre-trial criminal proceedings or judicial proceedings, or advise on instituting or avoiding judicial proceedings, thus clearly diverging from the FATF-defined legal professional privilege stipulated for STR reporting only.

e) Trust and company service providers (TCSPs) – Clause 5 of Sec.3(1) defines providers of services related to the creation and provision of operation of a legal arrangement or legal person as REs without specifying the situations in which they obtain the said status. Latvian law does not recognize trusts as a distinct type of legal arrangement. Except for the AML/CFT Law, the assessors have not been provided legislation setting out additional specific provisions relevant for their compliance with AML/CFT requirements under R.10.

227. *Criterion 22.2* – Reference is made to the analysis for R.11 on the general coverage of record-keeping requirements within Latvian legislation. Except, as described in the analysis for R.11, the assessors have not been provided legislation setting out additional specific provisions relevant for the compliance of DNFBPs with AML/CFT requirements under R.11.

228. *Criterion 22.3* – Reference is made to the analysis for R.12 on the general coverage of PEP requirements within Latvian legislation. Except for the AML/CFT Law, the assessors have not been provided legislation setting out additional specific provisions relevant for the compliance of DNFBPs with AML/CFT requirements under R.12.

229. *Criterion 22.4* – Reference is made to the analysis for R.15 on the general coverage of new technologies requirements within Latvian legislation. Except for the AML/CFT Law, the assessors have not been provided legislation setting out additional specific provisions relevant for the compliance of DNFBPs with AML/CFT requirements under R.15.

[178] Also, the Notariate Law contains certain provisions relevant for identification and verification of identity of customers (but not BOs).

230. *Criterion 22.5* – Reference is made to the analysis for R.17 on the general coverage of third party reliance requirements within Latvian legislation. Except for the AML/CFT Law, the assessors have not been provided legislation setting out additional specific provisions relevant for the compliance of DNFBPs with AML/CFT requirements under R.17.

231. According to Sec.29 AML/CFT Law, among the REs only credit and financial institutions are permitted to recognize and accept outcomes of identification and due diligence of customers and BOs, including information on the purpose and intended nature of the business relationship, which have been carried out by acceptable third parties[179]. However, this permission does not apply to any DNFBPs.

Weighting and Conclusion

232. Reference is made to the deficiencies identified with regard to R.10, R.11, R.12, R.15 and R.17. In addition, there is no provision for real estate agents to comply with the requirements set out in R.10 with respect to both the purchasers and the vendors of the property. Sworn lawyers, notaries, other independent legal professionals and accountants (tax advisors) are not covered by the requirement to terminate the business relationship where they are unable to obtain the necessary CDD information and documents in cases when they defend or represent their customers in pre-trial criminal proceedings or judicial proceedings, or advise on instituting or avoiding judicial proceedings, thus clearly diverging from the FATF-defined legal professional privilege stipulated for STR reporting only. **R.22 is rated PC.**

Recommendation 23 – DNFBPs: Other measures

233. In 2012 MER, Latvia was rated partially compliant with former FATF R.16. The assessment identified technical deficiencies related to the failure of the reporting obligation to refer to funds that are proceeds of crime and to cover funds suspected to be linked or related to or to be used for terrorism, terrorist acts or by terrorist organizations; the application of a restrictive list of indicators for suspicion; and the deficiencies in the incrimination of FT potentially limiting the reporting obligations.

234. In the analysis presented below, the deficiencies identified in relation to the compliance of FIs with the FATF requirements under respective Recommendations are also relevant, where applicable, for the DNFBPs, unless specified otherwise.

235. *Criterion 23.1* – Reference is made to the analysis for R.20 on the general coverage of STR reporting requirements within Latvian legislation.

236. Sec.30(1) AML/CFT Law requires the REs to report their ML/FT suspicions to the FIU. SRO of DNFBPs[180], which are defined as supervisory and control authorities under Sec.45 AML/CFT Law, have no legally defined competence for receiving STRs.

237. In relation to this, Latvian authorities refer to the Law on Taxes and Fees providing for the obligation of every subject of the AML/CFT Law to file reports to the SRS (as per indictors for determining suspiciousness of transactions from the standpoint of tax compliance) on transactions concerning taxes which are suspicious for the purposes of the AML/CFT Law. Whereas such a "parallel" system of STR reporting might potentially create confusion as to the appropriate

[179] The acceptable third parties are defined as credit and financial institutions.
[180] Such as the Latvian Association of Certified Auditors, the Latvian Sworn Notaries Council and the Latvian Council of Sworn Advocates

authority to deal with the ML/FT suspicions of the subjects of the AML/CFT Law, it has no relevance for the compliance of DNFBPs with AML/CFT requirements under R.20.

a) Sworn lawyers, notaries, other independent legal professionals and accountants (tax advisors) – The requirement set out in the AML/CFT Law to report unusual and suspicious transactions to the FIU applies to these categories of DNFBP whenever they qualify as REs (as described under the analysis for c.22.1(d)), except for the cases when, as prescribed in Sec.30(3) of the Law, they defend or represent their customers in pre-trial criminal proceedings or judicial proceedings, or advise on instituting or avoiding judicial proceedings except in the field of AML/CFT. This appears to be in line with the FATF-defined qualification for the said categories of DNFBP to comply and, where applicable, to be exempt from complying with the STR reporting obligation.

b) DPMS – The requirement set out in the AML/CFT Law to report unusual and suspicious transactions to the FIU applies to these categories of DNFBP whenever they qualify as REs (as described under the analysis for c.22.1(c). This appears to be in line with the FATF-defined qualification for the said categories of DNFBP to comply with the STR reporting obligation.

c) TCSPs – Latvian law does not recognize trusts as a distinct type of legal arrangement. The requirement set out in the AML/CFT Law to report unusual and suspicious transactions to the FIU applies to company service providers without specifying the qualifications for them to become REs (as described under the analysis for c.22.1(e)).

238. *Criterion 23.2* – Reference is made to the analysis for R.18 on the general coverage of internal control requirements within Latvian legislation. Except for the AML/CFT Law, the assessors have not been provided legislation setting out additional specific provisions relevant for the compliance of DNFBPs with AML/CFT requirements under R.18.

239. It should be mentioned that the requirement to have employee screening procedures, as set out in Sec.10(21) of the Law does not apply to any DNFBPs.

240. *Criterion 23.3* – Reference is made to the analysis for R.19 on the general coverage of the requirements regarding high-risk countries within Latvian legislation. Except for the AML/CFT Law, the assessors have not been provided legislation setting out additional specific provisions relevant for the compliance of DNFBPs with AML/CFT requirements under R.19.

241. *Criterion 23.4* – Reference is made to the analysis for R.21 on the general coverage of the tipping-off and confidentiality requirements within Latvian legislation. Except for the AML/CFT Law, the assessors have not been provided legislation setting out additional specific provisions relevant for the compliance of DNFBPs with AML/CFT requirements under R.21.

242. Sec.40(4) of the Law establishes that when sworn lawyers, notaries, other independent legal professionals and accountants (tax advisors) refrain a customer from the involvement in criminal offences, it shall not be deemed to be a disclosure of confidential information (i.e. amount to tipping-off). This appears to be in line with the FATF-defined situations for the said categories of DNFBP to comply with the non-disclosure obligation.

Weighting and Conclusion

243. Reference is made to the deficiencies identified with regard to R.18-21. In addition, the requirement to have employee screening procedures does not apply to any DNFBPs. **Latvia is largely compliant with R.23.**

Recommendation 24 – Transparency and beneficial ownership of legal persons

244. In the 4th Round Latvia was rated Compliant with R.33.

245. *Criterion 24.1* – (a) Types, forms and features of legal persons: In Latvia these consist of partnerships (general and limited), limited liability companies (LLC), stock companies, European companies, cooperative societies, associations and foundations. Separate legislation defines each type of legal person, as discussed under (b) below.

246. (b) Process for creation of legal persons: The Commercial Law, the Law on European Companies, the Cooperative Societies Law, and the Association and Foundations Law each govern the processes of creating the respective types of legal persons, including the obtaining and recording of basic data. All the necessary information for incorporation is available publicly in Latvian and English. As of the date of the onsite visit the legislation was amended to define BO (for partnerships and companies) in line with the FATF definition.

247. *Criterion 24.2* – The NRA addresses the ML/FT risks associated with legal persons in Latvia. According to the NRA, the LLC is the most common type of legal person in use in Latvia, followed by limited partnerships and stock companies (JSC). In terms of vulnerability to ML/FT the NRA notes that the LLC and foreign legal persons registered in low-tax or tax-free countries are the legal persons mostly involved in ML/FT schemes.

248. *Criterion 24.3* – All legal persons created in Latvia acquire their legal existence from the date when they are registered by the authorities in the ER.

249. The ER consists of 13 registers. The principle registers of legal persons are the Commercial Register (for partnerships, general and limited) and companies (LLCs and stock companies), the ER Journal (for co-operative societies) and the Register of Associations and Foundations (for associations, foundations, and trade unions). Legal personality can only be obtained after registration. The information collected and recorded for commercial companies covers all the requirements under this criterion (Commercial Law Sec. 8(3)(4) and Sec.149). All information in the Commercial Register is publicly available (Sec.7 Commercial Law). Co-operative societies are registered in the ER Journal (Sec.4(2) of the Co-operative Societies Law). The information collected and recorded for co-operative covers all the requirements under this criterion (Cooperative Societies Law Sec.11 and Sec.12 and ER Law Sec.6). Associations and foundations are registered in the Register of Associations and Foundations. The information collected and recorded for associations and foundations covers all the requirements under this criterion (Sec.13, Sec.26 and Sec.92 Associations and Foundations Law). According to Sec.4.10, Paragraph 1 of the Enterprise Register Law, state authorities receive information from registers held by the ER free of charge, mostly on-line.

250. *Criterion 24.4* – There is an explicit obligation on legal persons to keep the information filed in the ER up to date (Sec.16 Commercial Law, Sec.21 Associations and Foundations Law, Sec.42(5) Co-operative Society Law). All legal persons having shareholders are required to keep and maintain a register of their registered shareholders (Commercial Law ss.187 (LLCs) and 234 (stock companies)). All public limited liability companies are required to maintain also information on the category of stock. All partnerships are required to record information on the amount of contribution of each limited partner and the total amount of limited partner. There is no explicit obligation to keep the register within Latvia; however, a copy of every division (update) of the register of shareholders (Sec.187 (LLCs) and information on the new members joining partnerships

(Commercial Law Sec.78(3)) must be filed with the Commercial Enterprise Register; for stock companies, the competent authorities have statutory access to the shareholder register (s.236).

251. Criterion 24.5 – There is an explicit obligation on legal persons to keep up to date the information filed in the Commercial Register (Sec.16 Commercial Law, Sec.21 Associations and Foundations Law, and Sec.42 (5) Co-operative Society Law). Information and documents shall be submitted to the relevant Registers and within 14-15 days from the day when the relevant decision was taken. Sec.166.[3] AVC specifies the time frame and provides for administrative liability for failure to comply. The Commercial Law and the Law on the Enterprise Register provide for a number of measures for the registrar to verify information referred to under criteria 24.3 and 24.4.

252. *Criterion 24.6* – (a) & (b) BO is defined in the AML/CFT Law (Sec.1(5)). The Commercial law obligates nominee shareholders to notify the legal person if they hold shares for the benefit of another person (Commercial Law Sec.17(2)).

253. Natural persons shall immediately report to the legal person if they become BO of a legal entity (Sec.18[1] AML/CFT Law).

254. Legal persons under Sec.18[1] shall determine and identify company's BOs, if there are reasonable grounds to doubt that information submitted by the natural persons who are BOs is not accurate or relevant information has not been submitted.

255. According to Sec.18[2] legal entities (including partnerships) are required to submit an application on the UBO to the RE. However, this provision came into force after the onsite visit and cannot be considered for the purpose of this assessment.

256. (c) The AML/CFT law requires FIs and DNFBPs to gather information on the BO of their clients in one of the following ways: statement on BO by customer; using the information in the Commercial Register of Latvia or equivalent information from a foreign State; or make a BO determination themselves where it is impossible to obtain the information in any other way. (AML/CFT Law Sec.18).

257. *Criterion 24.7* – There was an explicit obligation on legal persons to keep up to date the information filed in the Commercial Register under the Register (Sec.16 Commercial Law, Sec.21 AFL, Sec.42 (5) Co-operative Society Law), which were in force at the time of the onsite visit. This provision was not applicable to other legal persons. Legal persons and partnerships registered in the ER shall, without delay and within 14 days of receiving knowledge, file changes in such information by updating it (Sec.18.[2](1) AML/CFT Law). However, this provision came into force after the onsite visit and cannot be considered for the purpose of this assessment. As indicated by the authorities ER exchanges information with other competent authorities, including SRS, to check that information submitted by the legal entities is accurate and up-to-date. REs are required to keep CDD information up to date, which includes also BO information (see c.10.7).

258. *Criterion 24.8* – Members of the board of directors of a company or a limited partnership or an association or foundation are authorized to disclose basic and UBO information to the authorities (Commercial Law Sec.17.[1](10), Associations and Foundations Law Sec.26). This includes disclosure to LEAs (which includes the police) and control authorities in the field of tax administration, public procurement or also public-private partnership which are entitled to access the information regarding BOs of a partnership and a capital company. However, there is no specific provision that requires one or more natural persons resident in Latvia or for the appointment of an accountable DNFBP to be responsible for maintaining BO and be accountable to the authorities.

259. *Criterion 24.9* – Records on legal persons must be retained by the liquidator for a 10 year period (Law on Archives, Commercial Law, Cooperative Societies Law, and the Association and Foundations Law). It is not clear whether this applies to BO information. The Commercial Register is not subject to a minimum records retention period but records are retained indefinitely according to the authorities. REs are obliged to maintain all information obtained within the scope of the CDD, including information on the customer, copies of the documents attesting to the customer identification data, CDD outcomes for a period of five years following the end of business relationships.

260. *Criterion 24.10* – LEAs and control authorities in the field of tax administration, public procurement or also public-private partnership are entitled to access to information regarding BOs of a partnership and a capital company (Commercial law Sec.17.[1](10), Associations and Foundations Law Sec.26). Additionally, Sec.18[3] of the AML/CFT Law provides that any person shall be entitled to receive online information on the BOs at disposal of the ER. Moreover, the FIU is entitled to request and receive information from the REs (Sec.51(2)(4) AML/CFT Law). Due to the low level of BO work in the FI sectors, and the deficient BO definition that was only corrected during the on-site, the assessors consider that the ability of LEAs and supervisory authorities to have timely access to BO information held by FIs is low.

261. *Criterion 24.11* – Bearer shares have been prohibited in Latvia since 2008. Bearer warrants are unknown under Latvian law. Existing bearer shares were dematerialized and registered with the Central Depository.

262. *Criterion 24.12* – Nominee shareholders: as noted above a person who holds shares in a legal person for the benefit of another person is required to disclose this fact to the legal person, including the name of the BO(s). This notion of BO appears to cover only simple types of nominees. Nominee Directors: LLC legislation imposes obligations and responsibilities on all persons who are directors and does not provide for nominal activity for nominee directors; however, there is no explicit prohibition against a person acting as a nominee director.

263. *Criterion 24.13* – Failure of legal persons to provide documents/information to the Commercial Register is punishable by fines ranging from EUR 70 to 430, which are increased to a maximum of EUR 700 for a repeat offence in a 12-month period (Sec.166[3] AVC). Providing false information to State Institution attracts a penalties range of up to EUR 38,000 (Sec.272 CL). Failure of any person to supply BO information to a legal entity or a natural person attracts a prison sentence, community service or a financial penalty (Sec.195.[1](1) CL). If these failures result in significant harm, the prison sentences increase to a maximum of one year, and the penalty increases to a maximum of 150 months of income.

264. *Criterion 24.14* – (a) Basic information in the Commercial Register is available free of charge on request, and on-line through the European Business Register of which Latvia is a member. (b) and (c) Competent authorities can use their powers under the CPL provides that a request of a foreign state regarding the provision of assistance in the performance of a procedural action shall be decided immediately, but not later than within 10 days after receipt thereof. If additional information is necessary for deciding of a request, such information shall be requested from the state that submitted the request. The state that submitted the request shall be, without delay, informed if the execution of the request or a part thereof has been rejected or if a foreign state has so requested. In addition, Sec.849(2) CPL stipulates that the institution executing a request of a foreign state shall, in a timely manner, inform the foreign state, on the basis of an order of the

competent authority, regarding the time and place of the performance of a procedural action. There are no specific provisions concerning the exchange of information on shareholders. Also see the analysis for R.37 and R.40.

265. *Criterion 24.15* – The FCMC is monitoring the quality of assistance being received. No information was provided from the other competent authorities on how the Latvian competent authorities assess the quality of the information they receive from other countries in response to requests for basic and BO information or requests for assistance in locating BOs residing outside Latvia.

Weighting and Conclusion

266. Latvia meets or mostly meets all criteria except: c.24.9., 24.12. and 24.15. Latvia achieves this by having legislation enter into force during the onsite visit addressing deficiencies in the definition of BO and having the information available to authorities. **R.24 is rated LC.**

Recommendation 25 – Transparency and beneficial ownership of legal arrangements

267. In the previous round Recommendation 34 was rated as NA.

268. *Criterion 25.1* – (a) In accordance with the Methodology c.25.1(a) does not apply to Latvia as neither trusts nor other legal arrangements are recognized under domestic law. However, there is no prohibition on foreign trusts operating in Latvia (see c.25.5). (b) There are no trusts governed under Latvian law (see (a)). The AML/CFT law applies to a natural or legal person having a business relationship with the customer and providing the following services: "… the duties of a trustee of an express trust or similar legal document or provides the fulfilment of such duties by another person" (Sec.1(10)(d) AML/CFT Law). Such services apply de facto to foreign trusts since trusts do not exist/are not recognised under domestic law; (c) A person acting as a professional trustee of a foreign law trust would be subject to the AML/CFT Law and subject to its record-keeping requirements. Clause 5 of Sec.3(1) defines providers of services related to the creation and provision of operation of a legal arrangement or legal person as REs without specifying the situations in which they obtain the said status. The deficiencies identified under c.10.11 would have an impact on the application of this requirement.

269. *Criterion 25.2* – Pursuant to Sec.11.[1] AML/CFT Law, REs that are trustees of foreign trusts are required to ensure the storage and regular updating of the documents, data and information obtained in the process of CDD.

270. *Criterion 25.3* – Although the AML/CFT Law stipulates that in cases when a person purports to act on behalf of customer, the subject of the Law shall identify and verify the identity of the customer and determine the customer's ownership and control structure, there is no requirement for trustees of foreign trusts to disclose their status to FIs or DNFBPs when forming a business relationship or carrying out an occasional transaction above the threshold.

271. *Criterion 25.4* – There is no provision in Latvian law which would prevent the disclosure of information regarding a foreign trust or legal arrangement (as noted above, neither trusts nor other legal arrangements are recognized under domestic law).

272. *Criterion 25.5* – The AML/CFT law applies to a natural or legal person having a business relationship with the customer and providing the following services:"… the duties of a trustee of an express trust or similar legal document or provides the fulfilment of such duties by another person" (Sec.1(10)(d) AML/CFT Law). Such services apply de facto to foreign trusts since trusts do not

exist/are not recognised under domestic law. There do not appear to be any impediments to the ability of competent authorities to access the information held by persons in Latvia acting as trustees of foreign trusts; however, since there is no requirement for such trustees to declare their status to the subjects of the AML/CFT Law, there is no systematic way for the competent authorities to determine whether such subjects are acting as trustee. According to c.31.1, competent authorities are able to obtain access to all necessary documents and information when investigating and prosecuting ML/FT and associated predicate offences.

273. *Criterion 25.6* – Latvia has the mechanism to provide international cooperation on trusts see c.24.14. Also see the analysis for R.37 and R.40.

274. *Criterion 25.7* – Person acting as a professional trustee of a foreign law trust will be subject to a sufficiently proportionate and dissuasive sanction for failing to comply with CDD and record-keeping requirements in the AML/CFT Law. See c.28.4 and R.35.

275. *Criterion 25.8* – While Latvia does not recognize trusts within the jurisdiction, there is no prohibition on the provision of trust services from within the country. Failure to comply with record keeping obligations by trustees of foreign trusts is sanctionable under the AML/CFT Law. CDD information held by FIs or DNFBPs that are trustees is fully accessible by competent authorities, if the authorities know the FI or DNFBP is acting as a trustee.

Weighting and Conclusion

276. Latvia meets c.25.2, c.25.4, c.25.5, c.25.7 and c.25.8 and mostly meets c.25.1 and 25.6. It partly meets c.25.3, since there is no requirement for trustees of foreign trusts to disclose their status to financial institutions or DNFBPs when forming a business relationship or carrying out an occasional transaction above the threshold. **R.25 is rated LC.**

Recommendation 26 – Regulation and supervision of financial institutions

277. In the 4th round MER Latvia was rated largely compliant with former R.23. Reinsurance companies were unsupervised for AML/CFT purposes. The assessors pointed out that the effectiveness of the AML/CFT supervisory activity was diminished by the uneven degree of application of AML/CFT requirements in different sectors by REs. Moreover, no financial sanctions were applied to directors and board members of supervised entities.

278. *Criterion 26.1* – Under the Single Supervisory Mechanism (SSM) the European Central Bank (ECB) is responsible for the prudential supervision of significant banks. However, AML/CFT supervision of banks, credit institutions, EMIs, insurance companies, companies providing financial guarantees and commitments (provided they are "credit institutions" as defined in the Law on Credit Institutions), private pension funds, insurance intermediaries providing life insurance services, investment brokerage companies, investment management companies and PIs (Sec.45(1)1 AML/CFT Law) is the responsibility of the FCMC. The BoL is responsible for regulating and supervising capital companies licenced by the BoL for the buying and selling of foreign currency cash (Sec.45(1)6 AML/CFT Law). The MoT supervises the Latvian Post (Sec.45(1)5 AML/CFT Law). The SRS supervises other institutions (if they are not participants of the financial and capital market) that provide the following services: a) lending, including financial leasing (if the service provision is not subject to licencing); b) issuance of sureties and such other letters of commitment, by which a duty is imposed; c) advising the customers in the issues of financial nature; d) encashment; e) virtual currency exchange services (Sec.45(2)(6) AML/CFT Law).

279. *Criterion 26.2* – Core Principles FIs: Credit institutions are licensed by the European Central Bank (ECB), which cooperates with the FCMC. Insurance Companies are licensed by the FCMC (Insurance & Reinsurance Law, Art.4.). Investment broker/management companies are licenced by the FCMC (Law on Investment Management Companies, Art.4). Alternative investment funds are required to register only if they manage fund assets (including any assets, acquired through use of financial leverage), that in total do not exceed a threshold of EUR 100 million, or fund assets, that in total do not exceed threshold of EUR 500 million, provided that portfolios of alternative investment funds consist of alternative investment funds that are unleveraged and have no redemption rights exercisable during a period of five years following the date of initial investment in each alternative investment fund (Law On Alternative Investment Funds and their Managers, Sec.7).

280. Other FIs: EMIs and PIs are licenced or registered by the FCMC under the Law on Payment Services and Electronic Money (Art.1 and 4). MVTS that are foreign currency cash buying and selling capital companies are licensed by the BoL when they are registered on the ER (Law on the BoL Sec.11(1)). Latvian post is a state-owned postal service operating a MVT service. It is currently supervised by the MoT, but this function has been agreed to be transferred to the FCMC according to the amendments to the AML/CFT Law which will come into force in June 2019. Cash collecting service providers are not subject to registration or licensing requirements. There are licensing requirements for lending activities conducted by non-bank FIs only if they provide consumer lending services.

281. The creation or continued operation of shell banks is prohibited in Latvia (Sec.21 AML/CFT Law).

282. *Criterion 26.3* – Persons intending to acquire or increase a qualifying holding must provide inter alia information on the person's financial stability, professional activities, administrative penalty and criminal record, other beneficiaries, for the legal persons information provided should include inter alia, information on the owners, members of the council and board. The FCMC evaluates compliance of the request with legislative requirements; this includes criteria on a "good repute" of the person. (Law on Credit Institutions Art.29). Art.16(3) of the law on Credit Institutions provides that the FCMC has the right to examine the identity, criminal record and documents of the persons defined under Art.19. As clarified by the authorities this is an obligatory requirement and is applied in all cases. Under Article 19 of the Law on Credit Institutions the FCMC is entitled to verify the identity of the founders of a credit institution.

283. Where the founder is a legal person itself, the FCMC has the right to verify information regarding their founders (stockholders (shareholders)) and BOs.

284. Under the Law on Credit Institutions the chairman of the management board, the members of the management board, the head of the internal audit service, the chief risk officer, the chief compliance officer, the person responsible for compliance with the AML/CFT requirements, the credit institution's controller, the head of a branch of foreign credit institution or a branch of credit institution in another Member State and the procurator of the credit institution should comply with the following criteria: person who is competent in financial management matters. The person who is competent in company's management matters may act as the person responsible for compliance with the AML/CFT requirements; persons who have the necessary education and three years relevant professional work experience in an undertaking, organisation or institution of relevant size; persons who have an impeccable reputation; persons who have not been deprived of the right of engaging in commercial activities.

285. A credit institution has the duty to remove, without delay, persons referred above that do not meet the requirements laid down in this Section.

286. Concerning the PIs and the EMIs - any person that wishes to acquire a qualified holding in a PI or EMI or increasing a qualifying holding are required to notify the FCMC in advance (Law on Payment Services and Electronic Money, Art.26). The notification shall indicate the amount of the holding as a percentage of the share capital or the shares or stock with voting rights of the institution. The notification shall be submitted together with the information that is set out in the FCMC's regulatory provisions and is necessary to assess the person's compliance with the criteria set out in the Law on Payment Services and Electronic Money (Paragraph 1 of Art.15). Under the Paragraph 1 of Art.15 of the Law on Payment Services and Electronic Money – the FCMC shall assess sufficiency of the person's free capital in respect of the volume of the shares or stock to be acquired in an institution, financial soundness of the person and the financial motivation of the proposed acquisition to ensure sustainable and careful management of the institution where the person intends to acquire the holding and the likely influence of that person on the management and business of the institution.

287. In the assessment process, the FCMC shall take into account also the following criteria: 1) good repute of the person and compliance with the requirements for an institution's shareholders or members/participants; 2) good repute and professional experience of the person that, as a result of the proposed acquisition, will direct the business of the institution; 3) financial soundness of the person, in particular in relation to the type of the business pursued or envisaged in the institution in which the acquisition is proposed; 4) whether the institution will be able to comply with the regulatory requirements set out in this Law and in other regulatory provisions and whether the group of commercial companies of which the institution will become a part has a structure that will not restrict the FCMC's possibilities to exercise the supervision functions vested to it by law, to ensure efficient exchange of information among supervisory authorities and to determine the allocation of supervisory responsibilities among the supervisory authorities; 5) whether there are reasonable grounds to suspect that, in connection with the proposed acquisition, ML or FT has been committed or attempted or that the proposed acquisition could increase the risk of such activity.

288. Under the Law on Payment Services and Electronic Money the FCMC shall take a decision on prohibiting the person from acquiring or increasing a qualifying holding where the person: 1) fails to comply with the criteria set out in Paragraph 1 of Art.15 of Law on Payment Services and Electronic Money; 2) fails or refuses to submit to the FCMC the information set out in this Law or the additional information required by the FCMC; 3) due to conditions beyond its control, cannot provide the information set out in this Law or the additional information required by the FCMC.

289. Under the Law on Payment Services and Electronic Money (Art.20) a person shall be entitled to become chairman of the executive board, a member of the executive board, chairman of the council (if formed), a member of the council, a person that, by taking important decisions on the institution's behalf, incurs civil liability on the institution, the person responsible for compliance with the AML/CFT requirements, and also a person that is directly responsible for managing the payment service operations or the issuance of electronic money, provided that he/she: 1) is competent in financial management matters; 2) has the necessary education and at least three years of work experience at a commercial company, an organisation or an institution of a similar size; 3) is of good repute; 4) has not been deprived of the right to engage in commercial activities.

290. PI/EMI has the duty to remove, without delay, persons referred above that do not meet the requirements laid down in this Section.

291. A person shall not be entitled to become chairman of the executive board, a member of the executive board, chairman of the council (if formed), a member of the council, a person that, by taking important decisions on the institution's behalf, incurs civil liability on the institution, the person responsible for compliance with the AML/CFT requirements and also a person that is directly responsible for managing the payment service operations or the issuance of electronic money where he/she: 1) has been convicted for a deliberate crime or to whom, for having committed a deliberate crime, an order about a punishment issued by a prosecutor has been applied; 2) has been convicted for a deliberate crime or to whom, for having committed a deliberate crime, an order about a punishment issued by a prosecutor has been applied, though he/she has been released from the punishment due to limitation, pardon or amnesty; 3) has been a subject in a criminal procedure for a deliberate crime that was dismissed due to limitation or amnesty; 4) has been a subject in a criminal procedure for a deliberate criminal offence that has been dismissed and the person has been released from criminal liability, where the criminal offence has not resulted in a detriment liable to criminal punishment or where a settlement with the victim or his/her representative has been reached; 5) has been a subject in a criminal procedure for a deliberate criminal offence that has been dismissed where the person had assisted in solving a serious crime or a particularly serious crime whose gravity or hazardousness exceeds the criminal offence committed by the person himself/herself; 6) has been a subject in a criminal procedure for a deliberate criminal offence that has been dismissed and the person has been conditionally discharged from criminal liability.

292. The competent management body of the institution shall have an obligation, either upon its own initiative or the Commission's request, to promptly suspend from office the persons referred to in Paragraph 1 hereof where the restrictions referred to in Paragraph 1 hereof may apply to them.

293. It is not clear whether this requirement addresses associates of persons with criminal records.

294. Prior to changing a participant having a qualifying holding in the capital company, a representative of the executive bodies or a holder of a procuration, the capital company shall obtain an approval for the change from the Licensing Committee of the BoL. The information to be provided to the BoL includes information on the criminal and administrative violation record. There are no requirements on BOs and associates of persons with criminal records.

295. Under the SSM, the ECB has responsibility for assessing the suitability of members of the management body and key function holders of significant banks, based on criteria including reputation and the existence of conflicts of interest: Art. 93 and 94 EU Regulation 468/2014. The ECB also authorises the acquisition of qualifying shareholding in all Latvian banks, irrespective whether they are significant or less significant banks. The criteria include looking at whether the transaction involves, or increases the risk of, ML or the FT: Art 23(1)(e) Directive 2013/36/EU (CRD) and Art. 85 to 87 EU Regulation 468/2014.

296. *Criterion 26.4* – a) Core Principles FIs: Latvia has not been subject to rated assessments of the Basel Committee Principles, the IAIS Principles or the IOSCO Principles and Responsibilities.

297. Supervision of Latvian banks, credit unions, insurance companies and insurance brokerage companies, participants of financial instruments market, as well as private pension funds, PIs and EMIs is carried out by the FCMC, including supervision and control of compliance with the requirements of the AML/CFT Law. According to Sec.5 of the Law on the FCMC the objective of the operation of the Commission is to promote the protection of the interests of investors, depositors and insured persons and the development and stability of the financial and capital market. According to Sec.7 AML/CFT Law the supervisory and control authorities shall determine the methodology for the detection and risk assessment of ML and FT in conformity with the activities of the REs.

298. According to Sec.112.2 of the Law on Credit Institutions the FCMC shall carry out consolidated supervision on the level of a consolidation group. The FCMC shall also carry out consolidated supervision on the level of a consolidation group of investment brokerage companies (investment firm) (Sec.142 of the Financial Instrument Market Law); investment management companies (according to Sec.8 Law on Investment Management Companies); insurance/reinsurance groups – (Sec.221 Insurance and Reinsurance Law); managers of an alternative investment fund (Sec.16(15) Law On Alternative Investment Funds And Managers).

299. b) Other Financial Institutions: According to Sec.45 (1)(6) AML/CFT Law BoL is responsible for supervision and control of compliance of capital companies licensed by it. Sec.7 AML/CFT Law referred above is also applicable for the BoL.

300. Sec.47(3) AML/CFT Law provides that the BoL shall, *inter alia*, determine binding requirements for capital companies which carry out buying and selling of foreign currency cash for the fulfilment of the obligations laid down in this Law in respect of the ML and FT risk assessment, internal control system and the establishment thereof, CDD and supervision of the transactions conducted by the customers.

301. In accordance with Sec.47 (3) AML/CFT Law the BoL has issued Reg. 141 for further clarification of requirements set out in the AML/CFT Law. No information is available on the obligation of the BoL to take into consideration the ML/FT risks in the sector.

302. As noted above the FCMC supervises money PIs and EMIs. Internal guidelines on monitoring and supervision of money PIs and EMIs have been elaborated by the FCMC in 2017.

303. *Criterion 26.5* – Sector supervisors are required to conduct "regular inspections according to the methodology developed by it" (Sec.46(1)(3) AML/CFT Law).

304. The Procedure for Assessing Risk of Bank Money Laundering and Terrorism Financing and for Determining Risk-Weight of ML/FT adopted by the FCMC on 26 October 2017 includes the ML/FT inherent risk assessment process and the ML/FT RBA used for the supervision of banks.

305. The frequency and intensity of AML/CFT supervision conducted by the FCMC is based on the following criteria which determine risk category of the institution: AML audit evaluations conducted by the independent auditors; ML/FT risk exposures defined in ML/FT risk management strategies of credit institutions (share of financial assets and credit turnover of all the customers who are subject to enhanced due diligence procedures and share of credit turnover of shell companies from the total credit turnover); risk appetite of credit institution and actual risk exposure (reported on quarterly bases to the FCMC); geography of corresponding relations (NOSTRO and LORO, including existence of USD correspondent accounts in US banks); financial

capacity (ability to withstand losses due to business decline (in case of restrictions or loss of business due to problems with corresponding relations) and to invest into development of internal control system); ability and readiness to change business model; other factors having impact on ML/FT risks (outcome of previous inspections, negative external information, law suites etc.); reputation threats to Latvia.

306. When establishing the inspection plan, the following onsite inspection frequency is observed: critical risk bank - once every six months; high risk bank - once every 18 months; medium risk bank - once every three years; low-risk bank - once every four years.

307. The BoL has enacted Reg. 953-6 governing supervision of capital companies subject to its oversight.

308. According to Sec.24 of Reg. 953-6, the plan of inspections of the operation (performance inspections) of capital companies shall be drafted so that the annual inspections cover at least 30% of all sites for purchasing and selling cash (including foreign currencies) and each such site is inspected at least every four years. The plan should also comply with the following principles: inspections shall cover a maximum number of capital companies to be inspected; inspection of capital companies with a larger market share shall be a priority; capital companies with atypical changes in transaction volumes shall be subject to inspections; capital companies where material breaches were identified by the previous inspections shall be re-inspected; other evidence pointing to potential non-compliance with legal acts shall be considered.

309. It is not clear whether the other financial sector supervisors are conducting inspections based on the assessment of ML/FT risks. The SRS is at an early stage in the development of AML/CFT supervisory methodology but has not carried out any assessments.

310. The MoT supervises only one FI – the Latvian Post. The MoT carries out inspections twice a year – one inspection is carried out onsite in the company, and one inspection is carried out off-site by requesting the information to be provided in writing, and when necessary, in reaction to complaints (very rarely).

311. The MoT has adopted internal regulations that include templates of inspection reports with questions regarding practical execution of the AML/CFT Law requirements. The MoT also conducts inspections to determine whether the deficiencies detected during previous inspections have been prevented. In assessing the Internal Control System of the Latvian Post the MoT takes into account national risks and the vulnerabilities of Latvian Post.

312. *Criterion 26.6* – The information provided describes the obligations of FIs to develop risk assessments. According to Sec.46(1)(11) and (12) AML/CFT Law the supervisory authorities should take supervisory measures, on the basis of ML and FT risk assessment; and carry out the risk assessment and regular revision thereof in accordance with the risk level. Under the Procedure for Assessing Risk of Bank ML/FT and for Determining Risk-Weight of ML/FT adopted by the FCMC the risk based supervision is reviewed periodically and the information used for the ML/FT inherent risk assessment and ML/FT risk score system is updated if necessary. The procedure is reviewed in a number of cases including when new ML/FT risk factors are or significant changes in the banking sector have been detected. No information is provided on the obligations on supervisors of non-bank FIs to review the risk assessments of the ML/FT risk profile of FIs or groups periodically, and when there are major events or developments in the management and operations of the FI or group.

Weighting and Conclusion

313. Latvia meets c.26.1, mostly meets c.26.6 and partly meets c.26.2, c.26.3, c.26.4 and 26.5. Some types of alternative investment funds are only required to register (no licensing); there are licensing requirements for lending activities conducted by non-bank FIs only if they provide consumer lending services. Associates of persons with criminal records are not covered in the national legislation. Not all financial supervisors are conducting ML/FT risk-based supervision. **Latvia is partially compliant with R.26.**

Recommendation 27 – Powers of supervisors

314. In the 4th Round Latvia was rated Largely Compliant with former R.29. The assessors concluded that the supervisory power of the MoT to monitor and ensure compliance of regulated entities with AML/CFT was insufficient. Effectiveness issues were also noted regarding limited expertise and conflict of interest in applying the RBA requirements by the MoT, as well as the supervision AML/CFT supervision of the insurance sector. In the 5th round effectiveness issues are no longer analysed in the TC Annex.

315. *Criterion 27.1* – In Latvia sectorial FI and DNFBP supervisors are also assigned responsibility for supervising their respective sectors for AML/CFT requirements and ensuring compliance with AML/CFT obligations (Sec. AML/CFT Law). Where there is no sectorial supervisor, responsibility for AML/CFT supervision has been assigned to the SRS (Sec.45(1)(2) AML/CFT Law) [181].

316. *Criterion 27.2* – The powers of the designated supervisory agencies include the power of inspections (Sec.46(1)(3) AML/CFT Law). The legal framework for conducting inspections includes the ability to visit the premises, to request information and documents, copies of relevant documents.

317. *Criterion 27.3* – The rights of the designated supervisory agencies include the power to compel production of information related to compliance with AML/CFT requirements (Sec.47(1)(2) AML/CFT Law). This includes the authority to request explanations from the REs.

318. *Criterion 27.4* – All financial supervisors are authorised under Sec. AML/CFT Law to sanction for failure to comply with the AML/CFT legislation. These include fines, temporary suspension of an official of the subject of the law, revocation of a licence and other measures provided for in the AML/CFT Law. In addition, sanctioning powers are also provided under the sectorial legislation. The FCMC has the power to apply sanctions for failure to comply with the obligations relating to prevention of ML and FT under Sec.198[1](1) of the Credit Institutions Law. These include powers to impose fines and to cancel the FI's licence.

319. In the securities sector, the FCMC has extensive authority to apply various penalties for violations of the Financial Instrument Market Law. The FCMC is also authorised under Sec.78 AML/CFT Law to sanction banks and other FIs for violations of the AML/CFT Law.

320. In the investment management companies sector, the FCMC may ("shall") impose a fine in the range of EUR 7,100 to 142,000 for activities resulting in an infringement of the requirements of

[181] The ECB conducts prudential supervision of the significant banks. Prudential supervision of the banks that are not considered significant is conducted by the national supervisors, with the ECB having the possibility to give guidance to national authorities. The ECB can decide to directly supervise less significant institutions if necessary to ensure that high supervisory standards are applied consistently.

regulatory enactments on the prevention of ML and FT (Law on Investment Management Companies, Sec.87(12).

321. In the money remittance sector, the FCMC may apply measures provided under Law on Payment Services and Electronic Money, Sec.56(2) for failure "to comply with the regulatory requirements in the area of the prevention of ML and FT".

322. The Licensing Committee of the BoL may suspend for a limited period of time or revoke the license for purchasing and selling foreign currencies, where the capital company fails to comply with the requirements set forth by laws and regulations with regard to the prevention of ML/FT, as well as the requirements set forth by the documents regarding the internal control systems policies and procedures

Weighting and Conclusion

323. **Latvia is compliant with R.27.**

Recommendation 28 – Regulation and supervision of DNFBPs

324. In the 4th Round Latvia was assessed partially compliant with the requirements under former R.24 due to the following deficiencies: onsite supervision performed by the SRS was weak and there were no procedures for off-site supervision; sanctions imposed were not considered dissuasive, effective and proportionate; supervision performed by the SROs was considered to be weak; there was a confusion in performing supervisory powers between Council of Sworn Notaries and the FIU.

325. *Criterion 28.1* – (a) Art.3 of the Gambling and Lotteries Law (GLL) provides that only licensed capital companies may organize gambling and lotteries in Latvia. Licences are issued by the Lotteries and Gambling Supervisory Inspection. Sec.46 of the GLL allows internet casinos to be licenced.

326. (b) Members of the Board and the auditor of the gambling operator must have unblemished reputations, and not be prohibited from the right to engage in business activities. This explicitly excludes those with criminal records from acting (Art.9(2) and (3) of the GLL)). However this does not cover the associates of criminals.

327. There are no relevant requirements covering persons holding (or being a BO of) a significant controlling interest, or their associates.

328. (c) The Lotteries and Gaming Supervisory Inspection (LGSI) is the designated casino supervisor responsible for AML/CFT supervision (Art.81 of the GLL; Sec.45 AML/CFT Law). The LGSI conducts onsite inspections of casinos.

329. *Criterion 28.2* – Latvia lists the following DNFBPs all of which are subject to the AML Law/CFT: real estate agents, DPMS, lawyers, notaries, auditors, accountants, and company service providers, including trustees. Latvia does not define or licence trustees as a separate category of DNFBPs.

330. The AML/CFT supervisors are as follows: Real estate agents are supervised by the SRS (AML/CFT Law Sec.45(2)(4)); DPMS are supervised by the SRS (AML/CFT Law Sec.45(2)(5)); Lawyers are supervised by the Latvian Council of Sworn Lawyers (AML/CFT Law Sec.45(1)(2)); Notaries are supervised by the Latvian Council of Sworn Notaries (AML/CFT Law Sec.45(1)(3)); Auditors are supervised by the Latvian Council of Certified Auditors (AML Law Sec.45(1)(4));

Accountants are supervised by the SRS (AML/CFT Law Sec.45(2)(1)); Company Service Providers (including trustees) and independent legal professional are supervised by the SRS (AML/CFT Law Sec.45(2) (2) &(3).

331. *Criterion 28.3* – See 28.2

332. *Criterion 28.4* – (a) Sec.45-47 AML/CFT Law appear to give the supervisors/SROs listed in 28.1. and 28.2 sufficient authority to supervise the various DNFBPs for compliance with AML/CFT obligations. The powers of the designated supervisory agencies include the power of inspections (AML/CFT Law Sec.46(1)(3)). The legal framework for conducting inspections includes the ability to visit the premises, to request information and documents, copies of relevant documents. The rights of the designated supervisory agencies include the power to compel production of information related to compliance with AML/CFT requirements (AML/CFT Law Sec.47(1)(2)). This includes the authority to request explanations from the REs.

(b) and (c) It is not clear from the material provided whether they (except for the notaries) have and can apply measures to prevent criminals from controlling DNFBPs. A supervisory and control authority shall impose the sanctions laid down in Sec.78 AML/CFT Law, if the offences of the legal framework in the field of AML/CFT are detected. Sanctions laid down in Ssec.78 with respect to the certified auditors and commercial companies of the certified auditors shall be imposed by the SRS upon the proposal of the supervisory and control authority - Latvian Association of Certified Auditors. The provisions of Sec.78 AML/CFT Law described under c.27.4 and the framework described in R.35 are applicable with regard to DNFBPs.

333. *Criterion 28.5* – (a) The SRS monitors compliance on the basis of the assessment of the national risks and the turnover of the subjects, but more information is needed for each supervised group and their understanding of the risks. Council of Sworn Notaries considers seven risk factors for risk assessment: results of previous assessments, employees' qualifications, experience, concerns of the Council of Sworn Notaries, reputation (complaints, disciplinary action), total debts, financial results and notary's professional activities outside the office.

(b) Supervisory risk profiles: The Council of Sworn Notaries uses the "control customer" method to determine high risk Notaries for inspection. The information provided is not granular and does not clarify what a high-risk Notary is. The SRS appears to prioritize entities with higher risk of tax evasion. The LGSI does not appear to follow a risk- based approach. Little or no information is provided about the sworn lawyers, DPMS, certified auditors, accountants and company service providers.

Weighting and Conclusion

334. Latvia meets c.28.1-28.3. It partly meets c.28.4 and 28.5, since it is not clear if there are measures in place to prevent criminals from controlling DNFBPs (except for the Notaries) and there are deficiencies in the ML/FT risk based supervision conducted by the supervisory authorities. **R.28 is rated PC**.

Recommendation 29 - Financial intelligence units

335. In the previous MER, Latvia was rated LC with the requirements related to the FIU. Deficiencies pertained to possible confusion in guidelines on reporting of suspicious transactions; the inadequate coverage of reporting FT in guidance; the fact that the content of the FIUs disseminations was not a part of the FIU's IT protected system against arbitrary modification

and/or deletion; and the need to require the prosecutor's approval for the FIU to have access to additional financial information. In addition, the effectiveness of the implementation of the requirements could not be fully proved.

336. *Criterion 29.1* – Chapter IX of the AML/CFT Law establishes the legal status; rights and obligations; and responsibilities of the FIU. Sec.50(1) provides that the Control Service, which serves as the Latvian FIU, is a specially established State authority which exercises control over UTRs and STRs, and acquires, receives, registers, processes, compiles, stores, analyses and provides information to pre-trial investigative institutions, the Prosecutor's Office and courts, which may be used for the prevention, detection, pre-trial criminal proceedings on or adjudication of ML, FT or an attempt to carry out such actions or another associated criminal offence.

337. *Criterion 29.2* – Sec.30(1)(1) AML/CFT Law establishes an obligation for the REs, as well as State authorities, derived public persons and their authorities to notify the FIU regarding both UTRs and STRs, which constitute the only categories of information that REs are required to disclose spontaneously.

338. *Criterion 29.3 – a)* As per Sec.30(2) AML/CFT Law, REs must provide the additional information requested by the FIU following a UTR/STR within 7 working days (the deadline can be extended by the FIU). The FIU can ask additional information to any RE based on a "report" from any legal or natural person in Latvia, as well as on the basis of information provided by foreign authorities.

b) The FIU has direct electronic access to a broad range of information and databases. The FIU is also the direct recipient of cross-border cash movement reports. Sec.54 AML/CFT Law provides that the State and the local government authorities have the obligation to provide the FIU with the information it requests for the implementation of its functions. Through that mechanism, the FIU has access, although only upon written request, to various State and Municipality databases, incl. the Bank Account Register and UBO information contained in the ER. As per Cab. Reg. 1092, the authorities have to respond within 14 days.

339. *Criterion 29.4* – Sec.50 and 51 AML/CFT Law provide that the FIU must undertake operational and strategic analysis based on the information received from REs and the other information available to it. Both types of activities are carried out by the FIU.

340. *Criterion 29.5* – The FIU is authorised to spontaneously provide information to pre-trial investigative institutions, the General Prosecutor's Office (GPO) or a court, if such information allows for substantiated suspicions that the relevant person has committed a criminal offence, including ML, FT or an attempt to carry out such actions (Sec.55 AML/CFT Law).

341. As per Sec.56 AML/CFT Law, at the request of the bodies performing operational activities, pre-trial investigative institutions, the GPO or a court, the FIU must provide information if the request is approved by the GPO, which restricts the FIU's discretionary power in providing information to other authorities (see c.31.4). Sec.56(5) adds criteria for refusing to fulfil an information request once received by the FIU (the provision of information "would adversely affect the current operational activities, pre-trial investigation, the analysis provided by the FIU or might endanger human life or health, or under other emergency circumstances, or if disclosure of information would be obviously incommensurate to the lawful interests of a natural or legal person or non-conforming to the purpose it was requested"). The scope of the criteria is unclear.

342. The FIU is able to cooperate upon request with the SRS (examination of income declarations of State officials by the SRS in cases of substantiated suspicion of false declaration), the FCMC and security institutions in specific situations related to ML/FT, but not in relation to predicate offences.

343. The FIU must implement the necessary administrative, technical and organisational measures in order to ensure the protection of information and prevent unauthorised access to, unauthorised tampering with, distribution or destruction of information. The dissemination of the information by the FIU is delivered by car courier. The FIU started to develop an e-tool for information exchange channel with LEAs in June 2017 (not yet in place as of the time of the onsite visit).

344. *Criterion 29.6* – The Head of the FIU appointed the Information FIU Systems' Security Manager, the Holders of Information Resources and the Holders of Technological Resources of the FIU Information Systems, establishing a number of security rules. A series of Information System Security Regulations have been issued governing the security and confidentiality of information, including procedures for handling, storage, dissemination, and protection of, and access, to information. In particular, Internal Regulations on "The procedure for the registration, processing, storage and disposal of the received information" were approved by the Head of the FIU by Order 64 (08.07.2011). The FIU is elaborating new versions of these regulations.

345. Sec.50(5) AML/CFT Law requires the Head and the employees of the FIU to comply with the requirements established in the Law on Official Secrets, in order to receive a special permit to access especially secret information.

346. All three STR- and UTR-related systems have role-based access and create log files. The FIU stores encrypted data backup copies in a special safe located in the BoL according to the Agreement between the FIU and the BoL (10.03.2017). Access to the FIU premises is controlled through identifying cards and mechanical keys for authorized persons; a physical security system against physical intrusion is continuously monitored by an external security organization; safes or metal shelves are used to store documents or data backups; etc.

347. *Criterion 29.7* – The FIU is a specially established State authority. The Head of the FIU is appointed for four years and dismissed by the GP. Sec.49.2 of the Office of the Prosecutor Law provides that the Head of the FIU may only be for: the commission of a criminal offence; intentional violation of law or negligence related to his/her professional activity with significant consequences; or shameful act incompatible with Head status. The last cause is unclear, although the FIU informed that such appreciation would be informed by the FIU's Code of ethics. Employees of the FIU are hired and dismissed by the Head of the FIU. Their remuneration is determined in accordance with the Law on Remuneration of Officials and Employees of State and Local Government Authorities.

348. The FIU can engage independently with foreign counterparts on the exchange of information (Sec.62 AML/CFT Law).

349. Domestic cooperation between the FIU and the State and local government authorities is governed by Cab. Reg. 1092 (under Sec.54 AML/CFT Act), which provides that the FIU shall conclude written agreements with domestic authorities on the extent of and conditions for access to information to be submitted electronically.

350. The FIU is not part of the GPO and as a general rule the FIU can carry out its duties without the approval of a prosecutor. However, the FIU operates under the supervision of the GPO and its structure and the number of offices are determined by the GP in accordance with the State budget funds allocated (Sec.50 AML/CFT Law). Additionally, some powers of the FIU are subject to the

prosecutor's decision, such as the dissemination of information upon request (Sec.56 AML/CFT Law). 10% of requests for information were refused for legal or practical reasons. Even though the authorities stated that no undue interference has been observed, the authorities should consider removing any ambiguity in the AML/CFT Law in relation to the FIU's operational autonomy from the GPO.

351. *Criterion 29.8* – The FIU has been an Egmont Group member since 1999.

Weighting and Conclusion

352. Latvia meets or mostly meets most criteria of R.29. **Latvia is rated LC with R.29.**

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

353. In the 3rd Round MER of 2006, Latvia was rated compliant with the former R.27; hence this recommendation was not assessed in Latvia's 4th Round MER of 2012. The new R.30 contains more detailed requirements.

354. *Criterion 30.1* – Latvia has a broad range of LEAs that have responsibility to investigate ML, associated predicate offences and FT. The competencies and responsibilities of LEAs in Latvia are defined in Sec.387 CPL.

ML and associated predicate offences

355. Unless otherwise provided by Sec.387 CPL, the SP shall investigate any criminal offence. The SP consists of several entities, including five regional units. Criminal offences related to ML are investigated both by these regional authorities and by the "Central Criminal Police Authority", more precisely its Economic Crime Enforcement Department. In compliance with that department's internal regulations, the latter comprises a "Unit 1" which investigates criminal offences in credit institutions and ML.

356. Sec.387 CPL sets out a number of other LEAs with the responsibility to investigate criminal offences, such as the following which are relevant in the present context: financial police (regarding criminal offences in the field of State revenue); the Corruption Prevention and Combating Bureau (regarding criminal offences related to violations of the provisions of the financing of political organisations and criminal offences related to corruption in the State Authority Service); the custom authorities (regarding criminal offences in the field of customs matters); and the State Border Guard (regarding criminal offences related to the illegal crossing of the State border).

FT offences

357. FT offences are investigated by the SeP, which is one of the three State security institutions in Latvia and which is subordinated to the Ministry of the Interior. In the field of national security, the SeP *inter alia* performs counter-intelligence and investigatory operations measures in order to combat a number of serious crimes. This includes organised and economic crime, terrorism, sabotage and other crimes endangering national security and authority, crimes committed by OCGs, corruption, money forgery, as well as non-sanctioned distribution of nuclear materials, narcotic and other (chemical, radioactive) substances of strong effect or double usage goods, firearms and weapons of another kind, explosives (Sec.15.2.1 of the Law On State Security Institutions). The SeP operates in accordance with the National Security Law, the Investigatory Operations Law, the Law on Police, Law on State Security Institutions and a by-law approved by the CoM (Sec.15.4 of the Law

on State Security Institutions). The SeP shall investigate criminal offences that have been performed in the field of State security or in State security institutions, or other criminal offences within the framework of the competence thereof and in cases where the GP has assigned the performance thereof (Sec.387.[2] CPL).

358. *Criterion 30.2* – In the course of a "traditional" criminal investigation, LEAs are performing activities to identify criminally acquired property. If during the investigation of a predicate offence a related ML/FT offence is revealed, then the latter case is referred to the competent authority regardless of where the predicate offences occurred, unless the need for investigative actions is imminent (in case of serious or particularly serious crimes, as defined in Sec.7 CL). The Corruption Prevention and Combating Bureau (KNAB) is authorised to investigate corruption-related ML. However, it is not fully apparent to which extent LEAs are authorised to investigate ML/FT offences during a parallel financial investigation. It appears that there are no (internal) provisions which require the routine conducting of (parallel) financial investigations.

359. *Criterion 30.3* – The LEAs mentioned above have the authority to identify, trace, and initiate the freezing and seizing of property (Sec.361 CPL). In pre-trial proceedings, an attachment shall be imposed on property with a decision of a person directing the proceedings that has been approved by an investigating judge; during trial a court shall take a decision. In 2009, the Economic Crime Enforcement Department of the SP assumed the competencies of an asset recovery office (ARO), with a view to tracing and identifying proceeds from crime or other related property. Due to a structural reform, a special unit ("Unit 2 of the Criminal Intelligence Department") of the SP was established in 2016 as an ARO, with the basic function of search, identification and recovery of illegally acquired property. An internal order/regulation by the Minister of the Interior is in place since 27 June 2017, obliging all criminal police officers/investigators to expeditiously evaluate the need in asset-tracing and confiscation and take a decision on engaging the above-mentioned special unit of the SP already at an early stage of each investigation. There is no similar regulation for other LEAs.

360. *Criterion 30.4* – Latvia does not have competent authorities which are not LEAs but pursue nonetheless financial investigations of predicate offences.

361. *Criterion 30.5* – The competence of the KNAB is to investigate criminal offences related to corruption committed in the State Authority Service. This includes predicate offences and related offences such as ML. If only ML indications are discovered, the competence is referred to the PGO. Usually the SRS or the SP will investigate such crimes. According to Sec.361 CPL, the KNAB is authorised to impose an attachment on property and initiate freezing and seizing of assets.

Weighting and Conclusion

362. **Latvia is largely compliant with R.30.**

Recommendation 31 - Powers of law enforcement and investigative authorities

363. In the 3rd Round MER of 2006, Latvia was rated compliant with the former FATF Recommendation 28; hence this recommendation was not assessed in Latvia's 4th Round MER of 2012. The new Recommendation 31 contains more detailed requirements.

364. *Criterion 31.1* – LEAs responsible for investigating ML, associated predicate offences and FT are able to obtain access to all necessary documents and information for use in those investigations. The range of tools available to ensure this includes the following:

a) The production of records held by financial institutions, DNFBPs and other natural or legal persons

365. Authorities are entitled to request from natural or legal persons, in writing, objects, documents and information regarding the facts that are significant to criminal proceedings, including in the form of electronic information and documents that are processed, stored or transmitted using electronic information systems (Sec.190(1) CPL). If natural or legal persons do not submit the objects and documents requested during the term specified, the authorities' person shall conduct a seizure or search in accordance with the procedures laid down in CPL (Sec.190(2) CPL). A seizure is conducted with the decision of the person directing the proceedings (Sec.187(1) CPL). Professional secrets may be requested only by a judicial order.

b) Search of persons and premises

366. A coercive search of premises, terrain, vehicles and individual persons is allowed for the purpose of finding and removing the object being sought, if there are reasonable grounds to believe that the object being sought is located at the site of the search (Sec.179(1) CPL). A search shall be conducted with a decision of the competent court. In emergency cases a search shall be performed with a decision of the person directing the proceedings (with the consent of a public prosecutor if the decision is taken by an investigator) and in due time the legality and validity of the search shall be examined by the investigating judge (Sec.179-184 CPL).

c) Taking witness statements

367. Sec.109 CPL provides for the possibility of interrogation of a witness during the pre-trial criminal proceedings. Witnesses are required by Sec.111 CPL to tell the truth and testify regarding everything that is known to them in connection with a concrete criminal offence. The same provision provides for the possibility to require witnesses to not disclose any information regarding the interrogation. The rules for the interrogation of, inter alia, witnesses are laid down in Sec.145-149 CPL.

d) Seizing and obtaining evidence

368. There is an obligation for natural and legal persons to hand over to the investigating authorities documents, objects or data which can be significant as evidence for a criminal investigation concerning ML, associate predicate offences or FT (Sec.190(1) CPL). Otherwise the authorities can seize them in accordance with the procedure under Sec.186 et seq. CPL. The heads of legal persons have a duty to perform a documentary audit, inventory, or departmental or service examination on the basis of a request of a person directing the proceedings, and to submit the requested documents (Sec.190(3) CPL). The compulsory order for the disclosure of data stored in an electronic information system is possible with the consent of the Prosecutor's Office or the investigating judge (Sec.192 CPL).

369. *Criterion 31.2* – In Latvia investigative techniques are regulated by the Operational Activities Law (OAL), which applies prior to the initiation of criminal proceedings[182] and during ongoing criminal proceedings covered by the CPL. Sec.24(1) OAL provides that information obtained in the course of operational activities may be utilised as evidence in a criminal proceeding only in

[182] Operational activities procedures may commence before criminal proceedings are initiated may take place during the period of investigation of a criminal matter and continue after termination thereof (Sec.18.2 OAL).

accordance with the procedures laid down in the CPL. Chapter 11 (Sec.210 et seq.) of the CPL deals with "special investigative techniques".

370. Competent authorities conducting investigations of ML offences and FT offences have access to a wide range of investigative techniques, including under Sec.6 OAL: 1) investigatory inquiring; 2) investigatory surveillance (tracing); 3) investigatory inspection; 4) investigatory acquisition of samples and investigatory research; 5) investigatory examination of a person; 6) investigatory entry; 7) investigatory experiment; 7.1) controlled delivery; 8) investigatory detective work; 9) investigatory monitoring of correspondence; 10) investigatory acquisition of information expressed or stored by a person through technical means; 11) investigatory wiretapping of conversations; and 12) investigatory video surveillance of a place not accessible to the public.

371. The following special investigative actions can be performed in accordance with the provisions of Chapter 11 of the CPL: 1) control of legal correspondence; 2) control of means of communication; 3) control of data in an automated data processing system; 4) control of the content of transmitted data; 5) audio-control of a site or a person; 6) video-control of a site; 7) surveillance and tracking of a person; 8) surveillance of an object; 9) a special investigative experiment; 10) the acquisition in a special manner of the samples necessary for a comparative study; and 11) control of a criminal activity.

372. Special investigative actions shall be performed on the basis of a decision of an investigating judge, except in emergency cases determined in Chapter 11 of the CPL (where a prosecutor gives consent but the investigating judge needs to approve within the next working day). The duration of a special investigative action to be performed in a publicly inaccessible location shall not exceed 30 days (but the period can be extended). The performance of special investigative actions shall be permitted only in investigating "less serious crimes" (i.e. 3 months – 3 years' imprisonment, Sec.7(3) CC), "serious crimes" (i.e. 3 – 8 years' imprisonment, Sec.7(4) CC), or "particularly serious crimes" (i.e. 8 years to life imprisonment, Sec.7(5) CC). Evidence obtained in violation of the CPL may not be used in criminal proceedings.

373. *Criterion 31.3* – Latvia has a range of laws in place to ensure that competent authorities have the mechanisms for the timely identification of whether natural/legal persons hold or control accounts, and for identifying assets without prior notification of the owner. Sec.5(1) of the Law on Account Register, which entered into force on 1 July 2017, lays down that credit institutions, credit unions and payment service providers shall provide information about account holders. Information about the BOs to the account register (Sec.5(3)) is included in that register. The Law on Account Register provides the possibility for investigation authorities and the Prosecution Office to receive information from the accounts register regarding the holders and BOs of the deposits at short notice, or regarding current accounts opened with credit institutions, financial providers or payment services providers. Sec.631 of the Law on Credit Institutions prevents credit institutions from informing a customer or a third person about the fact that information in respect of the customer's account or transactions have been provided to a court or the Prosecution Office. It should be noted that Sec.121.5 CPL requires, in order for the authorities to obtain non-disclosable information by financial institutions (i.e. information about a customer, including transactions) during the pre-trial investigation, the permission of an investigating judge. That judge can give the permission to monitor transactions for a (renewable) period of three months.

374. Criterion 31.4 – Competent authorities conducting investigations of ML, associated predicate offences or FT are able to request relevant information held by the FIU, as provided by Sec.56

AML/CFT Law. This section states that, at the request of the bodies performing operational activities, investigating institutions, the Prosecutor's Office, as well as a court, the FIU shall provide information in accordance with the requirements of the AML/CFT Law within the operational activities procedure or criminal proceedings. However, as noted already under c.29.5, this is subject to the approval of the GPO, which restricts the FIU's capacity to provide information to other authorities. Sec. 6 AML/CFT Law however also defines that, where there are objective grounds for assuming that the provision of information would adversely affect the current operational activities, pre-trial investigation, the analysis provided by the CS or might endanger human life or health, or under other emergency circumstances, or if disclosure of information would be obviously incommensurate to the lawful interests of a natural or legal person or non-conforming to the purpose it was requested, the FIU shall be under no obligation to comply with the request for information. While the authorities' possibility to ask for relevant information held by the FIU is not unrestricted under R.31, this exception is somewhat broad and unclear (see also the analysis under c.29.5).

Weighting and Conclusion

375. **Latvia is largely compliant with R.31.**

Recommendation 32 – Cash Couriers

376. Latvia was rated partially compliant with the former FATF Special Recommendation IX during the 4th round MER in 2012. The main deficiencies affecting technical compliance pertained to not having a provision to request and obtain further information in case of a false declaration/disclosure and to limited freezing capabilities of the Customs Authority.

377. *Criteria 32.1* – Latvia has implemented a declaration system for incoming and outgoing transportation of cash and bearer negotiable instruments (BNI) by physical persons leaving and entering the EU. EU Regulation (EC) No 1889/2005 on controls of cash entering or leaving the community obliges natural persons leaving or entering the EU to declare cash (including BNIs) of a value of EUR 10,000 or more. This obligation is implemented into Latvian law through Art.5 of the Law on Declaration of Cash at the State Border. Regarding the cross-border transportation of currency or BNIs via mail and cargo, the Community Customs Code No 952/2013 is applied and is covered by a customs declaration. Latvia has no mechanism to declare or disclose incoming and outgoing cross-border transportation of cash and BNI within the EU.

378. *Criteria 32.2* – Latvia has implemented a written declaration system for all travellers carrying amounts above a threshold of EUR 10,000. The declaration must be made in writing on a specified cash declaration form (Art.7/1 of the Law on Declaration of Cash at the State Border).

379. *Criterion 32.3* – This criterion is not applicable since Latvia has a declaration system.

380. *Criterion 32.4* – The possibility for the authorities to request and obtain further information from the carrier with regard to the origin and intended use of cash or BNIs which were wrongly or non-declared depends on the prior initiation of criminal proceedings by the Customs Police Department of the SRS. According to the authorities, such proceedings are however commenced on a routine basis on the spot for amounts exceeding EUR 19,000 (and for amounts below if the person concerned does not have a reasonable explanation for the legality of the money).

381. *Criterion 32.5* – Failure to comply with the customs legislation or the obligation to declare cash and BNIs is an administrative offence punishable by a fine of 5% of the undeclared or falsely

declared amount (Art.190/15 AVC). If non-declaration or false declaration of cash involves criminally acquired cash or is committed by an organised group, the applicable punishment is deprivation of liberty for a term up to three years or temporary deprivation of liberty, or community service, or a fine (Sec.195/2 CL, "Avoidance of Declaring of Cash"). The sanctions are proportionate, but regarding the administrative fine for non-criminally acquired cash, they do not appear to be sufficiently dissuasive (despite of having been raised in 2014 from EUR 280 to 5% of the undeclared or falsely declared amount).

382. *Criterion 32.6* – Information obtained from cash declarations, including information on false declarations, is stored in the Central Customs Information System and made available to the FIU according to Art.6/2 of the Law on Declaration of Cash at the State Border. Additionally, the information is stored on a monthly basis on the FTPS server for the FIU.

383. *Criterion 32.7* – The coordination in matters of state border security among authorities - including the State Border Guard, the Police and the SRS - is regulated by CoM Instruction No. 5 adopted in 2010. The coordination of customs regulations shall be organised by the SRS.

384. *Criterion 32.8* – The internal regulations of the SRS provide for the possibility to stop or restrain currency or BNIs for a reasonable time in order to ascertain whether evidence of ML/FT may be found. This applies in the case of concealment of cash or indications of illegal activities (including ML/FT). Where the amount of cash falsely or not at all declared exceeds 50 times the minimum monthly wage (an amount the equivalent of EUR 19,000 at the time of the onsite visit), restraining the cash is possible if documents proving the origin of the amount are either not provided or likely not to be authentic. However, it appears that amounts of less than EUR 19,000 which nevertheless exceed the threshold of EUR 10,000 for a mandatory declaration are not covered by these regulations, unless there is an indication for an illegal activity.

385. *Criterion 32.9* – Information obtained from cash declarations, including information on false declarations, is stored in the Central Customs Information System. If there is a reasonable suspicion of criminal offence the information is forthwith submitted to the competent authorities for further action (Sec.387 CPL). However, it remains unclear in what manner and for how long the Latvian authorities retain the information for the purposes of international cooperation.

386. *Criterion 32.10* – The confidentiality of information is safeguarded by Art.8 of EU Regulation 1889/2005 and further protected by EU Regulation 45/2001 (data protection). These provisions are implemented into Latvian law by the Personal Data Protection Law. As an EU member state, Latvia is part of the internal market, an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured (Art. 26/2 TFEU and Preamble of EU Regulation 1889/2005).

387. *Criterion 32.11* – Persons who are carrying out physical cross-border transportation of currency or BNIs that are related to ML/FT or predicate offences can be subject to criminal sanctions under either the ML and FT offences or for "avoidance of declaring of cash" under Sec.195[2] of the CL (carrying a punishment of up to three years' imprisonment). These are proportionate and dissuasive sanctions. Criminally acquired property, including cash and BNIs, shall be seized and later confiscated (Sec.355/1 and 358/1 CPL).

Weighting and Conclusion

388. Latvia does not have an EU-internal border declaration system for cash and BNIs. For EU-external borders, sanctions for non-declaration of false declarations are not dissuasive enough. **Latvia is partially compliant with R.32.**

Recommendation 33 – Statistics

389. In the 2012 MER, Latvia was rated PC with the previous R.32. Deficiencies identified were the following: insufficient information on the number of police/prosecution generated cases, FIU generated cases and autonomous laundering cases; lack of detailed statistics on confiscations; inconsistency of statistics received on confiscations from different authorities; no statistics on STRs and UTRs, or on the relation FIUs disseminations – LEA investigations/prosecutions/convictions; no detailed statistics available on the number of cases regarding the failure to comply with the obligation to declare and on information exchange with foreign counterparts regarding cash couriers; insufficient scrutiny of the collected statistics in the light of assessing AML/CFT system as a whole; no comprehensive central database for MLA requests; no statistics on the average time of response for MLA requests; and no statistics on time to reply to international requests under R.40.

390. *Criterion 33.1* – Latvia does maintain a range of statistics on each of the following topics:

a) STRs received, analysed and disseminated: Latvia provided statistics on STRs and UTRs received over the period 2012-2016 inclusive, including number of FT reports, numbers of transactions addressed and numbers of transactions covered in cases disseminated. Statistics also covered the numbers of reports filed by each reporting sector and these were broken down by type of FI or DNFBP. Some inconsistencies were noted in the datasets available to the evaluation team in relation to STRs.

b) Investigations, prosecutions and convictions. Latvia provided statistics on LEA information requests, and the number of cases to the various LEAs, the numbers of criminal offences reported to LEAs, convictions for predicate offences, criminal proceedings generated from FIU disseminations, ML proceedings, proceedings received by the Prosecution office and transferred to the courts, non-FIU- initiated proceedings, convictions and acquittals, penalties applied, and duration of proceedings.

c) Property frozen, seized and confiscated: Latvia provided statistics on property frozen. The authorities were not in the position to provide comprehensive statistics on property frozen, seized, confiscated and recovered post-conviction; separate statistics for the confiscation of instrumentalities; seizures by the FPD; and amounts confiscated. There were no statistics on confiscation resulting from cross-border cash movement information.

d) MLA or other international requests for cooperation made and received: SP international cooperation; anti-corruption Bureau international cooperation; FPD international cooperation; supervisory authorities international cooperation; MLA in relation to ML and FT cases; incoming and outgoing requests (GPO). No information is collected by all relevant authorities on time taken to respond to foreign requests.

Weighting and Conclusion

391. Some inconsistencies noted in the statistics on STRs. The authorities were not in the position to provide comprehensive statistics on property frozen, seized, confiscated and recovered post-conviction; separate statistics for the confiscation of instrumentalities; freezing orders from the

FIU; seizures by the FPD; and amounts confiscated. There were no statistics on confiscation resulting from cross-border cash movement information. No information is collected by all relevant authorities on time taken to respond to foreign requests. **R.33 is rated LC.**

Recommendation 34 – Guidance and feedback

392. In its 2012 report Latvia was rated Largely Compliant with the former R.25. The rating was based on insufficient feedback on FT reports, missing FI sector specific guidelines on ML/FT techniques and methods, specific guidelines on suspicion ground including red flags and indicators and guidance of FT suspicions for DNFBPs. It was also noted in the report the guidance for auditors and notaries did not provide assistance on suspicious transactions reporting and there was insufficient awareness of the SRS supervised DNFBP on the content of the specific guidance.

393. *Criterion 34.1* – Supervisory authorities of FIs and DNFBPs are required to carry out training of the employees of obliged entities under supervision and control and development of guidelines for the issues related to the prevention of ML and FT (AML/CFT Law sec.46(1)(2)). The obligation applies to the FCMC, the SRS, the BoL, the LGSI, the MoT, the Council of Sworn Notaries, and the Council of Sworn Advocates. The FIU is required to analyse the quality of STRs and their utilisation and to inform the REs thereof (AML/CFT Law Sec.51(1)(3). The FIU has similar related obligations covering other competent authorities set out in the AML/CFT Law Sec.51 (1).

394. The LGSI published Guidelines to the capital companies which have obtained a licence for organising and maintaining lotteries and gambling on developing internal control system for prevention of ML/FT. The Council of Sworn Notaries issued the Procedure Regarding Execution of Requirements of the AML/CFT Law by a Sworn Notary and Recommendations for Sworn Notaries on the AML/CFT. The Council of Sworn Advocates issued Procedure Regarding Assurance of Requirement Execution of the AML/CFT Law which is available to every advocate. The FIU publishes annual reports, which include typologies. In addition, the FIU has published a wide range of guidelines on its website.

395. The extent to which these various authorities address these obligations is addressed in the Effectiveness Analysis of the MER.

Weighting and Conclusion

396. **R.34 is rated C.**

Recommendation 35 – Sanctions

397. In its 4th round MER Latvia was rated partially compliant with R.17. The evaluators concluded that the BoL had no sanctioning powers over natural persons, and the range of sanctions under the BoL Law was not effective, proportionate and dissuasive. In addition, it was noted that the MoT was not invested with adequate legal sanctioning powers and there was no sanctioning regime for unsupervised financial institutions. Effectiveness of the sanctioning regime was considered limited. With regard to DNFBPs, it was noted that there was no specific AML/CFT sanctioning regime, general sanctions for DNFBPs were not dissuasive and there was a low incidence of sanctions imposed.

398. *Criterion 35.1* – The AML/CFT Law gives authority as noted below to impose penalties for violations of the AML Law.

399. Sec.78 AML/CFT Law stipulates the sanctions for failure of the AML/CFT legislation. These comprise a range of sanctions including: public announcements specifying the person liable for the offence and the nature of the offence, warning, fine up to EUR 1,000,000, revocation of a licence or cancellation of the record in the relevant register, temporary prohibition for a person liable for the offence to fulfil the duties prescribed for them by the subject of the Law; duty to perform certain action or refrain therefrom; obligation on the subject of the Law to dismiss the person liable for the offence from the position held.

400. Furthermore, more severe fines are provided under the same section for the credit and other financial institutions: fine on a legal person in the amount of up to 10% of the total annual turnover in accordance with the latest approved financial statement, drafted, approved and audited, if necessary, in accordance with the legal framework in the field of preparation of annual statements binding on a credit institution or financial institution. If 10% of the total annual turnover is less than EUR 5,000,000, a supervisory and control authority shall be entitled to impose a fine in the amount of up to EUR 5,000,000. If a credit institution or FI is a parent undertaking or a subsidiary undertaking of a parent undertaking, the corresponding total annual turnover shall be the total annual turnover or the income of the corresponding type in accordance with the relevant legal framework and the latest available consolidated statements, which have been approved by the key management body of the parent undertaking; fine of up to EUR 5,000,000 on the official, employee or a person, who, at the time of committal of the offence, has been liable for the performance of a particular action on assignment or in the interests of a credit institution or financial institution.

401. Sec.78 provides that a supervisory and control authority shall post on its Internet home page information regarding the sanctions imposed on the subject of the Law, as well as information regarding appeal of the imposition of sanctions, the outcome of the appeal and the decision on cancelling the sanctions. A supervisory and control authority may publish information mentioned, without identifying a person, if, following the initial assessment, it detects that a disclosure of personal data of a natural person whom the sanction has been imposed on may endanger the stability of the financial market or the course of the initiated criminal proceedings, or cause incommensurate harm to the involved persons.

402. The FCMC shall be entitled to impose the sanctions laid down in Sec.78 AML/CFT Law on the financial and capital market participants also for the offences of the requirements of the legal framework with respect to the financial restrictions laid down in the Law on International Sanctions and National Sanctions of the Republic of Latvia, up to the day of coming into force of the amendments to the legal framework prescribing the liability for offences of the requirements of the legal framework with respect to the financial restrictions not subject to criminal liability in accordance with Sec. 84 CL. No similar provisions are provided for other supervisory authorities.

403. Overall the powers of sanctions available for the supervisory authorities are proportionate and dissuasive.

404. *Criterion 35.2* – The following powers available under Sec.78 of the AML/CFT Law apply to individuals: temporary prohibition for a person liable for the offence to fulfil the duties prescribed for them by the subject of the Law an impose a duty on the subject of the Law to dismiss the person liable for the offence from the position held, to impose a fine up to EUR 5,000,000 on the official, employee or a person, who at the time of committal of the offence has been liable for the performance of a particular action on assignment or in interests of a credit institution or FI.

Weighting and Conclusion

405. There are no clear legal bases for all the supervisory authorities to apply sanctions for failure to comply with requirements of R.6. **Latvia is largely compliant with R.35.**

Recommendation 36 – International instruments

406. Latvia was rated LC with both previous R.35 and SR.I in the 4th round, because the FT offence was not covered as predicate offences for ML; the criminalisation of FT the offence was not fully in line with the TF Convention; and measures were missing to implement UNSCRs 1267 and 1373.

407. *Criterion 36.1* – Latvia is a party to the Vienna Convention, the Palermo Convention, the Merida Convention, and the TF Convention. Latvia is also a party to the Council of Europe's 2005 Warsaw Convention and 2001 Convention on Cybercrime.

408. *Criterion 36.2* – Latvia implements the provisions of the Vienna, Palermo, Merida and TF Conventions through domestic legislation.

409. Concerning Art.5(6)(b) Vienna Convention, the authorities indicate that, if criminally acquired property has been alienated, destroyed, concealed or disguised, and the confiscation of such property is not possible, the value of the property can be recovered (Sec.70 CL).

410. Concerning the Merida Convention, embezzlement in the public sector is criminalized through the combination of Sections 179, 180, 317, 318(2) and 319 CL. However, an ad hoc provision implementing Art. 17 of the Convention should be introduced for the purpose of legal certainty. The assessment team shares the concerns of the UN[183] regarding the consistency of the existing sanctioning system under the CL in relation to corruption (Art. 30(1) of the Convention). As regards the immunities referred to by Art. 30(2) of the Convention, Sec.120 CPL provides that the State President and members of the Parliament (Saeima) enjoy immunity from criminal proceedings, which can be lifted by a decision of the Saeima. Measures could be taken to avoid the potential risk that, while immunity is being lifted, evidence could disappear or be tampered with. Investigative action aimed at securing evidence could be allowed before lifting immunity; and procedural immunity could apply to criminal prosecution only (and not to pre-trial investigation), as the UN suggests.

411. Regarding the Palermo Convention, Art.5 has not been fully implemented, since conspiracy or participation in organised criminal groups are not offences under the CL, but instrumental elements of other offences. Art.12(4) is not explicitly reflected in Latvian legislation.

412. The international instruments annexed to the TF Conventions are broadly implemented by Latvia. However, the country is not a party to the 2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation.

Weighting and Conclusion

413. The Vienna, Merida and Palermo Convention are implemented in Latvia, except for a number of technical requirements which have not been transposed or have been transposed with insufficient clarity. Latvia also implements the TF Convention, although it is yet to become a party to one of the annexed treaties. **R.36 is rated LC.**

[183] http://www.unodc.org/documents/treaties/UNCAC/CountryVisitFinalReports/2014_10_24_Latvia_Final_Country_Report.pdf

Recommendation 37 - Mutual legal assistance

414. In the previous round, Latvia was rated respectively C and LC with previous R.36 and SR.V, as it was considered that shortcomings in the criminalisation FT offence might provide an obstacle to effective co-operation with foreign states.

415. *Criterion 37.1* – Latvia is a party to international agreements such as the 1959 European Convention on Mutual Legal Assistance in Criminal Matters, the 1990 Strasbourg Convention, the 2003 Merida Convention and the 2005 Warsaw Convention, amongst others. It is also a party to a number of bilateral MLA agreements.

416. MLA is regulated in "Part C" of the CPL, which establishes that Latvia provides international cooperation in the following areas: (1) extradition; (2) transfer of criminal proceedings; (3) execution of procedural actions; (4) execution of a security measure not related to the deprivation of liberty; (5) recognition and execution of a judgement; and (6) other cases provided for in international treaties (Sec.673 CPL). Direct international cooperation is also allowed (Sec.675 CPL).

417. Latvian MLA covers general assistance in the performance of procedural actions (Sec.673(1)(4) CPL), which must be fulfilled following the provisions of the CPL (Sec.847(1)): all procedural actions that can be taken in domestic investigations are applicable in the execution of foreign requests.

418. MLA is provided on the basis of bilateral or multilateral agreements, where available. Where there is no agreement, MLA can be provided on the basis of reciprocity (Sec.675 (3) CPL).

419. As per Sec.848 CPL, the admissibility of MLA requests should be assessed within 10 days. However, there is no legal provision that explicitly requires the "rapid" execution of MLA requests.

420. *Criterion 37.2* – Three competent institutions are appointed as central authorities, depending on the stage of the criminal proceedings: the SP[184] at the investigation stage; the GPO at the prosecution stage; and the MoJ after the transfer of a case to a court. The same central authorities have been appointed in the framework of the European Convention on Mutual Assistance in Criminal Matters. After receiving a request, the central authority assesses its admissibility and transfers it, if necessary, to the relevant competent authority.

421. Direct cooperation is also possible on the basis of Sec.675(2) and 846(3) CPL if a previous agreement between competent authorities has been reached.

422. In 2014, an Information System on Judicial Cooperation in criminal matters was established for use by the central authorities. Cab. Reg. 1045, issued under Sec.673 CPL, determines the procedures for maintaining and using the system, the information to be included therein, the procedures for including, using and deleting information, the time periods for storing information, as well as the institutions that have access to the system. The system should register the receipt, attribution and status of execution of assistance requests. However, Latvia has not provided information on the actual time of execution of MLA requests, which suggests that the Information System does not systematically gathers such data and cannot adequately manage and prioritize MLA requests. There is no clear process for the timely prioritisation of MLA requests. The authorities indicate that requests are processed in chronological order, although the time limit expected by the requesting country is taken into account in urgent cases.

[184] Unit No. 3 of the International Cooperation Department

423. The process for the execution of MLA requests is described in reasonable detail in "Part C" of the CPL. As noted under c.37.1, there is no deadline for providing a response. Legislation does not clearly ensure the timely execution of the MLA requests.

424. *Criterion 37.3* – The conditions to provide MLA, as laid down in Sec.850 CPL, are justifiable and generally common or accepted in the international cooperation domain (prejudice to sovereignty, security, social order, dual criminality, political exceptions).

425. *Criterion 37.4 – a)* The possibility to refuse assistance on the ground that the offence is also considered to involve fiscal matters is not provided for in the CPL. Furthermore, Art. 1 Latvia is a party to the 1978 Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, of which explicitly excludes this ground for refusal of assistance.

b) The provisions on professional secrecy or confidentiality in Latvian law do not appear to constitute an obstacle to rendering MLA in the AML/CFT field.

426. Criterion 37.5 – As per Sec.847(1) CPL, procedural assistance in MLA matters is subject to the CPL, which includes the fundamental principle of the secrecy of the pre-trial criminal proceeding (Sec.396). The information obtained in pre-trial criminal proceedings can be disclosed if the investigator or a public prosecutor authorises it.

427. *Criterion 37.6* – In general, the dual criminality principle is not a ground for refusing MLA requests (Sec.850 CPL). Dual criminality is not required with regard to requests from EU Member States for a number of offences, specified in a "positive list", including terrorism, ML, trafficking in human being and drug trafficking (s.6 and 13(e) in the Consolidated Act on International Enforcement of Certain Criminal Justice Decisions in the EU).

428. *Criterion 37.7* – As noted above, in general, the dual criminality principle is not a ground for refusing MLA requests. As per Sec.852 CPL, Latvia may refuse the application of a compulsory measure regarding an offence that is not criminally punishable in Latvia, if: 1) Latvia does not have a treaty regarding MLA in criminal cases with the state that submitted the request; 2) such treaty exists, but the foreign state has undertaken to apply compulsory measures in such state only regarding offences that are criminally punishable in such state. In any case, even in the application of the dual criminality principle, there is nothing in the Latvia legislation to suggest that crimes must necessarily fall within the same category of offence or have the same terminology. Latvian legislation states that foreign requests must include a description of the criminal offence and the legal classification of such offence (Sec.678(2) CPL).

429. *Criterion 37.8* – According to Sec.847(1) CPL, all procedural actions provided by the CPL in Latvia can also be applied in the execution of MLA requests. These actions include "investigative actions" (e.g., searches and seizures) and "special investigative actions"[185]. However, as per Sec.210(3) CPL, "special investigative action" cannot be taken in relation to "criminal violations", defined in Sec.7 CL as offences for which deprivation of liberty between 15 days and 3 months (temporary deprivation of liberty), or a type of lesser punishment is provided in the CL. Criminal violations include some predicate offences, such as the illegal deprivation of liberty, some tax crimes, some environmental crimes and the illicit trafficking of alcoholic beverages and tobacco.

[185] Under Sec.215 CPL, special investigative actions include control of legal correspondence, control of means of communication, control of data in an automated data processing system, control of the content of transmitted data, audio and video-control measures, surveillance of objects and persons, etc.

Weighting and Conclusion

430. Latvia has met or mostly met all but one criteria of the Recommendation. There are however minor issues, including the absence of a clear process for the timely prioritisation and execution of MLA requests, and of a clear case management system. **R.37 is rated largely compliant.**

Recommendation 38 – Mutual legal assistance: freezing and confiscation

431. In the 2012 MER, Latvia was rated PC with the Recommendation on MLA in relation to freezing and confiscation since the enforcement of foreign confiscation orders for property, other than instrumentalities and property obtained illegally was only available if confiscation was a penalty for the same offence in Latvia; and it was unclear whether requests for confiscation of property could extend to enforcement of confiscation of all proceeds of crime, intended instrumentalities and terrorist property.

432. *Criterion 38.1* – Latvian MLA covers general assistance in the performance of procedural actions (Sec.673(1)(4) CPL), which shall be fulfilled following the provisions of the CPL. There is no explicit requirement to take actions expeditiously. As noted under c.4.2, Sec.361-366 CPL allow for the freezing/seizing of the categories of property defined under c.38.1. However, as noted under R.37, "special investigative action" cannot be applied in relation to some predicate offences.

433. Sec.791(1) CPL states that foreign requests for confiscation could be granted only if the CL provides for confiscation as a basic or additional punishment for the same offence, or if the property could be confiscated as criminally acquired property. Confiscation of criminally acquired property (proceeds, instrumentalities or equivalent value) is governed by CPL Sec.791(2), which states that "confiscation shall be applied only in the amount established in the judgement of the foreign state, that the object to be confiscated is an instrumentality of the committing of the offence or has been obtained by criminal means". Part 2 explicitly states that confiscation of property provided for in a ruling of a foreign state shall be executed regardless in which proceedings it was applied in the foreign state, in this way ensuring the execution of non-conviction-based confiscation.

434. *Criterion 38.2* – Non-conviction-based confiscation is provided under Ch.59 of the CPL, and is available when the perpetrator is unavailable by reason of death, flight, absence or is unknown.

435. Non-conviction-based confiscation can only be applied when provisional measures (i.e., seizure or "attachment") have been previously applied (Sec.626(1) CPL). Therefore, the prior existence of provisional measures regarding the criminal property is a prerequisite to order a on conviction-based confiscation, including on the basis of a foreign request.

436. Concerning confiscation, Sec.791 CPL ensures the execution of foreign confiscation orders, establishing that the referred execution would be applied regardless of the proceeding applied in the foreign state. The authorities provided some examples proving that MLA regarding the execution of on conviction-based confiscation foreign orders is covered.

437. *Criterion 38.3* – (a) Latvia is member of the CARIN network, which is used on a case-by-case basis. The Latvian authorities also referred to some coordinated actions with other countries; nevertheless, Latvia does not have clear coordination arrangements in relation to seizure and confiscation actions.

(b) Managing mechanisms of seized, frozen or confiscated property are limited to the storage of property, and there is no provision regarding the use or administration (i.e. managing) of such

property (Sec.235, 239 and 365 CPL). Although these provisions apply to all material evidence, the possibility of disposal of seized and frozen property is limited to objects the long-term storage of which is not possible or causes losses to the State. While the scope of this mechanism is broad enough to cover perishable property and property that loses value with the passing of time, this could be clarified by expressly stating it. Disposal of confiscated property is mainly provided by the Law on Execution of Confiscation of Criminally Acquired Property, which regulates in detail different forms of executing confiscated property. The government has further determined the procedures for the storage and disposing of criminally acquired property through Cab. Reg. 1025 "on actions with material evidence and arrested property". Additionally, Sec.239(3) provides that material evidence, the long-term storage of which is not possible or the long-term storage of which causes losses to the State, if they may not be returned to the owner or lawful possessor thereof, according to a decision of the person directing the proceedings, shall be: (1) disposed or destroyed; (2) destroyed if they have been recognised as unfit for use or distribution.

438. *Criterion 38.4* – Sec.792 and 800 CPL provide the possibility to share confiscated property with other countries on a case-by-case basis. These provisions have been developed by Cab. Reg. 431, which describes the procedure for dividing property, but not the criteria, as required by Sec.792(7) in fine CPL. In any case, the approval of the MoJ is required. Property of corresponding value is not covered by the referred provisions.

439. Based on the statistics provided by Latvia, confiscated assets have been shared twice with other countries.

Weighting and Conclusion

440. Latvia meets or mostly meets the four criteria under R.38. **R.38 is rated largely compliant.**

Recommendation 39 – Extradition

441. In the 2012 MER, the C rating granted to Latvia in the 3rd round MER was retained.

442. *Criterion 39.1* – a) (Latvia is able to execute extradition requests for the purpose of criminal prosecution, trial or the execution of a judgement regarding offences that, according to both the Latvian and the requesting State's Law, are criminal (dual criminality principle). Latvia is a party to the European Convention on Extradition (1957) and, as an EU Member State, has implemented European Arrest Warrants (EAW). The extradition for criminal prosecution or trial is only possible when the corresponding offence is punished with a penalty of deprivation of liberty the maximum limit of which is not less than one year. Extradition for the execution of a judgement is only possible if the imposed penalty of deprivation of liberty exceeds 4 months. These conditions may differ if any applicable international agreement provides otherwise (Sec.696 CPL). ML and FT are both associated with maximum penalties of deprivation of liberty exceeding one year.

(b) There is no clear case management and prioritisation system in place (see c.37.2). Under the CPL, a public prosecutor first examines the admissibility of the foreign extradition request within 20 days (this term may be extended by the GP). If admissible, the request is submitted to the GP, who takes a final decision (there is no established term for that decision). A person to be extradited may appeal the decision to the Supreme Court within 10 days, but the Supreme Court is not subject to any time limit to make a decision. Within the EU, the term of the arrest of a person to be extradited shall not exceed one-year (Sec.702(5) CPL). These processes do not clearly ensure the timely execution of the extradition requests. The authorities indicated that EAWs are executed

within up to 2 months from the moment of detention and extradition requests from non-EU states within up to 1 year.

(c) In the framework of the Petruhhin case (Estonian citizen whose extradition was requested to Latvia by Russia), the judgment of the Grand Chamber of the Court of Justice of the EU impedes the direct extradition of a national of another EU Member State citizen to a non-EU Member State and requires Latvia, as EU State Member, to inform Estonia of the request so that Estonia can issue a EAW. It is not clear if this this requirement would also apply to simplified extradition procedures where the person concerned consents to extradition. In any case, the "Petruhhin requirement" is considered to be an unreasonably or unduly restrictive condition on the execution of extradition requests and might entail the application of the reciprocity principle.

443. Criterion 39.2 – In general terms, the extradition of Latvian citizens is not admissible (Sec.697(2)(1) and 714(5)(4) CPL). Regarding EU member States, if an EAW has been taken regarding a Latvian citizen, the extradition of such person shall take place with the condition that the person will be transferred back to Latvia, after the conviction thereof, in order to execute the imposed penalty of deprivation of liberty.

444. No extradition of a Latvian national to a non-EU member state has yet been requested. If extradition was refused on the ground that the person is a citizen of Latvia, the public prosecutor would hand over the extradition request to a competent investigating institution for initiating criminal proceedings (Sec.705(5) CPL) and the request for taking over or transferring[186] criminal proceedings shall be executed (Sec.725(3) CPL). Nevertheless, Sec.726 CPL establishes a number of limitations that would hinder the prosecution of Latvian nationals in Latvia (e.g. takeover is not possible without a specific agreement in place with the requesting State). The legislation prohibits the enforcement of foreign sentences in the absence of specific agreements on mutual recognition and execution of judgements.

445. *Criterion 39.3* – Dual criminality is an indissoluble requirement for the execution of extradition requests. However, no provision in Latvian legislation suggests that crimes must necessarily fall within the same category of offence or have the same terminology. No judicial decision confirms it, but the authorities indicate that the fact that both countries criminalise the conduct underlying the offence is sufficient to consider the dual criminality requirement satisfied. Latvian legislation states that foreign requests must include a description of the criminal offence and the legal classification of such offence (Sec.678(2) CPL).

446. Within the EU, dual criminality is deemed to be met for the so-called "list crimes" (see c.37.6). In these cases, extradition will take place regardless of the absence of dual criminality and with no consideration to the denomination of the offence, or other assessment of the offence.

447. *Criterion 39.4* – Simplified extradition is possible under the CPL with the written consent of the person to be extradited if this person is not a Latvian citizen (Sec.731 CPL).

Weighting and Conclusion

448. Latvia only meets or mostly meets three of the four criteria under R.39. Due to recent CJEU jurisprudence, Latvia may not be able to execute the direct extradition of EU nationals to non-EU

[186] The takeover of criminal proceedings is defined under the CPL as the continuation in Latvia of criminal proceedings commenced in foreign states, upon request of the foreign State or with its consent. The transfer of criminal proceedings is defined under the CPL as the suspension thereof in Latvia and the continuation in a foreign State.

countries. The CPL establishes a number of limitations that could hinder the prosecution of Latvian nationals in Latvia if their extradition was requested. **R.39 is rated PC.**

Recommendation 40 – Other forms of international cooperation

449. In the 2012 MER, Latvia was rated as C with the Recommendation on other forms of international cooperation.

450. *Criterion 40.1* – Latvian competent authorities have a broadly adequate legal basis for providing a broad range of international cooperation in relation to ML, associated predicate offences and FT, both spontaneously and upon request. However, in addition to a number of limitations described in c.40.2-6, c.40.8 and c.40.15, there does not seem to be an explicit obligation to provide cooperation "rapidly".

451. *Criterion 40.2* – (a) Generally, Latvian competent authorities have a legal basis for providing international cooperation: Sec.62 and 63 AML/CFT Law for the FIU, Sec.46 AML/CFT Law for supervisors, the CPL for LEAs. Latvia is also part of a number of international and bilateral treaties that provide a legal basis for international cooperation, including non-judicial.

(b) There are no impediments to using of the most effective means of co-operating.

(c) The FIU (through the Egmont Secure Web and FIU.NET) and the LEAs (through INTERPOL and EUROPOL) use clear and secure channels, circuits and mechanisms to facilitate transmission and execution of requests. BoL reports using secure ad hoc channels accepted by all involved partners. The FCMC indicates that it usually wires the information with the intermediation of the FIU; or, in any case, directly exchanges information following strict security procedures, including encryption of data. The LGSI does not report using special secure channels. No information has been provided by the other supervisors.

(d) In general terms, there are not clear processes of prioritisation of requests (see analysis for MLA under R.37 and R.39). Legislation does not include any prioritization obligation or criteria, or deadline, for the FIU to process requests. However, the FIU indicated that priority is given to those foreign FIU requests that concern possible FT, requests for immediate freezing of funds, and other urgent requests. No information on prioritization of foreign requests has been provided by the supervisors.

(e) Judicial information is safeguarded following the CPL. The FIU's measures for information protection described under c.29.3 also apply to information received from foreign partners (Sec. 53 AML/CFT Law). No information on processes established by supervisors has been provided (beyond the condition set by Sec.46 AML/CFT Law to engage in information exchange if confidentiality of data is ensured).

452. LEAs information is also safeguarded on the basis of the Police legal framework (Sec.375 CPL and Art.6(2) of the Police Act).

453. *Criterion 40.3* – In general, competent authorities do not need agreements to cooperate. However, Latvia is part of a large number of bilateral and multilateral agreements in order to facilitate cooperation. In particular, the FIU, has signed 33 MoUs. The FCMC has signed a number of MoUs with non-EU Member States authorities. The LGSI has signed a number of "Cooperation arrangements between gambling supervisory institutions of EEA member states in the field of online gambling", on information exchange, initiated by the European Commission. The SRS FPD has concluded several bilateral cooperation agreements with Estonia, Lithuania and Georgia.

454. Latvia is part of a large number of bilateral and multilateral agreements in order to facilitate cooperation. The FIU does not need agreements or arrangements to cooperate; however, to facilitate cooperation, the FIU has signed 33 MoUs. The FCMC does not need agreements or arrangements to cooperate with EU Member States and has signed a number of MoUs with non EU Member States authorities. The LGSI has signed a number of "Cooperation arrangements between gambling supervisory institutions of EEA member states in the field of online gambling", on information exchange, initiated by the European Commission. BoL does not need agreements or arrangements to cooperate in the area of AML/CFT and has not signed any cooperation agreements. The SRS FPD has concluded several bilateral cooperation agreements with Estonia, Lithuania and Georgia.

455. *Criterion 40.4* – In general terms, there is no legal limitation to providing feedback in a timely manner to foreign competent authorities. Being a member of the Egmont Group, the FIU has to provide feedback when required in accordance with Clause 19 of the Egmont Principles for Information Exchange. The FIU has an obligation to provide feedback "if possible". No specific feedback obligations or practices have been reported by the AML/CFT supervisors, except for the FCMC, which indicates having an obligation to responding to requests for feedback, if any. The SP indicated that it has mechanisms to provide feedback to foreign authorities. The FPD indicates that it provides feedback in a timely manner if requested.

456. *Criterion 40.5* – The Latvian legislation does not impose any of the restrictions mentioned under (a) to (d). There are however concerns in relation to other conditions for the FIU to engage in international cooperation: the dual criminality condition may be an obstacle to exchanging information with LEAs or courts in relation to offences such as participation in an organized criminal group; it is unclear how "other restrictions and conditions related to the use of information provided, in addition to those specified, as well as to request data on the use thereof" can be interpreted under Sec.62(2) AML/CFT; and Sec.62(3) 4) may be an obstacle to cooperation in relation to FT -related TFS.

457. *Criterion 40.6* – Sec.62 AML/CFT Law establishes clear safeguards on the use of information provided by the FIU to foreign authorities. Legislation is silent on safeguards to be implemented by the FIU in using information received from a foreign partner. However, such safeguards are included in MoUs.

458. Additionally, Sec.46 AML/CFT Law does not mention any control or safeguards beyond requiring mutual agreement on use of information exchanged.

459. In line with the Manual on Law Enforcement Information Exchange, the SP's ICD keeps track of all incoming and outgoing information to ensure that it is used only for the purposes, and by the authorities, for which the information was sought or provided.

460. *Criterion 40.7* – LEAs, the members of the FIU and the justice administration are bound by the duty of secrecy established in their respective laws.

461. Requirements on the protection of information by the FIU are applicable to all the information at its disposal that has been acquired pursuant to the AML/CFT Law regardless of how the information has been acquired, including from a foreign partner.

462. Sec.46(9) and 48 AML/CFT Law establish that the SCAs have to implement the necessary administrative, technical and administrative measures to ensure the confidentiality of information. The breach of this duty could be considered a crime under Sec.200 CL.

463. *Criterion 40.8* – Latvian MLA covers the general assistance in the performance of procedural actions (Sec.673(1)(4) CPL), which shall be fulfilled following the provisions of the CPL (Sec.847(1) CPL), meaning that all procedural actions that can be taken in domestic investigations are applicable for the execution of foreign requests.

464. There is no explicit authorization for the FIU and SCAs (see c.40.15) to conduct inquiries on behalf of foreign counterparts. The AML/CFT only refers to "information exchange". The FPD notes that such inquiries are possible.

465. *Criterion 40.9* – Chapter XIII of the AML/CFT Law establishes a wide range of international cooperation possibilities for the FIU, regardless of whether foreign FIUs are administrative, LE or judicial FIUs. This cooperation is subject to the dual criminality principle, and concerns exist in relation to the ability to cooperate when the request is only related to a crime of participation in a criminal group.

466. *Criterion 40.10* – As per new Sec.62(2) AML/CFT Law, "if possible, the FIU shall inform the provider of information regarding the use of the received information." The FIU notes that feedback is always provided unless: it is temporarily technically impossible to provide it; it is impossible to provide it within the timeframe set by the requestor; a force majeure takes place; or it is prohibited by another law or regulation or investigative circumstances (temporarily).

467. *Criterion 40.11* – There does not seem to by any limitation to the type of information the FIU can exchange under Sec.62 AML/CFT Law. Restrictions of exchanges are defined on the basis of the potential use of information (see c.40.5), not their nature.

468. *Criterion 40.12* – Under Sec.46(7) and 46(10), financial supervisors must, spontaneously or upon request, exchange information which foreign equivalent bodies if the confidentiality of data is ensured and the information is used for mutually agreed purposes only (see c.40.1). Sec.6 and 7 of the Law on the FCMC and Art.93 of the BoL Reg. 36 on the Purchasing and Selling of Cash Foreign Currencies complement that legal basis for the FCMC and BoL respectively.

469. *Criterion 40.13* – The legislative provisions stated above do not contain any limitations as to the type of information the financial supervisors would be able to exchange with their foreign counterparts. In particular, the FCMC is authorised to exchange any information which is needed for supervision purposes (on the basis of a MoU for non-EU supervisors).

470. *Criterion 40.14* – The above described legislative provisions do not restrict the scope of the information that can be shared with foreign supervisors and it therefore appears that financial supervisors are empowered to share also the information required under this criterion.

471. *Criterion 40.15* – The authorities indicate that technically there are no legal provisions requiring the FCMC or other financial supervisors, to act on behalf of foreign counterparts, including to conduct inquiries on behalf foreign counterparts. There is no explicit authorization to do so (the AML/CFT Law, the Law on the FCMC and the Law on Credit Institutions only mention "exchange of information").

472. It would be only possible in the particular case where, in relation to the FCMC framework, a EU Member State (or even a third country under some conditions) can carry out inspections at branches and representations of a credit institution of the relevant Member State registered in Latvia, as well as at such credit institutions and commercial companies thereof, which have submitted information to the supervisory authority of the Member State for the performance of

consolidated supervision (Sec.107.[1] and 107.[2] of the Credit Institutions Law), but this power does not fully covers c.40.15.

473. *Criterion 40.16* – As per Sec.46 AML/CFT, SCAs exchange information with foreign equivalent bodies if the confidentiality of data is ensured and under the condition that the exchanged information is only used for the purposes mutually agreed between the requesting and the requested financial supervisor.

474. *Criterion 40.17* – Provisions of the CPL, which is the legal basis for the cooperation of the Police, establishes a wide range of LEAs cooperation. Art.7 and 14 of the Police Law establish a broad range of cooperation of the Police department.

475. *Criterion 40.18* – Provisions of the CPL establishes a wide range of LEAs cooperation, including the possibility to obtain the necessary information from natural and legal persons. Police co-operation takes place particularly within the framework of conventions and agreements signed by Interpol, Europol or Eurojust with third-party countries (see also c.40.8).

476. *Criterion 40.19* – LEAs in Latvia are able to form and participate in joint investigation teams (JIT) set forth in Chapter 84 CPL. In particular, Sec.888 CPL allows the establishment of JITs and, additionally, promotes their establishment, stating that JITs shall be established for the purpose of eliminating unjustified delays when several countries are involved in the same case. The country is also part of EUROJUST and takes part in their joint investigations.

477. *Criterion 40.20* – Sec.62(4) AML/CFT Law allows the FIU to make request also to other non-equivalent foreign institutions for the purpose of exercising its functions. SCAs are empowered to send information to the FIU (Sec.49 AML/CFT Law), information that could be used by the FIU for the purpose of international cooperation.

Weighting and Conclusion

478. Latvia meets or mostly meets 14 of the 20 criteria of R.40. There is no explicit legal provision to provide assistance rapidly. There is no prioritisation of case management system to process foreign requests. Competent authorities, except for the FIU, do not have an obligation to provide feedback to foreign partners. The ability of the FIU to provide assistance appears to be limited by some legal restrictions. There are limited provisions ensuring the confidentiality of foreign requests and information contained therein. There is no explicit requirement or authorization for supervisors to conduct inquiries on behalf of foreign partners. **R.40 is rated PC.**

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
1. Assessing risks & applying a risk-based approach	C	
2. National cooperation and coordination	LC	• The cooperation and, where applicable, coordination mechanisms to combat the financing of proliferation of WMD are not clearly defined in the Latvian institutional system.
3. Money laundering offence	LC	• Participation in an OCG as an offence in its own right is not fully criminalised, but only with regard particularly serious offence (e.g. genocide, war crimes) • The criminalisation of the FT offence does not cover all the aspects required by the international standards and thus is somewhat limited as a predicate offence for ML.
4. Confiscation and provisional measures	C	
5. Terrorist financing offence	LC	• Generic FT offence does not cover indirect transfer as well as the direct and indirect provision or collection of funds. • The criminalisation of the financing of the travel for the purpose of terrorism does not explicitly cover the provision or receipt of terrorist training.
6. Targeted financial sanctions related to terrorism & TF	PC	• There is no formal mechanism to identify targets for designations and/or designation proposals under UNSCRs 1267 and 1373. • No clear evidentiary standard and procedure apply to designation proposals, including upon foreign request. No provision ensures that a prompt determination can be made on a third party listing request. • Freezing cannot apply to EU nationals at EU level (UNSCR 1373). • No clear provision ensures that as much information as possible would be given to third countries in case a listing request is made. • TFS are not implemented without delay. • The scope of persons subject to the freezing obligation and the scope of funds to be frozen are ambiguous in national legislation. • No permanent freezing order can be issued without a judicial order. • Sec.32 AML/CFT Law does not clearly apply to TFS. • De-listing procedures are not clearly established at national level. Procedures for allowing access to funds and other assets under certain conditions are not mentioned in the AML/CFT Law.
7. Targeted financial sanctions related to proliferation	PC	• Deficiencies noted under R.6 apply. • The scope of monitoring and sanctioning measures is unclear.
8. Non-profit organisations	PC	• No identification of the subset of NPOs meeting the FATF definition or systematic identification of higher FT risk NPOs and related threats. • No CFT specific review of the adequacy of measures on NPOs. • No periodically reassessment of the sector. • No specific CFT outreach to NPOs and donors, best practices or encouragement to use regulated financial channels. • The broad range of relevant measures applying to NPOs is insufficiently informed by FT risk. • The nature of the Enterprise Register checks on NPOs is unclear.
9. Financial institution secrecy laws	C	
10. Customer due diligence	PC	• The AML/CFT Law does not require the REs to undertake CDD measures when there are doubts about the adequacy of the previously obtained CDD data. • The AML/CFT Law does not require CDD of existing relationships at appropriate times, taking into account whether and when CDD measures

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
		have previously been undertaken and the adequacy of data obtained. • The only measure making enhanced CDD different from standard CDD is the enhanced monitoring of the customer's transactions, which is not defined anywhere in the applicable legislation to comprise certain key elements of enhanced CDD. • The subjects of the AML/CFT Law are not required to refrain from opening accounts, commencing business relationships, performing transactions, and to terminate business relationships whenever they are unable to comply with all relevant CDD measures.
11. Record keeping	LC	• The record-keeping provision is defined too specifically to presume that it necessarily encompasses the FATF requirement to maintain the results of analyses undertaken by the REs.
12. Politically exposed persons	LC	• The timeframe of 12 months established for derecognizing PEP status does not meet the definition of PEP in the FATF Glossary.
13. Correspondent banking	LC	• The definition of a shell bank appears to overlook certain elements of the FATF definition.
14. Money or value transfer services	LC	• The amount of fine determined for unregistered/ unlicensed MVTS activities is neither proportionate nor dissuasive in the Latvian context. • The AML/CFT Law does not provide for the obligation of MVTS providers to monitor agents for compliance with AML/CFT programs.
15. New technologies	LC	• National ML/FT risk assessments and other analyses do not reflect the work done by the authorities for the purpose of identifying and assessing ML/FT risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.
16. Wire transfers	LC	• The Regulation (EU) 2015/847 appears to fall short of the FATF requirement for an MVTS provider to take into account all information from both the ordering and beneficiary sides (as opposed to missing or incomplete information on the originator or the beneficiary). • It does not require to file a STR in the country affected by the suspicious wire transfer and to make relevant transaction information available to the FIU.
17. Reliance on third parties	LC	• The relying parties are requested to be able to immediately receive – but are not required to immediately obtain – the necessary information concerning CDD measures. • Compliance with the Latvian AML/CFT Law aimed to meet the requirements under c.17.1 and c.17.3 does not necessarily amount to compliance with the requirements set out in the FATF Recommendations 10-12 and 18.
18. Internal controls and foreign branches and subsidiaries	LC	• In terms of the relevant powers and responsibilities, the position of the Board member does not appear to qualify for that of the compliance officer appointed at the management level as required by the FATF Standard. • The requirement for employee screening applies to banks and PI/ EMIs only. • Availability of an independent audit function is made contingent on an undefined number of employees of the subject of the Law.
19. Higher-risk countries	LC	• There is room for improvement in taking proactive action to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries.
20. Reporting of suspicious transaction	LC	• While addressing the element of reporting in the presence of suspicions, the AML/CFT Law does not appear to cover the element of carelessness or negligence, i.e. the situations where there are reasonable grounds for suspicions, which are nevertheless neglected.

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
21. Tipping-off and confidentiality	C	•
22. DNFBPs: Customer due diligence	PC	• Reference is made to the deficiencies identified with regard to Recommendations 10, 11, 12, 15 and 17. • There is no provision for real estate agents to comply with the requirements set out in Recommendation 10 with respect to both the purchasers and the vendors of the property. • Sworn lawyers, notaries, other independent legal professionals and accountants (tax advisors) are exempt from the requirement to terminate the business relationship where they are unable to obtain the necessary CDD information and documents in cases when they defend or represent their customers in pre-trial criminal proceedings or judicial proceedings, or advise on instituting or avoiding judicial proceedings, thus clearly diverging from the FATF-defined legal professional privilege stipulated for STR reporting only.
23. DNFBPs: Other measures	LC	• Reference is made to the deficiencies identified with regard to Recommendations 18-21. • The requirement to have employee screening procedures does not apply to any DNFBPs.
24. Transparency and beneficial ownership of legal persons	LC	• There is no specific provision that requires one or more natural persons resident in Latvia or for the appointment of an accountable DNFBP to be responsible for maintaining BO and be accountable to the authorities. • Records on legal persons must be retained by the liquidator for a 10-year period. However, it is not clear whether this applies to beneficial ownership information. • The legislation does not provide for nominal activity for nominee directors; however, there is no prohibition for a person to act as a nominee director.
25. Transparency and beneficial ownership of legal arrangements	LC	• There is no requirement for trustees of foreign trusts to disclose their status to financial institutions or DNFBPs when forming a business relationship or carrying out an occasional transaction above the threshold.
26. Regulation and supervision of financial institutions	PC	• Alternative investment funds are only required to register (no licensing). • There are licensing requirements for lending activities conducted by non-bank FIs only if they provide consumer lending services. • Associates of persons with criminal records are not covered in the national legislation. • Not all financial supervisors are conducting ML/FT risk-based supervision.
27. Powers of supervisors	C	•
28. Regulation and supervision of DNFBPs	PC	• It is not clear if there are measures in place to prevent criminals from controlling DNFBPs (except for the Notaries). • There are deficiencies in the ML/FT risk-based supervision conducted by the supervisory authorities.
29. Financial intelligence units	LC	• The FIU has indirect access to a number of government databases. • The FIU's discretionary power in providing information on request is potentially limited by the GPO's filter and unclear criteria for approval at FIU level. • The AML/CFT Law could clarify that the role of the GPO in the organisation and activities of the FIU is consistent with the FIU's operational autonomy.
30. Responsibilities of law enforcement and investigative authorities	LC	• It is not fully apparent to which extent LEAs are authorised to investigate ML/FT offences during a parallel financial investigation.

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
31. Powers of law enforcement and investigative authorities	LC	• In exceptional circumstances, FIU is under no obligation to comply with a request for information.
32. Cash couriers	PC	• The declaration system applies only to movements (both inward and outward) of cash and BNI from and to the EU. • The administrative fines for non-criminally acquired cash are not sufficiently dissuasive. • For amounts below EUR 19,000, the internal regulations of the SRS provide for the possibility to stop/restrain currency or BNIs for a reasonable time in order to ascertain whether evidence of ML/FT may be found, only if there is indication for an illegal activity.
33. Statistics	LC	• Some inconsistencies noted in the statistics on STRs. • The authorities were not in the position to provide comprehensive statistics on property frozen, seized, confiscated and recovered post-conviction; separate statistics for the confiscation of instrumentalities; freezing orders from the FIU; seizures by the FPD; and amounts confiscated. There were no statistics on confiscation resulting from cross-border cash movement information. • No information is collected by all relevant authorities on time taken to respond to foreign requests.
34. Guidance and feedback	C	
35. Sanctions	LC	• There are no clear legal bases for all the supervisory authorities to apply sanctions for failure to comply with requirements of R.6.
36. International instruments	LC	• Some elements of the Vienna, Merida and Palermo Convention have not been transposed, or have been transposed with insufficient clarity. • Latvia is not a party to the Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation.
37. Mutual legal assistance	LC	• There is no explicit requirement to execute MLA requests "rapidly". • There is no clear process for the timely prioritisation and execution of MLA requests, nor is there a clear case management system. • Special investigative techniques do not apply to some predicate offences
38. Mutual legal assistance: freezing and confiscation	LC	• There is no explicit requirement to take "expeditious" action in response to confiscation requests • There are no formal arrangements for co-ordinating seizure and confiscation actions with other countries; and mechanisms for managing property frozen, seized or confiscated are incomplete.
39. Extradition	PC	• There is no clear process for the timely prioritisation and execution of extradition requests, nor is there a clear case management system. • Due to recent CJEU jurisprudence, Latvia may not be able to execute the extradition of EU nationals to non-EU countries. • The CPL establishes limitations that could hinder the prosecution of Latvian nationals in Latvia if their extradition was requested.
40. Other forms of international cooperation	PC	• There is no explicit legal provision to provide assistance rapidly. • Not all competent authorities have clear and secure gateways, mechanisms or channels for transmitting and executing requests, clear prioritisation of case management system for that purpose, or clear processes for safeguarding the information received. • All competent authorities do not have an obligation to provide feedback to foreign partners. • The ability of the FIU to provide assistance appears to be limited by some legal restrictions. • The are no clear controls and safeguards for all competent authorities on the use of information exchanged. • There is no explicit requirement or authorization for all competent authorities to conduct inquiries on behalf of foreign partners.

GLOSSARY OF ACRONYMS

ABCS	Advisory Board of the Control Service
ACAMS	Associations of Certified Anti-Money Laundering Specialists
AIFM	Alternative Investment Fund Managers Directive
AML/CFT Law Financing	Law on the Prevention of Money Laundering and Terrorism
ARO	Asset Recovery Office
BNIs	Bearer Negotiable Instruments
BoL	Bank of Latvia (Latvijas Banka)
CA	Court Administration
CARIN	Camden Assets Recovery Interagency Network
CDD	Customer Due Diligence
CIS	Commonwealth of Independent States
CL	Latvian Criminal Law
CO	Criminal Offences
CoM	Cabinet of Ministers
CPCB	Latvian Corruption Prevention and Combating Bureau (KNAB)
CPL	Latvian Criminal Procedure Law
CRPC	Consumer Right Protection Center
DNFBPs	Designated Non-Financial Business and Professions
DPMS	Dealer in Precious Metal Stones
DPRK	Democratic People's Republic of Korea
EAWs	European Arrest Warrants
ECB	European Central Bank
EMIs	Electronic Money Institutions
ER	Enterprise Register
EU	European Union
EUROJUST	EU's Judicial Cooperation Unit
EUROPOL	European Union Agency for Law Enforcement Cooperation
FATF	Financial Action Task Force
FCMC	Financial and Capital Market Commission

FIs	Financial Institutions
FIU	Office for the Prevention of Laundering of Proceeds Derived from Criminal Activity (Control Service)
SRS FPD	Financial Police Department of the State Revenue Service
FSDB	Financial Sector Development Board
FT	Financing of Terrorism
FTF	Foreign Terrorist Fighter
GDP	Gross Domestic Product
GP	General Prosecutor
GPO	General Prosecutor's Office
ICS	Internal Control System
INTERPOL	International Criminal Police Organisation
IO	Immediate Outcome
IOSCO	International Organisation of Securities Commissions
IT	Information Technology
JIT	Joint Investigation Team
KOMID	Korean Mining Development Trading Corporation
LACA	Latvian Association of Certified Auditors
LACB	Latvian Association of Commercial Banks
LCSA	Latvian Council of Sworn Advocates
LCSN/CNSL	Latvian Council of Sworn Notaries
LEAs	Law Enforcement Agencies
LGSI	Lottery and Gambling Supervisory Inspection
LIA	Latvian Insurers Association
LIKC	Latvian Islamic Cultural Centre
LLC	Limited Liability Company
LPSEM	Law on Payment Services and Electronic Money
MEQ	Mutual Evaluation Questionnaire
MER	Mutual Evaluation Report
MFA	Minister of Foreign Affairs
ML	Money Laundering
MoD	Ministry of Defence
MoE	Ministry of Economics

MoF	Ministry of Finance
MoI	Ministry of Interior
MoJ	Ministry of Justice
MoT	Ministry of Transport
MoU	Memorandum of Understanding
MVTS	Money or Value Transfer Services
NPOs	Non-profit Organisations
NRA	National Risk Assessment
NSC	National Security Committee of the Saeima
OAL	Operational Activities Law
OCG	Organised Criminal Group
OCMA	Office of Citizenship and Migration Affairs
PBOs	Public Benefit Organisations
PEPs	Politically Exposed Persons
PF	Proliferation Financing
PI	Payment Institutions
AML/CFT	Prevention of Money Laundering and Funding of Terrorism
RBA	Risk-Based Approach
RE	Reporting Entities
SARs	Suspicious activity reports
SBC	State Border Control
SeP	Security Police
SP	State Police
SRO	Self-Regulatory Organisations
SRS	State Revenue Service
SRS CD	Customs Departments of the State Revenue Service
SRS CPD	Custom Police Department of the State Revenue Service
SSM	Single Supervisory Mechanism
STRs	Suspicious transactions reports
TFS	Targeted Financial Sanctions
TCSPs	Trust and company service providers
UBOs/BOs	Ultimate beneficial owners/Beneficial owners

UNSCR	United Nations Security Council Resolutions
UTRs	Unusual transactions reports
WB	World Bank
WMD	Weapons of Mass Destruction

www.coe.int/MONEYVAL

July 2018

Anti-money laundering and counter-terrorist financing measures

Latvia

Fifth Round Mutual Evaluation Report

This report provides a summary of the AML/CFT measures in place in Latvia as at the date of the on-site visit (30 October to 10 November 2017). It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Latvia's AML/CFT system and provides recommendations on how the system could be strengthened.