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(2026)2

Anti-money laundering and counter-terrorist financing measures

Latvia

Sixth Round Mutual Evaluation Report

February 2026

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 sixth round mutual evaluation report on Latvia was adopted by the MONEYVAL Committee at its 69th Plenary Session held jointly with FATF (Strasbourg, 10-13 June 2025).

Table of Contents

EXECUTIVE SUMMARY

1. This report summarises the anti-money laundering and countering the financing of terrorism (AML/CFT) measures in place in Latvia as at the date of the on-site visit 4-15 November 2024. 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

a) Latvia's approach to identifying, assessing and understanding money laundering (ML) and terrorist financing (TF) risks is characterised by a genuine curiosity, and a commitment to integrate a wide variety of data sources to generate and maintain an evolving, continuous and an in-depth understanding of its past and present ML/TF risks. Activities of competent authorities and self-regulatory bodies (SRBs) are aligned with findings of national risk assessments (NRAs) and Latvia has established a well-functioning mechanism to co-ordinate both policy and operational responses to its risks.

b) Latvia's law enforcement agencies (LEAs) regularly use financial intelligence to identify ML and associated predicate offences. Latvia has significantly reformed its Financial Intelligence Unit (FIU), enhancing its financial, human, and information technology resources to effectively address ML/TF risks. The FIU produces and disseminates a wide range of high-quality financial intelligence products, including strategic and operational analysis.

c) Latvian authorities effectively identify and investigate ML cases, prioritising them according to their evolving risk profile. They use a range of tools and techniques, demonstrating substantial expertise and strong inter-agency co-operation. Prosecution and conviction rates have increased, though structural factors have hindered large-scale ML cases involving unknown or non-resident offenders involved in Latvia-based global laundromat schemes. Authorities pursue standalone ML and ML tied to predicate offenses, including complex international schemes, but legal persons are not prosecuted adequately given Latvia's risk and context. Custodial sentences for ML are proportionate and dissuasive, though sanctions for legal persons are not generally dissuasive. Alternative criminal justice measures are applied when ML prosecution is not possible, targeting legal persons for other offences.

d) Latvia prioritises asset recovery as a policy objective, which is reflected in institutional reforms and national ML action plans. The effective use of provisional measures has led to over EUR 3 billion in assets seized, primarily tied to a bank liquidation case. During the assessment period, Latvia confiscated over EUR 300 million, mainly through non-conviction-based confiscation (NCBC), although high-profile cases pending judicial decisions have created a gap between seized and confiscated assets. Latvia's freezing and seizing statistics align with evolving risks, though confiscation results still reflect the first risk profile due to the lengthy lifecycle of criminal proceedings.

e) Effectiveness of supervision of financial institutions (FIs) has increased since the last evaluation, resulting in significant reduction of risks in the most material banking sector. Whilst most sectors outside banking received less supervisory attention, the level of compliance in these sectors has increased through the assessment period; this was achieved through guidance and remediation. Many strong features are in place to support supervision of compliance by designated non-financial business or professions (DNFBPs), however, results of institutional risk assessments conducted by the State Revenue Service (SRS) – the largest supervisor of DNFBPs - are not considered by the assessment team (AT) to be consistent with national or sectoral risks and its supervisory effort may not always be directed to where ML risk is highest.

f) Latvia has an effective system in place to ensure transparency of basic and beneficial ownership (BO) data and timely and efficient access thereto. A dual approach is used to access BO information through the Enterprise Register (ER) and reporting entities (REs). The adequacy and accuracy of data contained in the Registry are ensured through verification checks by the authorities and a discrepancy reporting mechanism. Targeted mitigating actions taken by the authorities are largely proportionate to legal person related risks. Latvia's exposure to foreign legal arrangements is assessed to be minimal.

Effectiveness & Technical Compliance Ratings

	Effectiveness		Technical Compliance	
Risk mitigation through policy, co-ordination and co-operation				
Assessment of risk, coordination and policy setting	**IO.1**	HE	**R.1**	C
			R.2	C
International co-operation	**IO.2**	SE	**R.36**	LC
			R.37	LC
			R.38	C
			R.39	LC
			R.40	LC
Cross-cutting requirements			**R.33**	C
Prevention, detection & reporting of illicit funds across sectors				
Financial sector and virtual asset supervision and preventive measures	**IO.3**	SE	**R.9**	C
			R.10	LC
			R.11	LC
			R.12	LC
			R.13	LC
			R.14	LC
			R.15	LC
			R.16	LC
			R.17	LC
			R.18	LC
			R.19	LC
			R.20	LC
			R.21	C
			R.26	LC
			R.27	C
Non-financial sector supervision and preventive measures	**IO.4**	ME	**R.22**	LC
			R.23	LC
			R.28	LC
Transparency and beneficial ownership	**IO.5**	HE	**R.24**	LC
			R.25	PC
Cross-cutting requirements			**R.34**	C
			R.35	LC

Detection and disruption of threats, sanctions & deprivation of illicit funds				
Financial intelligence	**IO.6**	HE	**R.29**	C
Money laundering investigations and prosecutions	**IO.7**	SE	**R.3**	LC
Asset recovery	**IO.8**	HE	**R.4**	C
			R.32	C
Terrorist financing investigations and prosecutions	**IO.9**	SE	**R.5**	LC
Terrorist financing preventive measures and financial sanctions	**IO.10**	SE	**R.6**	LC
			R.8	LC
Proliferation financing financial sanctions	**IO.11**	HE	**R.7**	LC
Cross-cutting requirements			**R.30**	C
			R.31	C

Note: Effectiveness ratings can be either a High- HE, Substantial- SE, Moderate- ME, or Low – LE, level of effectiveness. Technical compliance ratings can be either a C – compliant, LC – largely compliant, PC – partially compliant or NC – non-compliant. While the technical compliance findings can be relevant across the effectiveness immediate outcomes (for example, R.1 or R.40), the table above illustrates the main technical compliance findings specific to each effectiveness immediate outcome and cross-cutting requirements for each of the intermediate outcomes. For more detail on the relevant technical compliance requirements relevant to each effectiveness immediate outcome, see the relevant paragraph at the beginning of each chapter. See also paragraphs 53 and 54 of the FATF 2022 Methodology for links between effectiveness and technical compliance ratings.

Risks and General Situation

2. Since 2017, Latvia's risk profile has undergone significant changes. The country is no longer a regional financial centre characterised by a banking sector heavily oriented towards servicing non-resident customers. This transformation has been driven by a strategic, high-level political commitment. In line with the considerable decrease in concentration of the foreign customer base in FIs and related cross-border movements of funds, the main ML threats now stem predominantly from predicate offences committed domestically. The main predicate offences are crimes related to the shadow economy, fraud, and corruption. Also, there are ML threats related to proceeds generated by foreign criminal offences, mainly related to laundering of the proceeds of fraud which are brought into Latvia physically or otherwise transferred to the Latvian financial system. TF risk is assessed as low.

3. Since its last evaluation, Latvia has made substantial efforts to remedy deficiencies identified during that process. In most respects, elements of an effective AML/CFT system are in place and the country has demonstrated a substantial or high level of effectiveness with all Immediate Outcomes (IO), apart from IO.4 (monitoring of, and application of preventive measures by, DNFBPs). This IO has been assessed as presenting moderate effectiveness, notwithstanding that there have also been many improvements in this sector. In terms of technical compliance, the legal framework has been enhanced in many aspects and all FATF Recommendations have been assessed as being compliant or largely compliant, apart from R.25, which is rated as partially compliant, following a recent change to the FATF Standards. However, Latvia's exposure to foreign legal arrangements is very limited, and so shortcomings in technical measures to promote transparency and availability of BO information are not considered to be material.

Assessment of risk, co-ordination and policy setting (Chapter 1; IO.1, R.1, 2, 33 & 34)

4. The risk and context in Latvia have changed considerably since its last mutual evaluation report (MER 2018), with significant and sustained political commitment to tackling Latvia's historic and legacy risks. This has resulted in a fundamental change in how Latvia approaches financial crime at all levels, as well as the nature of business served by Latvia's economy. Latvia has a well-developed understanding of its historic risks ("risk profile one"), the main current risk tied to domestic offences ("risk profile two"), as well as risks emanating from criminal offences committed abroad and imported into Latvia ("risk profile three"). Latvia has conducted two NRAs within the assessment period which further underpin the proper understanding of the key risks it faces.

5. The country has a well-functioning and clearly documented governance mechanism to co-ordinate its policy and operational activities, as well as the proper allocation of budget and resources. Competent authorities' objectives are in line with ML and TF risks identified in NRAs and consistent with national AML and CFT policies. This is ensured by each agency and department having their own action plans, which implement the national plan. Activities of competent authorities and SRBs are aligned with findings of NRAs, including a well-functioning mechanism to co-ordinate both policy and operational responses to the key risks faced by the country.

International co-operation (Chapter 2; IO.2; R.36–40)

6. Latvia maintains strong formal international co-operation with both EU and non-EU partners, ensuring thorough and timely responses to mutual legal assistance (MLA) and extradition requests. However, the manual case management system used by authorities does not systematically gather data on the execution time of MLA requests, complicating management and prioritisation. Nevertheless, Latvia increasingly uses international co-operation to pursue ML and associated predicate offences, regularly seeking and providing assistance for joint investigation teams (JITs), European investigation orders (EIOs), and other forms of co-operation. Co-operation on corruption cases remains limited, and follow-up actions regarding provisional measures and asset confiscation for assets identified abroad can still be improved. Latvia faces challenges from limited co-operation with certain jurisdictions, beyond its control, which hinders the prosecution and conviction of major ML schemes tied to liquidated banks (see also IO.7).

7. The framework for other forms of co-operation is well-developed, with crucial partnerships through Europol, Interpol, Eurojust and the Camden Asset Recovery Network (CARIN) for rapid information exchange worldwide. The State Police leads international co-operation efforts, while the FIU is a global leader, initiating projects like the International Financial Intelligence Task Force (IFIT) and developing new co-operation tools via forums such as the Egmont Group. Supervisors seek and provide international co-operation to varying extents, with the most material supervisors regularly engaging in these efforts.

Financial sector and virtual asset supervision and preventive measures (Chapter 3; IO.3, R.9-21, 26, 27, 34 & 35)

8. Licensing and registration authorities have processes in place to prevent criminals from entering the financial market, however, scrutiny and scope of checks vary. Whilst Latvian law does not cover a broad range of criminality or identify criminal association, authorities consider all crimes when assessing the reputation of an applicant. The SRS lacks legal powers to prevent criminals from entering the regulated VASP and lending market, however, it does not have a material impact on effectiveness due to the lower materiality and risk exposure of these sectors.

9. Latvijas Banka demonstrates a comprehensive understanding of ML/TF risk in supervised financial sectors which is especially advanced in the banking sector and has developed largely effective institutional risk assessment tools that are widely used for supervisory planning. Application of customer due diligence (CDD)/ enhanced due diligence (EDD) measures and internal controls by FIs has improved significantly since the last assessment, however, more efforts in the area of monitoring of clients' activities would be beneficial. Latvijas Banka supervisory focus on the most material banking sector has proven effective and resulted in a significant reduction of risk, however, other FIs received less supervisory attention. A broad range of effective, proportionate and dissuasive sanctions and prescribed remedial measures have been applied to the banking sector. The lower number of sanctions for other financial sectors (except for VASPs) is correlated with fewer on-site visits. Nevertheless, financial supervisors were able to demonstrate increasing compliance trends across the whole financial sector, with comprehensive guidance and remedial measures having had an impact here.

Non-financial sector supervision and preventive measures (Chapter 4; IO.4, R.22, 23, 28, 34 & 35)

10. Despite some remaining gaps in legislative provision, controls effectively prevent criminals and their associates from holding or being the BO of a significant or controlling interest or holding a management function in DNFBPs. All DNFBP supervisors, except for the Latvian Council of Sworn Advocates (LCSA), effectively collect information to identify ML/TF risks and apply a risk-based approach. However, results of institutional risk assessments conducted by the SRS (which, inter alia, supervises independent legal professionals and accountants) are not considered by the AT to be consistent with national or sectoral risks and, whilst it is clear that supervision takes account of risk, SRS supervisory effort may not always be directed to where ML risk is highest. Accordingly, its risk assessment methodology should be reviewed. The inspection model applied to advocates cannot be considered properly risk-based and such an approach should be developed. Effective use is made of remedial actions and sanctions by the SRS and Lotteries and Gambling Supervisory Inspection (LGSI). Generally, supervisory action has had a positive impact on levels of compliance by DNFBPs over time.

11. In most cases, DNFBPs have demonstrated a good understanding of risks, including how these have changed over time, and effective implementation of AML/CFT requirements. Proactive work by the FIU has helped to increase the total number of suspicious transactions reports (STRs) to the extent that under-reporting is now focused in the legal sector.

Transparency and beneficial ownership (Chapter 5; IO.5; R.24 & 25)

12. Latvia has a robust system to ensure transparency of basic and BO information and timely and efficient access thereto by competent authorities. A multi-pronged approach is used for accessing BO information, comprising information in the ER and information held by REs. Numerous verification checks by the ER (including the use of SRS information) and REs combined with a discrepancy reporting mechanism serve to ensure the accuracy of BO data.

13. Latvian authorities demonstrated a good understanding of legal person-related risks and apply targeted and effective mitigating measures, albeit more efforts need to be put towards increasing technical compliance in the area of nominee arrangements. Latvia does not recognise trusts or other types of legal arrangement and the country's exposure to foreign legal arrangements is very limited thus related technical shortcomings have a low impact on effectiveness.

14. Latvia has imposed a range of proportionate and dissuasive sanctions for non-compliance with reporting and disclosure requirements, including use of liquidation and penalties for non-compliance, as well as custodial sentences in the most egregious cases.

Financial intelligence (Chapter 6; IO.6, R.29 - 32)

15. LEAs and intelligence agencies in Latvia routinely access and utilise financial intelligence and other relevant information to investigate ML and associated predicate offences. The FIU has undergone substantial institutional reforms and is well resourced with significant information technology (IT) and human resources. The FIU conducts both operational and strategic analysis, adding significant value to existing cases and identifying a wide range of suspected offences. LEAs co-operate effectively with the FIU, forming specialised co-ordination groups when necessary to identify suspects and trace assets in complex cases. This has led to the successful identification of various ML and predicate offences, and the overall enhancement of Latvia's AML CFT regime.

Money laundering investigations and prosecutions (Chapter 7; IO.7, R. 3, 30 & 31)

16. The State Police, State Revenue Service Tax and Customs Police Department (SRS TCPD) and the Corruption Prevention and Combating Bureau (CPCB) are the main competent authorities identifying and investigating ML and associated predicate offences. These LEAs identify and investigate by drawing on a wide range of sources and using various investigative techniques to pursue ML and are well resourced for this task. ML is investigated in line with risks, but due to the absence of suspects in major ML schemes tied to Latvia's bank-based laundromat schemes, many offenders in large scale complex ML schemes could not be identified for prosecution. Authorities pursue standalone ML and ML tied to predicate offenses, including complex international schemes, but legal persons are not prosecuted adequately given Latvia's risk and context. Natural persons on the other hand are prosecuted for ML, and the sanctions that are applied are generally effective and dissuasive and are tied to the degree of severity of the offence. Latvian authorities are prosecuting and convicting standalone and third-party ML to a large extent.

Asset recovery (Chapter 8; IO.8, R. 1, 4 & 32)

17. Competent authorities responsible for asset recovery have a broad set of powers available, enabling them to pursue a policy of asset recovery that considers Latvia's unique risk and context, notably that of a major liquidated bank having facilitated ML schemes for foreign account holders. Operationally, this means that authorities pursue a significant amount of asset recovery based on NCBC, which accounts for 98% of all proceeds confiscated.

18. The effective use of provisional measures has led to over EUR 3 billion in assets seized, primarily tied to the bank liquidation case. During the assessment period, Latvia confiscated over EUR 300 million, mainly through NCBC, although high-profile cases pending judicial decisions have created a gap between seized and confiscated assets. While asset recovery networks are used effectively, there is room for improvement in confiscation and repatriation figures. Latvia also targets undeclared cross-border currency movements. Latvia's freezing and seizing statistics align with evolving risks, though confiscation results still reflect "risk profile one" due to the lengthy lifecycle of criminal proceedings.

Terrorist financing investigations and prosecutions (Chapter 9; IO.9, R. 5, 30, 31 & 39)

19. Competent authorities use different sources of information to identify and investigate potential TF activities. A number of initiatives have been undertaken in order to improve the understanding and interpretation of TF offences by LEAs, the Prosecutor's Office (PO) and judicial authorities. Several task forces and working groups (WGs) have also been created to improve and strengthen the system of TF identification and investigation. There were a few instances where possible TF activities were identified, based on intelligence from the FIU and the State Security Service. One of these cases led to an investigation, whilst for others, the authorities did not find sufficient evidence of TF to proceed with investigations. There has been no prosecution nor conviction for the TF offence in Latvia and therefore no occasion for prosecutors and the courts to develop case law on the evidence needed to secure a TF conviction. This notwithstanding, the authorities demonstrated that there is well established understanding that objective factual circumstances would be used to prove the intent and knowledge of the perpetrator of a TF offence. Latvia's 2021-2026 counter-terrorism strategy is an overarching strategy which also addresses TF issues, whilst measures to disrupt TF activities, when not practicable to secure a TF conviction, have been effectively applied in practice.

Terrorist financing preventive measures and financial sanctions (Chapter 10; IO.10, R. 1, 4, 6 & 8); Proliferation financing financial sanctions (Chapter 11; IO.11, R. 7)

20. Latvia has a robust legal and institutional framework ensuring timely implementation of targeted financial sanctions (TFS) related to TF and PF. Automatic enforceability of United Nations Security

Council Resolutions (UNSCRs) through European Union (EU) instruments, national laws, and co-ordinated efforts led by the Ministry of Foreign Affairs (MFA) and recently centralised under the FIU supports efficient application. While the recent institutional shift to the FIU as the national competent authority for sanctions implementation has strengthened potential for consistency, its full effectiveness has yet to be fully assessed. Despite Latvia's low TF and PF risk levels and absence of domestic UNSCR-based designations to date, authorities have clearly demonstrated operational readiness and capacity through effective enforcement of other sanctions regimes, including complex asset freezes. Risk-based supervision and oversight ensure that REs, particularly FIs and virtual asset service providers (VASPs), maintain a sound understanding and effective screening processes; however, certain DNFBPs, notably in the legal sector, show comparatively limited awareness of specific UNSCR obligations.

21. Latvia has assessed and identified NPO-sector vulnerabilities, implementing targeted risk-based measures broadly aligned with its low TF risk profile. The authorities have also conducted a thorough PF risk assessment, acknowledging minimal exposure related to UNSCR-based sanctions but recognising elevated risks from other contexts, confirming the operational capability to implement sanctions effectively should circumstances require.

ROADMAP OF KEY RECOMMENDED ACTIONS (KRAs)

1. Latvia underwent a mutual evaluation of its anti-money laundering/countering the financing of terrorism/countering proliferation financing (AML/CFT/CPF) measures in place during the on-site visit to the country from 4 to 15 November 2024. This evaluation was based on the 2012 FATF Recommendations (as updated from time to time) and was prepared using the 2022 Methodology.

2. The Mutual Evaluation Report identifies the strengths and weaknesses of Latvia's AML/CFT/CPF system, including both the level of effectiveness and the level of technical compliance, and makes recommended actions for improvement. The highest priority measures are identified as Key Recommended Actions (KRA) and are included in this KRA Roadmap.

3. The following presents the KRA Roadmap for Latvia as adopted by the joint FATF/MONEYVAL Plenary in June 2025. Based on effectiveness and technical compliance ratings, Latvia is placed in regular follow-up. This KRA Roadmap also serves as the basis for Latvia's follow-up process.

IO.1 (Assessment of risk, coordination and policy setting)

N/A

IO.2 (International co-operation)

N/A

IO.3 (Financial sector and virtual asset supervision and preventive measures)

N/A

IO.4 (Non-financial sector supervision and preventive measures)

a) The SRS should review and amend as necessary its current risk assessment methodology – addressing why the large majority of institutional risk assessments for the sectors under its supervision show a low ML risk, which is not aligned with national and sectoral risk assessments for those sectors. The methodology should clearly articulate how such institutional risk assessments and other factors subsequently form the basis for risk-based supervision.

b) The LCSA should collect additional information to assess and understand the institutional ML/TF risk present amongst those advocates that are subject to the FATF Standards and develop a fully risk-based approach to supervision that is supported by sufficient resources.

IO.5 (Transparency and beneficial ownership)

N/A

IO.6 (Financial intelligence)

N/A

IO.7 (Money laundering investigations and prosecutions)

N/A

IO.8 (Asset recovery)

N/A

IO.9 (Terrorist financing investigations and prosecutions)

N/A

IO.10 (Terrorist financing preventive measures and financial sanctions)

N/A

IO.11 (Proliferation financing financial sanctions)

N/A

PREFACE

This report summarises the anti-money laundering/countering the financing of terrorism/countering proliferation financing (AML/CFT/CPF) measures in place as at the date of the on-site visit. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of the AML/CFT/CPF system and recommends how the system could be strengthened.

This evaluation was based on the 2012 FATF Recommendations (as updated from time to time) and was prepared using the *2022 Methodology*. The evaluation was based on information provided by the country, and information obtained by the assessment team (AT) during its on-site visit to the country from 4 November to 15 November 2024.

The evaluation was conducted by an AT consisting of:

- Ms Jennifer HASLETT, Head of FATF and International Engagement, HM Treasury, United Kingdom (United Kingdom), financial expert
- Ms Gordana KALEZIC, Director of Directorate for supervision of AML/CFT compliance and financial and credit institutions consumer protection, Central Bank of Montenegro, financial expert
- Mr Lefteris KLIRONOMOS, Police Captain, Hellenic Police, Greece, legal expert
- Mr Ian MCDONALD, Associate Director of Financial Crime Strategy, Government of Jersey, law enforcement expert
- Ms Tatevik NERKARARYAN, Head of Legal Compliance Division, Financial Monitoring Centre, Central Bank of Armenia, legal and law enforcement expert

with support from the MONEYVAL Secretariat:

- Mr Lado LALICIC - Executive Secretary
- Mr Andrew LE BRUN - Deputy Executive Secretary
- Ms Kotryna FILIPAVICIUTE - Administrator
- Ms Maria GORECKA - Administrator
- Mr Michael MORANTZ - Administrator (FATF Secretariat).

The report was reviewed by the FATF Secretariat, Ms Amalia Hadjimichael (The Institute of Certified Public Accountants – Cyprus) and Ms Lia Umans (Scientific Expert - France).

Latvia previously underwent a MONEYVAL Mutual Evaluation in 2018 conducted according to the *2013 FATF Methodology*. The 2018 evaluation and 2019 follow-up reports (FURs) have been published and are available at https://www.coe.int/en/web/moneyval/jurisdictions/latvia.

The 5th round Mutual Evaluation concluded that the country was: compliant (C) with 6 Recommendations; largely compliant (LC) with 24; and partially compliant (PC) with 10. Latvia was rated C or LC with 4 of the following 5 Recommendations which were triggers for enhanced follow-up during the last round: R.3, 5, 10, 11 and 20).[1]

Based on these results, Latvia was placed in enhanced follow-up. Since its last evaluation, Latvia achieved 11 technical compliance re-ratings:

1. For the purposes of this report, a country will be placed in enhanced follow-up if any one of the following applies: (i) it has five or more PC ratings for technical compliance; or (ii) one or more NC ratings for technical compliance; or (iii) it is rated PC on any one or more of R.3, 5, 6, 10, 11 and 20; or (iv) it has a moderate level of effectiveness for six or more of the 11 effectiveness outcomes; or (v) it has a low level of effectiveness for one or more of the 11 effectiveness outcomes.

- Ten Recommendations upgraded from PC to LC: R.6, 7, 8, 10, 22, 26, 28, 32, 39 and 40
- One Recommendation upgraded from LC to C: R.2

Based on this progress, Latvia remained in enhanced follow-up for effectiveness deficiencies until June 2022.

Introduction to Money Laundering and Terrorist Financing Risks and Context

1. Located in Northern Europe, the Republic of Latvia (Latvia), covering over 64 589 square kilometres, is one of three Baltic States. Latvia shares European Union (EU) internal borders with Estonia to the north, Lithuania to the south, and external EU borders with 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. Latvia's gross domestic product (GDP) was approximately EUR 40 billion and GDP per capita was approximately EUR 21 000 in 2023. The official currency is the Euro (EUR) and the population of Latvia is 1.88 million.[2]

2. Latvia is a unitary parliamentary republic. According to the constitution of Latvia, the Parliament (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. In Latvia, judicial power is vested in district (city) courts, regional courts, the Supreme Court, and the Constitutional Court.

3. Latvia has been a member state of the EU since 2004 and a member of the Eurozone since 2014. The country is a member of numerous international organisations, such as the Council of Europe, the United Nations (UN), the Organisation for Security and Cooperation in Europe, the Organisation for Economic Co-operation and Development (OECD), the International Monetary Fund (IMF) and Interpol.

ML/TF Risks and Scoping of Higher-Risk Issues

Overview of ML/TF/PF Risks

4. Since 2017, Latvia's risk profile has undergone significant changes. The country is no longer a regional financial centre characterised by a banking sector heavily oriented towards servicing non-resident customers. In the banking sector – which accounts for over 70% of customers' assets - deposits of non-resident customers from outside the EU have decreased by 87%, credit turnover of customers with beneficial owners (BOs) from high-risk countries has decreased by 95%, and credit turnover linked to shell companies has decreased by 99% (comparing 2017 to 2023). This transformation has been driven by a strategic, high-level political commitment and an ambitious, well-coordinated action plan, rooted in an enhanced understanding of risks.

5. The ML/TF risks identified previously (until 2019) and exposure to cross-border illicit flows which arise from the former status of Latvia as a regional financial centre no longer pose a significant threat. In line with the considerable decrease in concentration of the foreign customer base in FIs and related cross-border movements of funds, the main ML threats now stem predominantly from predicate offences committed domestically. The main predicate offences are crimes related to the shadow economy (tax-related crimes, illegal movement of excise goods and narcotics, and smuggling), fraud, and corruption-related crimes. Also, there are ML threats related to proceeds generated by foreign criminal offences, mainly related to the laundering of funds generated by fraud and brought into Latvia physically or otherwise transferred to the Latvian financial system. Domestic risks remain generally stable with a slight downward trend.

6. Due to Latvia's geographical position as a transit point between east and west, its border with the Russian Federation and Belarus serves as an external frontier of the EU. This presents a potential risk for the cross-border transfer of financial assets such as cash, precious metals, and other valuables. Latvia can

2. Data source - 2024 Central Statistics Bureau of Latvia.

serve as a transit route for smuggled excise goods from the Russian Federation and Belarus to France, Germany, Scandinavia and the United Kingdom, as well as for narcotics trafficking in various directions. However, the risk situation at the border has changed recently due to the reduction in cross-border flows with countries of the Commonwealth of Independent States (CIS), attributed to EU sanctions and travel restrictions related to COVID-19. This has led to a decrease in the movement of goods and persons, altering the dynamics of cross-border smuggling and trafficking activities.

7. Due to Russia's war against Ukraine and related EU sanctions, EU sanctions evasion risk in Latvia has increased significantly since the last evaluation. PF risks are assessed as medium-low.

8. The shadow economy presents one of the main ML-related threats, especially when connected to tax-related crimes and smuggling in excise goods, along with the prevalent use of cash, including cross-border transportation of cash. The shadow economy continues to represent a relatively large proportion of Latvian GDP[3] (but with a tendency to decrease) and its size is close to the EU average.

9. TF risk is assessed as low. No racially/ethnically motivated terrorist groups operate in Latvia, and cross-border transfers have significantly decreased since the last evaluation. Currently, the State Security Service is involved in assessments of asylum seekers' requests due to concerns of potential exploitation of refugee flows by terrorist organisations to infiltrate the EU.

10. A notable reduction in vulnerabilities has been achieved since the last evaluation. The country's large banking scandal (Bank A) provided an opportunity to initiate far-reaching reforms, to establish effective public-private partnerships, to strengthen the capacity of competent authorities, and to establish and apply effective regulatory and enforcement action.

Country's risk assessment & Scoping of Higher Risk Issues

11. Since the previous mutual evaluation, Latvia has produced two national risk assessment (NRA) reports: the NRA covering the time period from 2017 to 2019 was published in 2020 (NRA1) and the NRA covering the time period from 2020 to 2022 was published in 2023 (NRA2). In drafting both NRAs, the World Bank methodology was used and adjusted to the needs and specifics of Latvia. The process of developing both NRAs was led by the Financial Intelligence Unit (FIU) Latvia. A wide range of stakeholders were involved through various working groups (WGs) on developing both NRAs and sectoral and topical (e.g., foreign legal persons' risk exposure) risk assessments. As part of the EU, Latvia is covered by the supranational risk assessments carried out by the European Commission in 2017, 2019, and 2022 and contributed to their development.[4]

12. The AT identified areas which required increased focus through an analysis of information provided by the Latvian authorities, including NRAs, and reliable open sources.

13. Banking sector. Given the liquidation of three banks since 2018, the AT closely looked into governance and internal control practices applied by banks, including implementation of AML/CFT measures and targeted financial sanctions (TFS) related controls - following the implementation of extended EU sanctions against the Russian Federation and Belarus. Additionally, the AT focused on the banking sector's efforts to reduce risks associated with non-resident customers and to terminate business relationships with shell companies.

14. ML investigations, prosecutions, and convictions. From 2021 to 2023, the number of prosecutions and convictions increased, including for ML offences committed by FI personnel. Among other cases, Latvia reported one bank case (Bank A), where high-level officials of the bank and the bank itself were indicted for aggravated ML, and the case is currently being adjudicated by a court. Latvia has also made important progress in identifying and addressing risk from foreign bribery offences[5] (see cases in IO.6

3. According to "Shadow Economy Index in the Baltic States" – Stockholm School of Economics.
4. The next risk assessment under the old EU framework is to be prepared in 2025. Latvia will also be involved in the EU risk assessment to be developed according to the new requirements of Directive (EU) 2024/1640 (the "6th AML/CFT Directive").
5. OECD Working Group on Bribery: Report on Latvia's progress in 2023.

and IO.7). At the end of 2023, the ex-head of the Latvian Central Bank was found guilty and sentenced to six years imprisonment by the Riga district court for accepting bribes (see case study in IO.7). Linked to this, the AT considered how the FIU adequately supports the identification and investigation of complex transnational ML schemes and examined recent institutional reforms in law enforcement and the judiciary and the way these have improved effectiveness, with a particular focus on capacity to conduct complex ML investigations and prosecutions. It examined whether progress achieved is commensurate with the main risks in the country.

15. Tax related offences and shadow economy. As tax-related offences are the only offences that carry a high risk of ML in Latvia and the shadow economy presents one of the main ML-related threats, the AT analysed progress made in reducing related risks and measurable results achieved so far.

16. Regional and transnational organised crime networks. Latvia's situation as a "gateway into the EU" means that it is exposed to risks from transnational organised crime groups (OCGs) involved in drug trafficking, cyber-crime, fraud, and smuggling. The ongoing war in Ukraine and the subsequent refugee and migrant labour flows into Latvia have also created conditions favourable to the involvement of OCGs in recruitment for illegal labour practices and human trafficking (notably human trafficking for forced labour and sexual exploitation). The AT examined the effectiveness of measures undertaken to address these risks.

17. Unintended consequences of liquidation of credit institutions. The wide-spread closure of Latvian credit institutions (e.g., Bank A) and movement of funds (with the likelihood that some would be illicit) were examined by the AT.

18. Residency by investment scheme. Whilst the risk level associated with foreign residency is decreasing, the AT examined legacy issues and measures taken since the liquidation of Bank A and related efforts to significantly reduce the potential for illicit non-European non-resident investment.

19. FIU-related reforms and their impact. Since the last evaluation, FIU Latvia has undergone several significant reforms to ensure that the FIU is independent and autonomous, and its competencies have been expanded (e.g. sanctions implementation). The AT examined the impact of these reforms on both operational and strategic levels.

20. DNFBP supervision and implementation of preventative measures. Taking into account the number and diversity of entities under the SRS's supervision, the AT examined the capacity of the State Revenue Service (SRS) to effectively oversee numerous different categories of DNFBPs. The AT focused on understanding the extent to which DNFBPs are involved in real estate transactions and scrutinised their level of implementation of AML/CFT preventative measures.

21. The areas which were identified for reduced focus due to low materiality and/or ML/TF risk were the following: life insurance providers (including intermediaries), private pension funds, and corporate loan and savings companies.

Materiality

22. Latvia's GDP was approximately EUR 40 billion and GDP per capita approximately EUR 21 000 in 2023. Stable economic growth in Latvia with rates exceeding the EU average continued until 2019 (the COVID-19 pandemic) with an average GDP growth of approximately 2.9% per year. Due to the significant negative impact of the pandemic on economic development, GDP shrank by 3.5% in 2020. Since then, GDP growth-decline fluctuations have been observed, with the economy becoming more stable in the second half of 2023. This is due to support measures by the Government and EU funds, as well as increased investment and private consumption.

23. Since 2019, the percentage of cash usage has decreased and fallen to 27%[6] in 2023. During the last

6. Share of cash transactions to total transactions.

five years, cashless payment has increased from 56% to 73%. The prohibition on making cash transactions above EUR 7 200 has also contributed to the decline in the use of cash.

24. Tax-related criminal offences (tax evasion, tax fraud, etc.) and the shadow economy estimated at 23% of GDP[7] are seen as significant challenges in Latvia.

25. Three commercial ports of Riga, Ventspils and Liepaja, as well as Riga Airport, serve for transportation. Riga and Ventspils are both "free ports", and Liepaja is one of three special economic zones, all of which offer reduced costs, easier customs procedures and other benefits to legal persons. Whilst the annual cargo volumes at the free ports are decreasing (due to Russia's war against Ukraine), turnover of legal persons in special economic zones is increasing, though they account for a very low share of total national business activity.

Financial sector, VASPS and DNFBPs

26. An overview of the financial sector, virtual asset service providers (VASPs) and designated non-financial businesses and professions (DNFBPs) is provided in the tables below.

Table 0.1. Overview of financial sector and VASPs (December 2023)

A- Type of entity - in descending order of size	B- Number operating	C- Number registered or licensed	D- Client assets under management (EUR)
Banks - Credit institutions	13	13	31 976 million
Collective investment schemes - Investment management companies	10	10	8 431million
Lenders/leasing (consumer credit service providers)	37	37	1 060 million (credit portfolio, consumer credits), 744 million (new consumer credits) 1 million (count, consumer credit agreements)
Other FIs - Private pension funds	7	7	811 million
Life insurance companies - Life and other investment linked insurance	6	6	736 million
Securities firms - Investment firms	9	9	700 million
Collective investment schemes - Alternative investment fund managers (AIFMs)	30	31	376 million
Exchange offices	15	15	204 million (volumes of currency bought and sold)
Money or value transfer services - payment institutions (PIs)	3	4	142 million
Other FIs - Savings and loans associations (Credit Unions)	29	29	19.4 million
Issuing or managing means of payment - Electronic money institutions (EMI), Postal remittance	4	7	8.7 million
Life insurance intermediaries (insurance brokers)	17	33	238 817
VASPs	3	7	360 230 (total value of transactions)

7. According to SSE Riga research data: https://www.sseriga.edu/shadow-economy-index-baltic-countries.

Table 0.2. Overview of DNFBP sector (June 2024)

A- Type of entity - in descending order of size	B- Number registered or licensed[8]
Outsourced accountants[9]	4 944
- firms	3 862
- individuals	1 082
Other independent legal professionals	1 870
- firms	1 487
- individuals	383
Sworn advocates	1 354 sworn advocates in total (490 sworn advocates providing services listed under R.22)
Real estate agents	1 304 (handling around 10 000 deals per annum)
Company service providers[10] (CSPs)	628
Dealers in precious metals and stones (DPMS)[11]	110
Sworn notaries	105
Gambling operators	20 (with annual turnover of around EUR 300 million)

27. The AT ranked sectors based on their relative importance in Latvia, their respective materiality and ML/TF risks. This approach was applied throughout the evaluation and was further used to weight positive and negative effectiveness issues aimed at informing conclusions and overall ratings.

28. The banking sector is weighted the most important in Latvia based on its materiality and risks. Banks hold 75% of all financial assets held by FIs supervised by Latvijas Banka (central bank). Whilst the NRA2 identified the banking sector as presenting a medium ML risk, the inherent risk exposure of banks is highest when compared to other FIs due to the nature of their services. The assessors also took into account recent closures/liquidations of banks and the legacy risks relating to servicing a large proportion of non-resident customers.

29. The securities sector is considered to be highly important since a number of investment firms (investment brokerage companies) operating securities trading platforms have been licensed and their business model includes co-operation with other financial service providers - lending companies. A significant part of lending companies conducts business activities in countries and regions with a higher risk (Africa, Asia, South America, etc.). Given the historically low number of STRs made by outsourced accountants (hereafter referred to as accountants) for ML, recent introduction of licensing requirements, and level of shortcomings identified in on-site examinations (which remains high compared to other sectors), accountants are also considered to be highly important.

30. Entities operating in the payment sector (EMIs and PIs), exchange offices, gambling operators, real estate agents (use of which is not mandatory in real estate transactions), sworn advocates (hereafter referred to as advocates), independent legal professionals and sworn notaries (hereafter referred to as notaries) are considered to be moderately important predominantly due to the nature of their services (with independent legal service providers having higher importance in this moderate band due to an ongoing ML investigation). Lenders, credit unions, leasing companies, insurance companies, VASPs and CSPs are considered to be less important, the latter because the substantial majority of company service

8. One DNFBP can simultaneously provide various services. Numbers include activities outside the scope of the FATF Standards.
9. An outsourced accountant is a qualified and experienced person who, on the basis of a written contract with an undertaking (except for a work-performance contract), pledges to provide or provides accounting services to the client.
10. The substantial majority of company service work is undertaken by advocates, and to a lesser extent by independent legal professionals and accountants. There are just ten standalone CSPs registered with the SRS with limited activity. Other CSPs are inactive or conducting activities outside scope of the FATF Recommendations, or both.
11. On the basis that it is not possible to use cash in Latvia for amounts exceeding EUR 7 200, in practice, just five DPMSs have accepted cash of EUR 10 000 or more through linked transactions during the period between 2019 and 2024, and the vast majority (which number around 110) are not subject to R.22 or R.23.

work is undertaken by advocates and to a lesser extent by independent legal professionals and accountants. There are just ten standalone CSPs registered with the SRS with limited activity.

Legal persons and legal arrangements

31. In Latvia, various types of legal persons can be formed: (i) those related to business activities, such as limited liability companies (LLCs), joint stock companies (JSCs), limited and general partnerships, co-operative societies, and European companies; and (ii) those created for representation of various interests – associations, foundations, trade unions, religious organisations, political parties, and European economic interest groups.

Table 0.3. Priority ranking of legal persons - 31 December 2023

Type of legal person	Total number registered	Total turnover in 2023 (EUR)	Number of STRs linked to legal persons (2023)	Proportion of foreign BO
LLC	131 993	69 446 million	4 838	8%
JSC	912	13 357 million	328	21%
Co-operative Society	1 482	801 958 230	0	0%
Association	24 765	560 685 321	85	2%
General Partnership	573	462 952 194	14	7%
European Company	9	418 960 681	2	25%
Foundation	1 606	110 150 253	8	3%
European Economic Interest Group	4	59 853 317	0	100%
Religious organisations	958	32 508 311	6	4%
Trade Union	357	14 982 077	0	0%
Limited Partnership	143	14 312 297	4	27%
Political parties	84	7 183 298	4	0%

32. The most prevalent form of a legal person is the LLC (81%). The second largest business-related legal person – JSCs - form only 0.5% of all legal persons registered in Latvia. A decline in new company registrations from 10 579 in 2018 to 8 707 in 2023 is noted.

33. Ownership of legal persons is predominantly domestic. The majority, i.e., 92% of BO of LLCs, are Latvians followed by Lithuanians and Estonians. A similar situation is observed with JSCs. The majority of new LLCs in 2022 were founded by Latvians, and foreign founders predominantly come from Estonia and Lithuania. Only a very small proportion of LLCs - 6.5% - have only other legal persons as shareholders, the BO of which are mainly Latvian (81%).

34. Approximately one-third of LLCs and JSCs have classified their economic activity as wholesale and retail sales. These industries were also ranked as the largest industries by the total amount of taxes paid in 2023 – EUR 4.31 billion (41% of total tax contributions by companies).

35. In the non-profit (NPO) sector, the dominant legal forms covered by the FATF Standards are associations and foundations. The sector is small and accounts only for 2 084 legal persons (or 1.3% of all registered legal persons), 97% of which have disclosed Latvian BOs. Payments and donations are predominantly domestic (98% and 87% respectively).

36. Foreign legal persons who perform taxable activities in Latvia must register branch or representative offices at the Enterprise Register (ER) or the SRS. Business activity without registration is monitored by the SRS and is subject to administrative penalties.

37. Legal arrangements cannot be created under Latvian Law, however, trustees of a foreign law trust (outside the EU) residing in Latvia are legally required to register within the ER. No such registrations have been made to date.

Structural Elements

38. Latvia has all of the key structural elements required for an effective AML/CFT/CPF system, including political stability, government, rule of law and a professional judiciary. Whilst well publicised past cases of banking failures, liquidations and high-scale corruption show systemic vulnerabilities, continuous high-level commitment by the state authorities to address ML/TF/PF issues noticeably mitigates risks.

39. As a member of the EU, Latvia is bound by EU law. EU Regulations apply directly and in their entirety in Latvia. EU Directives, which are also binding as to the results to be achieved, are transposed through domestic law.

Background and other Contextual Factors

40. Latvia has taken significant steps to improve its AML/CFT system since the last mutual evaluation by focusing on an overhaul of its financial system through substantial reforms. These reforms have bolstered Latvia's ability to prevent the misuse of its economy for ML/TF purposes and support Latvia's legal framework's compliance with all FATF 40 Recommendations. Latvia has a robust and efficient domestic co-operation and co-ordination mechanism in place, as well as strong political commitment to strengthen its AML/CFT/CPF system.

41. Since 2019, risks in the financial sector have notably decreased. As noted above, non-resident deposits have fallen significantly and there has been a decrease of 20% in total cross-border cash flows since 2019.

42. According to the Transparency International Corruption Perceptions Index, Latvia's corruption perception index has slightly improved in 2023 (ranked 36th). Financial exclusion is not a widespread issue in the country, since 96% of the population (resident natural persons) have a bank account (data for 2023).

43. In 2024, the IMF acknowledged that Latvia had made significant progress in strengthening its AML/CFT system,[12] e.g., AML/CFT risk-based supervision, availability of BO information of legal persons registered in Latvia and sanctions evasion risks.

AML/CFT/CPF strategy

44. Since the previous evaluation round, Latvia's Government has demonstrated a continuous political commitment to preventing ML/TF/PF. In pursuit of these objectives, the Government has endorsed two main strategies.

45. Between 2019 and 2023 the AML/CFT/CPF Action Plan served as the key national strategic document setting the following priorities: (i) strengthening supervisory capacity and ensuring effective management of the liquidation of Bank A; (ii) developing an effective information exchange system aimed at increasing effectiveness in the field of investigation; (iii) increasing human resources (including their expertise) in supervisory and law enforcement agencies (LEAs); (iv) introducing effective IT data management solutions; (v) enhancing the TFS system. The plan was continuously revised and updated. Between 2019 and 2024, several other strategic documents and topical action plans were developed targeting corruption, supervision, shadow economy, etc.

46. In early 2024, the National Strategy for the Prevention and Combatting of Financial Crimes was published. The objectives in this strategy are based on NRA2 and there are five strategic pillars: (i) strengthening national and EU security; (ii) identifying and recovering the proceeds of crime; (iii) strengthening the AML/CFT/CPF framework through digital transformation; (iv) strengthening Latvia's

12. Country Report No. 24/284 Republic of Latvia: 2024 Article IV Consultation-Press Release; and Staff Report, dated September 2024 (https://doi.org/10.5089/9798400287800.002).

international reputation; and (v) ensuring proportionality of AML requirements to promote competitiveness. Under pillar (v), a banking strategy has been adopted aimed at achieving a balance between proportionate application of regulatory requirements and limiting and preventing negative consequences.

47. In order to implement these strategic objectives, the new AML/CFT/CPF Action Plan for 2024 to 2026 has been developed as well as the National Counter-Terrorism plan. The AML/CFT/CPF Action Plan aligns with Government priorities by incorporating targeted mitigating measures. Budget allocation is an integral part of the AML/CFT/CPF Action Plan.

Legal & institutional framework

48. The AML/CFT/CPF Law is the central element of legislation for AML/CFT/CPF matters. Other relevant pieces of legislation include sectoral laws, the Criminal Law (CL), the Criminal Procedure Law (CPL), Law on International Sanctions, the Commercial Law, the Civil Law, Law on Execution of Confiscation of Criminally Acquired Property, and Operational Activities Law.

49. The institutional framework includes a large number of authorities, the most significant of which are:

Competent authorities

50. **Ministry of Finance (MoF)** – which is responsible for drafting and implementing policies and regulations in the AML/CFT/CPF Law. In addition, the MoF fulfils the secretariat role for the Financial Sector Development Board (FSDB) and is responsible for the Co-operation Platform of Supervisory and Control Authorities.

51. **Ministry of Justice (MoJ)** – which is responsible for drafting and implementing laws and regulations related to AML/CFT/CPF measures within its overall competence. The MoJ oversees the judicial system's role in prosecuting crimes and facilitates international co-operation.

52. **Ministry of Foreign Affairs (MFA)** – which is responsible for Latvia's policy on international sanctions.

53. **Ministry of the Interior (MoI)** – which is responsible for the development and implementation of policies and strategies aimed at preventing ML/TF/PF including preparing AML/CFT/CPF action plans to ensure that AML/CFT/CPF policy is consistent with identified risks.

54. **Latvijas Banka** (central bank) – which licences (registers) and supervises credit institutions, payment and EMIs, insurance companies, pension funds, investment firms, managers of alternative investment funds (AIFs), investment management companies, savings and loan associations, and currency exchange firms. In 2019, the former AML/CFT supervisor - the Financial and Capital Market Commission (FCMC) - was incorporated into the Latvijas Banka.

55. **Financial Intelligence Unit Latvia (FIU Latvia)** - implements the functions set out in R.29, co-ordinates national AML/CFT/CPF efforts (leading agency), and oversees TFS implementation.

56. **Prosecution Office (PO)** – which is responsible for the prosecution of criminal offences.

57. **State Police** – which is responsible for the investigation of the widest range of criminal offences, including theft, violent crime, economic crime (except for tax crime), which are not under the competence of other specialised LEAs.

58. **Corruption Prevention and Combating Bureau (CPCB)** – which is a central institution for the prevention and combating of corruption, as well as supervision of financing political parties.

59. **State Security Service** – which conducts intelligence operations and is tasked with identifying, assessing, and countering threats to the country's security and stability.

60. **State Border Guard (SBG)** – which is responsible for safeguarding the borders of Latvia, ensuring national security, and controlling the movement of people, goods, and vehicles across its borders.

61. **State Revenue Service (SRS)** – which is the tax authority, licenses accountants, and supervises, inter alia, financial leasing (if provision of services is not subject to licensing), VASPs, real estate agents, DPMS, independent legal professionals, accountants and CSPs.

62. **Tax and Customs Police Department (TCPD)** – which is a specialised law enforcement agency responsible for the detection, prevention and investigation of criminal offences and other violations of law in state revenue and customs matters (operates within the SRS).

63. **Consumer Rights Protection Centre (CRPC)** – which registers and supervises consumer credit providers.

64. **Lotteries and Gambling Supervisory Inspection (LGSI)** –which is the licensing and supervisory authority for gambling activities.

65. **Enterprise Register (ER)** – which is responsible for registering enterprises (including legal persons), merchants, their subsidiaries and representative offices in Latvia. It maintains BO information for legal persons and, in some cases, legal arrangements.

66. **Latvian Council of Sworn Advocates (LCSA)** – which is responsible for accreditation of advocates, ensuring their compliance with legal and ethical obligations (including AML/CFT compliance), and addressing disciplinary matters.

67. **Latvian Council of Sworn Notaries (LCSN)** – which oversees the activities of sworn notaries in Latvia (including AML/CFT compliance).

Co-operation mechanisms

68. **Financial Sector Development Board (FSDB)** – which is a high-level co-ordinating body aimed at improving co-operation between public institutions and the private sector in the prevention of ML/TF/PF.

69. **Crime Prevention Council (CPC)** – which is a collegial body that co-ordinates efforts among relevant stakeholders to prevent crime.

70. **FIU Advisory Board** – which co-ordinates the FIU's co-operation with institutions responsible for pre-trial investigation, prosecution, court supervisory authorities, ministries and reporting entities (REs).

71. **National Criminal Intelligence Model (NCIM**) – which establishes a co-operation framework among various stakeholders aimed at optimising resources of law enforcement and enhancing their operational efficiency.

72. **Sanctions Coordination Council (SCC)** – which ensures coherent application of sanctions-related measures.

73. **FIU Co-operation Coordination Group (CCG)** – which is a public-private (and public-public) co-operation platform that facilitates operational activities and collaboration among various stakeholders involved in combating and preventing ML/TF/PF, and related criminal activities.

74. **Co-operation Platform of Supervisory and Control authorities** – which facilitates the exchange of information amongst FI, VASP and DNFBP supervisors.

75. At EU level, the relevant authorities with competence in AML/CFT are: (i) the Authority for Anti-Money Laundering and Countering the Financing of Terrorism **(AMLA)**[13] - entrusted with exercising

13. While AMLA was legally established in June 2024, it will commence carrying out its tasks progressively as of June 2025 (with direct supervision starting in 2028).

direct supervision over certain FIs, ensuring convergence of supervision for other REs and co-ordination and support of EU FIUs; and (ii) the European Public Prosecutor's Office **(EPPO)** - responsible for investigating, prosecuting and bringing to judgment the perpetrators of, and accomplices to, criminal offences affecting the financial interests of the EU, including ML. In that respect, the EPPO undertakes investigations, carries out acts of prosecution and exercises the functions of prosecutor in the competent courts of member states, until the case has been finally disposed of.

76. The European Central Bank **(ECB)** is the prudential banking supervisor in the Banking Union,[14] working together with the prudential supervisory authorities of participating member states within the Single Supervisory Mechanism **(SSM)**.[15] It is therefore another important actor in the institutional framework. While not an AML/CFT supervisor, the ECB carries out certain functions which are relevant both to AML/CFT and for prudential supervision purposes, such as granting or withdrawing licences for all credit institutions established in the Banking Union and carrying out suitability assessments of members of management bodies of significant credit institutions. In this context, the ECB co-operates with relevant AML/CFT authorities within the EU/ European Economic Area (EEA).

77. Other EU-level bodies and agencies have a supporting role, including Europol and Eurojust.

Preventive measures

78. The AML/CFT Directive[16] sets out AML/CFT preventive rules, including the scope of REs, provisions on the assessment of risks, CDD measures and record keeping requirements, BO transparency requirements, reporting obligations, as well as the powers and tasks of FIUs and supervisors and information exchange and co-operation between authorities.[17] Traceability of fund transfers is regulated under Regulation (EU) 2015/847.[18]

79. Preventative measures are set out in the AML/CFT/CPF Law and are broadly compliant with the FATF Standards. Supervisory authorities have issued additional guidance documents to assist FIs and DNFBPs with the full implementation of AML/CFT/CPF requirements.

80. The following three types of entities are not subject to the AML/CFT/CPF Law: (i) stock exchange (only organises transactions and does not engage in cash and securities settlements which are carried out by the Central Securities Depositary); (ii) Central Securities Depository (only settles securities on and off-exchange for members of the depositary who are licensed financial institutions (FIs)); and (iii) crowdfunding platforms (the risks are mitigated by requiring crowdfunding service providers to engage an authorised payment service provider for payments' facilitation and/or to obtain a payment institution (PI) licence). The AML/CFT/CPF Law extends to some activities not covered by the FATF Standards, such as auditing, tax advice, and cash collection.

Supervisory arrangements

81. Section 45 of the AML/CFT/CPF Law defines supervisory authorities responsible for overseeing compliance of FIs, VASPs and DNFBPs. Relevant authorities include Latvijas Banka, the SRS, CRPC, LGSI, LCSA, and LCSN.

14. The Banking Union currently comprises 21 member states: Euro Area member states and those other member states that establish close co-operation.
15. The SSM refers to the system of banking supervision in the Banking Union. The SSM itself comprises the ECB and the national supervisory authorities of participating countries.
16. Directive (EU) 2015/849 as amended by Directive (EU) 2018/843 (the "5th AML/CFT Directive").
17. A new Regulation and Directive came into force (but not effect) on 9 July 2024 and Directive (EU) 2015/849 will be replaced by Regulation (EU) 2024/1624 (the "EU AML/CFT Regulation") and Directive (EU) 2024/1640 (the '6th AML/CFT Directive').
18. Subsequently replaced by Regulation (EU) 2023/1113.

International co-operation

82. Latvia has a comprehensive framework for international co-operation, with incoming and outgoing mutual legal assistance (MLA) and extradition requests touching upon a wide range of geographies. There are three competent institutions appointed in Latvia responsible for handling international co-operation requests depending on the state of criminal proceedings: (i) in the pre-trial stage - the PO examines and decides on the request of a foreign country; (ii) up to the commencement of a criminal prosecution - the State Police; and (iii) after transfer of a case to a court - the MoJ.

83. Due to its strategic location between east and west, Latvia is a transit route for smuggled excise goods. During the review period, cash controls at the borders were significantly strengthened, resulting in an increase in identified criminal offences relating to illicit cash movement across the land border with the Russian Federation and within the Baltic States.

84. In the period between 2020 and 2022, cross-border financial flows with CIS countries and offshore jurisdictions (as defined by the authorities) have sharply decreased (by 89% and 93% respectively). At the same time, payments with Lithuania – the largest foreign trade partner – have doubled, due to Latvian residents seeking business relationships with Lithuanian FIs.

85. The most significant of Latvia's international co-operation partners are - Lithuania, Estonia, Poland, Germany, and the United Kingdom. Between 2019 and 2022, FIU Latvia established and chaired a specialised Task Force aimed at investigating a well-publicised banking failure case which brought together representatives from 25 countries.

Chapter 1. Assessment of Risks, Co-ordination and Policy Setting

The relevant Immediate Outcome considered and assessed in this chapter is IO.1. The Recommendations relevant for the assessment of effectiveness under this chapter are R.1, 2, 33 and 34 and elements of R.15.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Latvia's approach to identifying, assessing and understanding ML, TF and PF risks is characterised by a genuine curiosity, and a commitment to integrate a wide variety of data sources to generate and maintain an evolving, continuous and an in-depth understanding of its past and present ML/TF/PF risks.

b) The NRA process acts as a milestone in documenting and externally communicating an overview of the country's evolving risk environment. Notwithstanding, Latvia has made improvements to its NRA processes which have resulted in a continuously adaptive and responsive understanding of the country's ML and TF risks across agencies, supervisory and control authorities (SCAs) and the private sector, rather than a reliance on the NRA itself.

c) There has been a marked shift in the ML risks faced by Latvia over the assessment period, as well as a significant reduction in the risk appetite of Latvian authorities. This is reflected in the dramatic change in Latvia's economy and the provision of professional services away from foreign deposits and non-residents to domestic and geographically proximate clients.

d) The activities of competent authorities and SRBs are aligned with the findings of the NRAs through the implementation of individual AML/CFT/CPF action plans, which sit beneath the overarching national Action Plan. This is enhanced by robust interagency collaboration on strategic and operational levels aided by the well-developed public-private partnership mechanism.

e) Latvia has a small number of exemptions from applying AML/CFT requirements, primarily based on the availability of information from EU Member States, including the removal of dual reporting requirements. Risk assessments and case studies confirm that these exemptions are aligned with risks.

f) Latvia has a well-functioning mechanism to co-ordinate both policy and operational responses to its risks, which are underpinned by a detailed and transparent resourcing and budgeting process.

Key Recommended Actions (KRA)

N/A

Other Recommended Actions

a) Authorities should utilise the detailed knowledge of the geographic risk that Latvia faces, as captured in the NRA, to better articulate the specific geographic risks that should inform the application of risk-based measures, by REs.

b) Authorities should continue to monitor the impacts of recent reforms in specific sectors, e.g. real estate and construction business, to understand the residual risks once mitigation measures have come into effect.

c) Authorities should continue to utilise the CCG model, building on the success for both analytical and operational purposes.

Overall Conclusions on IO.1

Competent authorities and other relevant stakeholders have a robust and comprehensive understanding of the ML/TF risks that the country faces. Inclusiveness of the NRAs processes and amount of information/data analysed has enabled proper, accurate and realistic identification and assessment of Latvia's past and current ML/TF threats and vulnerabilities. Whilst NRA2 effectively outlined the shift in Latvia's risk profiles throughout the assessment period, the NRA processes overall are underpinned by an evolving and responsive ecosystem of risk evaluation through a wide range of sources and close collaboration and co-ordination amongst authorities. There is room for minor improvements in some areas in articulating the comprehensive understanding of risks.

Latvia has demonstrated a clear political commitment to tackling ML and TF, and to robustly identifying and resourcing the necessary actions to achieve this. There is a clear nexus between the conclusions of NRAs and the subsequent AML/CFT/CPF action plans, which along with supporting budget documents, are regularly reviewed and monitored.

The results of NRAs and standalone assessments are comprehensively communicated to FIs and DNFBPs, and private sector representatives are central in domestic co-ordination and development of risk understanding.

The development of the CCG is a highly effective platform for co-operation and has resulted in a broad range of tangible operational outcomes.

Latvia is rated as having a high level of effectiveness for IO.1

86. The risk and context in Latvia have changed considerably since its last MER. There has been significant and sustained high level political commitment to tackling Latvia's historic and legacy risks. This has resulted in a fundamental change in how Latvia approaches financial crime at all levels, as well as the nature of business served by Latvia's economy. This increased political focus and governance have resulted in significant resources being directed towards tackling financial crime. Financial crime has also developed into a professional specialism within the law enforcement and justice community with dedicated specialist resourcing, for example the establishment of the Economic Affair Court which deals with ML cases.

87. From the more historical perspective, the 2018 MER findings in relation to Latvia's risk understanding concluded that despite some authorities broad understanding of the then risks (such as the FIU and the FCMC), there was uneven and overall inadequate appreciation of the potentially ML-related cross-border flows of funds. A large number of recommended actions were thus put forward, ranging from a need to increase participation of competent authorities, improved understanding of major ML threats and vulnerabilities, harmonisation of policies and action plans with a view to them being aligned with emerging risks, improvements of private sector awareness of risks, and many others.

88. Since its 2018 MER, Latvia has enacted multiple changes in its AML/CFT policy-making, co-ordination and risk understanding. These changes include increased participation of competent authorities in this area, improved understanding of ML threats and vulnerabilities, harmonisation of policies and action plans to better align with emerging risks, and improvements to private sector awareness. While the legal framework was strengthened to further establish the FIU as a leading agency in carrying out NRA and related activities, a number of other reforms were also carried out. These are discussed in the following sections of this Immediate Outcome.

1.1. Country's identification, assessment and understanding of its ML/TF risks

1.1.1. ML risks

89. Latvia has a well-developed understanding of its historic risks ("risk profile one"), the main current risk tied to domestic offences ("risk profile two"), as well as risks emanating from criminal offences committed abroad and imported into Latvia ("risk profile three"). Latvia has conducted two NRAs within the assessment period: NRA 2017-2019 (NRA1) and NRA 2020-2022 (NRA2).

90. Both of these reports are publicly available. Procedures applied, involvement of relevant authorities, the way the NRAs findings and results were disseminated and subsequent efforts to communicate them to all REs present a matter of good practice which enabled Latvia's key players in the AML/CFT/CPF field to profoundly analyse, acknowledge and understand the relevant risks and their underlying factors.

91. Latvia goes beyond the requirements of the FATF standards in assessing its risk, and this is particularly the case with the PF related risks. NRA reports are supplemented with a number of annual assessments on emerging risks and on virtual assets, as well as with targeted risk assessments. Both NRAs used the World Bank methodology, with additions on a number of areas to reflect local risk and context. Approximately 30 different entities and agencies were involved in NRA2, with an average of two to four persons for each entity. Prior to the publication of the NRA all entities involved must sign-off on the content of the report.

92. Authorities demonstrated clear improvements in the NRA process between NRA1 and NRA2. The main procedural change between the two has been a greater devolvement in responsibility and leadership for analysis from the FIU to individual LEAs, and to the SCAs for sectoral risk assessments. NRA2 was driven forward by 11 WGs. Divisions of the WG responsibilities/competencies were based on different criteria. The first criterion set up the basis for creation of five WGs, that focused on the nature of threats/predicate crime that each WG would discuss and analyse.[19] The evolving nature of approaching and analysing threats, vulnerabilities and overall risks for purposes of NRA2, have clearly added value to the process as it led to a stronger engagement by the competent authorities, ultimately leading to a better understanding and ability to mitigate the emerging risks. Private sector representatives were also included in some of these WGs, as participants. For example, the authorities referred to the participation and contributions made by the Latvian branch of Transparency International (organisation "DELNA") to the WG on corruption related criminal offences.

93. A second group of three WGs focused on sectoral risk assessments.[20] The authorities emphasised that NRA2 included only brief summaries of each sector's risk assessment, whilst each SCA conducted a more comprehensive sectoral risk assessment periodically (in a one to three-years period), with participation of the private sector.

94. The remaining three WGs dealt with (i) NPO and legal persons' risk assessments, (ii) TF and PF risk assessments, and (iii) ML risk scenarios. The latter WG was atypical, with the relevant sections of the NRA composed based on the work of all other WGs.

19. (i) threats and ability to combat corruption; (ii) threats posed by tax offences and ability to combat that phenomenon; (iii) threats posed by drug trafficking offences and capacities to combat them; (iv) threats posed by property offences and ability to combat them; and (v) threats posed by autonomous ML, including risks posed by cash transactions.
20. (i) credit institutions, (ii) financial institutions and (iii) the non-financial sector.

95. The above list of areas examined for identifying ML/TF risks is not exhaustive. Authorities continuously strengthen their risk understanding; examples include the (i) FIU's assessment of ML/TF risks posed by virtual assets and (ii) the annual report on overall trends in criminality and the associated risk levels, compiled by the State Police, but featuring insights from all LEAs, FIU, and the PO. These assessments were also examined as part of NRA2 and their relevant findings feature therein.

96. The distribution of responsibilities and inclusive approach positively contributed to the NRA process. The process effectively harnessed the leadership and subject-matter expertise of different institutions and enabled a more comprehensive and holistic assessment of risks. This has been demonstrated throughout the on-site discussions encompassing not only the issues relevant for IO1, but also other IOs (such as IO3, IO7, and IO8). Authorities also outlined that this devolvement of responsibility made the overall NRA process more efficient - significantly reducing the time taken to produce NRA2. This has been supported by a move away from manual data collection to automated data collection across a number of data points. The CPCB, State Police, the SRS and Latvijas Banka demonstrated a consistent methodology amongst the WGs for identifying the data to collect, which is supported by a codified guidance document on producing the NRA.

97. Risk assessment processes confirm that the main ML risks have shifted from the laundering of foreign proceeds of crime to domestically generated proceeds. This conclusion is further supported by a general trend in the reduction of banking and other services for non-resident natural and legal persons. For example, there has been a reduction in non-EU deposits within Latvian FIs of 87%, from EUR 7.17 billion to EUR 0.93 billion during the assessment period. This is mirrored in the nature of STRs being received, which indicates that the primary risks are now domestically generated. At the time of the last MER, 50% of STRs were for stand-alone ML (which included cross-border transfers), and this has now reduced to 22% of STRs, with almost 80% of STRs referring to specific predicate offences.

98. As noted above, authorities identify three risk profiles:

- Risk profile 1: the risks Latvia faced prior to 2018. As a regional financial centre, Latvia provided financial and to some extent non-financial services to non-resident clients, with a high volume of non-resident deposits.
- Risk profile 2: the risks emanating from Latvia's current economy which is largely domestically and regionally focused and predominantly serves domestic and resident clients. In this risk profile the main risks emanate from the shadow economy (tax and excise related offences, drugs related offences), fraud, and corruption.
- Risk profile 3: the risk of ML generated as a result of criminal offences committed abroad, mainly fraud and stand-alone ML which are imported into Latvia or transferred to the Latvian financial system.

99. Risk assessments draw on a wide variety of sources of information, including financial intelligence, existing risk assessments, external and public reporting, as well as interviews with competent authorities, market participants, civil society and representative groups. Authorities outlined a holistic approach in using both qualitative and quantitative data and demonstrated that they could identify areas where conclusions drawn from statistical data did not align with the qualitative information gathered from law enforcement and SCAs. For example, the CPCB noted that investigative and prosecutorial data related to ML associated with corruption did not align with the STR data. Authorities drew reasonable conclusions to explain this and summarised that the majority of domestically generated proceeds of corruption were being laundered overseas. This resulted in an action item within the AML/CFT/CPF Action Plan for authorities to further develop their understanding of overseas laundering methodologies linked to corruption. Similarly, authorities demonstrated that where data collected during the NRA process indicates an anomaly, this is identified, and additional work is undertaken to understand the context before determining risk ratings. For example, during NRA2 authorities enquired on an unexpectedly high volume of donations to a Latvian NPO from a higher risk country. Consequently, the relevant supervisor examined the specific transaction, determined it to be low-risk, and the authorities' overall finding that the NPO sector is low risk was not challenged.

100. NRA2 identified that the ML threats primarily relate to tax offences, with excise offences (including smuggling), drug offences, corruption and fraud also being material. Domestically generated proceeds now pose a considerably higher threat than foreign generated proceeds. NRA2 identified a reduction in national vulnerability to ML, mainly driven by increases in investigative and prosecutorial capacity as well as increases in domestic co-operation and access to BO information. Sectors identified as posing the highest ML risk (medium-high) are investment firms, accountants, lottery and gambling operators, real estate agents, and tax advisors. Notably, credit institutions are identified as presenting only medium risk (see also IO.3). Assessment and ratings attached to these risks appear reasonable and well grounded. The NRA includes a detailed list of sectors' vulnerabilities with the highest risk sectors being analysed in detail in terms of their business models, types of transactions, and STR reporting. The analysis also includes risks posed by five free trade zones (three special economic zones and two freeports). The import, store, trade, production, and re-export of various goods and services were thus analysed with respect to key ML threats and vulnerabilities. Data was gathered on cargo volumes and turnover to better identify ML risks. The quality of analysis and mitigating measures applied confirms that the authorities properly understand the risks posed by free trade zones. They also ensured that the risks posed by free trade zones are properly monitored given the possible changes in this specific risk environment.

101. Furthermore, developments related to a Bank A under liquidation also informed Latvia's evolving understanding of risks. The liquidation process resulted in increased supervisory controls and interagency co-operation. The FCMC (now Latvijas Banka) required liquidators to develop the AML/CFT/CPF methodology for the AML/CFT compliance monitoring process of the bank's creditors. The measures of the methodology included enhanced due diligence (EDD), independent audit reviews, transaction monitoring, and sample testing of client files. The FCMC imposed strict requirements for payouts from the deposit guarantee fund, disbursements to creditors and asset sales.

102. The FIU acquired data on all transactions within the bank covering the period from 2013 which resulted in creating tailored datasets for the 25 most affected jurisdictions demonstrating the financial flows originating from and coming to the bank under liquidation accounts, beneficiaries from these countries and other data. The most prevalent typology observed was the use of shell companies in the United Kingdom and Canada when effecting transfers. The actions taken by the authorities in response to these risks are further discussed (through case studies and related analysis) under IOs 2, 3, 6, 7 and 8.

103. Authorities outlined that the results of the NRA2 were broadly as expected. Authorities attribute this to a more proactive and continuous risk identification process, the utilisation of automatically collected data that underpins the production of NRAs, as well as greater day-to-day inter-agency engagement. One example of more routine examinations of data is the monitoring of cross-border flows by Latvijas Banka, which was previously undertaken annually but is now monitored monthly. Authorities provided a range of examples demonstrating how they had used this data to identify anomalies that indicated new or increased risk. This information was then used to inform greater awareness in the private sector, and to ensure EDD was undertaken in relevant circumstances.

104. Authorities demonstrated that during the assessment period they have been able to identify areas where their risk understanding is less well developed and the steps that have been taken to address these gaps in risk understanding and put in place risk mitigation measures. For example, following increased scrutiny of residency by investment schemes within the EU, authorities undertook a standalone assessment of Latvia's residency by investment scheme (outside of the NRA process). This included a review by the FIU of all applicants between 2019-2024 and a review of operational cases involving real estate purchases made by those who had obtained residence through investment in real estate. As a result of this assessment additional controls were put in place, including the FIU becoming an authority with responsibility to review proposed investments by applicants.

105. In relation to this, it is worth mentioning that the construction sector consistently ranks as the economic sector with the highest share of the shadow economy. Risks related to high cash turnover and unreported activity in construction business as well as threats posed in terms of tax evasion by those involved in construction and real estate business are well recognised and articulated in the NRA2. Notwithstanding this

and facts and trends discussed in NRA2, it appears that both the private sector and the competent investigative authorities would further benefit from the presentation of these risks through practical examples and lessons learnt from them.

106. From an overall perspective of risk analysis and their understanding, information and sources provided to the AT, it can be concluded that Latvian authorities demonstrate an agile and proactive approach to identifying emerging risks, as well as working with key international partners to understand regional risks (risk profile 2). For example, in 2023, the FIU partnered with the Estonian and Lithuanian FIUs to examine regional cross-border cash flows, documenting a number of key risks as well as recommendations for mitigation measures.

107. Risks assessment processes covered a broad range of areas to identify the country's key ML threats and vulnerabilities. The analyses presented in the NRAs are comprehensive and detailed enough, with reasonable and well-grounded conclusions on key risk areas. Taking into account the methodology applied in carrying out the NRA exercises, level of involvement of competent authorities, the multi-agency approach, quality and quantity of data analysed and cross cutting nature of some specific analysis (such as the one in relation to the liquidation of Bank A), it is apparent that the NRAs result from a thorough and far-reaching understanding of ML/TF risks by the Latvian authorities.

108. Private sector representatives from across FIs and DNFBPs broadly agreed with the findings of the NRA and understood how the identified risks impacted their business areas. There was some disagreement in the real estate sector, accounting and gambling sectors about the medium-high risk rating assigned to the sectors, taking account of vulnerabilities that have reduced since completion of NRA2. Estate agents noted the change in risk profile over the assessment period, including a reduction in property purchased by foreign nationals, and a significant reduction in the purchase of property for the purposes of gaining residency through Latvia's investment programme. The medium-high risk rating in NRA2 is reflective of the legacy risks in the real estate sector, and that there is still a comparable level of foreign national investment into real estate: EUR 152 million in 2023 compared to EUR 209 million in 2018. Despite the 98% reduction of property purchased through the residency by investment scheme between 2014 and 2023 and the mitigating measures put in place since 2022 in relation to both the residency by investment programme and the real estate sector as a whole, Latvian authorities should maintain their heightened focus on these areas and continue to periodically reassess related ML risks.

1.1.2. TF Risks

109. In NRA2, Latvia assessed the threat of terrorism to be low and TF threat as also low. To reach this conclusion, authorities carried out detailed analysis and considered the nexus between international terrorist organisations and Latvian nationals, domestic data on asylum seekers from high-risk countries and illegal border crossings, the vulnerability of the financial services sector by analysing cross border payments both by volume and specifically related to higher risk countries, as well as a range of other typologies associated with TF. In addition, authorities undertook an extensive analysis of all NPOs financial activity. Overall, the AT found the TF risk rating to be justified and well grounded.

110. Authorities conducted a large-scale exercise to identify and understand TF risks. Competent authorities used a wide range of quantitative data – STRs, statistics gathered by supervisors (inflows and outflows to high-risk countries (including neighbouring countries)), BO details, and information from the State Security Service on their threat assessments on topics such as the radicalisation of individuals, migrants entering Latvia, and activities of terrorist organisations (such as Al Qaida and Daesh) and their eventual connections with individuals, groups or entities in Latvia.

111. In support to this process and with the aim to further strengthen inter-institutional co-operation, a specialised CFT Task Force has been established under the CCG. Under the leadership of the FIU, other relevant agencies (State Security Service, Latvijas Banka, Customs and SRS) form a part of the Task Force. Its activities include (i) analyses of cross-border payments to high-risk jurisdictions and identification (ii) monitoring of activities of Latvian legal persons with BOs from these countries; and (iii) examination of

suspicions on TF and their referral to criminal investigation or other regulatory action. In addition, it co-ordinates the monitoring of NPOs that fall within the FATF definition and applies risk-based mitigation measures to them.

112. Authorities also confirmed their proactive engagement and analysis on the private sector when assessing TF risks; the sector's TF related reporting against inflows and outflows related to high-risk jurisdictions was analysed. Given the Latvian context, this analysis also included reporting on sanctions evasions and was then further used to inform guidance for private sector reporting on cross-border flows. Notwithstanding, STR reporting for TF has been very limited: seven reports between 2021-2022, covering on average 20 transactions. Whilst the low TF risk profile and limited exposure to higher risk countries and typologies could justify the low number of STRs, this area needs ongoing attention and timely action by the competent authorities in case of any changes in the TF risk environment. Discussions held on-site confirmed that the competent authorities, and mostly the State Security Service and the FIU, remain vigilant and are aware of this, as also evidenced through the work of CFT Task Force.

1.2. National policies and activities to address identified ML/TF risks

1.2.1. Policies and activities to address ML risks

113. Latvia has a well-functioning and clearly documented governance mechanism to co-ordinate its policy and operational activities, as well as to allocate budget and resources, in line with its ML and TF risks. At the conclusion of both NRA1 and NRA2, action plans with specific tasks and measures were developed to address the identified risks and priorities. These AML/CFT/CPF action plans were adopted by the CoM. The AML/CFT/CPF Action Plan is also used for setting funding and resources. Each agency and department must also have their own resulting action plan and report back to the MoI, which is tasked with monitoring the national AML/CFT/CPF Action Plan and reporting regularly to the FSDB. The FSDB meets no less than twice a year, but on average meets quarterly.

114. Whilst the AML/CFT/CPF action plans and governance framework provide clear priorities and lines of accountability, they do not constrain agencies and departments from being agile in risk identification and mitigation.

115. Latvia's legislative programme supports national AML/CFT/CPF policies and implements measures to address identified risks. For example, sequential legislative amendments have extended BO reporting requirements over the review period, initially for domestic legal persons, then to certain foreign legal persons, and then to a further class of foreign legal persons in 2024. Similarly, in April 2024, Latvia established a dedicated function within the FIU to oversee the implementation of UN and non-UN sanctions, recognising its growing risk exposure (in relation to non-UN sanctions).

116. Monitoring of STRs when typology reports are published shows an upward trend in reporting, indicating that REs use information within reports as part of their risk understanding and direct resources towards identified risks. For example, following the publication of the "Indicators and case studies of corruption" report in 2021, related STRs increased by 64% (67 to 104).

1.2.2. Policies and activities to address TF Risks

117. Despite the risk from TF being assessed as low, authorities continuously deepen their understanding of actual and potential future TF risks, as well as develop their professional expertise on TF, as part of their 2024-26 Action Plan. This includes using the bi-annual meeting of the Expert Advisory Council of the Counterterrorism Centre to discuss developments in CFT and their application in the domestic context. Latvia also has a dedicated CFT Task Force under the CCG legal framework devised for both strategic and operational purposes.

1.3. Exemptions, enhanced and simplified ML/TF measures

118. Latvia has a very limited number of AML relevant exemptions in place. The exemptions that are in place are aimed at avoiding dual reporting/registration requirements across EU Member States. For example, trusts that are subject to disclosure requirements in other EU members states are exempt from reporting requirements with the Latvian ER (see also IO.5). These exemptions are driven by the avoidance of dual reporting, rather than on the basis of a documented AML/CFT assessment. This is relevant given that Latvia's NRAs identify foreign ML risks as primarily emanated from EU and geographically proximate countries. However, overall, the exemptions in place do not relate to areas identified nationally as presenting a higher risk and should have, at most, a minor impact on effectiveness.

119. NRA2 comprehensively outlines geographic links for each predicate offence. This is key given the nature of STR reporting and the specific risks that Latvia faces. However, despite a commendably clear and detailed documentation of geographic risk for each predicate offence, at the time of the onsite visit there was some unclear public articulation of risk outside of the NRA. At the time of the onsite the FIU publicly identified "jurisdictions of increased risk" (AML/CFT/CPF Law, Section 11(1) (3) point 2) as "high risk countries", including:

- The European Commission's list of third countries that are insufficiently combating ML and TF;
- FATF determined high-risk jurisdictions and FATF jurisdictions under increased monitoring;
- Countries with a high level of corruption identified (Transparency International - Corruption Perceptions Index); and
- Countries specified in Latvian legal acts.

120. Collectively, these encompassed a large number of countries, and did not align with the geographic risks identified in NRA2. These lists were also used in non-public thematic assessments when determining geographic risk, for example in relation to foreign legal persons, and so assessments may not truly reflect Latvia's specific geographic risk. The lists were also not reflective of the feedback received from authorities during onsite interviews that risks primarily emanate from within the EU and geographically proximate countries, few of which appear on any of these lists. Some authorities displayed a more nuanced understanding of geographic risk, and Latvijas Banka advised that it maintains its own independent list of geographic risks as a result of feedback from the private sector. The authorities are encouraged to draw on more detailed knowledge of geographic risk relating to predicate offences and related ML typologies in order to better communicate the specific geographic risks faced by Latvia and to inform the application of enhanced measures, such as EDD by REs. However, since the time of the onsite, the FIU has updated its external communications to more clearly articulate the nuances of the specific risks faced in Latvia, reducing the over reliance on these lists. This is a positive development, however as this occurred after the time of the onsite, it is not possible to assess the impact of this change.

1.4. Objectives and activities of competent authorities and SRBs

121. LEAs and other relevant authorities' objectives are in line with the ML and TF risks identified in NRA2 and are consistent with the national AML and CFT policies outlined in the Action Plan. This is ensured by each agency and department having its own action plans, which implement the national Action Plan.

122. LEAs demonstrated a risk understanding consistent with NRA2, as well as a good knowledge of the specific data that underpinned the analysis and conclusions of the NRA and were clearly sensitive to evolving risks and emerging threats. This understanding supports LEAs in aligning their activities, including prioritisation and allocation of resources, in line with the risk areas identified. Authorities demonstrated that they adapt their resourcing and structures in line with the evolution in the risks faced by Latvia. For example, in April 2024, Latvia established a sanctions function within the FIU and created an internal sanctions taskforce in response to an increasing number of STRs on sanctions circumvention.

123. Supervisors' objectives and activities are broadly consistent with national AML and CFT policies and the ML and TF risks identified. Their understanding of risk informed the NRAs, rather than being derived from it. Most supervisors' view of ML and TF risk is aligned with NRA2 and supervisors generally apply more focus and resources to the areas of highest risk therein. Supervisors demonstrated changes to AML guidelines in line with identified risks. For example, following the 2022 Sectoral Risk Assessment, AML guidelines for AIFs were updated to reflect the increased risk rating for AIFMs.

1.5. National co-ordination and co-operation to develop and implement policy

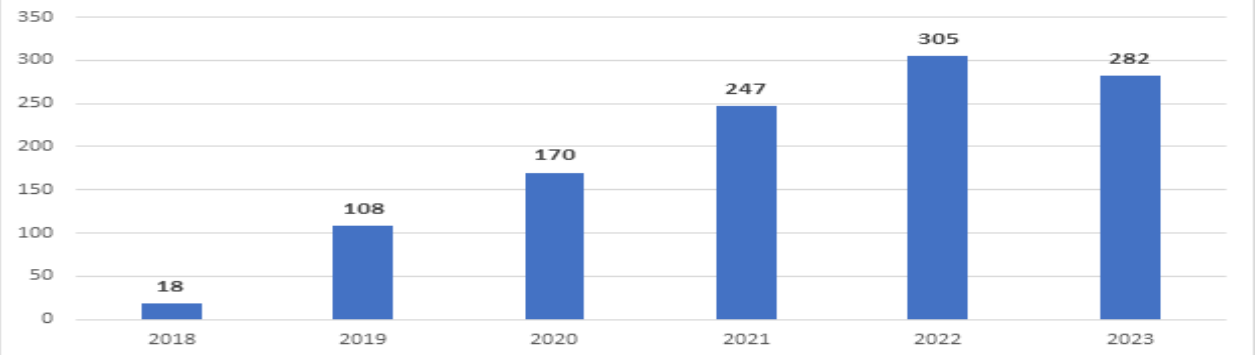
124. The FSDB, which is chaired by the Prime Minister, is the ultimate body responsible for co-ordinating and implementing policies to combat ML and TF. The FSDB consists of the ministers of relevant departments and heads of relevant institutions as well as private sector representatives. The FSDB is underpinned by a range of co-ordination mechanisms. For example, the Advisory Board of the FIU is the body that would be used for co-ordinating strategic co-operation amongst state authorities and includes representatives from: the MoI, the MoJ, Latvijas Banka, Financial Sector Association, Latvia Insurers Association, Latvian Sworn Auditors Association, LCSN, LCSA, the Supreme Court and the PO. In 2023, a dedicated co-ordination platform for SCAs was handed over to the MoF, having previously operated under the FIU since 2018 (see also IO.4).

125. Policy co-operation is clearly documented through the national AML/CFT/CPF Action Plan. The 2024-2026 Acton Plan, which was adopted in May 2024 following the completion of NRA2, contains 97 detailed actions across 12 priority themes. The AML/CFT/CPF Action Plan is underpinned by an extremely detailed budgeting process which captures both ongoing costs and new funding requirements necessary to deliver the Action Plan.

1.6. National co-ordination and co-operation for operational purposes

126. In 2018, Latvia introduced a public-private partnership mechanism, the CCG. This mechanism is also used for public-public co-ordination and collaboration. The CCG is used for both operational and strategic analysis purposes. The CCG brings together the FIU, LEAs, PO, SRS, SCAs and REs, with the composition of each CCG varying depending on the specific issue. The FIU is the convening party for the CCG and has initiated 65% of meetings to date, though any agency can request the forming of a CCG and to date the FIU has granted all requests. Other than the FIU, LEAs and PO initiated approximately 20% of CCG meetings. The SCAs engage with the CCGs to a lesser extent, with their engagement primarily focussed on strategic rather than operational issues, but case studies demonstrate that SCAs have engaged with operational CCGs to achieve operational outcomes.

Table 1.1. Number of CCG meetings



127. The CCG has proved a highly effective mechanism for co-ordinating operational and strategic analytical activity. In 2021 authorities introduced a specific indicator to show when an STR has been submitted following a CCG meeting. Authorities demonstrated STRs being submitted as a direct result of information shared through the CCG. The CCG has also resulted in a number of operational and strategic outcomes. Examples illustrating this practice are provided in the box below.

Box 1.1. Strategic and operational co-operation

Strategic co-operation in relation to a high-risk predicate

In 2021 the FIU, within the CCG framework, gathered experts from the FIU, PO, CPCB as well as four largest Latvian credit institutions. The experts developed corruption and ML indicators and added to them relevant case study material. The material is to be used by credit institutions (as well as other REs) and LEAs in detecting and investigating corruption. The document includes a list of red flag indicators for transactions which may be corruption related and also other factors that may lead to a suspicion of corruption. As a result, a study was finalised and then published on FIU's webpage. In the aftermath of the publishing of the study, there was a significant increase in STRs tied to the predicate of corruption (67 in 2021; 104 in 2022).

Operational co-operation case: combatting human trafficking and ML

Following an analysis of risk data provided by the State Labour Inspectorate and criminal intelligence, the State Police initiated an investigation on trafficking in human beings in 2020. To ensure a swift and co-ordinated response, a CCG meeting (via the FIUs tailor made online platform for secure communications) was immediately convened. State Police informed participants of the circumstances of the case and planned activities, while ensuring its confidentiality. The FIU issued orders via the secure channel of goAML to FIs (providing each FI only with information concerning their respective customers) to monitor transactions on the accounts of the persons suspected of the crime and rapid co-operation with foreign FIUs led to temporary freezing of funds abroad ahead of MLA. As a result, significant assets were seized and frozen. In May 2024, a criminal case indicting 10 natural persons and one legal person for trafficking in human beings and aggravated ML was brough before the Economic Crime Court where trial is underway.

Policy level co-operation by the FSDB

The FSDB plays a crucial role in ensuring high-level policy co-ordination and strategic oversight of AML/CFT/CPF efforts. In 2023, the drafting of NRA2 was finalised. The findings of the NRA were presented to the FSDB, providing an overview of the identified risks and recommendations for mitigating measures. Following the review, the FSDB adopted the NRA and tasked the MoI, in co-operation with relevant institutions, to develop proposals for actions to be included in the AML/CFT/CPF Action Plan for 2024–2026 based on the NRA's conclusions and proposed risk mitigating measures. Consequently, the Government reviewed and adopted the AML/CFT/CPF Action Plan for 2024–2026 with the proposed risk mitigating measures and mandated the FSDB to oversee its implementation. This collaborative approach ensures the proper and regular co-operation and co-ordination at policy level resulting in proper implementation of AML/CFT/CPF measures.

128. Authorities were unanimous on the benefits of the CCG, highlighting the main benefit as the speed at which action can be taken. For example, authorities cited fraud cases where the speed of information sharing had led to the freezing of funds overseas that, but for the speed of collaboration and information sharing through the CCG, would not have occurred. Authorities also noted that the use of the CCG had allowed greater co-ordination and sequencing of administrative and criminal action. Case studies demonstrated that effective co-ordination between LEAs and Latvijas Banka to pursue criminal cases against individuals and legal persons as well as complementary action by Latvijas Banka related to administrative failings.

Chapter 2. International Co-operation

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 and elements of R.9, 15, 24, 25 and 32.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Latvia maintains good formal international co-operation with EU and non-EU partners, ensuring thorough and timely responses to MLA and extradition requests. Despite the increasing number of international co-operation requests, the manual case management system used by authorities does not systematically gather data on the actual execution time of MLA requests, making management and prioritisation more challenging.

b) Latvia is increasingly using international co-operation for pursuing ML, as well as associated predicate offences. Authorities regularly seek and provide assistance for JITs, EIOs and other forms of international co-operation. Overall, Latvia seeks international co-operation in line with its risk profile. However, co-operation on corruption cases is still relatively limited. Follow-up actions regarding provisional measures and asset confiscation for assets identified abroad are not adequately considered. Co-operation challenges with some non-EU countries, which are beyond Latvia's control, prevent prosecution and conviction of potential criminal cases, particularly for the major ML/laundromat schemes orchestrated via the liquidated banks.

c) The framework for other forms of co-operation is well developed, with crucial partnerships through Europol, Interpol, Eurojust, and the CARIN for rapid information exchange worldwide. The State Police is the leading partner in international co-operation. FIU Latvia is also a global leader in international co-operation, with initiatives like the IFIT project, providing assistance through various international co-operation mechanisms and developing new co-operation tools via forums such as the Egmont Group.

d) Supervisors are seeking and providing international co-operation to differing extents. Most material supervisors regularly seek and provide international co-operation.

Key Recommended Actions (KRA)

N/A

Other Recommended Actions

a) Latvia should continue to improve and automate its case management system for monitoring the timely execution of international co-operation requests.

b) Latvia should seek international co-operation more proactively on corruption cases, given the threats identified by the country in NRA2. More emphasis should be given to asset recovery and repatriation/sharing for corruption cases and for cases where proceeds are moved abroad.

c) Latvia's non-bank supervisors should seek information from counterpart authorities on a risk-related basis.

Overall conclusions on IO.2

Latvia has most of the characteristics of an effective system as it proactively co-operates with foreign jurisdictions and authorities and engages to a wide degree with counterparts in relation to ML, TF and associated predicate offences. Latvia prioritises international co-operation, provides and seeks MLA, engages in JITs, and works closely with fellow European countries on EIOs. However, asset tracing and identification requests for seizure and confiscation abroad are rarely showcased. International co-operation on corruption cases has also not yet yielded results in regard to confiscation and restitution of assets abroad. Improvements are needed to operationalise their case management system for formal requests.

LEAs in Latvia co-ordinate informally, exchanging financial intelligence and leading cross-border co-operation. FIU Latvia actively seeks and provides informal assistance through various channels and forums such as the Egmont Group. Bank supervisors are active in international co-operation, while DNFBPs and other financial supervisors are less engaged.

The AT considers the identified shortfalls as moderate, since the overall international co-operation is not hindered by any major challenges and Latvia continues to demonstrate a strong approach to international co-operation.

Latvia is rated as having a substantial level of effectiveness for IO.2.

129. International co-operation is crucial for Latvia's AML/CFT system. Since the last evaluation, Latvia's ML risk profile has evolved from risks associated with being a regional financial centre to various predicate offences. Initially, ML cases were tied to crimes abroad, with significant assets in Latvian banks traced to foreign predicates and global laundromat schemes. Now, there are increasing numbers of investigations into domestic ML and associated predicate offences.

2.1. Providing constructive, timely and quality mutual legal assistance and extradition

2.1.1. Providing evidence and locating criminals

130. Latvia has a robust legal framework for MLA, which enables the authorities to provide a broad range of assistance (see Recommendations 36, 37 and 38 in the TC annexe for more information on the legal framework). Latvia actively engages in effective international co-operation,[21] and co-operates with foreign counterparts in a constructive manner as confirmed by the feedback received from the global community, which highlighted the good quality and timeliness of assistance provided by Latvia. Responses to incoming requests are comprehensive and the information provided is well-regarded by the requesting competent authorities.

131. The State Police, the PO, and the MoJ are the main actors in formal international co-operation. The PO handles requests during investigations and prosecutions, forwarding them to relevant LEAs. The State Police manages co-operation on investigations within its capabilities. The MoJ oversees co-operation during

21. Main partners include Estonia, Lithuania, and other EU counties such as Poland, Czechia, Austria, and Germany, as well as the United States of America.

trials.[22] All authorities in Latvia are well-resourced for international co-operation and have good internal co-ordination. If an MLA request is received by an incorrect authority, it is quickly transferred to the appropriate one, with immediate communication via phone or mail.

132. All central authorities in Latvia have clear procedures for prioritising MLA requests. However, the manual case management system currently in use does not systematically track the execution time of these requests, making management and prioritisation of requests challenging. An automated system is planned as part of broader judicial reforms to be completed by 2029. Despite the high volume of international co-operation requests, Latvia's international partners have not provided negative feedback and are generally satisfied with Latvia's responsiveness.

133. In the period reviewed, authorities received 4 230 EU requests and 2 668 non-EU requests for MLA, handled on average within 60 days and 73 days respectively. Following the closure of Latvian banks involved in laundromat schemes and Latvia's shift away from being a regional financial centre, financial flows with all countries, including higher-risk non-EU jurisdictions, have declined. This reduction, coupled with geopolitical and security developments, has led to decreased co-operation with these countries throughout the review period.

134. The authorities demonstrated that in urgent or simple cases, requests are handled faster. Breaking the requests down, roughly 60% of all requests are from EU countries. The remaining 40% are from other non-EU jurisdictions and have seen a steady decline since 2021, with around half as many requests as the previous period.

Table 2.1. Incoming MLA/EIO requests for all central authorities (2018-2023)

Year	Received during the year		Of which pending at the end of the year**		Refused		Executed		Average time of execution in days	
	MLA	EIO*	MLA	EIO	MLA	EIO	MLA	EIO	MLA***	EIO
Yearly Average	**444**	**705**	**15**	**25**	**7**	**14**	**423**	**666**	**70**	**59**
Total	**2 668**	**4 230**	**90**	**151**	**44**	**82**	**2 538**	**3 996**	**70**	**59**
Combined		6 898		241		126		6 534		64

Note: *Information available for PO and State Police;
**Information available for PO;
***Average time of execution measured during one month period of year (30 days) as sample

135. There have been no cases of unsubstantiated refusals of MLAR/EIO and no such cases were mentioned in the international co-operation feedback. One refusal involved retaining seized assets needed as evidence in ongoing proceedings in Latvia. As indicated in the previous report, the dual criminality is required for the Special investigative actions (Sec. 853 CPL); however, there have been no refusals on this ground.

136. Incoming MLARs and EIOs are related most frequently to fraud and ML, followed by OCG, tax crime, corruption and bribery, as well as drug trafficking. Two TF related MLAs were received.[23] MLARs/EIOs are also reviewed regarding any circumstances for initiating criminal proceedings in Latvia. For example, a large-scale stand-alone ML case was investigated based on the findings in the execution of a MLA request, which led to the NCBC confiscation of approximately 10 million EURs.

22. All central authorities make use of other channels of co-operation to foster formal international co-operation. Namely, MoJ is also serving as European Justice Network contact point, frequently used to resolve problems regarding judicial co-operation within EU jurisdictions. Eurojust is actively used by the PO and one of the prosecutors of International Cooperation Division is performing the duties of a seconded expert at Eurojust. The State Police makes use of all possible channels such as the Europol (through liaison officers stationed in Europol), Interpol, CARIN, and one liaison officer stationed in the United Kingdom.
23. In relation to the TF cases, Latvia's involvement was limited, and the country did not play a central role in any TF scheme. The requests pertained mainly to ancillary information to advance TF cases in other countries.

137. Latvian authorities regularly use requests of information to trigger domestic investigations. Often, requests for information include provisions of evidence to Latvia on a spontaneous basis (i.e. without a prior request), and thus, Latvian authorities proactively initiate investigations into persons and activities in Latvia. The authorities also presented a recent case study showing the ability to pursue asset recovery based on evidence provided by an international partner (see box 7.1 below).

Box 2.1. Initiating a criminal investigation based on an incoming MLA request from the USA

In 2018, a US MLA linked to a corruption and ML case involving telecommunication Company T was sent to Latvia. Company T admitted to paying approximately USD 331 million in bribes to Person G, an associate of a former Central Asian president in 2017. The bribes were funnelled through offshore shell Company M, which received USD 11.9 million in its Latvian bank account from a Liechtenstein bank.

Latvia investigated domestic accounts of the suspects and seized USD 14 029 346, EUR 1 059 423, GBP 999, and CHF 1 000 as suspects could not explain the origin of the funds. Legal co-operation with Liechtenstein and the United States of America was implemented.

In 2021 approximately EUR 12.5 million were confiscated in NCBC procedure, and criminal proceedings were terminated in December 2021.

2.1.2. European Arrest Warrants and Extradition

138. Extradition requests and European Arrest Warrants (EAWs) are generally executed promptly. From 2018 to 2023, Latvia received 390 requests: 306 EAWs and 84 extradition requests, mostly from EU countries. From 2021 to 2023, 78% of extradition requests came from EU members. Extradition requests take an average of 263 days, while EAWs take 36 days. High-profile cases, including dual-use goods and EU sanctions violations, are also included. Latvia refused to execute 30 extraditions and 60 EAWs out of 84 and 306 requests, respectively. In cases where requests are refused, the refusals were substantiated.[24]

Table 2.2. Incoming extradition requests and European arrest warrants (2018-2023)

	Received during the year		Of which pending at end of the year		Refused		Executed		Avg. Time to execute (days, weighted)	
	Extr.	EAW	Extr.	EAW	Extr.	EAW	Extr.	EAW	Extr.	EAW
Yearly average	**14**	**51**	**7**	**7**	**5**	**10**	**8**	**35**	**263**	**36**
Total	**84**	**306**	**43**	**39**	**30**	**60**	**45**	**207**	**263**	**36**
Combined		**390**		**82**		**90**		**252**		**76**

2.1.3 Identifying, freezing, seizing, confiscating and sharing criminal assets

139. Although all authorities have powers to identify and trace assets, the ARO of the State Police is the main authority to handle requests on asset identification. 14 asset recovery requests were received during the reporting period. The table below shows the statistics on confiscation, repatriation and sharing of assets based on incoming requests. These sums are quite low; however, this is due to the small number of incoming requests on asset recovery, sharing and repatriation.

24. Most refusals of extradition/EAW requests are due to the request being withdrawn, the person dying or leaving the country, or the requesting country failing to provide further documentation. Additionally, requests are refused if they aim to prosecute the person based on race, religion, nationality, or political views, or if there are grounds to believe the person's rights may be violated for these reasons (e.g., extradition was denied for a political opposition member facing repression).

Table 2.3. Value of confiscation, repatriation and sharing of assets requests (2018-2023, EUR)

	Confiscation	Recovery	Repatriation	Sharing
Average yearly	258 019	89 208	75 572	9 340
Total	1 548 112	535 244	453 434	56 044

2.2. Seeking appropriate and timely mutual legal assistance and extradition

2.2.1. Seeking evidence and locating criminals

140. Latvia proactively seeks international co-operation and frequently engage in EIOs, JIT and other forms of international co-operation to address transnational ML schemes. The same mechanisms and procedures are used for seeking international co-operation as described under the execution of incoming international requests. While co-operation is increasing in line with its risks of ML and associated predicate offences, some predicate offences (e.g. corruption) are still not adequately represented in respect to the overall international dimensions and risk profile of the cases reviewed. There are also difficulties in obtaining information from certain countries, hindering Latvia's ability to pursue large-scale ML non-resident offenders, highlighting, *inter alia*, challenges and limitations to international co-operation.

141. Compared to its 2018 MER, Latvia now has more outgoing than incoming MLA requests. Investigators are trained on international requests to advance cases and achieve successful prosecutions. Recent statistics show Latvia seeks more co-operation from EU countries, with 5,730 EIOs in the reviewed period. This trend is in line with country's risk profile, since international co-operation and financial flows have decreased with some non-EU jurisdictions, particularly those bordering Latvia, due to a range of geopolitical and security reasons. Requests to third countries (where vulnerabilities and risks connected to these countries remain potentially strong) are lower.

142. Latvia faces significant challenges in obtaining information from certain neighbouring countries. Major suspected ML offenders from abroad have exploited Latvia's (now-defunct) banks (such as Bank A) to commit large-scale professionalised ML, activities for global laundromat schemes. Due to ineffective co-operation with these countries—characterized by unresponsive or low-quality replies— Latvian authorities struggle to pursue the individuals behind these major ML schemes. In response to lower levels of international co-operation, Latvia relies on domestic legal provisions for NCBC to pursue suspected proceeds of crime from ML committed in Latvia. This approach shows their commitment to a "follow-the-money" strategy and addresses poor responsiveness from international counterparts. However, it highlights a fundamental structural difficulty in international co-operation and co-ordination that is beyond Latvia's control.

Table 2.4. Outgoing MLA and EIO Requests (sent by Latvia)

	Sent during the year		Of which pending at the end of the year**		Refused**		Executed**		Average time of execution	
Year	MLA	EIO*	MLA	EIO	MLA	EIO	MLA	EIO	MLA***	EIO*
2018	382	611	13	20	4	8	137	168	223	58
2019	455	744	20	13	7	6	269	271	226	56
2020	548	1 145	64	13	8	5	301	373	222	60
2021	285	1 041	27	8	4	2	254	260	233	66
2022	448	1 008	28	4	3	9	154	296	229	51
2023	420	1 181	29	17	6	2	159	275	215	55
Average	**423**	**955**	**30**	**13**	**5**	**5**	**212**	**274**	**225**	**58**
Total	**2 538**	**5 730**	**-**	**-**	**32**	**32**	**1 274**	**1 643**	**-**	**-**

Note: *Information available for PO and State Police;
**Information available for PO;

***Average time of execution measured during one month period of year (30 days) as sample

143. Most frequently, the outgoing requests are sent regarding tax crimes, ML and fraud. Given the modus operandi identified by the NRA regarding tax crimes the proceeds of which are laundered abroad, as well as ML threats identified, outgoing international requests on these cases are in line with Latvia's risk profile.

Box 7.2. Seeking international co-operation on a professional complex ML case

Intelligence from the SRS TCPD in 2021 led to an investigation into a large-scale ML operation by a professional group in Latvia. The group controlled over 15 foreign companies registered to third-country nationals, along with their bank accounts in EU and non-EU countries, providing ML services to foreign entrepreneurs and concealing the origin, ownership, movement, and location of funds.

TCPD reached out to Armenia, Ukraine, the United Kingdom, Azerbaijan, Singapore, the Russian Federation, Hong Kong, Türkiye, and Kazakhstan with MLAs. Seven EIOs were sent to Bulgaria, Hungary, Poland, Lithuania, Cyprus, Estonia, and Austria, with additional requests to the AROs of Estonia and Ukraine. A Europol liaison officer facilitated legal assistance requests from the United Kingdom and Türkiye. Swift, positive co-operation with Lithuania, Estonia, Armenia, and Kazakhstan provided valuable account information on foreign companies.

The investigation was completed on 24 November 2022 with charges against 7 individuals. EUR 567 551, as well as 6 real estate properties with a value of EUR 1.5 million, 5 vehicles and the shares of one company were seized.

144. This trend is in line with country's risk profile, since international co-operation and financial flows have decreased with some non-EU jurisdictions, particularly those bordering Latvia, due to a range of geopolitical and security reasons that have developed over the past times. Requests to third countries (where some vulnerabilities and risks connected to these countries remain potentially strong) are relatively lower. In regard to corruption, the most recent NRA and the Action Plan have emphasised the need for enhancing the understanding of overseas laundering methodologies linked to corruption (see IO.1). While many corruption cases do not generate illicit proceeds,[25] there are instances where major, large-scale corruption cases have shown to have assets moved to foreign jurisdictions and involved foreign entities and persons.[26] CPCB sent 135 international requests in corruption cases abroad, but efforts have led to only one asset seizure and no repatriations. Authorities should continue seeking international co-operation with a focus on asset recovery.

145. Latvia regularly joins JITs for major cases like OCG and narcotics crimes, with 19 ongoing JITs with EU states (e.g., Lithuania, Estonia) and third countries (e.g., Ukraine, Georgia, Republic of Moldova) by the end of 2023. Outgoing requests also have been used to trigger investigation by the receiving jurisdiction. Such examples were provided by the State Police, as well as PO of Latvia.

2.2.2. Extradition and EAWs

146. Latvian authorities seek both extradition and EAWs in any case when the subject person is known. Extradition requests are generally executed in a timely manner. In cases when it is not possible to identify persons subject to extradition, the cases are tackled by in rem procedure of NCBC.

147. Latvia sent an average 68 extradition requests, with 6 refused and 23 executed, taking about 269 days. For EAWs, Latvia sent 418 requests and 25 were refused, with 218 executions with an average of 43 days to receive the executed request (see table below).

25. Of the 184 corruption cases identified, roughly 60% were known to generate illicit proceeds. Of the cases from 2019 to 2023, 36 ended with NCBC and 6 were pursued for prosecution for ML.
26. As noted in IO.1, authorities summarised that the majority of domestically generated proceeds of corruption were being laundered overseas. This resulted in an action item within the Action Plan for authorities to further develop their understanding of overseas laundering methodologies linked to corruption.

Table 2.5. Extradition requests received by Latvia (2018-2023)

	Received during the year		Of which pending at the end of the year		Refused		Executed		Average time of execution in days	
Year	Extr.	EAW	Extr.	EAW	Extr.	EAW	Extr.	EAW	Extr.	EAW
2018	4	100	2	51	1	8	1	43	288	48
2019	4	91	3	49	0	5	1	42	251	36
2020	2	61	2	29	0	4	0	28	0	44
2021	15	42	8	12	2	3	5	27	258	48
2022	24	76	13	23	2	4	9	49	283	42
2023	19	48	11	18	1	1	7	29	265	39
Total	68	418	39	182	6	25	23	218	269	43
Combined		486		221		31		241		64 (avg)

Box 2.3. Extradition request from Latvia

On 25 February 2020, the State Police launched a criminal case involving at least EUR 555 653 from frauds in Germany, Poland, France, and Spain. The funds were transferred to accounts of 92 clients at a Latvian bank. Following a bank's report on suspicious transfers and withdrawals, special investigations uncovered a 10-member OCG led by suspect "DS". An EAW was issued for "DS" in February 2022; he was arrested in May and extradited from Germany in July. All group members were convicted, with "DS", sentenced to 5.5 years and ordered to pay EUR 115 275 to the Treasury; proceeds were confiscated from the others.

2.2.3. Seeking to identify, freeze, seize, confiscate and share criminal assets

148. The ARO supports asset tracing cases, with ARO-to-ARO requests typically executed within 15 days or even hours in urgent cases. Support to domestic LEAs rose from 49 cases in 2018 to 375 in 2023, tracing nearly EUR 100 million (2018–2023). While international co-operation in asset tracing is increasing, it mainly identifies funds abroad, with limited data on seizure, confiscation, and asset sharing.

149. Between 2018 and 2023, Latvia requested seizures in 126 cases, covering nearly EUR 20 million (including cryptocurrencies), vehicles, real estate, and investment certificates. It successfully secured confiscations abroad in five cases, mainly for tax offences and ML, totalling EUR 1.3 million.

150. Between 2018 and 2023, Latvia requested seizures in 126 cases, resulting in the seizure of nearly EUR 20 million (including cryptocurrencies), as well as vehicles, real estate, and investment certificates. Confiscations abroad were successfully requested in 5 cases, mainly involving tax offences, ML, fraud, and human trafficking, leading to the confiscation of EUR 1.3 million. However, the gap between the identification of almost EUR 100 million, seizure of EUR 20 million, and confiscation of EUR 1.3 million suggests that tracing assets abroad does not necessarily lead to recovery. This is a common challenge in many jurisdictions. Here, it is partly due to asset restitution to victims, empty bank accounts, the lifecycle of cases, and challenges in co-operating with certain neighbouring countries, representing a minor shortfall overall.

2.3. Seeking and providing other forms of international co-operation for AML/CFT purposes, including asset recovery

151. Latvia is actively engaged in non-MLA co-operation, which is regulated by international treaties, multilateral or bilateral agreements and memoranda of understanding (MoUs) or take place on an ad hoc

basis. Direct and informal international co-operation is a usual practice, especially with other Baltic countries and EU jurisdictions (e.g. Czechia, Estonia, Finland, and Lithuania).

152. The PO has signed MoUs with foreign partners to enhance non-MLA relationships and promote fluent international co-operation. Eurojust, Interpol and Europol networks are regularly used, and Latvia has liaison officers at these networks (e.g., liaison officers in Europol from SRS, State Security Service, and State Police) and also in third countries. There is limited information on the promptness of informal co-operation provided by Latvia, except for the FIU and the Latvijas Banka.

2.3.1. FIU

153. FIU Latvia actively exchanges information with foreign counterparts, regardless of co-operation agreements or MoUs. It has signed 46 MoUs with foreign FIUs and 1 MoU with a non-counterpart on using the FIU.net information exchange platform. Co-operation typically occurs via the Egmont Secure Web, covering a broad range of information.[27] FIU Latvia uses various international co-operation mechanisms and develops new informal co-operation tools through forums like the Egmont Group, including the establishment of the IFIT.

Box 2.4. International Financial Intelligence Task Force (IFIT)

In February 2018, a notice identified Bank A as a primary ML concern. By June 2018, Bank A, (Latvia's third largest), initiated voluntary liquidation, and its license was revoked, with EUR 2.4 billion still owed to creditors. Allegations included transactions for UN-designated entities, corrupt PEPs, and laundering billions through shell companies. The case's complexity highlighted the need for enhanced international co-operation. A specialized IFIT was formed under FIU Latvia's leadership, with support from the Egmont Centre of FIU Excellence and Leadership (ECOFEL) and participation from 25 most affected jurisdictions.

The IFIT kick-off meeting was held during the Egmont Group Plenary in The Hague in 2019, with FIUs from countries that had the most transactions with Bank A. FIU Latvia aimed to share and obtain operational information, provide partners with best practices for investigating global financial crimes, and enhance co-operation and information-sharing among FIUs. The goal was to increase awareness of ML exposure, foster a shared understanding of the issues, and co-ordinate cross-border actions. The IFIT served as a platform for both bilateral and multilateral financial, operational, and strategic intelligence sharing. Co-operation continued until 2022.

While the IFIT was operational, FIU Latvia's international co-operation increased significantly, with over 2 000 requests and 446 spontaneous dissemination reports sent to IFIT FIUs over three years. The Task Force achieved notable results, including:

- Over 360 reports disseminated to local LEAs.
- EUR 120 million frozen; court fines in the tens of millions of euros.
- Proposed amendments to national AML/CFT legislation.
- Increased analytical staff and expanded database access.
- New tools for analysing large transaction data volumes.
- New ML typologies detected.
- Expanded public-private partnerships (PPP).

27. (E.g. origin or further trace of funds, BOs, 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).

- Development of targeted training for REs.

FIU Latvia also compiled a best practice paper on multilateral information exchange, presented at the Egmont Group Plenary in Riga in 2022 and received the Best Egmont Case Award for this case and the work of the IFIT.

154. From 2018 to 2020, FIU Latvia received an average of 483 requests per year. Only three FIU requests have been refused over the last six years. Due to the swift execution of incoming requests, averaging around 14 days, there are no pending requests to report.

Table 2.6. Incoming Requests to FIU (2018-2023)

Year	Number of requests received	Average time of execution in days
Yearly average	483	14
Total	**2 901**	-

155. FIU Latvia also receives spontaneous disseminations from foreign FIUs, as well as cross-border disseminations (XBDs) and cross-border reports (XBRs) from EU FIUs. Incoming information is prioritised and analysed, sometimes leading to requests for further information and disseminations to LEAs. Due to the high volume of XBDs and XBRs, the FIU uses a semi-automated, risk-based approach with keyword searches. This process is common for both spontaneous disseminations and XBDs, often including relevant information for foreign FIUs.

156. Regarding outgoing requests, most requests (over 3 400 of the 4 542) sent by the FIU are aimed at enriching the FIU's analysis, and a handful of requests involve requests for freezing.[28] The remaining requests (1 104) were sent on behalf of domestic LEAs (see table below). The FIU systematically and spontaneously disseminates information when there are suspected links with foreign jurisdictions. The high number of outgoing requests substantiates Latvia's well-functioning system of informal co-operation. This is supported by numerous case studies and the FIU's proactive outreach to counterparts via informal channels, including Egmont Secure Web, secure EU channels, and direct bilateral engagement.

Table 2.7. Outgoing requests from FIU

	Number of requests sent	Requests sent on behalf of domestic LEAs
2018	443	111
2019	900	272
2020	828	135
2021	1 022	170
2022	772	184
2023	577	232
Total	**4 542**	**1 104**

2.3.2. Law enforcement agencies (LEAs)

157. Latvia's LEAs engage effectively and regularly in informal international co-operation. The below tables show the breakdown of the number of incoming informal requests (2 719) versus the number of outgoing requests (3 342). The State Police, SRS TCPD, and, to a lesser extent, the CPCB are the main purveyors and recipients of informal information requests to international counterparts. The State Security Service may occasionally seek information.

158. The SRS TCPD received most requests with 2 561 out of the 2 719 total incoming requests. These generally pertained to information requests on tax and customs matters on persons and companies residing

28. During the assessment period, FIU Latvia sent a total of 76 requests for freezing bank accounts abroad.

or transiting through Latvia, and with some requests for participation in joint investigations.[29] A remaining number of requests went to the State Police (132) and CPCB (26). Overall, it does not appear that there have been any important delays or issues in agency responses to incoming requests.

Table 2.8. Total number of incoming informal requests (2019-2023)

Year	State Police	CPCB	TCPD
Yearly average	26	5	434
Total	**132**	**26**	**2 172**

159. Regarding outgoing requests, the State Police is actively sending requests, with 1 201 requests over the assessment period (2018-2023) (see table below). These exchanges are most often via police-to-police information exchange channels, ARO channels, and co-operation with liaisons of foreign LEAs. Europol also plays a significant role in establishing and maintaining these channels of co-operation. Meetings with liaison officers are also held to exchange information about modus operandi. The outgoing requests, assisted by the international co-operation department or ARO, can be for a wide range of information, such as tax information, residency, criminal records, travel information, etc. and represent a proactive approach to international cases. These requests pertain to all forms of inquiry, not only relating to ML, and reflect a strong level of informal co-operation among the State Police.

160. During this period, the CPCB sent a total of 19 requests (see table below). These requests typically sought information about personal property, vehicles, companies, addresses, positions held, means of communication, and more.

Table 2.9. Total number of outgoing informal requests (2018-2023)

Year	State Police	CPCB	TCPD
2018	N/A	N/A	245
2019	165	4	318
2020	345	3	427
2021	151	5	407
2022	198	3	331
2023	342	4	394
average	**240**	**4**	**354**
Total	**1 201**	**19**	**2 122**

161. Latvia's State Police extensively uses JITs for large cases such as OCG and narcotics crimes across the EU and with close partners. Over the past five years, the number of JITs with other member states has steadily increased. These groups co-ordinate essential investigative activities and often execute joint action days for searches, arrests, and seizures.[30] Authorities indicated that they have participated in Eurojust's co-ordination and co-operation meetings a number of times which led to successful international operations against crime. JITs are established with a wide range of countries. By the end of 2023, there were 19 ongoing JITs with EU Member States and third countries. One recent JIT led to joint action against a EUR 2 billion ML network via Lithuanian FIs, with Eurojust supporting operations in Italy, Latvia, and Lithuania, also addressing a EUR 15 million Italian public money fraud.[31]

29. Requests to TCPD are responded to according to the level of urgency of the requester; urgent requests are treated as a matter of priority.
30. Eurojust assists with setting up and financing the JITs. It has also organised co-ordination meetings to prepare for action days and set up a co-ordination centre to provide cross-border judicial assistance.
31. See: Full-scale action against EUR 2 billion money laundering network via Lithuanian financial institution | Eurojust | European Union Agency for Criminal Justice Cooperation.

162. Apart from actively seeking Police-to-Police co-operation, in 2021 the State Police together with partners from Lithuania, Estonia, and Europol launched "Development and application of innovative and proactive tools, fighting top level drug trafficking organisations in the EU" or "FIDR" Project to strengthen national capacities to fight drug trafficking, ML, and organised crime. Through their robust engagement with other jurisdictions, the State Police have participated in more than 50 cross-border operations over three years.

2.3.3. Supervisors of FIs, VASPs and DNFBPs

163. Supervisors have sought and provided international co-operation to differing extents. Latvijas Banka regularly engages and exchanges, whereas supervisors of DNFBPs and other financial sector supervisors engage in practically no exchanges for international co-operation. Noting that Latvia's banking sector represents the most material risk (for cross-border schemes in particular), these gaps are moderate.

164. Latvijas Banka directly co-operates with foreign counterparts and has MoUs in place with relevant foreign prudential supervisors. Latvijas Banka has more than 50 different agreements.[32] Latvijas Banka engages in international co-operation on market entry and supervisory issues. For AML/CFT supervision, it may request information on customers, beneficial ownership, account details, transactions, inspection results, and remediation actions. Latvijas Banka also co-operates with third countries, even without mutual or bilateral agreements. For example, Latvijas Banka recently co-operated with the Commonwealth of Dominica for information that it used to verify source of funds of a potential investor in a credit institution.

165. Outgoing requests from Latvijas Banka mostly concern data and information required for supervision and sanctions compliance and assessment of key function holders. It sends on average 21 requests per year (total 105 requests over five years) to EU and third countries (see table below).

Table 2.10. Outgoing Requests from Latvijas Banka (2019-2023)

	Fit and proper measures	Of which EU countries	Of which outside the EU	Supervision and sanctions	Of which EU countries	Of which outside the EU	Yearly total
Average	12	10	2	9	8	1	21
Total	**59**	**51**	**8**	**46**	**40**	**4**	**105**

166. There have not been any refusals for outgoing requests for the purpose of AML/CFT supervision (2019-2023). Exceptionally, there has been one case with substantial delay due to one non-cooperative country, but all have been responded eventually.

167. Incoming requests mostly concern banks, although most recent requests have dealt with foreign partners usually requiring bank/customer related information, account statements, information of BOs of customers to support their investigations. From 2019 to 2023 Latvijas Banka received 228 requests, mainly pertaining to fit and proper measures, and mainly from EU countries.

Table 2.11. Incoming Requests to Latvijas Banka (2019-2023)

Incoming requests	Fit and proper measures	Of which EU countries	Of which outside EU	Supervision and sanctions	Of which EU countries	Of which outside EU	**Total**
Average	30	28	2	8	6	2	38
Total	**179**	**167**	**13**	**49**	**38**	**11**	**228**

168. As a minor shortfall, various other supervisors do not engage in international co-operation at all, and some engage to a very limited extent. No information has been provided regarding international co-operation

32. Includes for bilateral, multilateral, for specific purpose, for general information exchange etc. Many agreements have been signed by the FCMC, but all counterparties have been informed that as of 1 January 2023, Latvijas Banka took over all the powers and functions of the FCMC and became successor of all the FCMC's rights and liabilities.

on VASP sector supervision (although this sector currently has low materiality), which may change once Latvijas Banka takes over its supervision.[33]

2.3.4. Customs and tax authorities

169. The SRS TCPD sends a large volume of requests in relation to tax enquiries with 2 122 outgoing requests as seen from the statistics provided in the table above. Although most cases relate to tax and customs related (transaction) information, the TCPD also exchanges information on persons criminal records, professional activities, etc. Exchange of information with EU Member States related to alleged tax crimes can be conducted by using the Europol's Secured information exchange application (SIENA). The SRS TCPD can also communicate with tax administrations of EU Member States by using the SCAC tax administrations information channel.

33. Latvijas Banka has established and functioning co-operation channels for information exchange that could (in principle) be used for VASPs.

Chapter 3. Financial Sector and Virtual Asset Supervision and Preventive Measures

The relevant Immediate Outcomes considered and assessed in this chapter is IO.3. The Recommendations relevant for the assessment of effectiveness under this chapter are R.9-21, 26, 27, 34 and 35 and elements of R.1, 29 and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Whilst generally all licensing and registration authorities have processes in place to check criminality of BOs and managers, legal limitations apply. The licensing authorities are not required by law to follow an all-crimes approach and consider criminal associations when conducting fit and proper checks. However, Latvijas Banka has a regulation in place covering these matters. Nevertheless, limitations still apply to registration processes of the SRS and CRPC (which register the least material sectors), although the authorities claim that in practice a broader range of criminality including criminal associations is being considered under good repute criteria. SRS lacks legal powers to prevent criminals from entering the regulated VASP and lending markets, however, it conducts post-entry checks regarding criminality of resident BOs.

b) Latvijas Banka demonstrates a comprehensive understanding of ML/TF risks in the supervised sectors, which is especially well developed in the banking sector. The understanding of risks by the CRPC and SRS in the least material lending and VASPs sectors is developed to a lesser extent. Sectoral risks are widely considered in allocation of supervisory resources. Institutional risk understanding would benefit from further improvements (minor – for material sectors and moderate to substantial – for the least material sectors supervised by the CRPC and SRS) which mostly relate to the granularity and/or meaningfulness of risk data.

c) All FIs and VASPs demonstrate a very good understanding of national and sectoral risks and threats to which their specific businesses are exposed, however, the understanding of inherent risks pertinent to their businesses would benefit from further improvements. Whilst supervisory data shows that application of CDD/EDD measures and internal controls has improved significantly since the last assessment round, more efforts in the area of monitoring aimed at identifying suspicion of ML/TF would be beneficial. Whilst a broad range of guidance papers are already available to assist REs with implementation, sector specific guidance on recognition of suspicion and business risk assessments would further enhance RE implementation.

d) Latvijas Banka's supervisory focus on the most material banking sector has proven effective and resulted in a significant reduction of risk. Other FIs received less supervisory attention, i.e., a lesser number of on-site visits or none at all, however, they were subject to off-site reviews. Whilst on-site examinations by Latvijas Banka appear to be of a good quality, enhanced focus on monitoring scenarios would be beneficial. SRS and CRPC on-site examinations should focus more on practical implementation of preventative measures, especially increased sample testing.

e) A broad range of effective, proportionate and dissuasive sanctions and prescribed remedial

measures have been applied to the banking sector. Few sanctions were applied in the securities sector which is attributed to a lower number of on-site visits. The lack of sanctioning for all other FI sectors (except for VASPs) might be correlated with fewer on-site visits. Whilst many inspected FIs have not been subject to sanctions, supervisors were able to demonstrate that compliance by FIs and VASPs is increasing. This is achieved through remedial actions, guidance and training.

f) Providers of consumer and business loans are licensed/registered and supervised by three different supervisors: Latvijas Banka (where loans are provided by licensed FIs), SRS and CRPC (registered providers). This has an impact on targeted and efficient use of supervisory resources and does not support a level playing field.

Key Recommended Actions (KRA)

N/A

Other Recommended Actions

a) Latvia should remedy technical gaps to ensure all licensing authorities are required by law to consider a significantly broader range of criminality and criminal associations when assessing fitness and propriety of BOs and managers. Additionally, the SRS should be given explicit legal powers to prevent criminals from entering the regulated market.

b) Supervisors should revisit their institutional risk assessment methodologies with a view to considering granularity and meaningfulness of data aimed at assessing institutional ML/TF risks and supporting sectorial risk assessments: minor adjustments are required for the Latvijas Banka and moderate – for the SRS and CRPC.

c) Latvijas Banka should increase the number of on-site examinations outside the banking sector and apply proportionate sanctions/remediation should breaches be identified. It should enhance its focus on monitoring practices aimed at the identification of suspicion by FIs during on-site visits. SRS and CRPC should enhance on-site checks aimed at the practical implementation of AML/CFT requirements by increasing sample testing.

d) Supervisors should further develop a sector specific guidance on (i) conducting business wide ML/TF risk assessments and (ii) recognition of suspicious activities and monitoring.

e) Latvia should ensure consistent application of registration and supervisory practices to all FIs offering consumer and business loans, avoiding duplication of supervisory efforts and ensuring the most efficient use of resources.

Overall conclusion on IO.3

Since 2018, the risk environment in Latvia has changed significantly; as a result, banks and other less significant FIs have changed their business models concentrating on servicing predominantly residents (this is less applicable to the securities sector). In combination with increased scrutiny of supervision, along with extensive sanctioning, risks in the banking sector have significantly diminished and the application of preventative measures has improved. Whilst fewer material non-banking FIs (except for VASPs and lenders) received less supervisory attention, the level of compliance with AML/CFT obligations has nevertheless increased. Business-wide ML/TF risk assessments remain an area where FIs need to advance the most when compared to CDD obligations, followed by monitoring.

Latvijas Banka has an overall good understanding of sectoral and institutional risks, which is especially well developed for the banking sector. Supervisors would benefit from revising methodologies for institutional risk assessments to further deepen risk understanding: minor improvements are required for the methodologies of the Latvijas Banka and moderate-substantial improvements for the SRS and CRPC.

Throughout the assessment period, the most material sector – the banking sector - was prioritised for on-site examinations with fewer (or no) visits to other FIs under Latvijas Banka supervision; however, FIs were subject to targeted reviews. The quality of on-site examinations by Latvijas Banka is generally good with no substantial improvements required. The least material sectors supervised by the SRS and CPRC (VASPs and consumer and business loan providers) generally received an appropriate number of on-site visits, however, the approach to on-site examinations needs to be further strengthened by both supervisors.

Supervisors were able to demonstrate that supervisory intervention through on-site examinations, guidance and awareness raising, as well as application of sanctions and remedial measures, has had a positive impact on FI and VASP levels of compliance.

Technically, market entry-related legislative provisions aimed at preventing criminals are somewhat narrow - only a small fraction of criminality is considered under the AML/CFT/CPF Law (unless sectoral regulation prescribes otherwise), and criminal associations are not defined. Latvijas Banka expands this approach under a regulation allowing it to consider criminal associations and all crimes under good repute criteria, but the approach to registration by the SRS and CRPC needs to be significantly strengthened.

Latvia is rated as having a substantial level of effectiveness for IO.3.

170. For the purpose of assessing IO.3, the banking sector has been given the highest priority based on its materiality and risks and thus supervisory actions and implementation of AML/CFT preventative measures by this sector are weighted most heavily. The importance of other sectors is explained in the introduction. Since the SRS and CRPC supervise sectors of low materiality, the level of analysis of licensing and supervisory controls is adjusted accordingly.

171. Since the last evaluation, significant efforts have been made by the Latvian authorities to increase the effectiveness of financial supervision, with the highest priority focus on banks through increases of resources in all supervisory authorities, more effective domestic co-operation and co-ordination, enhanced scrutiny of supervision, and application of dissuasive sanctions to the banking sector for AML/CFT breaches. Supervisors now have adequate human resources to fulfil AML/CFT compliance monitoring duties: the Central Bank – 26 staff[34] (solely for AML/CFT duties), the SRS – 49 staff (solely AML/CFT duties), and the CRPC – 17 staff (AML/CFT duties combined with other tasks).

172. Latvijas Banka has implemented an additional layer of supervisory measures, such as market exit controls for credit institutions undergoing insolvency or liquidation (including voluntary liquidation) to ensure appropriate and effective AML/CFT/CPF compliance. These controls involved legislative amendments requiring liquidators to develop methodologies for fulfilling AML/CFT/CPF requirements during the liquidation process, including payouts from the deposit guarantee fund, disbursements to creditors, and asset sales. These methodologies are subject to approval by the Latvijas Banka. Exit controls are aimed at ensuring a transparent and controlled exit of credit institutions from the financial market, and the entire process is closely supervised by Latvijas Banka.

34. Human resources increased sharply – from 6 full-time equivalent staff in 2015 to 26 in 2024.

3.1. Licensing, registration and controls for FIs and VASPs preventing criminals and associates from entering the market

3.1.1. Market entry controls

173. Generally, legislative requirements are not broad enough to cover all types of criminality and criminal associations. The AML/CFT/CPF Law lists only a limited number of crimes to be considered at the market entry stage and these crimes cease to be considered for criminality criteria purposes once a criminal record is annulled or cleared (expiration of punishment, amnesty, etc.).[35] The narrow criminality approach is expanded in the sectoral laws applicable to FIs under Latvijas Banka supervision, however, not to a full extent. Notwithstanding, Latvijas Banka has a regulation in place that sets out additional requirements (please see below).

Latvijas Banka

174. Fitness and propriety checks by Latvijas Banka are conducted under a regulation,[36] according to which BOs and controllers have to have an impeccable reputation. Latvijas Banka informs that - in practice - all aspects of criminal activity are considered under good repute criteria,[37] including any administrative records. As part of consideration of the good repute of an applicant, the reputation of a person having close family ties or a business relationship with the person are considered. This covers criminal associations. Latvijas Banka demonstrated through a case study that it was able to refuse market entry (acquisition of a qualifying holding) on the basis of criteria of "impeccable reputation" despite the absence of a criminal record.

175. Generally, Latvijas Banka applies a unified approach to licensing and/or approval checks (change of shareholding, management position and qualifying holding),[38] however, scrutiny of checks may vary depending on materiality and risk. All applicants are commonly required to present a criminal record certificate from all countries they have been residing in which is further verified. Criminal associations are checked through various databases, negative media searches, and using information submitted by the applicant on its professional and business affiliations. Additional relevant checks include source of wealth and funds used to provide capital (supportive documentation required on this, such as tax declarations, audited statements or similar), as well as the assessment of business model and related ML/TF risks.[39]

176. Licence applications processed per year vary between one and five. No licence applications have been refused over the assessment period as Latvijas Banka tends to have a dialogue with the applicant which leads to withdrawal by the applicant. Two cases appealing decisions on refusal to approve an acquisition of qualifying holdings were brought to court. Both claims were dismissed, and proceedings terminated and Latvijas Banka's decisions remained in force. As for managerial role assessments, reasons for withdrawal have been related to insufficient competence; there were no refusals.

177. Within the assessment period, three banking failures occurred that were closely related to improper conduct or handling of business operations by BOs and/or controllers. While investigations are ongoing, and

35. The AML/CFT/CPF Law states that the BO of the FI may not have been sentenced for committing intentional crime against the State, property or administrative order, committing intentional crime in the national economy or service of State authorities or for committing such crime which is related to terrorism, unless the criminal record is set aside or extinguished; unless it is otherwise provided for in other laws and regulations (AML/CFT/CFP Law, Section 101(11)).
36. Regulation on acquiring or increasing qualifying holding in financial institutions (applicable at the primary licensing and subsequent changes).
37. Or impeccable reputation criteria.
38. Some differences exist, e.g., different registration and licensing thresholds for EMIs and registration of AIFs. Latvijas Banka has prepared amendments to the law that would require stricter market entry controls for the whole AIF sector (see more at R.26).
39. From an AML/CFT perspective, assessment of a business model is used to understand the applicant's operations, including the products and services to be offered, business complexity, geographic footprint, expected customer base, and delivery channels. This understanding helps in identification of potential ML/TF risks inherent to the business model. The analysis is further used to evaluate the applicant's AML/CFT risk assessment, policies and control procedures thereby ensuring that the AML/CFT documentation is appropriately tailored to the specific characteristics of the business model.

thus more detail cannot be revealed at this stage, these events nevertheless call into question potential gaps in assessing the suitability and good repute of BOs and managers and/or related decisions on refusals.

SRS and CRPC

178. The SRS applies controls to prevent criminals from entering the regulated market (based on the requirements of the AML/CFT/CPF Law which are somewhat narrow as regards crimes to be considered - see above), however, processes need further improvement. FIs supervised by the SRS are required to submit a report to the authority following registration within the ER. Further criminality checks by the SRS are conducted in the post-registration stage (approximately within 2 weeks after the report is submitted) and during routine on-site examinations. Whilst the SRS consults national databases regarding criminality of BOs and managers, there are no established requirements for foreign managers and BOs to present conviction certificates to the registration authority. This shortcoming is currently not material, as there are no non-resident VASP BOs, as confirmed by the SRS. The SRS does not have explicit legal powers to prevent registration of newcomers if the authority does not consider them to be fit and proper, nor to dismiss BOs or managers after registration. Limitations concerning the narrow scope of criminality and coverage of criminal associations as explained above equally apply here.

179. CRPC's internal regulations allow broader criminality to be considered than the SRS, however, shareholders and BOs are subject to a significantly lesser degree of criminality requirements than managers and are limited to ML/TF/PF offences only. Whilst the CRPC suggests that an all-crimes approach can be considered under good repute criteria, consistency of application of this approach cannot be evidenced as no formalised rules exist. The CRPC has refused one application due to concerns relating to the source of wealth invested as capital. BOs are additionally checked during on-site visits.

3.1.2. Detecting and addressing breaches

180. Latvijas Banka has established internal processes for detecting unlicensed service providers through the following means: customer complaints, media monitoring, whistleblowers, and information from the State Police or other authorities. Latvijas Banka has several tools to fulfil its monitoring tasks.[40] In the review period, Latvijas Banka has identified four instances of foreign investment service providers offering services in Latvia without authorisation which resulted in blocking their websites. The SRS has identified two unregistered VASPs that were subject to administrative fines and suspension of business activity.

3.2. Supervisors identifying understanding and promoting FI and VASP understanding of ML/TF risks

3.2.1. Identifying and maintaining an understanding of the ML/TF risks in the different sectors and types of FIs and VASPs, and of individual FIs and VASPs over time

181. All supervisors are able to articulate sectoral risks, with Latvijas Banka having a more in depth understanding, which is especially well developed in the banking sector, in line with the materiality and risk exposure. Over the assessment period, following strategic structural reforms within the country, risk exposure of the financial sector has decreased significantly - largely due to the shift towards servicing predominantly Latvian residents (except for securities) and change of business models in the banking sector. The most material banking sector is rated as presenting a medium ML risk. The securities sector – second in terms of importance – is rated as presenting a medium-high ML risk predominantly due to the complexity of business models (i.e., operation of investment platforms, activities in elevated risk regions and online delivery channels) and less robust controls compared to those adopted by the banking sector. All other financial sectors outside banking and securities are rated as presenting a medium ML risk, with the exception

40. A specific programme for monitoring the resources available on the Internet, which, inter alia, provides analysis of the resources available on the Internet by keywords about specific service providers; programme LETA station.lv for media monitoring where information on Latvijas Banka, the financial sector, payment services etc. is selected by keywords; several public databases (e.g., Lursoft) that are used for the monitoring framework.

of insurance and credit unions (rated medium-low) and private pension funds and life insurance intermediaries (rated low).

182. There is no distinction between risk categorisation methods used for different types of FIs – entities in each sector are divided into four risk categories irrespective of the size, materiality (complexity) and/or risk of the sector (see table 5.1). This signals that the differentiation of risk across individual financial sectors can be further re-evaluated with a view to assessing the impact on efficient allocation of supervisory resources aimed at monitoring FIs' compliance.

183. All supervisors have methodologies in place for conducting institutional risk assessments that take account of varying risk criteria. Whilst the methodological approach by Latvijas Banka is developed to a good degree and covers all necessary risk categories (client, service/operation, delivery channel, geography) for inherent risk assessment, as well as controls,[41] minor improvements would serve in deepening the institutional risk understanding. For example, the approach to inherent risk assessment of the banking sector could benefit from: (i) additionally looking at clients that have complex ownership structures, as well as clients that have nominee arrangements in their control and/or ownership chain; (ii) re-considering the approach to assessing "high risk clients" element under inherent risk as this criterion might not always objectively and directly mirror inherent risk exposure (especially if this is not tied to the controls' assessment, which in these circumstances should provide an exhaustive list of criteria according to which client risk is assessed, and the approach to weighting those criteria); (iii) re-considering the approach to weighting some of the risk categories, e.g., delivery channel risk for the securities sector is weighted least heavily representing only 10% of total weight (same approach as for the banking sector), despite remote onboarding and remote delivery of services being one of the key determinants for securities ML risk being assessed as medium-high.

Table 3.1. Institutional risk categorisation matrix: residual ML/TF risks (2023)

Entity	Risk rating				Total number of entities
	Low	**Medium-low**	**Medium-high**	**High**	
Banks	3	5	5	-	**13**
PIs	2	1	1	0	**4**
EMIs	3	3	1	0	**7**
Investment firms	2	5	2	0	**9**
Investment management companies	6	1	3	0	**10**
AIFMs	12	19	0	0	31
Life insurance companies	3	3	0	0	**6**
Currency exchange offices	0	10	5	0	**15**
Credit unions	27	2	0	0	**29**
Private pension funds	6	1	0	0	**7**
Life insurance intermediaries (insurance brokers)	33	0	0	0	**33**
Lenders/leasing (consumer credit service providers) (CRPC)	3	26	8	0	**37**
Other FIs – credit, including financial leasing (SRS)	266	0	23	21	**310**
VASPs	6	0	0	1	**7**

184. Processes for institutional risk assessments used by the SRS and CRPC have good elements in place aimed at measuring ML risk, however, need further improvement. Whilst risk matrices contain some data points (e.g., transactional activities and number of clients) that contribute to the ML risk assessment, they need to be further expanded to fully and specifically fit ML/TF risk assessment purposes; that would also mean taking out data points that are not relevant for ML/TF as they may water down the ML/TF risk level. Controls-related questions should be separated from inherent risk related questions for the same reasons.

41. Residual risk is calculated based on inherent risks and controls.

Additionally, there are no specific questions addressed to FIs or VASPs on data points that would serve to measure TF risk.

3.2.2. Promoting FI and VASP understanding of ML/TF risks and AML/CFT obligations

185. Latvian authorities are active in promoting FIs' understanding of ML/TF risks and preventative measures. This is achieved through several measures: training seminars and presentations, individual feedback and consultations, as well as various guidelines that assist in the identification of suspicious behaviour, reporting and implementation of AML/CFT controls. Between 2019 and 2024, 83 training seminars were conducted by Latvijas Banka that predominantly focused on general internal controls, ML/TF risk prevention and sectoral risks. Whilst these efforts are commendable, it would also be beneficial to consider a more targeted outreach based on inherent risk exposure and control vulnerabilities identified through off-site and on-site means.

186. Supervisors issued a wide range of guidelines on various topics related to the implementation of AML/CFT measures. A number of topical guidance papers aimed at identification of suspicious operations have been issued by the FIU including: (i) suspected corruption identifiers; (ii) suspicious real estate linked transactions; (iii) human trafficking identifiers; (iv) ML identifiers linked to payments and accounts, including correspondent accounts held by PIs/EMIs; (v) laundromat-type transactions; and (vi) TF indicators. Additionally, investment sector specific ML indicators have been issued (non-public document) and disseminated to FIs operating in this sector.

187. The FIU also manages a virtual training platform to further assist REs with the implementation of reporting obligations. The FIU can be commended for its efforts in assisting FIs with reporting obligations which have proved to be effective. However, all sectors would benefit from sector-specific guidance on business-wide ML/TF risk assessments and some sectors (such as banking, payment sector, VASPs) from sector specific ML/TF indicators to identify suspicion. In addition, specific guidance to VASPs on the implementation of AML/CFT controls would be beneficial. VASPs met on-site were open about the implementation challenges they are facing today (e.g., implementation of the travel rule), albeit this sector is not material in the context of Latvia.

3.3. FI and VASP understanding of existing and evolving ML/TF risks

188. FIs and VASPs commonly conduct business-wide ML/TF risk assessments (BRA) by taking into account supranational (EU), national (NRA), sectorial (SRA) and business-specific risks. For inherent risks, FIs typically look into clients, services (products), geographies and delivery channels – these risk categories are further differentiated to include more detailed data points (the comprehensiveness of which varies depending on the size of an FI and nature of its services; the same applies to internal controls' (vulnerabilities) assessments). Sophistication of the technological solutions used for risk assessments largely depends on the size of an FI/VASP: large credit institutions and fintech-type FIs use more advanced data analytics solutions, Power BI, and other IT tools, whilst smaller firms rely on MS Excel and other manual solutions. All supervisors uniformly agree that the level of compliance with the BRA requirements has considerably increased during the assessment period both in terms of documentation (including frequency of updates) and comprehensiveness (quality). These conclusions are largely based on reviews of BRAs during on-site activities or specific targeted off-site reviews. Latvijas Banka reports that in 2023 all supervised FIs documented their risk assessments, whereas in 2019 some smaller FIs did not have BRAs available (e.g., 45% of credit unions and 85% of AIFMs). The SRS and CRPC report that there were cases of failures by VASPs and credit services providers to conduct BRAs, however, both supervisors were able to follow up on the remediation of such deficiencies. Significant improvements have also been noted regarding quality; for example, in 2021 23% of banks had critical (very severe) deficiencies in their risk assessments, in comparison to 2023 where no critical deficiencies were identified, 10% required moderate improvement and 80% required minor improvements. A similar situation was observed in the securities

sector, where the level of compliance has increased since 2019 with minor improvements required in most cases and moderate improvements in around 10% of cases.

189. Over the assessment period, following strategic structural reforms within the country, the risk exposure of the financial sector has decreased significantly largely due to the shift towards servicing predominantly residents; linked to this, many banks and securities market participants changed their business models.

190. Generally, and in line with the above, all FIs and VASPs met on-site were able to comprehensively articulate national and sectoral ML/TF risks and the impact of those on their business, as well as related mitigation techniques. Whilst FIs document their BRAs and supervisors do not consider that supporting methodologies need further improvement, it was noted by the AT that most entities met on-site overly rely on risks and threats outlined in the NRA and SRA - which translates into hypothetical threats appearing in their BRAs. Most FIs were less articulate on inherent ML risks relating to certain categories of high-risk clients and/or products/services. For example, some FIs highlighted corruption as one of the main risks to their business without being able to articulate exact reasons, as they had very little or no PEP clients. Geographical risks are well understood by all FIs/VASPs met on-site which in turn allows for a comprehensive understanding of TF risk components (clients, BOs, payments with geographical component). All REs can also be commended for having a very good grasp on how their businesses (products and services) can be abused for ML/TF purposes (threats perspective), which, in turn, translates into appropriate CDD controls and monitoring scenarios to prevent this.

191. These findings are supported by supervisory data which confirms that required improvements to existing BRAs largely relate to the comprehensiveness of data sets being considered for risk assessment purposes. These shortcomings might be partly attributed to insufficiently detailed guidance on BRAs. Whilst general requirements on conducting BRAs are outlined in the AML/CFT/CPF Law and Latvijas Banka and the CRPC make additional guidance available, these are not sufficiently detailed. In particular, FIs and VASPs would benefit from having: (i) a more comprehensive list of examples of criteria for assessing inherent risks (recognising sectoral differences); and (ii) further guidance on calculation methods (in combination with thresholds, weightings) and approach to assessing and weighting internal controls (vulnerabilities).

3.4. FI and VASP understanding and compliance with AML/CFT obligations and mitigating measures

3.4.1. CDD, record-keeping, BO information, ongoing monitoring

192. CDD, BO identification, verification and record keeping requirements are generally well understood and implemented by all FIs met onsite, however, the scale and depth of monitoring could be further expanded.

193. Latvijas Banka's data confirms these findings, acknowledging that systemically important banks are largely compliant with CDD/EDD requirements, while less significant banks demonstrated a partial level of compliance until 2023 and were re-assessed as largely compliant in 2024. In the investment and payment (PIs and EMIs) sectors the level of compliance improved significantly. In 2021, 63% of investment firms were found not to comply with EDD/CDD requirements whilst mostly minor shortcomings were identified in 2023. Similarly, in 2019 50% of PIs/EMIs were found not to comply with CDD/EDD requirements, whereas in 2023 all achieved either full or substantial levels of compliance. Similar results were seen in compliance with transaction monitoring requirements. Overall, currently, no critical deficiencies have been detected across different sectors.

194. BO requirements are generally implemented in a satisfactory manner; mandatory discrepancy reporting aids better effectiveness. All supervisors confirmed that the level of compliance with BO verification requirements has increased over the assessment period with no systemic or severe deficiencies identified in 2023, although there were cases of severe/systemic breaches at the beginning of the reporting

period. This is supported by interviews with FIs met on-site: all were able to clearly articulate processes designed for gathering and verifying BO data. With the exception of securities firms, FIs met on-site focused on servicing predominantly residents (some did not have cross-border clients at all given significant changes in their business models since 2019). All acknowledged challenges in verifying BO information in complex structures but were able to explain verification sources and channels used. Some FIs displayed a sophisticated understanding of BO verification methods. Nevertheless, identification and verification of legal persons via on-line onboarding channels remains challenging, especially for some securities firms, e.g. those that operate investment platforms. Also see at IO.5.

195. Supervisory data by Latvijas Banka shows that all FIs significantly improved their transaction monitoring practices and STR reporting over the assessment period. Interviews with FIs support this view. The AT found that, generally, all FIs are good at identifying suspicious activities linked to geographical risk component, changes to client risk profile, fraud (main typology) and display a very good understanding of threats to their businesses; however, on-site interviews show that FIs' efforts need to be intensified to identify a broader scope of suspicious activities linked to more diverse criminal typologies, high risk business, services and clients.

3.4.2. Enhanced or specific measures

196. FIs met on-site were well aware of the enhanced and specific measures and were able comprehensively explain implementation practices. All FIs demonstrated comprehensive knowledge of geographical risk and mitigation controls relating to high-risk countries, i.e., EDD on clients, BOs and transactions with high-risk countries.

197. PEP-related risk and mitigation techniques are well understood, however, overreliance on domestic PEP lists was noted with a lesser focus on handling close associates of PEPs. According to supervisory data, no serious breaches were identified in the area of PEP compliance and, in general, the volume of PEP-related transactions decreased significantly over the assessment period (e.g., in the banking sector from 1.9% in 2019 to 0.6% in 2023) due to foreign high-risk clients, including foreign PEPs, exiting Latvia's financial market.

198. New technology-related risks typically relate to the use of commercial software (e.g., for negative media, sanctions, PEP screening, etc.), and remote onboarding solutions (predominantly in the securities and fast credits sector) are tested by FIs. The launch of new products or services is uncommon, which aligns with significant and conservative changes to business models (the securities sector being an exception).

199. Payment sector representatives are well aware of the wire transfer rules, with VASPs acknowledging implementation challenges. No compliance failures have been identified in this area except for a small rejection rate with insufficient information on outgoing payments (this is correlated with the specific design of payment systems).

3.4.3. AML/CFT reporting obligations, tipping off

200. Generally, compliance with STR reporting obligations is increasing, according to supervisory data. Typically, there are no tipping off concerns. The FIU is satisfied with the general quality of STR reports. Latvijas Banka's data suggests that systemically important banks are largely compliant with STR reporting requirements, while less significant banks only achieved a partial level of compliance until 2023 with a recent improvement to largely comply in 2024. Banks are the top reporting sector, however, reporting trends in some other sectors outside banking might need further improvement, for example, in the securities sector due to their cross-border exposure. Fulfilment of reporting obligations is directly linked to the appropriateness of monitoring scenarios which is a prerequisite for the identification of suspicion. See above.

3.4.4. Internal controls, procedures and audit to ensure compliance

201. FIs have internal controls in place for the implementation of preventative measures. The scrutiny of such controls is largely attributed to the materiality of different financial sectors and size of individual FIs.

FIs under Latvijas Banka supervision have internal policies and procedures in place, conduct training for employees and have periodic audits (be it internal or external, scope and frequency vary and are largely dependent on size and complexity). Latvijas Banka notes that over the assessment period, the overall level of compliance has increased in all sectors. However, the number of staff dedicated to AML/CFT is relatively low outside the banking sector. Latvijas Banka considers that staff resources are in line with risk exposure and encourages increasing the AML/CFT expertise of the existing staff. The AT found that some of the least material small FIs met on-site did not have fully functioning and separated "three lines of defence", e.g., one credit union has a single employee responsible for all daily activities. Latvijas Banka considers that internal controls of less material FIs are proportionate to the size and risk profile of their business. In addition, an external audit is often sought.

202. Lenders and VASPs, whilst generally less equipped to have comprehensive internal controls due to the size of their business, have most basic elements in place: internal control documents, training, AML/CFT Officer, etc.

3.4.5. Legal or regulatory impediments to implementing AML/CFT obligations and mitigating measures

203. There is nothing that would prove the existence of legal or regulatory impediments to implementing AML/CFT obligations and mitigating measures.

3.5. Supervisors risk-based monitoring or supervising compliance by FIs and VASPs

204. All supervisors have internal control procedures in place specifying requirements for risk-based supervision. In practice, the extent to which supervision is risk-based varies across supervisors.

Latvijas Banka

205. Over the assessment period, the supervisory capacity of Latvijas Banka has increased significantly,[42] resulting in more effective risk-based supervision where significant resources are dedicated to supervising systemically important higher risk banks. 26 staff members, including a head of department, are split into two divisions, where 15 are responsible for off-site supervisory matters (off-site reviews, guidance, enforcement, etc.) and the remaining 11 staff members are responsible for conducting onsite AML/CFT examinations.

206. Latvijas Banka's approach to planning supervisory activities is largely risk driven. Off-site reporting and automated monitoring tools are used to detect risks at an early stage (including major changes in management and operations) and form a documented view on individual risks of supervised institutions (see also section 3.2). The frequency of off-site reporting depends on individual and sectoral FI risk scores and is revised annually. Horizontal or thematic off-site reviews are carried out - where frequency depends on sectoral risk level and scope is dependent on the specific elements of risk identified through off-site reporting and mandatory external audits (see below).

207. Planning of on-site examinations is largely risk-based (see section 3.2 on risk categorisation). The type, frequency and nature of supervisory actions are determined based on both sectoral and institutional risk. This means that higher risk and material sectors receive more intense on-site examinations, as compared to lower risk sectors, and the frequency and type of examination are tailored to FIs' risks. Risk-based measures based upon residual risk levels are further adjusted for impact (materiality/size related considerations) and might change the allocation of supervisory measures. An annual on-site inspection plan is prepared, but Latvijas Banka may conduct ad-hoc inspections beyond the planned frequency in response

42. Following legislative amendments, the Central Bank and the former financial supervisor - FCMC – have functioned as a single entity as of 1 January 2023 – the Latvijas Banka. All staff previously tasked with AML/CFT affairs at the FCMC were transferred to the Central Bank.

to identified risks. Periodically, the frequency and intensity of on-site inspections are reviewed to address changes in sectoral and individual risks.

208. FIs are subject to full scope and thematic or targeted examinations. For example, low risk banks are subject to full scope on-site visits every five years, moderately low risk – every three years, moderately high risk – every two years, and high-risk banks are subject to regular enhanced monitoring activities. In addition, a targeted review is performed on high-risk banks every six months if an inspection is not possible within one year's time. A similar approach to examinations is followed for non-banking FIs with a lower frequency of on-site examinations.

209. In addition to on-site examinations, FIs (banks, PIs, EMIs, and securities firms) are required to conduct independent audits aimed at testing AML/CFT systems. The frequency of such reviews depends on the risk profile of individual institutions.

210. Whilst Latvijas Banka's focus on the banking sector is justified by risk, more attention needs to be paid to FIs outside the banking sector. The number of on-site visits to non-banking FIs is considerably lower. There were instances where planned inspections were not completed due to a necessity to carry out ad hoc inspections for higher risk FIs, changes in the market, delays in the implementation of remediation plans and temporary staffing challenges. Some lower risk sectors, e.g. insurance, have not received any on-site examinations over the entire review period (see table 5.2.). However, sectors with no or very low numbers of on-site visits have been covered by targeted reviews.[43]

Table 3.2. On-site examinations 2018-2024

Segment	Full scope		Targeted/thematic		Ad hoc
	Planned	Completed	Planned	Completed	
Banks	34	27	21	19	38
PIs	6	6	-	-	2
EMIs	3	3	-	-	3
Investment firms	9	7	1	-	-
Investment management companies	5	5	-	-	2
AIFMs	-	-	4	3	-
Life insurance companies	1	-	-	-	-
Currency exchange offices	54	61	7	7	1
Credit unions	1	1	-	-	1
VASPs	22	22	0	0	0
Credit, including financial leasing	215	215	0	0	0

211. Despite this, AML/CFT on-site examinations conducted by Latvijas Banka are of a good quality, with an average of 30 files sample-checked during each on-site visit. The number of sample files is adjusted in accordance with the risk-based approach and increased for higher risk entities.[44] A greater focus on monitoring scenarios aimed at detecting suspicious activities during on-site examinations would be beneficial, in particular with a view to concluding whether monitoring scenarios are comprehensive enough to capture varying types of threat and risk exposures (and whether the efficiency and effectiveness of monitoring scenarios are periodically reviewed and adjusted to needs and changing risk environments).

212. In addition to routine AML/CFT examinations, Latvijas Banka conducts thematic/targeted reviews. For example, upon the introduction of a legal prohibition to service shell companies in 2018, the FCMC (former supervisor) conducted several types of supervisory activities after changes to the AML/CFT/CPF Law prohibited co-operation between FIs and certain types of shell companies. It: (i) designed specific off-

43. Targeted reviews are desk-based assessments that revealed minor deficiencies in internal controls and resulted in mandatory remediation. Only one targeted review revealed moderate deficiencies (credit union) which resulted in an on-site examination.
44. For example, CDD/EDD samples in on-site examinations conducted throughout 2024 range between 26 and 88; transaction monitoring alert samples range between 26 and 50.

site reporting; and (ii) conducted several on-site inspections in 2018 and 2019, of which seven were targeted and five full scope – all examining shell company-related controls and potential links between prohibited shell companies and newly onboarded legal persons. As a result, serious and systemic deficiencies were found (failure to apply EDD and to comply with the prohibition to terminate business relationship with shell companies) in five banks which led to fines.[45] Two of the fined banks have since ceased to exist - one left the market voluntarily and the licence for the other was revoked in 2022. The other three banks have made significant progress in reducing ML/TF risks and preventative measures. Targeted supervisory activities have not revealed any potential links between newly onboarded clients and shell companies with which business relationships were terminated.

SRS and CRPC

213. The frequency of monitoring visits by the SRS and CRPC is dependent on calculated risk levels (see limitations concerning institutional risk assessment at 5.2.2 that also have an impact here), where high-risk entities are checked at least once a year, medium risk every three years and low risk based on trigger events. Ad-hoc examinations are carried out based on trigger events (e.g., negative information on market players, etc.). Both supervisors, however, tend to adopt a *check list* approach to conducting on-site examinations and, whilst it is positive that they look at internal controls and procedural matters, there should be more emphasis on implementation (and related sample testing). The number of on-site examinations by the SRS is generally high with a low number of shortcomings identified.

214. Providers of consumer and business loans may be licensed/registered and supervised by three different supervisors: Latvijas Banka (where loans are provided by licensed FIs) – banks and credit unions) and SRS and CRPC (registered providers).[46] The Central Bank supervises FIs that provide consumer and business loans as part of a broader set of services individually, However, registration and supervisory approaches by the SRS and CRPC may overlap. There are 20 loan providers that are registered by both the SRS and CRPC and thus supervised by the two authorities. The complexity of such registration and supervision regimes creates unnecessary difficulties and does not support full consistency in supervision and might negatively affect targeted and efficient use of supervisory resources. This view was supported by the consumer and business loan providers met on-site who were in favour of one single supervisor; with some pointing out that they would appreciate consistent application of supervisory measures and less intrusive supervision, e.g., two onsite visits around the same time from two different supervisors. One provider acknowledged already following the guidance issued by Latvijas Banka despite the fact that it is supervised by another authority.

3.6. Impact of monitoring, supervision, outreach, remedial actions and effective, proportionate, and dissuasive sanctions on FI and VASP compliance

215. All supervisory authorities demonstrated having a positive impact on FIs and VASP compliance through sanctioning, remedial measures and guidance. As evidenced above (this section needs to be read in conjunction with sections 3.3 and 3.4 where compliance trends are discussed) levels of compliance with preventative measures have improved over the assessment period. This is demonstrated through supervisory data and interviews with FIs and VASPs.

Sanctions and remedial actions

216. A wide range of remedial actions and sanctions have been applied by Latvijas Banka on banks with dissuasive fines for severe and systemic AML/CFT compliance failures. This includes dissuasive monetary fines, change of management, restriction of activities and license withdrawals (see table 5.3.). Sanctions for other sectors (except for VASPs) were only a few, however, they seem to be proportionate to the size of

45. EUR 906 610; EUR 647 070; EUR 1 028 850; EUR 5 854 865; and EUR 1 556 046.

46. Crediting, including financial leasing, where the provision of services is not subject to licensing is subject to the supervision of the SRS, while persons engaged in providing consumer credit services and to whom the CRPC issues a license for the provision of consumer credit services is subject to the supervision of CRPC.

business activities; and supervisors were able to demonstrate their positive impact on the level of compliance. Low number of on-site examinations as discussed in Chapter 3.5 also has an impact here.

Table 3.3. Sanctions applied to FIs and VASPs for AML/CFT breaches in 2018-2023

	No of written warnings	No of fines	Amount of fines (EUR)	No of removal of manager/ compliance officer	No of withdrawal of license	No of operational restrictions
Banks	4	14	20 232 424	1	2	7
PIs	3	3	36 754	2	-	2
EMIs	2	2	80 975	1	-	2
Investment firms	-	3	58 177	1	-	1
Investment management companies	-	2	70 932	-	-	2
Credit unions	-	-	-	-	1	-
Life insurance	-	-	-	-	-	-
Currency exchange	8	27	77 065	1	4	4[47]
VASPs	0	7	105 450	0	0	2
Lenders/leasing	6	4	23 000	-	3	-

217. Whilst Latvijas Banka considers controls by securities firms to be less robust and overall risk to be higher than in banks, very few sanctions have been applied to the securities sector. Latvijas Banka explains that targeted supervisory actions, such as prescribed external audits, targeted inspections, awareness raising and remedial actions, have had a positive impact on the investment sector's compliance. As for PIs and EMIs, sanctions applied were not significant in monetary terms, however, these sectors are small and the services they provide present a lower risk. No sanctions have been applied to the insurance sector, however, its risk exposure and materiality are low.

Box 0.1. Examples of sanctions applied by Latvijas Banka

Change of a business model of a credit institution after supervisory intervention

Several supervisory actions have been undertaken between 2018 and 2023 regarding a credit institution that resulted in the application of sanctions, such as a monetary fine and operational restrictions. As a result, the credit institution significantly reduced the ML/TF/PF risks linked to its customer base, and overall AML/CFT/CPF compliance has improved.

Withdrawal of a credit institution's licence

Despite several supervisory interventions by Latvijas Banka, a high-risk profile bank continuously failed to comply with AML/CFT requirements. Therefore, a decision was adopted to withdraw the license of the credit institution. Several layers of AML/CFT exit controls were imposed, such as the development of a specific AML/CFT methodology regarding payouts and asset sales, to ensure a transparent and controlled exit from the financial market.

218. Whilst occasionally sanctions are appealed, there were no instances where applied sanctions were annulled by the court. Latvijas Banka has a sanctioning policy in place to ensure that sanctions are proportionate to the level of severity of a breach (repeated, systemic nature of shortcomings, as well as

47. Suspension of licence.

aggravating factors are taken into account). Publication of sanctions adds to the dissuasiveness of the sanctioning regime.

219. In addition to sanctions, remedial actions, such as an imposed requirement to remedy deficiencies within a specified timeframe and supervisory follow up, are applied as a routine practice. Latvijas Banka has the right to demand an external audit to test AML/CFT control systems (for some sectors, such as banking, this is a mandatory legal requirement) which is paid for by the FI and is frequently used as part of remediation.

220. The SRS and CRPC approach to sanctioning is considered less dissuasive due to the "consult first"[48] principle, however, both supervisors were able to prove that follow-up and remediation practices still have a positive effect. During the assessment period, all VASPs have been inspected with dissuasive and proportionate fines applied. A small number of fines have been applied to lenders which are considered to have limited dissuasiveness; however, lenders' sector ML/TF risk exposure is limited.

221. All of the above measures had a proven effect on REs' compliance, however, there is still room for further improvement (see Section 3.4 above – FIs' and VASPs' implementation of preventative measures).

Guidance and training

222. AML/CFT knowledge and awareness raising efforts by supervisors are commendable (see Section 3.2) and add to increasing the level of compliance by REs.

48. Supervisors initially take necessary actions to increase RE compliance through training, consultation, and mandatory remediation practices. Sanctions are applied as a secondary measure. "Consult first" is commonly applied to newcomers and it is not possible for repeated/severe breaches and/or follow up examinations.

Chapter 4. Non-financial Sector Supervision and Preventive Measures

The relevant Immediate Outcomes considered and assessed in this chapter is IO.4. The Recommendations relevant for the assessment of effectiveness under this chapter are R.22, 23, 28, 34 and 35 and elements of R.1, 29 and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Despite some remaining gaps in legislative provisions applying to the SRS, controls effectively prevent criminals and their associates from holding or being the BO of a significant or controlling interest or holding a management function in DNFBPs. Breaches of licensing and registration requirements are effectively detected and addressed.

b) All supervisors, except for the LCSA, effectively collect information to identify ML/TF risks. Whilst supervisors of gambling operators and notaries have also demonstrated a good understanding of risk, results of institutional risk assessments conducted by the SRS - which are based on around 60 risk criteria - are not considered by the AT to be consistent with national or sectoral risks. The LCSA has not provided sufficient evidence to demonstrate that it understands the institutional ML/TF risk presented by advocates that it supervises.

c) All supervisors have effectively promoted understanding of national and sectoral ML/TF risks and AML/CFT requirements, including to higher risk DNFBPs.

d) In most cases, DNFBPs have demonstrated a good understanding of national, sectoral and institutional risks, and how these have changed over time, though the SRS continues to identify shortcomings in business-wide risk assessments and risk mitigation in sectors identified as presenting a medium-high ML risk (a declining trend).

e) In most sectors, DNFBPs have demonstrated effective implementation of AML/CFT requirements. Proactive work by the FIU has helped to increase the total number of STRs to the extent that under-reporting is now focused in the legal sector. Notwithstanding, weaknesses remain in the application of reporting obligations by accountants.

f) All DNFBP supervisors have internal regulations in place to support risk-based supervision and around 10% of DNFBPs are inspected each year. Whilst it is clear that inspections are risk-based, SRS supervisory effort may not always be directed to where ML risk is highest. The LGSI effectively monitors compliance by gambling operators with AML/CFT requirements. The LCSN has applied elements of a risk-based approach which are considered to be sufficient, but the inspection model applied to advocates cannot be considered properly risk-based and is limited by resources that are available to the LCSA.

g) Effective use is made of remedial actions by the SRS and LGSI, which are followed-up to ensure that particular shortcomings have been addressed. There has also been quite extensive use of fines by the SRS and LGSI, and, together with publicity given to enforcement action can be considered sufficient to ensure future compliance and to be dissuasive of non-compliance by others. It has not been demonstrated that sanctions applied by the LCSA can be considered effective. Generally, supervisory action has had a positive impact on levels of compliance by DNFBPs over time.

h) Currently, a competent authority does not oversee the work of the LCSA or LCSN (self-

regulatory bodies (SRBs)), though the MoF (and before that the FIU) chairs a committee that co-ordinates the work of all supervisors (including for FIs).

Key Recommended Actions (KRA)

a) The SRS should review and amend as necessary its current risk assessment methodology – addressing why the large majority of institutional risk assessments for the sectors under its supervision show a low ML risk, which is not aligned with national and sectoral risk assessments for those sectors. The methodology should clearly articulate how such institutional risk assessments and other factors subsequently form the basis for risk-based supervision.

b) The LCSA should collect additional information to assess and understand the institutional ML/TF risk present amongst those advocates that are subject to the FATF Standards and develop a fully risk-based approach to supervision that is supported by sufficient resources.

Other Recommended Actions

a) A competent authority should be established to oversee the work of professional bodies (SRBs), including how conflicts of interest are identified and managed.

b) The authorities should take measures, which may include legislative amendments, to: (i) prevent associates of criminals from holding significant or controlling interests in DNFBPs; (ii) consistent with the constitution, review, and as appropriate, extend the range of criminal offences that prevent a person from holding interests in DNFBPs; and (iii) prevent criminals and their associates from acquiring interests or being appointed to a management function in an independent legal professional or TCSP.

c) The authorities should continue to take action to increase ML/TF reporting levels by advocates and independent legal professionals so that they are commensurate with size and risk exposure.

d) Supervisors should periodically analyse results of supervisory engagement in order to support the collection and maintenance of data that identifies whether supervision has a demonstrable positive impact on compliance by DNFBPs over time.

Overall conclusions on IO.4

Many strong features are in place to support the supervision of compliance by DNFBPs with AML/CFT requirements.

However, “fit and proper” controls applied to independent legal professionals, a minor number of whom are under investigation for possible third-party ML, cannot prevent initial criminal ownership or management. This sector is considered to have higher importance in the moderate importance band and this shortcoming has been given a higher weighting. Moreover, the results of the risk scoring system used by the SRS are not consistent with national or sectoral risks and, whilst it is clear that supervision takes account of risk, SRS supervisory effort may not always be directed to where ML/TF risk is highest. These shortcomings apply, amongst others, to accountants which are considered to have high importance in Latvia, and so have been weighted more heavily. Weaknesses have also been identified in institutional risk assessments and inspections of advocates, but these shortcomings have not been weighted heavily, given the materiality and risk of the sector.

DNFBPs have demonstrated a good understanding of national, sectoral and institutional risks,

and, in most cases, have demonstrated effective implementation of AML/CFT requirements. The FIU now considers that under-reporting of suspicion of ML by DNFBPs is limited to the legal sector. Notwithstanding, weaknesses remain in the application of reporting obligations by accountants, where the number of shortcomings identified in on-site examinations remains high compared to other sectors. Given that these shortcomings apply to independent legal professionals and accountants, they have been weighted more heavily.

Latvia is rated as having a moderate level of effectiveness for IO.4.

223. Four separate supervisors are responsible for oversight of DNFBPs: (i) the SRS; (ii) the LGSI; (iii) the LCSA; and (iv) the LCSN. Professional bodies are responsible for overseeing compliance by advocates and notaries. Numbers licensed or registered and relative importance of DNFBP sectors are provided in introduction (Section *Financial sector, VASPS and DNFBPs*). In addition, the MoE is responsible for licensing real estate agents and the MoJ licences notaries and oversees any sanctions applied to them.

224. The SRS is the largest supervisor of DNFBPs - responsible for the supervision of approximately 9 500 entities (including some FIs and VASPs). Of these, around 7 000 fall within the scope of the FATF Recommendations. An overall breakdown is not available on the number of DNFBPs by sector that are within the scope of the FATF Standards. The SRS has established an AML Department (49 employees) which is responsible for AML/CFT supervision which makes substantial use of IT systems of the tax authority and is considered to have sufficient expertise and resources.

225. The LGSI has two staff who are directly responsible for AML/CFT inspections for around 20 gambling operators, supported by an additional four inspectors with responsibility for more general oversight. There is one full-time employee available to support the work of 19 un-renumerated practising advocates who are appointed by the LCSA and supervise the work of around 1 400 lawyers (including around 500 that are subject to AML/CFT requirements). Similarly, a small number of un-renumerated practising notaries (up to 14 in total) are elected by the LCSN and responsible for oversight of around 100 notaries. Un-remunerated lawyers and advocates participate in inspections.

226. Currently, a competent authority does not oversee the work of the two professional bodies (SRBs), though the MoF (and before that the FIU) chairs a committee co-ordinating the work of all supervisors (including for FIs). Advocates and notaries involved in supervision are expected to identify any supervisory conflicts and recuse themselves from inspections. In practice, conflicts have not presented an issue given the numbers of professionals involved in supervision.

227. The 2018 MER identified quite a number of shortcomings, including: (i) absence of satisfactory entry requirements e.g. real estate agents; (ii) moderate to low levels of understanding of ML/TF risks by supervisors; (iii) very limited application of risk-based supervision; (iv) ineffective sanctioning; (v) limited impact of supervision; and (vi) failure by DNFBPs to demonstrate knowledge of the key constituents of an ML/TF risk mitigation framework and poor implementation of preventative measures. There have been many improvements since then, which are considered below.

4.1. Licensing, registration and controls for DNFBPs preventing criminals and associates from entering the market

4.1.1. Market entry controls

228. Despite some remaining gaps in legislative provisions applying to the SRS,[49] licensing, registration and other controls effectively prevent criminals and their associates from holding or being the BO of a significant or controlling interest or holding a management function in DNFBPs.

229. Gambling operators, real estate agents and accountants are subject to upfront "fit and proper" checks which include: (i) a check that BOs and senior management have a clean criminal record;[50] and (ii) a more general review of reputation, which is sufficiently broad to cover offences not covered in legislation, source of funds for investment, criminal links, ongoing criminal investigations, and linked third parties. Checks are supported by reliable sources and cover foreigners. Whilst controls to prevent criminals and their associates from acquiring interests or being appointed to a management function in an independent legal professional or TCSP are not in place, supervisory powers can be used to affect change.

230. Subsequent changes to BOs and senior management of legal persons are generally notified ex post to the SRS by the ER within one day of the change. All owners and controllers are then checked (all crimes) by the SRS against reliable sources on a fortnightly basis. In practice, checks have not identified criminal links. Changes to BOs and senior management are notified ex post by the ER and gambling operator to the LGSI within five days of the change and, in addition, casino licences are renewed on an annual basis when any changes of ownership or control are again assessed.

231. Criminality precludes accreditation of individuals as advocates and notaries. Both SRBs obtain evidence of a clean criminal record, and the LCSA releases a pre-exam candidate list for advocates to flag any reputational concerns, e.g. links to criminals. Consent of the LCSA is needed also to register a firm of advocates as a partnership or LLC. Only an advocate may be a member or sit on the board of a partnership or LLC. Checks are subsequently performed on advocates at least once a year. Notaries may practice only as individuals. Checks on notaries are updated on an annual basis, but changes would be picked up sooner, e.g. through complaints.

232. All supervisors have presented examples of applications that have been refused and licences revoked due to criminality.

4.1.2. Detecting and addressing breaches

233. Breaches of licensing and registration requirements are effectively detected and addressed. Public registers of DNFBPs make it possible to identify those that are conducting non-authorised business.

234. In order to identify unauthorised DNFBP activities, the SRS makes use of extensive data sources held to support tax collection and monitors social networks, adverts, and complaints. It also conducts on-site inspections where economic activity is detected without registration. Fines have been applied to real estate agents and accountants for unauthorised activities during the assessment period – averaging around EUR 2 333 for real estate agents and EUR 600 for accountants. The SRS has also suspended activities of unauthorised accountants until they have been authorised and other violations eliminated. The LGSI monitors media sites, land-based activities and other information in the public domain or held by other competent authorities to identify unauthorised activities and keeps a register of unlicensed operators. Neither

49. Some of these are set out at c.28.4((b). Measures in place to prevent criminals from holding significant or controlling interests do not cover all criminal offences. Measures are not in place to prevent associates of criminals from holding a significant or controlling interest.
50. For real estate agents, checks cover property-related offences, economic offences and offences related to terrorism. For accountants, checks cover criminal offences against the national economy or in the service of state institutions and offences related to terrorism.

the SRS nor LGSI have identified cases where unauthorised activities continued after breaches were initially identified.

4.2. Supervisors identifying, understanding and promoting DNFBP understanding of ML/TF risks

4.2.1. Identifying and maintaining an understanding of the ML/TF risks in the different sectors and types of DNFBPs, and of individual DNFBPs over time

235. All supervisors, except for the LCSA, effectively collect information to identify ML/TF risks. Whilst the LGSI and LCSN have also demonstrated a good understanding of risk, results of institutional risk assessments conducted by the SRS – which are based on around 60 risk criteria (conditions) - are not considered by the AT to be consistent with national or sectoral risks. The LCSA has not provided sufficient evidence to demonstrate that it understands the institutional ML/TF risk presented by advocates that it supervises.

236. All DNFBP supervisors have prepared and published sectoral risk assessments during the period under assessment (most recently for the period from 2020 to 2022) and have taken part in preparation of the most recent NRA. Both national and sectoral assessments show how risks have changed over time. Based on internal regulations, risk assessments are also prepared at institutional level for DNFBPs and are periodically updated.

237. In the case of the SRS, institutional risk is calculated automatically (using the SAP HANA IT technology platform (SAPA HANA)) based on a combination of: (i) data held in information systems of the tax administration (on DNFBPs and their clients) to support tax compliance; (ii) external information systems; and (iii) around 60 wide-ranging risk conditions. Sources (i) and (ii) are updated bi-monthly which means that fortnightly assessments are conducted in "real time" and always based on up-to-date data. Risk conditions are reviewed at least annually – taking account of changing national and sectoral risks and findings from inspections. However, the results of institutional risk assessments do not align with national or sectoral risks. Whilst a large majority of DNFBPs have been assessed by the SRS as presenting a low risk (on average around 90% throughout the assessment period), this is in sectors identified as presenting a medium-high or medium ML risk in national and sectorial risk assessments, where risks identified apply irrespective of business size. The AT considers that this could be due to the risk-scoring system which gives a higher score to DNFBPs with the greatest number of higher risk clients - and so may not adequately recognise that DNFBPs with a small number of clients can also present an inherently higher ML risk.

238. The LGSI assesses institutional risk on an annual basis, or when new risks are identified. It does so using information that is: (i) collected on a quarterly and annual basis from gambling operators; (ii) held in the Unified Gaming Machine Control and Monitoring System (AKUS) which analyses statistical data; and (iii) available remotely from on-line operators on transactions. Institutional risk assessments also take into account the results of the NRA, financial information, market share, and information available from the SRS – tax administration. Matrices are then used by the LGSI to calculate institutional risk. Those operators with limited activities tend to be rated as presenting a low risk (around 25% on average during the assessment period), whereas others are rated as medium or high risk, which is in line with national and sectoral risk assessments.

239. The risk assessment for advocates focuses only on the extent to which activities are conducted that are within the scope of the FATF Recommendations (including those related to the creation, operation or management of legal persons) and so does not support the application of risk-based supervision. No additional information is requested to support an assessment of risk, apart from on internal control systems (October 2024).

240. In the case of notaries, the LCSN has access to: (i) the Register of Authorisations Certified by Sworn Notaries which records information on all notarised transactions; (ii) SRS – tax administration databases; (iii) STRs made by notaries; (iv) formal and informal complaints made about notaries; and (v) test results

following training. Each year, notaries also submit a self-declaration to the LCSN in which they provide relevant information and a self-assessment of risk (risk score and mitigating factors). The risk level of each notary is assessed at least annually, based on eight risk factors. The majority of notaries are now assessed as presenting a low or medium risk (around 5% are high risk), which is in line with national and sectoral risk assessments.

4.2.2. Promoting DNFBP understanding of ML/TF risks and AML/CFT obligations

241. All supervisors have effectively promoted understanding of national and sectoral ML/TF risks and AML/CFT requirements, including to higher risk DNFBPs.

242. The authorities have taken extensive steps to ensure that the results of the NRA and SRAs are widely known, including amongst higher risk DNFBPs, and there is a high level of awareness of risks identified. Inter alia, they do so through co-operation with industry associations, participation in conferences and seminars, and use of webinars, including at the time of introduction of licensing requirements for accountants (medium-high risk sector). In support of these assessments, the authorities have also produced a number of helpful documents for all medium-high risk sectors (though at the end of the assessment period).

243. The SRS makes use of its EDS to send information, respond to questions and publish training materials. The LCSA has created a section on its website where all relevant information about ML/TF/PF prevention can be found. On an annual basis, the LCSN compiles the most important conclusions from its inspections, including most common errors and best practices observed, and presents a report to all notaries at a meeting organised for this purpose.

244. The SRS has developed a number of e-learning courses and made use of video seminars and social media to support compliance with AML/CFT requirements. E-learning courses are used only by a relatively small number of DNFBPs under supervision. The LGSI, LCSA and LCSN run different training events each year, which are well attended.

4.3. DNFBP understanding of existing and evolving ML/TF risks

245. In most cases, DNFBPs have demonstrated a good understanding of national, sectoral and institutional risks, and how these have changed over time, though the SRS continues to identify shortcomings in business-wide risk assessments and risk mitigation in sectors identified as presenting a medium-high ML risk (a declining trend). Gambling operators, real estate agents and accountants consider that the NRA and SRAs now overstate the level of ML risk, taking account of vulnerabilities that have reduced since completion of NRA2. Understanding of TF risk is sufficient, given that the risks of TF in Latvia are low.

246. Real estate agents and accountants demonstrated a very clear understanding of ML risks and how these had changed during the assessment period. Other than through company formation, independent legal professionals did not articulate well how they could be used in ML. Gambling operators, advocates and notaries demonstrated a good understanding of ML risk, which has changed significantly for advocates during the assessment period as cross border business has dried-up.

247. DNFBPs assess risk and develop risk assessments, which are reviewed at least every three years. Compliance with this requirement is assessed by the SRS as part of every on-site inspection. Inspections have identified some cases where institutional risk assessments have not been conducted, all risk factors have not been identified (including results of NRA) and assessments have not been documented (a declining trend). This includes sectors assessed as presenting a medium-high ML risk. Based on inspections, the LGSI, LCSA and LCSN have concluded that DNFBPs have properly identified risks and established internal control systems to address those risks, and no major shortcomings have been identified.

4.4. DNFBP understanding and compliance with AML/CFT obligations and mitigating measures

248. In most sectors, DNFBPs have demonstrated effective implementation of AML/CFT requirements. This is consistent with the rather modest number of supervisory inspections that have identified systemic AML/CFT infringements. Proactive work by the FIU has helped to increase the total number of STRs to the extent that under-reporting is now focussed in the legal sector. Notwithstanding, weaknesses remain in the application of reporting obligations by accountants.

4.4.1. CDD, record-keeping, BO information, ongoing monitoring

249. Inspections by the SRS show that risk based CDD and record-keeping measures are in place in most cases. However, weaknesses remain in the application of CDD and ongoing monitoring by accountants. In 2019, the LGSI identified a number of infringements linked to the application of CDD, but this has improved since then. The LCSA has identified only two cases where advocates have failed to properly document the BO of a client, and LCSN inspections indicate "general success" in determining the scope of applicable CDD with no deficiencies having been identified.

250. In practice, customer identification questionnaires are used to collect CDD information, which is verified, BO is found out, and the source of funds collected (which may be verified in higher risk cases). Checks are made against public sources for adverse information. To develop client profiles, advocates also request information on tax status, independent legal professionals collect CDD through an interview with their potential client, and accountants and advocates request information on major partners and consider the management experience and economic substance of the potential client.

251. Where a customer is a legal person, then, inter alia, information collected on BO is compared to information held in the ER (or foreign equivalent where available) and consideration given to the possibility that persons other than the shareholder may have control. Changes in BO and control of legal persons are automatically picked up through subscription to databases of enterprises. Complex ownership structures are not common.

252. Upon entry to land-based casinos, customers (natural persons) must first register which is conditional upon providing proof of identity and some basic CDD information. As soon as bets placed or winnings cashed equal or exceed EUR 2 000, then further CDD information is collected, including source of funds (and may be verified for high-risk customers). Steps are taken to ensure that all activity at cash desks and gaming tables is linked to each customer. The same approach is applied in the case of slot machines.

253. All gambling operators use third party IT solutions to identify negative information, unusual activity (based on set parameters) and suspicious transactions (using "red flags"). All land-based operators have implemented IT solutions for monitoring of slot machines and identifying customer activity that passes the CDD threshold of EUR 2 000. Systems generated "hits" are handled within 24 hours.

254. Generally, estate agents, independent legal professionals, advocates and notaries perform individual transactions and so there is no need for ongoing monitoring. Based on risk, accountants monitor transactions in order to check that they align with the customer's business and expected cash flows, looking for inconsistencies or potential irregularities.

255. Business has been refused or terminated by DNFBPs on the basis of the provision of incomplete CDD information. In the case of advocates, it is not common for business to be declined since potential clients tend to withdraw applications before this stage.

256. Records are held in line with, or for more than, the statutory requirement.

4.4.2. Enhanced or specific measures

257. SRS and LGSI inspections show that enhanced measures are generally in place to deal with higher risk customers. Weaknesses remain in the application of enhanced CDD measures by accountants, where the number of shortcomings identified in on-site examinations remains high compared to other sectors. LCSA inspections show that advocates have measures in place to identify and deal with customers that have connections to high-risk countries. No discrepancies have been detected by the LCSN in the application of enhanced measures, including to PEPs.

258. PEPs (including the customer and BO) are identified through self-certification and use of the PEP Register maintained by the SRS. Gambling operators, accountants and advocates also use third party IT solutions to identify PEP connections. Otherwise, reliance is placed on information held on the Internet to identify foreign PEPs. Extensive use is made of lists of high-risk countries provided by the FIU. PEPs and those with a connection to high risk third countries are subject to additional CDD.

259. Outside online gambling operators, little use is made of technology in the provision of services to customers by DNFBPs, and so the application of measures has not been assessed. In the case of gambling, new technological solutions have not been used or introduced in the provision of services to customers.

4.4.3. AML/CFT reporting obligations, tipping off

260. Overall, low DNFBP reporting in terms of the total STR volume and number of entities reporting has been identified as a problem in the two most recent NRAs, and reporting levels during the assessment period have not been commensurate with the size and risk exposure of the DNFBP sector as assessed under national and sectoral assessments. Proactive work by the FIU has helped to increase both: (i) the total number of STRs; and (ii) the number of DNFBPs making reports (from around 20 in 2018 to around 140 in 2023), particularly accountants – to the extent that under-reporting is now focussed in the legal sector. Notwithstanding, weaknesses remain in the application of reporting obligations by accountants, where the number of shortcomings identified in on-site examinations remains high compared to other sectors.

261. Whilst supervisory findings confirm that the majority of DNFBPs comply with reporting requirements, the SRS has identified 182 cases between 2019 and 2023 (4% of inspections) where an accountant failed to file the required STR to the FIU. This is a significant number relative to the total number of STRs made by accountants and DNFBPs more generally in the period under assessment. In addition, the SRS regularly reports suspected underlying criminality of DNFBP customers to the FIU (25 cases in 2023) in cases where an STR has not already been made by the private sector. The majority of these reports have related to accountants.

262. Based on examples of STRs and case studies presented, the AT concludes that DNFBPs are reporting activity that is useful for law enforcement. This is confirmed by the FIU. There have been no tipping off issues.

4.4.4. Internal controls, procedures and audit to ensure compliance

263. Strong internal control systems are generally in place. Given the profile and size of DNFBPs, except for gambling operators, there is no independent testing of systems in place and owners usually act as responsible persons (compliance officer). DNFBPs do not operate through groups.

264. The SRS has found that most DNFBPs invest significant resources in internal control systems which reflect business risks. Nevertheless, inspections have identified shortcomings in the application of internal controls and procedures, including for sectors which present a medium-high ML risk, in particular accountants. According to statistics maintained by the LGSI, 88% or more of gambling operators have updated internal control procedures on an annual basis between 2020 and 2023. The LCSA considers that advocates carry out an updated risk assessment at least every three years in line with requirements. The LCSN considers that notaries have implemented an adequate internal control system.

265. Larger DNFBPs supervised by the SRS are screening staff before and during employment. The position for gambling operators has not been explained.

266. Findings from SRS inspections show that DNFBPs train their staff. According to statistics maintained by the LGSI, all staff were provided with AML/CFT training in 2023 (up from 77% in 2018). As noted above, the LGSI picked up shortcomings in the quality of training in its inspections of land-based casinos in 2023. Advocates generally record training and test the effectiveness thereof, though supervisory inspections in 2023 by the LCSA highlighted a small number of failures to attend or record training. They report to the LCSA on how much training has been provided. Employees of notaries are tested after training and the LCSN has detected only a few cases where staff have had insufficient knowledge on AML/CFT matters.

4.4.5. Legal or regulatory impediments to implementing AML/CFT obligations and mitigating measures

267. There are no legal or regulatory impediments to implementing requirements and mitigating measures.

4.5. Supervisors risk-based monitoring or supervising compliance by DNFBPs

268. All DNFBP supervisors have internal regulations in place to support risk-based supervision and around 10% of DNFBPs are inspected each year. In addition to supervising compliance with preventive measures, the SRS conducts very detailed inspections of client transactions (recognising that it is an integral part of the tax administration). Whilst it is clear that supervision takes account of risk, SRS supervisory effort may not always be directed to where ML risk is highest. The LGSI effectively monitors compliance by gambling operators with AML/CFT requirements. The LCSN has applied elements of a risk-based approach which are considered to be sufficient, but the inspection model applied to advocates cannot be considered properly risk-based and is limited by the current level of LCSA resources.

269. On-site inspections by supervisors focus on understanding of risk, application of internal control systems, application of CDD measures, identification of BO and (where applicable) monitoring. Except for advocates, inspections take account of findings of the NRA and other risk assessments. However, it is not clear to what extent the intensity of inspections (i.e. duration and scope) takes account of risk.

Table 4.1. Supervisory activity (excluding follow-ups) – all DBFBPs (including those outside the scope of FATF Standards)

DNFBP*	2019		2020		2021		2022		2023	
	On-site	Off-site	On-site	Off-site	On-site	Off-site	On-site	Off-site	On-site	Off-site
Accountants (4 944)	730	536	429	41	247	22	358	3	365	40
Independent legal professionals (1 870)	176	0	147	35	120	29	295	3	151	28
Real estate agents (1 304)	61	230	76	29	124	31	159	4	101	27
TCSPs (628)	145	57	75	8	42	9	172	1	30	2
DPMS (110)	11	47	7	0	2	1	5	0	8	1
Gambling operators (20)	32	0	17	0	9	28	20	20	21	17
Advocates (490)**	131	1369	23	1 212	8	64	0	1179	0	0
Notaries (105)	107	0	9	8	103	0	15	6	5	0

*Number of DNFBPs as per 30 June 2024 in brackets (for advocates- only those within scope of FATF Standards). One inspection may cover more than one DNFBP sector.

**For offsite inspections, except for 2021, reference is made here to the collection of information from advocates on activities conducted – to determine the extent to which those activities are covered by the scope of the FATF Standards.

270. The SRS is the largest DNFBP supervisor and, between 2019 and 2023, has conducted around 80 inspections over the course of each month, a commendable amount (around 10% of DNFBPs per year). However, not all of these inspections relate to DNFBPs within the scope of the FATF Standards, and some DNFBPs could have been inspected more than once during the course of a year.

271. Whilst it is clear that the basis for selecting DNFBPs to inspect takes account of risk, there is only a partial link between the results of SRS institutional risk assessments and its inspection plan. Each fortnight, SAP HANA identifies the 50 riskiest DNFBPs out of several hundred high risk DNFBPs, and this list is then reviewed by seven analysts in the AML Department. Given that the underlying data used to calculate risk is refreshed on a bi-monthly basis, the list of 50 DNFBPs changes from assessment to assessment but is reviewed by analysts in order to ensure that the same DNFBPs are not continually inspected. In finalising the fortnightly inspection plan, analysts also take account of: (i) current red flags, typologies and trends; and (ii) need for inspections to cover all DNFBP sectors. During the assessment period, inspection plans have covered: (i) real estate agents and accountants that have not registered in line with newly introduced licensing requirements; (ii) DNFBPs subject to higher risk of use in sanctions evasion (following the introduction of new TFS against the Russian Federation and Belarus); and (iii) DNFBPs assessed as presenting a medium or low risk – following detection of a risk event by SAP HANA, e.g. delivery of an STR or receipt of a complaint. The effect of this is that supervisory effort may not always be directed to where ML/TF risk is highest, e.g. where the focus is on unauthorised activities or non-TF related TFS. Notwithstanding, most on-site inspections have been focussed in those sectors identified as presenting a medium-high risk in the NRA and sectoral assessments.

272. On-site inspections by the SRS are all full-scope and are conducted by two inspectors and, in addition to testing application of preventive measures, inspections include detailed reviews of transactions of underlying customers (for AML/CFT purposes) using information available to support collection of taxes. Inspectors spend one day on-site. Off-site –supervision - also full scope - is used to support SRS inspections, focussing on entities that: (i) have registered erroneously; or (ii) are linked to isolated STRs but recently visited. Off-site checks are used also to follow-up on orders to remediate.

273. In the course of a year, all high-risk gambling operators, 50% of medium-risk operators and 20% of low-risk operators are inspected on-site by the LGSI, based on an inspection plan. Inspections focus on targeted areas and themes. After analysing statistical data and financial intelligence provided by the FIU, on-site inspections in 2023 included a review of training at nine land-based gambling venues of six different operators. As explained above, the LGSI also has off-site access to information on transactions conducted by online operators and through gaming machines (land-based operators) which are checked at random. Overall, the scope of inspections conducted by the LGSI is considered sufficiently broad.

274. Since 2020, the focus of on-site inspections by the LCSA has been on: (i) reviewing internal control systems for all new registrations; and (ii) dealing with complaints about violations of AML/CFT requirements. In the case of reviews of registrations of larger law firms, these have been followed up with an on-site inspection when issues have been identified. In practice, there have been three full scope on-site inspections (covering ten advocates)[51] between 2021 and 2024, though there were more inspections in the two preceding years. In 2021 and October 2024, the LCSA also collected and reviewed (off-site) policies and procedures – in the case of the former for three large offices of advocates (covering 64 advocates) and in the case of the latter for all offices of advocates. Taking account of all factors, inspection of activities within the scope of the FATF Standards is not properly risk-based and is limited by the current level of LCSA resources.

275. The LCSN agrees an annual inspection programme. With the exception of 2019 (when all notaries were subject to a full scope review) and 2022 (see below), LCSN on-site examinations have focussed on: (i)

51. One on-site inspection (covering eight advocates) between 2021 and 2023 and two inspections in 2024.

notaries presenting the highest risk; and/or (ii) those starting to practice as notaries – within one year of taking office. Taking into account the homogeneous nature of the sector, low assessment of ML risk, number of licensed notaries (just over 100), and full scope coverage of all notaries in 2019, the AT considers that such an approach is sufficient to mitigate risk and to ensure compliance with AML/CFT requirements.

4.6. Impact of monitoring, supervision, outreach, remedial actions and effective, proportionate, and dissuasive sanctions on DNFBP compliance

276. Effective use is made of remedial actions by the SRS and LGSI, which are followed-up to ensure that particular shortcomings have been addressed. There has also been quite extensive use of fines by the SRS (over 1 000 applied between 2019 and 2023) and LGSI (ten applied between 2019 and 2023) and, together with the publicity given to enforcement action, can be considered sufficient to ensure future compliance and to be dissuasive of non-compliance by others. It has not been demonstrated that sanctions applied by the LCSA can be considered effective. Whilst there is an absence of analyses on trends in supervisory findings, there is a sufficient number of examples (apart from advocates) to show that supervisory action has had a positive impact on levels of compliance by DNFBPs over time.

277. Remedial measures are applied under the "consult first" principle - where shortcomings are minor and fully remedied during or immediately after an inspection. Notwithstanding, in line with guidelines for imposing sanctions, active use is made of fines (particularly for accountants and gambling operators). Decisions are also publicised by the SRS and LGSI on supervisory websites (within days of decision), including the name and registration number of the person. This is a strong feature in a country with a relatively small financial sector.

278. The SRS conducts follow-up inspections on a case-by-case basis to check on improvements linked to the application of remedial measures. It does so through specific off-site inspections or through full scope on-site inspections. The number of follow-up inspections conducted by the SRS has ranged from 10 in 2020 to 254 in 2022 (the latter inflated by follow-ups linked to EU sanctions against the Russian Federation and Belarus) and a good number of fines have been subsequently applied where a DNFBP has failed to address shortcomings originally identified by the supervisor. The LGSI undertakes follow-up checks only on an exceptional basis (five in the period under assessment). The LCSN also monitors application of remedial measures through off-site checks and the supervisor has found that there have been significant improvements. In the case of the LCSA, there has been no need to follow-up inspections since shortcomings are generally resolved during the inspection process.

279. SRS guidance recommends setting a fine of up to 10% of the latest "net turnover" or income from economic activity in the case of a significant infringement,[52] and a number of case studies have been presented to support this. However, there are other cases where the fine applied has been much lower than permitted and, overall, the value of fines applied is low taking into account average DNFBP turnover[53] (including non-regulated activities). Taking into account the publicity that is given to these fines, it is considered that the cumulative effect of sanctions is to ensure future compliance and to be dissuasive of non-compliance by others. The SRS has also used powers to suspend activities of DNFBPs and has done so on over 160 occasions between 2019 and 2024.

280. The LGSI makes use of warnings and fines. For serious and systematic infringements, the supervisor may impose a fine up to 5% of the operator's turnover. In practice, the value of fines applied is higher than for other DNFBPs (three in excess of EUR 45 000) and considered to be effective in promoting future compliance.

281. Two sanctions (both written warnings) have been applied (in 2022) by the Disciplinary Commission against advocates for failing to apply AML/CFT requirements - both related to application of CDD. In

52. A significant infringement is where at least one of the following is established: (i) an internal control system is not in place; or (ii) material requirements of regulatory enactments have been violated.
53. According to the SRS, average turnover for DNFBPs (including non-DNFBP activities) is around EUR 50 000.

addition, sanctions (mainly written warnings, but also one suspension of activities for a month and one exclusion from membership) have been applied against 15 advocates (between 2019 and 2024) for failing to co-operate with the supervisor. Given the predominant use of written warnings, it has not been demonstrated that the effect of sanctions has been to ensure future compliance and to be dissuasive of non-compliance by other advocates. The number of measures applied to notaries for failing to apply AML/CFT requirements has been low since most inspections have not revealed any breaches.

282. Section 4.2 highlights the many positive measures taken by supervisors to promote understanding of risk and AML/CFT requirements.

283. The percentage of SRS inspections without identified AML/CFT infringements has increased from 63% in 2019 to 86% in 2024. The SRS has also provided more detailed statistics on findings by sector, by year, by area examined, and by seriousness, and has seen improvements over time. Similar statistics and analyses have not been provided by other supervisors, except the number of significant breaches of CDD requirements by gambling operators which has fallen since 2019 and is attributed to effective supervisory action. Overall, whilst supervision has had a positive effect over time on DNFBP compliance with AML/CFT requirements, the extent and nature of improvements has not been tracked or recorded by supervisors.

Chapter 5. Transparency and Beneficial Ownership

The relevant Immediate Outcome considered and assessed in this chapter is IO.5. The Recommendations relevant for the assessment of effectiveness under this section are R.24-25, and elements of R.1, 10, 37 and 40. [54]

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Authorities demonstrated a comprehensive understanding of risk posed by domestic legal persons, and a sufficient but more nascent understanding of the risks posed by foreign legal persons. Latvian law does not allow for the creation of domestic legal arrangements. Latvia's exposure to foreign legal arrangements is assessed to be minimal, as no legal arrangements had registered at the time of the on-site and no legal arrangements have been reported as clients of FIs.

b) A range of effective risk mitigation measures are in place, primarily focused on the collection and verification of BO information, which is made public on the ER, strengthened legal requirements, stricter controls on bearer shares and enforcement actions as well as a prohibition on shell companies. Whilst no specific FATF prescribed mitigating measures have been introduced in law to prevent the misuse of nominee arrangements, there are some mitigants in place. Reporting requirements have been extended to non-EU legal arrangements and foreign legal persons with physical establishment and/or economic activity in Latvia that have been identified as having the closest economic activity connected to Latvia, and therefore presenting an increased ML/TF risk.

c) A multi-pronged approach is used for accessing BO information, comprising of information in the ER and information held by REs. Authorities have direct access to basic and BO information through the ER, as well as powers to compel the disclosure of information from REs. 89% of all registered legal persons have filed BO information (the rest being low risk by either having an account which is visible through the Account Register and having been subject to CDD measures or by being inactive or by being subject to liquidation, as evidenced through filings with the SRS). Effective tools are employed to ensure information on the register is accurate, adequate and up-to-date. This is ensured through numerous checks by the ER, as well as supplementary information by the SRS, mandatory discrepancy reporting requirements, active use of liquidation procedures and penalties for non-compliance.

d) Latvia has imposed a range of proportionate and dissuasive sanctions for non-compliance with reporting and disclosure requirements, including custodial sentences in the most egregious cases.

Key Recommended Actions (KRA)

N/A

54. The availability of accurate and up-to-date basic and beneficial ownership information is also assessed by the OECD Global Forum on Transparency and Exchange of Information for Tax Purposes. In some cases, the findings may differ due to differences in the FATF and Global Forum's respective methodologies, objectives and scope of the standards.

Other Recommended Actions

a) Latvia should continue ensuring through appropriate enforcement action that all legal persons are filing the required information with the ER.

b) Latvia should further enhance its understanding of the inherent risk of foreign legal persons with a sufficient link to Latvia and the impact of risk mitigations.

c) Latvia should take actions envisaged by the FATF to prevent the misuse of nominee arrangements.

d) Latvia should take actions to increase a level of compliance with R.24 and 25, primarily focusing on the most significant deficiencies.

Overall conclusion on IO.5

Latvian authorities demonstrated a comprehensive understanding of the historic, legacy and current risks posed by the domestic legal persons and has taken a number of measures to prevent the misuse for ML/TF. Authorities demonstrated a sufficient but more nascent understanding of the nature of Latvia's exposure to foreign legal persons. The understanding of the inherent geographic risks emanating from foreign legal persons can be further enhanced. During the review period, Latvia has undertaken a number of measures to mitigate legal persons-related risks - such as strengthening legal requirements, mitigating the risk of shell companies and controlling bearer shares - which proved effective. Some technical deficiencies exist in relation to nominee arrangements; however, these do not materially impact effectiveness due to the existence and application of offences related to false declaration to the ER on both the nominee and nominator and the public availability of BO information. Latvia should address the TC deficiencies related to nominee arrangements.

The ER is the main source of basic and BO information in Latvia, which is assessed as broadly adequate and accurate due to verification checks conducted by the registry. FIs (especially banks) that are commonly used by LEAs as a supplementary source for BO information, demonstrate a good level of compliance with BO requirements with no serious infringements identified in the past three years. The accuracy of information is enhanced through mandatory discrepancy reporting by REs with effective follow-up actions taken.

Latvia has applied dissuasive, proportionate and effective penalties and sanctions for non-compliance with the reporting requirements.

A small number of technical deficiencies exist, but these have limited impact on effectiveness due to the extensive availability of BO information for legal persons, the clearly evidenced lower risk for domestic legal persons who have not filed information with the ER and do not maintain a Latvian bank account, and the very limited exposure of Latvia to foreign legal arrangements.

Latvia is rated as having a high level of effectiveness for IO.5.

284. Latvia's system for capturing basic and beneficial ownership information for legal persons and arrangements has undergone a series of reforms since its last Mutual Evaluation. Latvia operates a central registry model, with current basic and BO information publicly and freely available, and historic material available upon authorization or on request. Latvia has demonstrated the use of information held by Latvian REs and foreign authorities to ascertain BO information on legal persons. Latvian legal persons must be registered with the ER in order to exist. In Latvia a legal person can be created directly, without the involvement of a CSP. The use of legal professionals to file information is growing due to increased reporting

requirements in relation to legal persons. Authorities estimate that around 50% of Latvian legal persons currently employ the services of a legal professional though precise figures are not available.

285. The risk profile of Latvian legal persons has changed significantly since the last MER. The risk of legal persons and legal arrangements over the review period can be split into two distinct risk types. At the beginning of the review period the primary risks emanated from foreign legal persons with accounts and activity in Latvia, who laundered the proceeds of foreign crimes through Latvia. There were also risks from domestic legal persons to launder the proceeds of crime out of Latvia. These risks have now largely been addressed (see core issue 5.2). The remaining risks from legal persons in Latvia relate to minimal use of Latvian legal persons in tax crimes, with proceeds laundered domestically or to geographically proximate countries (mainly EU Members States and the United Kingdom) and linked to this, the use of foreign legal persons in these jurisdictions linked to this crime type.

286. Foreign ownership of domestic legal persons has reduced significantly over the reporting period. For example, of the 131 993 LLCs registered at the end of 2023, just under 3% (3,608 LLCs) were wholly owned by foreign legal persons. This represents a 56% reduction from 2017 to 2023. The country of residence for shareholders aligns with geographic proximity to Latvia, and trade connections and Latvia's assessment of ML risk (see IO1). Similarly, foreign legal persons, customers of Latvian FIs, also decreased sharply during this period (see core issue 5.1), however, their deposits still amount to 13% of all deposits held by legal persons in Latvian credit institutions. Latvijas Banka continuously monitors this information and uses it further for supervisory purposes. A small number of branches of foreign companies and foreign permanent representative offices (tax liability) are present in Latvia and registered on the ER and with the SRS.

287. Since the last MER, authorities have taken significant legal action against foreign legal persons with illicit financial deposits in Latvian FIs. This has primarily been the use of non-conviction-based asset recovery powers against foreign legal persons with illicit financial deposits in one Latvian FI that was subject to liquidation (see also IO.6). Authorities demonstrated through the provision of case studies and statistics that they have pursued criminal prosecutions relating to the use of foreign legal persons to launder money into Latvia (see IO.7), as well as administrative and legal action where domestic legal persons have failed to comply with their domestic reporting obligations. This has resulted in a significant reduction in the legacy risk of foreign legal persons with connections to Latvia, and additional mitigation measures have increased Latvia's resilience to the risk from foreign legal persons.

288. Latvia does not have domestic legal arrangements, but does allow for the operation of foreign legal arrangements in Latvia (trustees of a foreign law trust). As of January 2024, non-EU foreign legal arrangements who meet certain criteria are required to register with the ER (see core issue 5.4). No legal arrangements have registered with the ER. According to the study conducted by the authorities, no Latvian FIs have foreign legal arrangements as customers, though few DNFBPs identified foreign legal arrangements as customers, and few legal arrangements have been identified within the ownership change of a small number of ownership chains.

5.1. Identifying, assessing, and understanding ML/TF risks of legal persons and arrangements

289. Latvia has assessed the risk posed by legal persons and legal arrangements. Latvia's NRA2 details the risk of domestic legal persons and the legacy risks (risk profile 1) of foreign legal persons with accounts with Latvian FIs. The NRA2 identified the risk posed by legal persons as: (i) Foreign "shell" companies using Latvian financial system (legacy risk); (ii) transfer of shell company activities from overseas to Latvia (legacy risk); (iii) criminals establishing a legal person that does not meet the definition of a shell company (legacy and present risk); and (iv) EU registered companies and companies in geographically proximate countries involved in transaction schemes to evade tax (present risk).

290. Of the 162 888 domestic legal persons in existence at the end of 2022, less than 3% were identified as having a "complex" structure. 90% of declared BOs were Latvian residents, and of the 10% of foreign

national BOs, half were EEA residents. LEAs confirmed that the current risks emanating from domestic legal persons are the use of domestic legal persons to evade tax, in conjunction with the use of legal persons or financial accounts in EU Member States and/or geographically proximate countries. This professional judgement was supported by the provision of case studies and statistics.

291. The NRA2 contained detailed information on the historic risks posed by foreign legal persons, based primarily on analysis of STR data and the freezing of EUR 695.38 million between 2020-2022 of foreign legal persons with accounts in Latvian banks subject to liquidation. Given the change in economic profile and customer base in Latvia, as well as updates to the FATF's Recommendation 24, in 2024 the FIU Latvia, together with the MoJ and the ER, undertook a standalone non-public assessment of the current risks posed by foreign legal persons based on defined criteria. The assessment focused on the jurisdictional risks, deposits held by foreign legal persons in the Latvian banking sector, while also considering publicly available information, including adverse media checks, sanction screening, and information from FIU Latvia internal systems. The assessment reached a broad conclusion that "given the fact, that these foreign-created legal persons hold accounts within Latvian FIs, they are subject to rigorous oversight from an AML/CFT perspective" and overall, currently existing mitigating measures are sufficient. The assessment does not demonstrate an in depth understanding of geographic risk relating to foreign legal persons, however there was a thorough analysis of the nature of deposits of foreign legal persons and the impact of mitigation and control mechanisms. While foreign legal persons still hold considerable assets in Latvia: just under EUR 1.4 billion as of 2023. Over 75% of these deposits belong to legal persons from EU Member States – among the countries with the largest deposits are neighbouring jurisdictions and Cyprus (second largest). Non-EU countries with largest deposits are the United Kingdom (83%), British Virgin Islands (8%), the United Arab Emirates (UAE) (5%), Switzerland (2%) and US (2%). Of these a third of deposits with Latvian FIs were from foreign financial corporations. Latvian authorities broadly concluded that the risks of foreign legal persons are low due to the fact that business relationship with the Latvian FIs are mostly maintained with EU legal persons. The AT is of the opinion that the assessment would benefit from a more comprehensive analysis of the varying inherent geographical risks of foreign legal persons (e.g., non-EU and varying risk levels within the EU jurisdictions) and a more comprehensive analysis of significant investments by foreign legal persons and business activities that foreign legal persons having links with Latvia are engaged in would further benefit the assessment.

292. Latvian authorities have taken considerable action against foreign legal persons in regard to ML, freezing almost EUR 670 million in a three-year period, to address legacy risks from its historic risk profile, see table 6.1 below).

Table 5.1. Frozen funds of foreign legal persons (million EUR)[55]

	2020	2021	2022	Total
Belize	1.64	6.51	18.4	26.55
British Virgin Islands	87.97	16.43	89.1	193.5
Canada	X	6.29	13.6	19.89
Cyprus	37.51	21.44	14.9	73.85
Hong Kong	X	2.06	5.9	7.96
Malta	10.15	X	X	10.15
Marshall Islands	5.03	5.09	23	33.12
Panama	X	7.38	7.8	15.18
Seychelles	13.04	17.61	16.3	46.95
Singapore	X	13.96	X	13.96
UAE	40.82	2.52	X	43.34
United Kingdom	28.27	29.93	73.4	131.6
Other	10.52	2.74	37.6	50.86
				668.91

Legal arrangements

293. Latvian law does not permit for the creation of Latvian legal arrangements, but foreign legal arrangements may operate within Latvia. Interviews with LEAs demonstrated that foreign legal arrangements have not been found to pose an ML threat in Latvia, either historically or presently. There has been some limited involvement of foreign legal arrangements in complex ownership structures that featured in Latvia's historic ML risk profile. Authorities demonstrated that no foreign legal arrangements are registered as holding account with Latvian FIs. Supervisors articulated that Latvian REs would treat foreign legal arrangements as inherently high risk and as a result conduct EDD in such cases.

294. Exposure to foreign legal arrangements by Latvian DNFBPs is estimated to be low. Of the 2 031 DNFBPs sampled by Latvian authorities, only seven reported providing services to either a foreign legal arrangement or a foreign legal person with a legal arrangement in the ownership or control chain. However, given there is no explicit legal obligation for a trustee to declare that they are acting as a trustee when procuring services from a RE (see R.25), it is possible that the number of clients that are legal arrangements may be higher than assessed. The impact of the lack of legal requirement for trustees to declare that they are acting as a trustee when procuring services from a RE is considered minor due to low materiality.

5.2. Mitigating measures preventing misuse of legal persons and arrangements

295. Latvia has taken a number of measures to mitigate the risks associated with legal persons and foreign legal arrangements. These include enhanced transparency and timely access of BO information by making current BO information publicly available through the ER, with historic information available upon authorisation or upon request. All LEAs in Latvia have direct and unhindered access to current and historical information.

Domestic legal persons

296. Since 2018, Latvia has required domestic legal persons to register BO information with the ER. 89% of all registered legal persons have filed BO information (see core issue 5.3). A number of additional measures to prevent the misuse of legal persons have been taken, which primarily relate to increasing the accuracy of information on the ER (see core issue 5.3). LEAs and private sector representatives unanimously identified the ER and the public nature of the registry as a significant factor in the mitigation of risk

55. The asset freezing outlined in the table primarily pertains to one credit institution under liquidation, the operations of which ceased in February 2018.

emanating from domestic legal persons. LEAs also noted the proactive outreach and training provided to them by the ER, which enabled law enforcement to effectively understand, search and use the available information.

297. In 2017, Latvia extended the legal obligations relating to BO collection so that there is now a duty for BOs to disclose their status to the legal person, as well as an obligation on the legal persons to collect and submit information to the ER. Latvia enhanced the penalties for non-compliance with reporting obligations to the ER, for example, in 2019, Latvia extended criminal liability for failure to provide information, and for supplying false information. Latvia has demonstrated through the provision of statistics and case studies that these penalties are being used (see core issue 5.5).

298. In July 2020, Latvia introduced an obligation for REs to report discrepancies between CDD information they have collected, and information held on the ER. This aims to further enhance the accuracy of information held on the ER and utilising the obligation for REs to conduct CDD independently of the information held on the ER. Supervisors demonstrated that they monitor discrepancy reporting in their supervised sectors.

299. In 2018, amendments to the AML/CFT/CPF Law prohibited credit institutions, PIs, EMIs, investment firms and investment management companies to have business relationship with shell companies. Following the amendments to the AML/CFT /CPF Law, horizontal examinations were carried out by Latvijas Banka to check compliance with these requirements. Latvian authorities' data shows that: (i) since 2017, shell arrangements' credit turnover has fallen by 99.6%; (ii) since 2015, incoming and outgoing payments of foreign customers have fallen by 84%; and (iii) since 2019, the number of customers with BO outside the EU has fallen by 68% in comparison to 2023.

300. Latvia introduced legal requirements to register bearer shares; the shares of legal persons failing to do so are annulled (see also R.24).

301. The SRS plays a significant role in risk mitigation for domestic legal persons (through tax related information, suspicious legal addresses, etc.), and SRS concerns about tax risks are the primary reason for refusal to incorporate domestic legal persons, with rejections rising from 50 in 2021, to 178 in 2022.

302. Overall, Latvia has allocated necessary resources to ensure transparency of basic and BO information. This includes increased staff, as well as their capacity and expertise, relevant training, financial resources, IT and other technical improvements concerning basic and BO information maintained at the ER.

Nominee arrangements

303. Directors[56] must be natural persons, legal persons cannot act as directors of domestic legal persons. There is no express prohibition in law prohibiting nominee director and no express disclosure obligation for nominators and nominees (c.24.13(a)). However, a "nominator" who has another individual, the "nominee", register themselves as the board member is still under a legal obligation to register themselves as a BO (due to exercising control by virtue of being able to appoint a board member) and this information is publicly available on the ER. The nominee would be committing a criminal offence of false declaration when they register themselves as the board member and as a BO. Authorities demonstrated the application of a criminal sanction in a case where nominee registered themselves to conceal the identity of the true director and BO.

304. Therefore, whilst there is a technical compliance deficiency for c.24.13 as there is no explicit obligation for a nominator to declare themselves specifically as a nominator the combination of the offence of false declaration for the nominee and the obligation for the nominator to register themselves as a BO and that BO information is publicly available, means that the technical deficiency is not considered to have a meaningful impact on effectiveness as the combination of requirements, the public availability of BO

56. There is no defined term "director" in Latvian law. The term "director" in this report is used to describe executive or supervisory board members of legal persons undertaken roles comparable to those of directors.

information and the criminal liability for false declaration mean that in practice nominee arrangements cannot lawfully take place.

305. Some CSPs (authorities estimate there are seven operational that seem to offer company formation services) can also offer nominee services and must be registered with the SRS to do so. Authorities informed the AT, that currently nominee services are not being offered in Latvia. This conclusion is based on analysis and field visits by authorities which conclusively demonstrated that the limited number of advertisements found online for nominee services are historic and outside of the evaluation period. However, no routine supervisory practices are established to monitor when the existing CSPs start and/or cease offering nominee services. Latvia has introduced enhanced checks and co-operation between the ER and SRS in certain higher risk scenarios that supports the identification of informal (sometimes referred to as "straw men") nominee arrangements. For example, when an application is received to create a new legal person and a board member is already registered as a board member for several legal persons, or where a person is already registered as a BO of several legal persons, or where several companies are already registered at a physical address, this will be referred for investigation.

306. Board members can formally delegate some elements of their duties/powers to a procurator. In these circumstances both the board member and the procurator are recorded publicly on the register as is the nature of this appointment. This arrangement is not considered to meet the FATF glossary definition of a nominee arrangement (see paragraph 135 of beneficial ownership guidance). If a situation arose where this arrangement was within scope in the specific circumstances, the disclosure requirements meet c.24.13(a).

Foreign legal persons

307. Latvia has in place registration requirements for foreign legal persons with the closest nexus to Latvia. At the end of 2023 a total of 735 foreign legal persons were registered with the ER and the SRS in different capacities: (i) 444 branches; (ii) 160 representative offices; (iii) 131 permanent establishments. Additionally, the ER takes note of foreign legal persons in the ownership capacity of domestic legal persons - as sole shareholders of domestic capital companies (3 627 identified foreign legal persons) and as parent companies and entities through which the BO of the domestic legal person exercises control (5 734 identified foreign legal persons).

308. Latvia has an account registry in place that encompasses information on all clients including foreign legal persons holding demand deposit, payment or investment accounts opened in a credit institution, savings and loan association or a provider of payment services. As part of this information, BOs are being recorded. This is also used to access BO information in addition to the ER information.

309. Between 2020 and 2022, Latvian authorities froze EUR 680 million in assets belonging to foreign legal persons holding accounts in Latvian FIs (see also, table 6.1 above, and IO.8). Latvian authorities demonstrated the use of international co-operation to request information from foreign authorities on foreign legal persons as well as the use of public information on foreign registries. Authorities also demonstrated their ability to identify BOs of foreign legal persons where international co-operation has not been provided, for example, through the use of CDD information, analysis of financial flows and transaction data and other methods.

310. Latvijas Banka took proactive measures to mitigate the risks of foreign legal persons. For example, when reporting requirements were introduced for domestic legal persons, Latvijas Banka identified the risk of individuals seeking to use foreign legal persons to circumvent domestic reporting requirement and access the Latvian financial system. This was mirrored by the former supervisor FCMC who undertook a series of targeted and full scope inspections relating to EDD undertaken by credit institutions on legal persons. See IO.3 for more information.

311. Authorities are not able to precisely determine the scale of foreign legal person customers of Latvian DNFBPs, however, DNFBPs interviewed during the onsite visit all outlined a very low number of foreign legal person clients.

5.3. Legal persons: Timely access to adequate, accurate and current basic and beneficial ownership information

The registry approach

312. Latvian authorities can obtain adequate, accurate and up-to-date information on domestic legal persons through the ER in the vast majority of cases through several sources: the ER and FIs/DNFBPs. Latvian authorities demonstrated through the use of numerous case studies the use of information held on the ER by competent authorities to investigate ML involving Latvian legal persons. This includes analysis across the entire ER data to identify any connections between companies or individuals or addresses linked to the identified companies.

313. All legal persons are required to submit basic and BO information to the ER. 89% of the legal persons have filed their BO information, while there is some level of non-filing amongst certain types of legal persons created prior to these obligations being introduced or who have not made any changes to their ownership or representation information since 2021 and are therefore not legally required to file information. At the end of 2023, just over 11% of legal persons had not filed BO information (representing over 18 000 legal persons). Filing rates amongst the highest risk legal persons LLCs and JSCs is 99.87% and 99.56% respectively. The deadline for JSCs to file shareholders information to publish in the Commercial Register was 30 September 2024. Data as of 5 November 2024 shows that 84.4% (748 firms) of the JSCs have filed shareholders information to the ER. The ER has sent out reminder notices to the remaining 138 JSCs. Filing levels are particularly low for Associations, where 15 912 Associations have not filed any BO information. An additional 5 238 Associations have filed that there is no natural person meeting the definition of a BO. Statistical analysis demonstrated that out of 16 763 legal persons that had not filed BO information at the time of the onsite, 62% had a Latvian bank account. Of the remaining 6 436 legal persons that have not filed any information and do not have a Latvian bank account, 98% are identified as essentially dormant, having not filed returns with the SRS since prior to 2021 and meet the requirements to be subject to simple liquidation procedure. The remaining circa 100 legal persons are filing annual returns with the SRS demonstrating that they have no, or almost no annual turnover. Non-filing of information on the ER by legal persons who maintain Latvian bank account is not considered a material deficiency due to the availability of CDD information, as well as the fact that in almost all cases for three types of legal persons the BOs will either correspond to the board, and this information is available on the ER already, or there will be no BOs due to the way control is dispersed for these types of legal persons. The lack of availability of information on the circa 6 436 legal persons that have not filed information and do not have a Latvian bank account is considered a minor deficiency due to the low risk of these types of legal persons for ML, the overall low rating for NPOs in Latvia for TF[57] and the demonstrated lack of economic activity of those legal persons.

314. Latvia identifies LLCs as having the highest inherent risk of misuse for ML. The compliance rate with reporting requirements is assessed to be at 99.87%, but with 1 627 legal persons declaring that they cannot identify their BOs.[58] The ER outlined that, where a legal person confirmed that it cannot identify its BO, that rational is checked by the ER to verify that there is no BO, for example, due to the disparate decision making of the legal person and spread of share ownership. This information is also shared with relevant LEAs. The controller (senior managing official) of a legal person is identified at all times.

315. The number of applications for new legal persons has remained broadly stable over the review period, averaging around 16 000 applications a year. There has been an uptick in refusals in 2022 and 2023 for the creation of new legal persons, though these remain only around 1% of applications. Refusals in relation to changes of information for existing information are considerably higher, averaging around 5% between 2017-23, though they have been steadily decreasing and in 2023 were at 3.7%.

57. Authorities provided a breakdown of the small number NPOs considered at a heightened risk for TF; amongst them, BO information was not declared for only 5 legal persons.
58. Ownership-related data in this context.

316. Information submitted to the ER is subject to a range of checks that are being used effectively to ensure accurate information is contained on the register. The ER has postponed the creation in around a third of cases and postponed changes to existing information in around 20% of cases, on average. This can and has been done due to incomplete information or non-payment of fees. The ER has and continues to undertake research each year to understand the rational for refusals and postponements, based on sampling. From this research authorities conclude that postponements began to be made in 2018 in relation to failure to submit the required BO information, for example, on the nature of ownership or control. To date, refusals for the creation of new legal persons have largely been made based on tax risks identified by the SRS. However, examples were provided demonstrating refusals based on incomplete or insufficiently substantiated BO information. As part of checks, ownership structures are being checked by a state notary, including by checking foreign BO databases in case of need and asking additional supporting documents. Sanctions screening has taken place by the ER on all currently held information every time sanctions lists are changed and on all newly submitted information at the point that it is submitted. An automated digital solution is expected to be in place in June 2025 that will result in continuous screening in real time. In addition, domestic BOs (i.e., founders and executive board members) are checked for criminality (i.e., for deprivation of rights) by accessing relevant law enforcement databases on criminal records. Similar information linked to criminal records is not sought for foreign BOs. Whilst there is no mechanism to monitor how promptly legal persons or arrangements submit required information to the ER following the changes, the authorities rely on discrepancy reporting mechanism that up until now has not signalled delays in reporting required BO information. As a result of the checks undertaken, and the ongoing review of reasons for refusals and delays to incorporation and changes, the impact of discrepancy reporting (see below), information contained on the register is assessed to be sufficiently accurate. For more information on the adequacy and timeliness of reporting, refer to R.24 and R.25 in the TC Annex.

317. Whilst the overall process of obtaining and accessing adequate, accurate and up-to-date information on the BO in a timely fashion has significantly improved, when compared to the start of the review period, authorities identify that challenges remain in verifying this information, especially for entities with complex ownership structures or those established in jurisdictions with differing regulatory standards. Authorities demonstrated how the ER assesses and records information on complex international ownership structures to determine the BOs of legal persons.

Foreign legal persons

318. As noted above, foreign legal persons that perform taxable activities in Latvia are obliged to register branches or representative offices at the ER or SRS. Business activity without registration is monitored by the SRS and is subject to administrative penalties. Between March 2021and 13 February 2023, a total of 1 323 branches and representative offices that did not disclose BOs have been excluded (struck off) from the register. As of 14 February 2023, an impressive 99% of branches and representative offices, totalling 561 out of 568, had successfully registered information on their BOs, with the remaining 1% going through administrative procedures.

Nominee shareholders and directors

319. There are no requirements for nominee directors and shareholders to disclose their status or to register or licence, except for registration requirements applicable to CSPs that might indirectly capture some providers of nominee services. However, this service is not explicitly disclosed when registering. As such, there are no explicit legal requirements for nominees' information to appear in the ER or other relevant registries. However, failure to declare a BO constitutes a criminal offence, according to the CL. The introduced enhanced checks and co-operation between the ER and the SRS in certain higher risk scenarios, as well as the application of CDD measures by the REs, serve as additional means to identify nominee arrangements in practice and access such information. See Section 5.2 for further information on mitigants and materiality.

Bearer shares

320. In June 2022, the Commercial Law was amended to prevent the issuance of new bearer shares and to require existing bearer shares to be dematerialised and registered in the central securities depository by July 2023. Any shares not registered by the deadline cease to have legal force. See also R.24.

Information held by FIs and DNFBPs

321. Latvian authorities can access information held by REs, which typically takes between three to seven business days, however, the timeframe for disclosure can be legally specified by the requesting LEA. LEAs outlined that they will always use the ER to access BO information in every case involving a Latvian legal person, however, they might also compel the disclosure of information from FIs, mostly banks and to a lesser extent DNFBPs.

322. Deficiencies identified by supervisors typically relate to not properly documenting checks carried out on beneficial ownership rather than non-identification on BOs. Instances of serious BO failings have reduced over the reporting period. REs cited the imposition of EU Russian sanctions as a significant factor in increasing their focus on identification of BO information given Latvia's risk and context. LEAs outlined that even in cases where criminality has been identified involving provisions of services to domestic and foreign legal persons serviced by Latvian REs, CDD information held by Latvian FIs and DNFBPs was found by LEAs to be sufficiently accurate.

323. As outlined in core issue 5.2, several measures are made to ensure the accuracy of information held both by the ER and by REs. The effectiveness of these two individual approaches is complemented by mandatory discrepancy reporting by REs, who as of July 2020, must report any discrepancies to the ER no later than three working days after identifying the discrepancy. Between July 2020 and December 2023, 1 641 discrepancies were reported to the ER. It is not clear whether the information held in the ER database is checked against that held on the Account Register. Table 6.2. shows the actions that have resulted from these reports. Over 90% of discrepancy reports were submitted by credit institutions, with DNFBPs responsible for only 13 reports.

Table 5.2. Discrepancy reports made to the register between 2020-2023: further actions

Total number of discrepancy reports: **1 641**			
No discrepancy found: **35**			
Reports to State Police: **1 606**	**Reports subject to analysis**	Departmental inspections	**296**
		Joint departmental inspections	**50**
		Criminal proceedings initiated	**560**
		Added to pre-existing criminal proceedings	**16**
	Refusal to commence criminal prosecution	Refusal to start criminal proceedings	**399**
		Criminal proceedings that have been terminated	**115**
		No grounds to believe that BO information is false, warnings on the register subsequently deleted	**165**
	Reports resulting in prosecution	Handed to PO for initiation of criminal proceedings	**7**
		Ongoing legal proceedings	**6**

Information held by legal persons themselves

324. Legal persons are legally required to maintain a register of their registered shareholders (Commercial Law) and keep and update information on BOs (AML/CFT/CPF Law, 18.1(4), see R.24). Latvian LEAs have necessary powers to compel this information and use it, when necessary. There are no routine monitoring

mechanisms (e.g., checks at the physical premises) established, however, mandatory reporting to the ER combined with the discrepancy reporting by the REs and verification checks by the ER ensures accuracy of BO information, as discussed above.

5.4. Legal arrangements: Timely access to adequate, accurate and current basic and beneficial ownership information[59]

325. Latvia does not allow for the creation of Latvian legal arrangements. However, trustees of a foreign law trust can operate in Latvia and form business relations with a FI/DNFBP.

326. As of 2 January 2024, foreign legal arrangements that are created in non-EU countries are required to register with the ER within 14 days. This obligation covers: (i) a trustee that is a natural person resident in Latvia; (ii) a trustee that is a legal person registered in Latvia; (iii) a trustee that is a natural person residing outside of the EU and plans to start a business relationship or purchase real estate in Latvia; and (iv) a trustee that is a legal person registered outside of the EU and plans to start a business relationship or purchase real estate in Latvia.

327. At the time of the onsite, no registrations of non-EU trusts had been made to the ER. In addition, no companies with shareholders that are legal arrangements have been registered in the ER. This is consistent with a lack of exposure by Latvia to non-EU legal arrangements. No identified business relationship between Latvian FIs and foreign legal arrangements supports this conclusion and only a small number (seven in total) of clients/BOs legal arrangements of DNFBPs. However, as noted above, the lack of explicit legal obligation for natural persons acting in the capacity of a trustee to declare this to REs may potentially impact the visibility of persons acting as a non-professional trustee, however, this may be mitigated to some extent through CDD obligations.

5.5. Effectiveness, proportionality and dissuasiveness of sanctions

328. Latvia has demonstrated, through the provision of statistics, that sanctions are applied to natural persons for failure to comply with basic and BO information requirements. Between 2019 and 2023, 182 charges were brought against natural persons for failure to comply with basic and BO reporting requirements. In total, fines were imposed 12 times for the total amount of EUR 30 560, community service orders – 115 times for the total amount of 12 547 hours and 16 times the person was sentenced to a deprivation of liberty for a total amount of 24 months (see table 6.3. below). During the evaluation period, convictions through prosecutor's penal orders were brought in 106 cases, with EUR 27 120 of fines imposed (roughly just over EUR 2 500 per fine) and just under 11 000 hours of community service. Given the nature of the non-compliance community, service orders are considered proportionate and dissuasive, potentially more so than financial penalties. In addition, for the 62 cases that had reached the court of first instance by the end of 2023, 36[60] have resulted in the imposition of penalties, community service orders or a custodial sentence, which resulted in the application of fines averaging EUR 1 720, community service orders averaging just under 80 hours per case and custodial sentences averaging two months per case. In one case, where a *strawman* acting on behalf of true BO was found guilty of committing a criminal offense, a sentence of three years and six months in prison was applied.[61] These above are considered proportionate and dissuasive for the type of non-compliance identified in these cases.

329. Although a number of some types of legal persons have not filed BO information (see core issue 5.2), the obligation to file for these types of legal persons that existed before reporting requirements took effect in 2018 is only to file information at the point of which the ownership (membership), representation information or BO changes (rather than filing it by a specific date or as part of an annual return).[62] It is

59. See the *Methodology* for Recommendation 25 regarding beneficial ownership information for legal arrangements.
60. The remining 26 cases were ongoing at the time of the onsite.
61. The final sentence is a suspended sentence of four years with a probationary period of four years.
62. Section 18.2(2) of the AML/CFT/CPF Law.

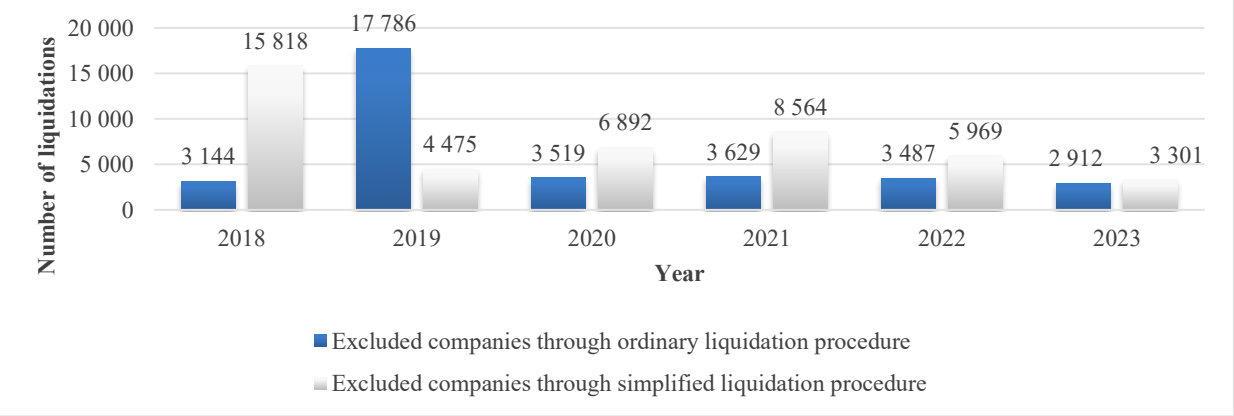
therefore not possible to conclude whether these entities are in compliance with BO reporting requirements. The lack of action against this population to date is considered a minor deficiency given the low risk presented by these entities. Authorities should, however, further prioritise action against these entities now that legal action against higher risk legal persons has concluded and this population is broadly in compliance with disclosure and reporting requirements.

Table 5.3. Outcomes of criminal prosecutions for natural persons for non-provision of information and provision of false information

	2019	2020	2021	2022	2023
Sanction -number of fines	3	-	3	2	4
Sanction – value of fines EUR	5 590	-	9 500	5 500	9 970
Sanction – community service orders (hours)	1 540 (15 cases)	1 380 (17 cases)	2 750 (28 cases)	4 247 (33 cases)	2 630 (22 cases)
Sanction – deprivation of liberty	4	2	4	-	6
Sanction – deprivation of liberty value	2 months and 60 days	4 months	8 months	-	16 months

330. Latvia has demonstrated that a large number of companies have been struck from the register(s) following the BO reporting requirements coming into effect. Companies can be liquidated due to economic inactivity, by virtue of a decision by the tax authority, non-communication, or non-submission of BO information. Authorities outlined that these powers to strike off have primarily been targeted at companies that are assessed to be inactive, rather than those that are active but refuse to comply with requirements. Liquidation is assessed to be a proportionate response to non-compliance in these situations. The overall numbers of non-compliance are decreasing overtime, in line with the requirement that new legal persons, irrespective of their type, must disclose their BOs at the time of creation, with lesser opportunity for non-compliance.

Figure 5.1. Number of companies under liquidation



331. Latvia demonstrated that supervisors have detected failings across FI and DNFBP sectors relating to both basic and BO information. Supervisors commonly apply sanctions for cumulative number of AML/CFT breaches, where identification and verification of legal persons and BOs are checked during broader scope of AML/CFT examinations. The severity of the breaches detected has reduced since 2019 in the banking sector, as have the number of onsite inspections. For example, in 2019, nine onsite inspections found 5 cases of serious breaches, with no serious breaches found in 2022 or 2023. A good level of compliance with CDD/BO requirements is also supported by the on-site interviews with the banking sector. The trend varies across the DNFBP sector, e.g., of the 1 277 onsite inspections for accountants for 2018-2020 (inclusive) no failings were found relating to basic or BO information, whereas for the 970 on-site inspections between

2021-2023 (inclusive) 61 failings were found. A similar theme is evidenced from statistical data relating to estate agents and legal professionals.

Chapter 6. Financial Intelligence

The relevant Immediate Outcomes considered and assessed in this chapter is IO.6. The Recommendations relevant for the assessment of effectiveness under this chapter are R.29-32 and elements of R.1, 2, 4, 8, 9, 15, 34, and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Latvia has implemented substantial reforms to its FIU in the period since the previous evaluation. The FIU has received considerable increases in financial, human, and IT resources, which it deploys effectively to address the country's ML/TF risks. The FIU in Latvia has undergone a significant transformation, becoming a highly effective institution.

b) FIU Latvia and other competent authorities regularly access a broad range of reports, data, and other relevant, accurate, and up-to-date information. This includes high-quality STRs, threshold declarations, and cross-border declarations. This data is used extensively in strategic and operational analysis.

c) Latvia's FIU produces and disseminates high-quality financial intelligence, as evidenced by the successful initiation of ML cases and the utilisation of data. The FIU in Latvia has a strong strategic analysis function which identifies, and analyses ML/TF risks, enhances reporting, as well as suggests risk mitigating measures.

d) Strategic and operational analysis products are created both proactively and on request. The use of financial information and intelligence by competent authorities in Latvia is extensive and forms a critical component of their investigative and prosecutorial process. However, it would be beneficial for some LEAs to further enhance their utilisation of the FIU's strategic analysis capabilities with a view to proactively target specific types of criminal activity in the new risk profile, such as tax offences.

e) Authorities co-operate and exchange information and financial intelligence via secure channels and mechanisms. The FIU engages co-operatively and proactively with relevant LEAs through specialised co-ordination groups for complex cases.

Key Recommended Action (KRA)

N/A

Other Recommended Actions

a) LEAs should make best use of the recently introduced "Black-Box" mechanism to support investigations relevant to Latvia's second risk profile.

b) The SRS should increase its use of the FIU's tactical and operational analysis products, especially with regards to professional ML cases linked to tax evasion cases.

c) FIU Latvia should ensure that the rigour of its analytical products continues to develop given the evolving nature of the country's risks.

Overall conclusion on IO.6

Latvian authorities regularly access and effectively use financial intelligence and related information to investigate ML and associated predicate offences. The use of financial intelligence in TF cases is more limited; however, this reflects Latvia's low TF risk rather than any deficiency in capability. Authorities have demonstrated the ability to apply financial intelligence to TF cases when required.

Competent authorities benefit from well-established and secure co-operation mechanisms, including innovative platforms such as the CCG and the OpCEN. These mechanisms facilitate regular and effective exchange of financial intelligence, supporting both operational and strategic case development. Authorities also develop and use financial intelligence independently, although further integration of these tools into investigative and supervisory workflows would enhance effectiveness for some agencies. Such improvements are considered minor in scope.

The FIU has undergone substantial reform since the last evaluation. With significantly enhanced human, financial, and technological resources, the FIU now operates as a highly effective institution. It plays a central role in Latvia's AML/CFT framework at both the operational and strategic levels, leading national co-ordination, driving the NRA process, and providing technical training, feedback, and strategic guidance.

Latvia is rated as having a high level of effectiveness for IO.6.

6.1. Timely access to relevant, accurate and up-to-date information

332. The FIU and LEAs have access to, and use, various sources of information to conduct robust, risk-based, and useful analyses to identify and advance their pursuit of ML, TF, and associated predicate offences.

6.1.1. By the FIU

333. The FIU has extensive direct (and immediate) access to a broad range of reports and data including the national account register, the ER (includes BO information), cross-border cash declaration data, and taxation databases for both individuals and entities. The FIU also has direct access to all criminal justice databases including courts (court decisions and convictions) police (wanted/missing persons, crime reports), and customs/border control (border crossings, cash declarations). Any information on databases not directly accessible can be obtained upon request. In practice, both public and private sector agencies usually respond in a timely manner, often within hours.

334. Where available, data is accurate and up to date. As outlined in IO.3 and IO.4, STR submissions from FIs largely meet expectations in terms of timeliness, quantity and quality. However, certain parts of the DNFBP sector (specifically lawyers and legal professionals) require improvements (see IO.4 section on AML/CFT reporting obligations, tipping off).[63] The quality and relevance of STRs has been the subject of sector-specific guidance, and the FIU has conducted extensive outreach and training with FIs and DNFBPs to both improve the quality of STRs, and to reduce defensive reporting.

335. FIU analysts use a wide range of data and information from a variety of sources (financial and otherwise) to develop and refine their work. The information is also processed through a range of advanced

63. Overall, the number of STRs made by DNFBPs is not commensurate with the size and risk exposure of the DNFBP sector, as measured through the NRA (see also Chapter 4, IO.4). This discrepancy could impact the FIU's scope of access to, and use of relevant information. The FIU mitigates this impact to a large extent with additional strategic analysis and accessing and using multiple sources of information to develop intelligence. The FIU also engages with REs to enhance reporting quality. They disseminate comprehensive guidelines for reporting, such as goAML manuals and guidelines on suspicious transactions as well as various typology and indicator materials, often in collaboration with other institutions under the CCG format.

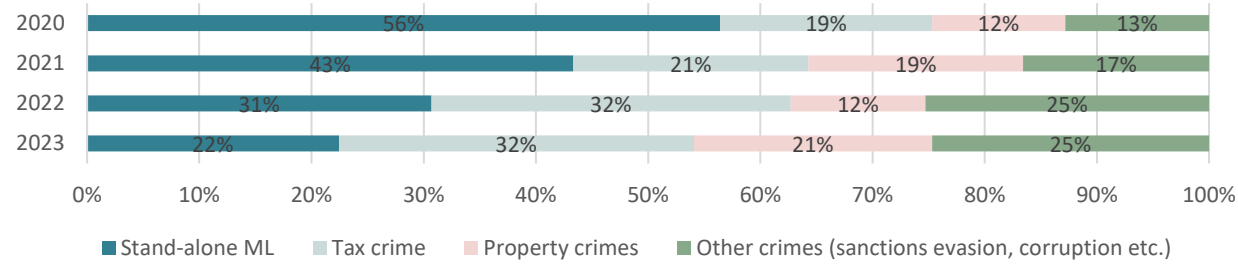
IT tools, enabling the authorities to develop accurate and insightful products. This includes online and direct access to 16 public and private resources, with more than 120 subsystem data sets. For example, the FIU Latvia has direct access to the SRS database with 31 subsystems (tax declarations, VAT partners, corporate income tax, personal income tax, information on employees, taxpayer status, dossier on taxpayer, customs declarations etc).[64]

336. The FIU uses various information sources to develop intelligence, leading to complex investigations. In one such instance, they used tax data to confirm suspicions from STRs about tax offences, successfully sharing this information with tax and police authorities.

337. Since the previous MER, the Suspicious Transaction Report (STR) reporting system has been significantly amended and improved.[65] In October 2021 Latvia adopted a new reporting system (goAML) which replaced the previous case management, analysis and electronic reporting system. The revised reporting system supports the STRs, Suspicious Activity Reports (SARs), and Threshold Reports (CTRs). The yearly number of STRs in the current period is under 6 000 a year (2018-2023); meanwhile, there are on average 76 000 CTRs yearly that are used in various forms of analysis.

338. The reduction and alignment of STRs with Latvia's evolving risk profile demonstrates significant progress in ensuring that reporting corresponds to the country's identified threats and vulnerabilities. The chart below highlights a clear transition from Latvia's historical risk profile—from ML tied to foreign-originated criminal offences and schemes —to a focus on domestic predicate offences, particularly tax and property crimes. Indeed, the table below shows an increasing proportion of STRs linked to tax evasion (32% in 2022 and 2023) and other local offences (25%), which aligns with Latvia's NRA and evolving threat and risk profiles.

Figure 6.1. STRs and the suspected predicate offence indicated by reporting entity



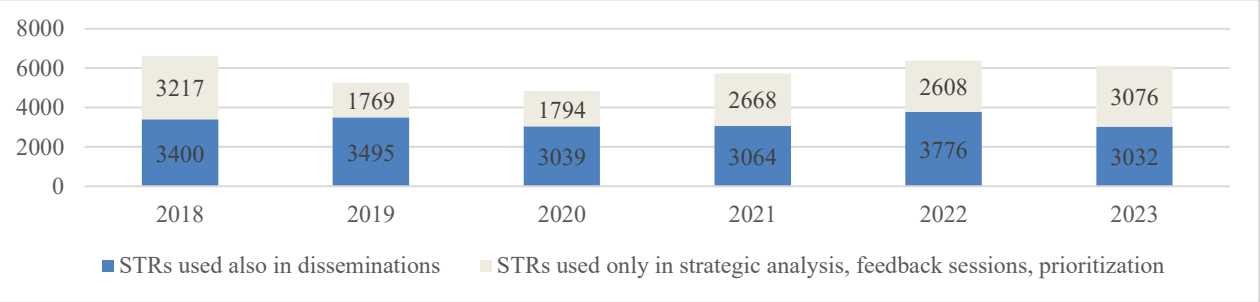
339. STRs received are generally of high quality, evidenced by their use in disseminations to LEAs and in strategic and operational analysis. The quality of STRs is assessed by measuring a number of criteria, for example, number of STRs returned to REs for amendments; the transaction amount included in STRs; STR attachment size; indication of predicate offences; typologies or other supplementary indicators (for instance STR is filed following a CCG meeting). Overall, STR relevance to the risk profile is also monitored by such metrics as number of legal persons per STR; share of STRs indicating most relevant ML risks (like tax

64. There are many databases in Latvia where no additional agreements are necessary for access to data (such as Construction information system, Information on freight licenses, licenses for consumer credit services, registers of the state, etc.) As a result of wide access to outside databases in 2023 the FIU has sent only 14 written requests (1.80%) for information to public registers. Average response time to those has been 10.92 days. Other requests are made directly online – e.g., there have been 33 580 online searches in the ER in 2023.

65. Latvia abolished UTR reporting and introduced threshold declarations (CTRs) in late 2019. The new reporting approach differentiates between STRs and CTRs and fewer defensive reports. The previous MER recommended that Latvia move away from the UTR reporting system. In the previous MER it was found that many of the REs did not understand the difference between "suspicious" and "unusual" transactions as these terms are not differentiated in the Latvian language. This led to significant over-reporting. Regulations, which entered into force in 2019, removed UTRs and introduced threshold declarations (CTRs). This type of reporting was determined to be more useful for conducting strategic analysis as it does not rely on suspicion as a trigger for reporting. Further changes in legislation took place in 2021.

offences or fraud) and others. All STRs are used in one way or another (i.e. for broader strategic analysis). This includes strategic and tactical analysis products; NRA and other risk assessments; updating of STR priority matrix; and a substantial proportion are used in FIU operational disseminations to LEAs.

Figure 6.2. STR use in FIU operational and strategic analysis



340. Regarding TF, FIU Latvia received 30 STRs linked to suspected TF during the review period, with the highest numbers reported in 2018 and 2019. All TF-related STRs are given the highest priority, in line with internal risk scoring system and procedures. Upon receipt, each report is promptly assessed and undergoes a detailed analysis using internal databases, open-source information, and co-operation with national and international partners. This high-priority treatment ensures timely sharing of intelligence with the appropriate authorities.

6.1.2. By other competent authorities

341. State Police, SRS TCPD and the CPCB have direct and timely access to the same key databases that are available to the FIU (i.e. national account register, ER, and taxation databases). Overall, authorities have access to over 70 databases and their sub-systems. Their access is most often immediate, and the data is accurate and up-to-date.

342. The FIU has introduced a mechanism for LEAs to rapidly check and verify the availability of relevant data held by the FIU through an innovative electronic gateway known as the "Black-Box" system. This system minimizes unnecessary, speculative requests for financial information or analysis and allows LEAs to independently conduct preliminary checks of FIU databases to verify the presence of relevant information (such as SARs/STRs/CTRs) before submitting a request to the FIU for detailed reports. Out of the 1 926 searches conducted by LEAs using the Black-Box system from March 2024 to the start of the on-site visit, 324 or 17% resulted in a positive match. Fully operational from August 2024, this system has significantly increased searches and positive matches compared to the previous average of 266 information requests per year. The Black-Box system allows early-stage checks and should be seen as an example of best practice. All Latvian LEAs and competent authorities should be encouraged to make full use of the Black-Box system. All LEAs should embed this process into their standard operating procedures in all appropriate investigations.

6.2. Production and dissemination of financial intelligence

343. Latvia produces high-quality financial intelligence, greatly supporting competent authorities. LEAs praised the FIU's analyses and reports, which were validated through detailed presentations and case reviews. These reports help identify new cases, including unknown persons and trends, and suspected TF activity.[66] Successful international co-operation also aids in tracing accounts and persons abroad. Disseminations align with risks.

66. The FIU has demonstrated a structured and proactive approach to handling STRs related to TF. Despite the national risk level for TF being low, FIU Latvia treats TF as a high-priority area.

344. Disseminated products are used to initiate and support investigations. The primary recipients of FIU Latvia's disseminations are the State Police, SRS TCPD, CPCB, and the State Security Service. In six years (2018-2023) the FIU sent 2 778 disseminations to 9 different LEAs.[67] Almost 70% of all disseminations in the period are sent to the State Police. Of these, majority (close to 80%) are used in criminal proceedings- 57% led to new criminal proceedings and 43% were incorporated into existing cases. The FIU's products include disseminations of both operational and strategic analysis to LEAs (both upon the FIU's own initiative and upon LEA request), annual feedback of RE reporting trends and challenges, analysis done for SCAs prior to licencing a new RE or conducting supervisory inspections.

345. When a case is not initiated by the FIU, the FIU enhances LEAs' own intelligence with reports from REs and authorities, providing actionable intelligence. By analysing and enriching this information, using multiple data sources and advanced tools, the FIU provides actionable intelligence that contributes to a broader understanding of potential criminal activity. Additionally, in many cases when ML investigations are initiated by an LEA's own sources the FIU assists with information and financial intelligence prepared as a response to LEA information requests. The FIU has built robust Open-Source Intelligence (OSINT) capabilities[68] to bolster their analytical capacity.

346. In 2023 alone, LEAs and PO sent 258 information requests to the FIU, 170 of which were from State Police. As an example, in 2020, FIU Latvia investigated a suspected professional ML scheme involving proceeds from an EU-based OCG laundered through Latvian bank accounts. Following extensive analysis, international co-operation, and CCG meetings, the FIU disseminated findings to the LEA and froze assets totalling approximately EUR 3.5 million, including those of a foreign electronic money transfer service and its BO.

347. The FIU's ability to support the operational needs of competent authorities has improved due to institutional reforms.[69] In 2019, the FIU of Latvia transitioned from being part of the Prosecutor General's Office to becoming an autonomous institution under the Prime Minister via the Minister of the Interior. Since then, the FIU has significantly grown in personnel and resources, from 36 positions with a budget of EUR 1.5 million to 91 personnel in 2023 with a budget of approximately EUR 7.8-8.9 million.[70] Since 2024, the FIU has deployed four analysts with specialisations on TF. This resourcing is in accordance with the volume and risk of TF-related reports across its divisions (including those handling initial analysis, strategic assessments, and international co-operation). The FIU has also made substantial investments in technological solutions, which analysts use daily.

348. The FIU has also made significant strides in enhancing the turnaround time[71] for processing STRs/SARs. Every received STR is prioritized on arrival based on the indicated criminal offence, the amount of potentially illicit funds, and other metrics (priority metrics are updated on an annual basis, at minimum). The median STR "turnaround time" for the FIU is 51 days.[72] The increasing turnaround time in more recent years in the table below (2022-2023) corresponds with the risk profile shift - moving from large number of STRs with "refraining" (suspension of transactions) characteristic of the 1st risk profile (see IO.1), to the more complex domestic cases involving public and private sector co-operation and ongoing information exchange (using the OpCEN and CCG mechanisms). The increased reporting of EU sanctions evasion has further heightened the importance of swift and accurate processing of STRs/SARs. The emergence of EU sanctions evasion as a key national risk has added complexity to the production and dissemination of

67. Includes the Internal Security Bureau, EPPO, The Defence Intelligence and Security Service and Internal Security Office by SRS.
68. OSINT analysis leverages both commercially available tools and custom-designed resources to effectively search, compile, and analyse open-source data. This capability significantly enhances the FIU's ability to add value to reports received from REs and other competent authorities.
69. This change addressed an important shortfall identified in the previous MER, and today allows for greater administrative autonomy, including budget management and operational independence.
70. Including 19 persons dedicated to sanctions enforcement.
71. This refers to the time from receipt of a report by the FIU to its subsequent dissemination to one or more competent authorities.
72. This represents the number of days between receiving of an STR into the FIU to its onward dissemination.

financial intelligence. LEAs and the FIU report a growing volume of cases involving attempts to circumvent EU sanctions, often requiring detailed cross-border analysis.

Table 6.1. Median STR turnaround time at the FIU Latvia

2018	2019	2020	2021	2022	2023	2024	Average
44 days	45 days	45 days	46 days	46 days	69 days	63 days	51 days

349. Some complex cross-border cases (e.g., OpCEN cases) take several months for dissemination. These cases require ongoing interaction with relevant LEAs through CCG. The median figures don't capture small-scale fraud cases (fewer days) or large-scale tax evasion schemes involving more than 10 STRs per case (more days).

350. Around half (51.4%) of the country's ML investigations to LEAs are initiated based on intelligence disseminated spontaneously by the FIU.[73] Spontaneous disseminations are largely aligned to the risk profile of Latvia. The table below outlines the number of disseminations per year, according to the major crime types.

Table 6.2. STRs disseminated by FIU to LEAs by suspected offence (2020-2023)

Crime Type Listed in Disseminated STR[74]	2020	2021	2022	2023	Total
Tax Crimes[75]	823	948	1 779	2 060	5 610
Standalone ML	1 675	1 356	960	234	4 225
Property Crimes (incl. Fraud)	200	324	142	141	807
Other Predicates[76]	139	132	354	127	752
Sanctions evasion	0	0	72	267	339
Corruption	18	31	72	40	161
TF	1	1	0	0	2
TOTAL	2 856	2 792	3 379	2 869	11 896

351. Both statistics of total STRs received and those disseminated clearly reflect the evolving risk profile of Latvia. The share and number of STRs with Standalone ML (that is mostly associated with 1st risk profile) disseminated have steadily decreased while STRs of relating to domestic predicate offences (such as tax crimes, fraud and sanctions evasion) now dominate in FIU disseminations.

Table 6.3. ML Investigations initiated based on FIU intelligence disseminated spontaneously

	2019	2020	2021	2022	2023	Total
Total Number of ML Investigations	257	344	340	398	235	1 574
Number of ML Investigations initiated by FIU disseminations	119	219	155	243	86	822
Percentage of ML Investigations initiated by FIU disseminations	46%	64%	46%	61%	37%	52%

352. The FIU also conducts regular strategic analysis to enhance risk awareness, support policy development, and identify emerging trends and typologies related to ML and financial crime. This analysis helps stakeholders, including LEAs, SCA and REs to better understand the evolving risk landscape and adapt

73. Although the proportion of FIU-triggered investigations is lower in proportion than it was to the previous assessment period, the overall number of investigations has increased. Additionally, the lower ratio can be accounted for by higher numbers of investigations initiated by LEAs with stronger ML identification techniques.
74. The yearly data was not synchronised before 2020, and therefore the data is only available for the past four years.
75. Tax Crime STRs are sent automatically to SRS by the FIU and are additionally analysed by the FIU in regard to potential ML. This is a positive feature that enables both the SRS to utilise STRs for tax purposes and in parallel allows the FIU to utilise them to detect ML.
76. Under "Other Predicates" are STRs with indications of corruption, drug trafficking, smuggling, and human trafficking.

their approaches to mitigate these risks effectively. Strategic analysis often involves the examination of large datasets to detect patterns indicative of ML or other illicit activities.

353. An example of the FIU strategic analysis material is detailed below. This showcases how the FIU applies advanced analytical tools and expertise to uncover sophisticated ML methodologies.

Box 6.1. FIU strategic analysis

FIU strategic analysis material – for typologies of ML (3rd revised edition)

In 2020, FIU Latvia developed methodological material on ML typologies and red flag indicators, updated in 2021 and 2024. It is widely used by REs, FIU, LEAs, and courts, summarizing ML typologies typical of schemes in Latvia. These typologies are identified through strategic analysis and practices of foreign FIUs and international institutions like FATF. The material is cited in FIU disseminations and used in investigations and prosecutions, supporting evidence evaluation in court for ML cases.

For more examples of FIU strategic analyses, refer to IO1, and the FIU Latvia webpage (https://fid.gov.lv/en/roles-and-responsibilities/strategic-analysis-and-guidelines)

354. Prosecutors routinely rely on FIU analytical products referred to as "Conclusions of the Competent Authority." These detailed, evidence-based reports are admissible in court and have been pivotal in securing convictions in complex cases, particularly in cases involving cross-border ML and fraud.

355. For suspected TF, the FIU produced 15 intelligence reports disseminated to the State Security Service and foreign FIUs and engaged in at least 15 operational cases requiring further information from REs, LEAs, and international counterparts. FIU Latvia actively participates in international task forces to stay aligned with global TF trends.

356. LEAs also carry out parallel financial investigations using their own intelligence. Between 2018 and 2023, 24% of ML investigations were initiated through such parallel investigations (alongside the 51.4% initiated through FIU disseminations). The State Police, TCPD, and State Security Service, have independent intelligence-gathering capabilities but rely heavily on the FIU for intelligence and analysis. The SRS TCPD has increased its analytical capacity with more analysts, IT upgrades, software purchases, and enhanced training, using advanced systems for data analysis. In 2021, the CPCB expanded its analytical team from 4 to 14 analysts by 2023 to support criminal cases and proactive data collection. These capabilities include human intelligence (HUMINT), communication interception, and covert surveillance, complemented by specialized financial investigators. Despite these efforts, the FIU remains the central point for financial intelligence expertise and co-ordination.

357. SCAs create their own financial analysis but this typically leads to administrative procedures rather than major ML investigations. Latvijas Banka's 2022 review found increased cross-border payments, prompting inspections and uncovering control deficiencies. Other SCAs aggregate data to identify violations. However, the FIU remains the main hub for financial intelligence, providing continuous feedback on emerging risks and strategic analysis.

6.3. Co-operation and exchange of information/financial intelligence

358. The FIU actively engages with relevant LEAs and SCAs through co-operative and proactive collaboration, which leads to strong co-operation and exchange of information and intelligence in Latvia. This includes sharing timely intelligence with LEAs, providing strategic insight and participating in joint operational planning to ensure that investigations are as effective as possible.

359. Co-operation and exchange of information and financial intelligence between relevant agencies occurs regularly and securely, ensuring effective collaboration while maintaining strict confidentiality. Latvia's model for public-public and public-private information exchange, known as the CCG, has proven to be a

highly effective mechanism for fostering collaborative operational and tactical support between public authorities and REs. This model allows any agency or RE to initiate information exchange through secure and encrypted communication channels, ensuring the integrity and protection of sensitive data during the sharing process. CCG meetings occurred at an increasing rate over the past years. With around 300 CCG meetings annually, they effectively develop information for financial investigations in a secure environment, leveraging extensive information and expertise. Authorities provided case examples of successful CCG use, leading to identification and dissemination of suspected ML and related offences. For instance, CCG co-ordinates with FIU, LEAs, and banks to issue freezing orders, avoiding tipping-off and ensuring success.[77]

360. For complex cases, the FIU established the "Operational Centre"(OpCEN), a secure office space for FIU and LEA analysts to collaborate. This setup ensures efficient intelligence sharing and investigation while maintaining security. Analysts can access their IT platforms temporarily, ensuring confidentiality and system integrity. OpCEN's infrastructure includes separate access credentials, encrypted data transfer, and strict information handling policies. Alongside the CCG model, these demonstrate Latvia's commitment to fostering innovative, secure, and effective mechanisms for tackling financial crime through co-operation between public and private stakeholders.[78]

361. Security and confidentiality are fundamental to the FIU's systems, ensuring compliance with data protection laws and best practices. Agencies use secure IT platforms with access controls, encryption, and monitoring to prevent unauthorized access. FIU analysts and LEA personnel are trained in information security protocols to maintain data confidentiality.

362. The case of Bank A below illustrates Latvia's comprehensive response to professional, complex, stand-alone ML linked to its historical status as a regional financial centre ("first risk profile"). The bank was allegedly involved in the systematic laundering of funds involving EUR 300 billion worth of transactions through shell companies and non-resident accounts from 2013 to 2018, utilizing a professional ML service ("laundromat") that facilitated the registration of shell entities and their accounts. Following international scrutiny, Latvia initiated a controlled liquidation process overseen by the FCMC (now Latvijas Banka) with targeted supervisory actions.[79]

363. The outcome of these targeted supervisory actions was that FIU Latvia was granted direct, comprehensive access to the bank's historical data. As a result, the FIU issued more than 1 000 disseminations to LEAs, resulting in the initiation of 584 criminal proceedings. In addition, EUR 1.18 billion was frozen and EUR 119 million has already been confiscated thus far.

364. International co-operation was pivotal. FIU Latvia co-ordinated with the IFIT, involving FIUs from 25 jurisdictions, exchanging data, and identifying ML typologies. The IFIT contributed to the freezing of EUR 120 million and confiscation of EUR 25 million globally in the IFIT countries abroad. It also fostered improvements in national AML/CFT legislation, enhanced analytical capacities, and the development of new tools and methodologies in the participating jurisdictions. (This case earned international recognition, including the Egmont Group's Best Case Award in 2022).

77. Data is for the latest three years. For more precise numbers of CCG meetings by participant please see IO1. Banks regularly participate in CCG meetings (in 2023 banks participated in 93 or 33% of all CCG meetings).
78. In straightforward cases, the FIU will transmit disclosures directly to the appropriate competent authority via the goAML platform. Corresponding requests for supplementary information from the competent authority are likewise submitted to the FIU through the same system. In instances where LEAs are independently developing financial intelligence based on their own operational intelligence, preliminary queries against FIU-held data are conducted through the secure "Black-Box" interface.
79. The liquidation process was marked by increased supervisory controls and interagency co-operation. Measures included EDD, independent audit reviews, transaction monitoring, and sample testing of client files. The FCMC imposed strict requirements for payouts to creditors and asset sale.

Box 6.2. FIU analysis of Bank A laundromat schemes

In 2018, a Latvian bank (Bank A) was publicly identified by a foreign authority as central to a global laundromat scheme. Latvian authorities promptly suspended its licence, and the FIU launched an in-depth investigation. The FIU found that, since 2011, the bank had onboarded high-risk foreign clients—including shell companies, non-resident politically exposed persons (PEPs), and customers from CIS countries—without conducting proper due diligence.

The FIU analysed over EUR 300 billion in transactions and received more than 3 000 STRs under a specialised analysis framework. It froze assets in over 1 100 accounts worth EUR 1.18 billion. Disseminations to the State Police, other LEAs, and the PO included over 1 000 operational analyses and risk assessments, identifying typologies such as TBML, fictitious business activity, foreign shell companies, and deviations from normal conduct.

This intelligence led to at least 584 criminal proceedings against bank clients, with EUR 1.17 billion seized and over EUR 119 million already confiscated. Eight bank officials have been charged with ML for facilitating the scheme. The FIU's role in exposing this laundromat operation was a catalyst for significant reform of Latvia's AML legal and institutional framework.

365. FIU Latvia, along with the PO, SRS TCPD, and major credit institutions, developed a comprehensive list of tax crime typologies and indicators. While not publicly available, this document was shared with REs and LEAs, enhancing the quantity and quality of tax crime STRs received by FIU Latvia and subsequently disseminated to the SRS. Co-operation between relevant authorities on financial intelligence shows sustained co-operation and exchange of relevant information between authorities and even with the private sector.

366. The co-operation and exchange of information with supervisors is also substantial. The FIU meets regularly with the banks (credit institutions) in Latvia to exchange on developing improvements in their AML/CFT regime. For example, in April 2020, the FIU Latvia informed FCMC (Latvijas Banka) on the lower quality of some of the STRs submitted at the beginning of the process. After meetings, the FCMC used this information to supplement the methodology with additional provisions regarding reporting, thus improving the overall quality of STRs. As noted in Core Issue 6.1 above, some DNFBP reports are lacking in quality and quantity and to address this, the FIU provides regular (annual) feedback to several groups, such as the LCSN for notaries and LGSI for casinos on reporting quality and other relevant information. For example, in 2020 co-operation with the LCSN led to identification of discrepancies in CDD for property transactions and prompted targeted inspections.

367. Prosecutorial authorities are closely engaged in the use and development of financial intelligence. The Specialised Prosecutors' Division provides early-stage guidance in TF and ML cases. Prosecutors also co-develop general investigative guidelines (e.g., for TF) with investigative agencies like the State Security Service.

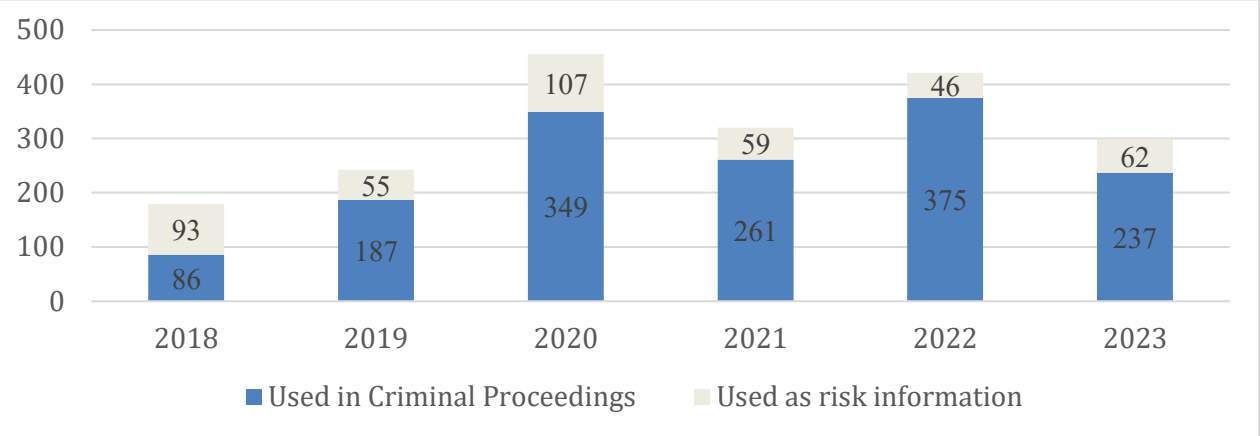
6.4. Using information/financial intelligence

368. The use of financial information and intelligence by competent authorities in Latvia is extensive and forms a critical component of their investigative and prosecutorial processes. The integration of financial intelligence into these processes enhances the ability of competent authorities to trace illicit financial flows, identify hidden assets, and uncover networks of criminal actors.

369. Most FIU Latvia disseminations are relevant and of use to the LEAs. For example, most of the disseminations sent to State Police were used in criminal proceedings (see figure below). 57% of

disseminations initiated new criminal proceedings and 43% were added to existing criminal proceedings. These high levels of use demonstrate the utility of financial intelligence to develop evidence and identify and trace criminal proceeds.

Figure 6.3. Total number of disseminations to State Police and subsequent use



370. The FIU supports investigations and prosecutions by submitting "Conclusions of the Competent Authority," which are detailed reports based on financial intelligence. These reports explain complex financial schemes, methods used by perpetrators, and links to broader criminal activities, aiding judges, prosecutors and investigators in securing convictions for sophisticated ML or financial fraud cases. This practice demonstrates the strong collaboration between the FIU, LEAs, and the judiciary. It also reflects the trust placed in the FIU's analytical capabilities and the quality of its financial intelligence products, which have proven instrumental in achieving successful outcomes in challenging and high-profile cases.

Box 6.3. FIU operational analysis supporting ongoing LEA investigation

In September 2022, the State Police launched an investigation into a Latvia-Scandinavia-based OCG involved in drug trafficking and ML. In October 2023, FIU Latvia was requested to assist in tracing related financial flows. Over five months, FIU Latvia held CCG meetings, analysed over 100 financial accounts, and identified typologies including fictitious rentals, fraudulent documentation, and unexplained wealth exceeding declared income.
The FIU's analysis revealed the use of legal entities to launder proceeds through real estate, luxury goods, bank accounts, and cryptocurrencies. Findings were disseminated to law enforcement, contributing to the detention of 16 individuals and the seizure of significant assets in a co-ordinated EU action in September 2024. The case was referred to prosecution in December 2024.

See also: https://www.europol.europa.eu/media-press/newsroom/news/one-of-latvia%E2%80%99s-most-notorious-criminals-arrested-europol%E2%80%99s-support

371. Latvia's updated risk profile now prioritizes domestic crimes like tax evasion over historic financial centre-related risks.

372. Analyses combine multiple STRs with OSINT, international data, and foreign FIU responses, especially in cases involving foreign shell companies and cross-border networks. The FIU has shifted focus to tax and property crime-related STRs, which have increased in volume, reflecting a better understanding of current national risks by authorities and REs. These enriched analyses have led to investigations by the SRS TCPD, including high-profile tax evasion cases. Between 2020 and 2023, SRS used STRs to carry out 2 286 control measures and conducted over 1 900 AML/CFT compliance checks, leading to numerous findings of law violations and the imposition of 97 penalties. Overall, this shows the use of financial intelligence in tackling tax crimes has become more targeted and strategic.

373. Available data and case examples show that authorities such as the State Police, CPCB, and PO make frequent and visible use of FIU Latvia's analysis products. While fewer documented examples exist for the SRS, recent activity regarding tax crimes indicates increasing operational use of financial intelligence in line with Latvia's risk profile. For instance, in 2022–2023, FIU Latvia conducted strategic and operational analysis linking multiple STRs and a foreign dissemination, uncovering a complex tax evasion and ML scheme involving over EUR 5 million in cross-border transactions. SRS TCPD used the resulting analysis to trigger a criminal investigation. This case demonstrates the SRS's growing engagement with financial intelligence products in addressing serious tax-related ML threats. Given the SRS's central role in addressing tax-related ML—one of Latvia's key domestic risks—greater use of FIU analysis could enhance its ability to identify and respond to complex tax evasion and professional ML schemes.

374. The FIU plays a crucial role in identifying and tracing (and freezing criminal proceeds (see IO.8 for more information)).

Box 6.4. FIU operational analysis identifying and tracing funds

In 2018, FIU Latvia received an STR concerning a client of a Latvian credit institution— a non-EU company linked to a Maltese corruption case. FIU Latvia conducted in-depth operational analysis, collecting information from REs, public sources, and foreign FIUs. The investigation revealed that accounts held by third parties across multiple jurisdictions were used to obscure the origin of funds, involving non-EU entities controlled by suspected strawmen used to obscure beneficial ownership.

The transactions lacked economic purpose, featured round-number transfers over short periods, and showed characteristics of transit activity. FIU Latvia ordered the freezing of EUR 28.1 million and referred the case to a Latvian LEA, which initiated criminal proceedings for large-scale ML.

375. Over time, the focus of FIU Latvia's identification and tracing measures have evolved. Historically, actions were linked to Latvia's role as a regional financial centre, often involving high-risk international cases ("first risk profile") recently, the emphasis has shifted toward tracing funds linked to domestic crimes such as tax evasion and property offenses ("second risk profile") where the risk of illicit funds leaving law enforcement's reach is lower. To identify assets, FIU Latvia relies on high-quality STRs, strategic and operational analysis, and referrals from foreign FIUs. Threshold declarations and cross-border cash declarations also play a role in uncovering suspicious activity.

Chapter 7. Money Laundering Investigations and Prosecutions

The relevant Immediate Outcomes considered and assessed in this chapter is IO.7. The Recommendations relevant for the assessment of effectiveness under this chapter are R. 3, 30, 31 and elements of R.1, 2, 15, 32, 37, 39 and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Latvian authorities effectively identify and investigate ML cases. They prioritise ML and approach this in line with their evolving risk profile from a wide variety of sources. Authorities access and use a range of tools and investigative techniques and have developed substantial levels of expertise in pursuing ML and conducting parallel financial investigations. Co-operation among relevant agencies is strong.

b) Prosecution and conviction figures have significantly increased, and authorities pursue a range of ML offences, including stand-alone ML and ML tied to predicate offences. Authorities demonstrated their ability to investigate and prosecute complex ML schemes including with international dimensions. However, due to structural factors, many large-scale ML cases could not be prosecuted, as offenders or their ultimate BOs are often unknown, non-residents, or located in non-cooperative jurisdictions. Additionally, legal persons are not prosecuted to a significant extent.

c) During the period under review, significant developments took place in relation to jurisprudence regarding third party ML cases and stand-alone ML prosecutions which were supported by Supreme Court decisions regarding admissibility of circumstantial evidence. Whilst these decisions by the highest judicial authority reflect an advanced interpretation on assessing evidence in ML-related criminal proceedings, the lower judicial authorities are currently undertaking the implementation of these principles.

d) Custodial sentences for ML and associated offences are applied and they are proportionate and dissuasive. Sanctions for natural persons are proportionate and dissuasive. Latvia has demonstrated the application of some coercive measures against legal persons, but number of legal persons pursued remain low and sanctions are not substantial.

e) The Latvian authorities apply several alternative criminal justice measures in cases where a ML prosecution is not possible, for justifiable reasons. For example, authorities pursue legal persons for other criminal offences where ML may have occurred.

Key Recommended Action (KRA)

N/A

Other Recommended Actions

a) Given the risk profile and context of Latvia, authorities should increase focus on the investigation and prosecution of legal persons, specifically through targeted training to LEAs, the PO and judicial authorities. These specifically tailored trainings should include means and methods on how legal persons could be used as vehicles for ML activities, and best practises in investigating such cases, including the application of appropriate security measures against legal persons and securing adequate sanctions for ML.

b) LEAs should continue to prioritise and pursue complex ML offences in line with the evolving risk profile of Latvia. This would include large scale ML tied to corruption, tax offences, smuggling, and fraud, ensuring that ongoing and future cases are pursued to conviction of persons, as appropriate.

c) Latvia should review its training programme for judicial authorities and put emphasis on tools and mechanisms at judicial authorities' disposal, with the aim of capitalizing on the evolving jurisprudence on the use of circumstantial evidence. In addition, training should also focus on the application of alternative measures (such as "confiscation of legally acquired property" as referred to Latvian legislation), along with other criminal sanctions.

Overall conclusion on IO.7

Latvia has a robust legal and institutional framework for identifying and investigating ML cases, with dedicated resources and training. Authorities are well aware of ML risks and co-operate effectively.

The component parts of the AML system (investigation, prosecution, and where possible, convictions) seem to be functioning coherently. The number of convictions related to the first risk profile is low compared to the volume of investigations and asset recovery measures associated with these offences. This gap arises because of the mandatory approach to investigations, and the fact that, while instances of ML are well-documented, the offenders are often unknown, non-residents, or located in non-cooperative jurisdictions, which undermines the country's overall effectiveness against ML. However, this deficiency is given less weight as it is considered a structural issue.

Penalties for ML against individuals are effective, proportionate, and dissuasive. However, fines, prosecutions and convictions of legal persons are inadequate given their use and involvement in ML schemes. When ML prosecution is not possible, authorities pursue other criminal justice measures.

Latvia is rated as having a substantial level of effectiveness for IO.7.

7.1. ML activity identified and investigated

376. Latvia proactively identifies and investigates ML through a variety of sources. Authorities have made significant improvements since the previous evaluation and judicial authorities and LEAs use all tools at their disposal to identify and investigate ML cases. This has yielded results in identification and investigation of ML and associated predicate offences.

Legal Framework and Relevant Law Enforcement Agencies

377. Latvia maintains a sound legal and institutional framework with clearly delegated authorities and responsibilities for identifying potential cases of ML and investigating these along a spectrum of importance and impact, and alignment with risk. Investigation and prosecution of a criminal offence is mandatory (Section 6, CPL, see also R. 30). Any LEA which identifies possible ML while investigating a predicate

offence has a duty to investigate. As Latvia follows all-crimes approach, every crime that generates criminal proceeds can be the predicate offence for ML. In Latvia, there are nine LEAs (investigating authorities) with competence of investigating ML.[80] The vast majority of ML and predicate offences have been investigated by the following authorities:

- **State Police** investigates a wide range of criminal activities nationwide, excluding tax crimes. It operates through a 3-level system - with the Main Criminal Police Department,[81] 5 regional departments, and local stations. The Economic Crime Enforcement Department (ECED) within the Main Criminal Police Department handles complex ML cases, especially those threatening national economic interests. Around 20% of ML cases are investigated by ECED at the highest level of priority. 70% of cases are investigated at the regional level, and the remaining 10% are conducted with local police.

- **SRS TCPD** leads investigations into state revenue crimes (e.g., tax evasion, tax fraud) and customs offences (e.g., smuggling, illicit movement of narcotics, illegal production, storage, movement, or disposal of alcohol, and tobacco products).

- **CPCB** leads investigations into corruption offences for public officials, including public procurements.

Identification and Investigation

378. Identification of suspected ML is done effectively through various means, i.e., FIU disseminations, parallel financial investigations, formal or informal incoming foreign requests, criminal intelligence, cross-border currency and cash seizures, submissions by a person, supervisory and regulatory institutions, open-source information and others. LEAs have developed mechanisms to identify ML cases and new trends via strategic and tactical analysis and criminal intelligence.

379. In total, Latvian authorities identified and pursued 1 755 ML investigations between 2018-2023. This number of cases shows a significant improvement since the previous assessment period (2013-2017) which counted 466 ML cases. As outlined in IO.6 Latvia's FIU co-ordinates closely with relevant authorities to ensure adequate understanding of the suspicions and the relevant financial elements of the cases it disseminates, which aides in the identification of ML and associated predicate offences. 898 cases, or 51%, have been initiated based on FIU disseminations, mostly tied to ML in banks undergoing liquidation procedure (first risk profile), while parallel financial investigations account for 435 cases, or 25%; and domestic open-source information (or information from other LEAs) accounts for 9% of cases. Others, such as supervisory authority submissions or tip-offs,[82] foreign intelligence and cash controls on borders account for the remaining 14% (see table below). LEAs' capacity to identify ML, in addition to FIU disseminations, is reflected by the growing proportion of investigations from parallel financial investigations and domestic intelligence.

80. There are also another six LEAs which are not mentioned here because they accounted for less than 1% of ML investigations.
81. Which includes three criminal police sub-departments – for organised crime, cybercrime and economic crime.
82. Person's submission.

Table 7.1. Number of ML investigations by source (2018-2023)

Source	2018	2019	2020	2021	2022	2023	**Total**	**Percentage**
FIU dissemination	74	119	219	157	243	86	**898**	**51%**
Parallel financial investigations	34	54	62	107	90	88	**435**	**25%**
Domestic intelligence, OSINT, other intel.	32	20	28	26	18	35	**159**	**9%**
MLA and other foreign intelligence	0	2	2	1	3	6	**14**	**1%**
Other sources*	20	27	20	42	17	12	**138**	**8%**
Cash control on borders	1	42	17	26	19	7	**112**	**6%**
Total	161	264	348	359	390	234	**1 756**	**100%**

*This includes preliminary investigation, departmental examination, SCA, submissions by natural/legal persons

380. The three case studies below illustrate instances of ML identification from different sources.

Box 7.1. Identification from various sources

Case 1: ML case from incoming EIO

In 2021, criminal proceedings for aggravated ML were initiated based on an incoming EIO. The State Police found large amounts of cash and two gold ingots. A parallel financial investigation led to the seizure of the suspects' movable and immovable property in Latvia. NCBC proceedings ensured timely confiscation of EUR 9 732 190, USD 877 500, RUB 385 400, and two gold ingots (valued at least EUR 100 000). The criminal investigation is ongoing.

Case 2: Cash at the border

In 2019, Person A crossed the Latvian border from the Russian Federation with USD 243 000 and EUR 36 000, declaring it as family savings for daily expenses. Suspicious of ML, authorities initiated a criminal proceeding. Investigations revealed forged loan agreements and discrepancies in declared income, identifying Person A as a money mule. On 21 April 2023, the Riga Regional Court found Person A guilty of aggravated ML, sentencing them to 5 years' imprisonment with 1 year probation. Cash totalling EUR 36 000 and USD 243 000 was seized and confiscated.

Case 3: FIU identified professional fraud scheme

In 2016, State Police initiated criminal proceedings based on operational analysis of the FIU in the form of a Conclusion of the Competent Authority. The report provided evidence of suspicious transactions linked to a professional fraud scheme outside Latvia, with ML stages occurring in Latvia using a Latvian bank and involving Latvian nationals. The subsequent investigation, lasting about 2.5 years, revealed a Ponzi scheme involving over 240 victims in 11 countries. Active international co-operation led to a parallel financial investigation and asset seizures in Latvia. In 2020, two individuals were charged; one was found guilty and sentenced to 3 years' imprisonment in 2022, while the other was acquitted. Total confiscated assets amounted to EUR 1 014 342.

381. Authorities are well-aware of the country's ML risks, and the threats stemming from the first and second risk profiles (see IO.1), as well as typologies (laundering and layering techniques) associated with these risks. Parallel financial investigations are conducted as a policy and LEAs use all available tools, resources, and special investigative techniques. ML cases are prioritized according to General Prosecutor's Office (GPO) Guidelines[83] and internal LEA guidelines, aligning with national policy directives.[84]

83 Such as the 22 July 2024 PO guideline: '*Order on Prioritising ML Investigations'*.

84. For example, the *Guidelines on Parallel Financial Investigations and the Prosecutor's Order on Prioritization of ML investigations, Guidelines on Priorities for investigating criminal offences in the area of money laundering, Guidelines on Prioritisation of ML by GPO in 22-07-2024.*

Alignment with Risk

382. Latvia conducted around 78 000 criminal investigations in total. ML investigations represent around 2.3% of all investigations (1 756 ML). Given that Latvia follows a mandatory approach to criminal proceedings (under Section 6 of the CPL), and most of the criminal cases reflected in the table below involve low-proceeds-generating offenses (which do not suggest ML), this proportion is sufficiently high.

Table 7.2. Total Predicate Offences Investigated in Latvia (ML and non-ML)

Predicate Offence	Total	Percentage
Robbery or theft	35 813	45.6%
Illicit trafficking in narcotic drugs and psychotropic substances	10 396	13.2%
Fraud	7 090	9.0%
Counterfeiting currency	5 421	6.9%
Smuggling (including in relation to customs and excise duties and taxes)	4 093	5.2%
Forgery	2 312	2.9%
Misappropriation	2 216	2.8%
Environmental crime	1 943	2.5%
Rape, Sexual Violence, Leading to Depravity	1 942	2.5%
Illicit arms trafficking	1 819	2.3%
ML	**1 755**	**2.3%**
Other	3 737	4.8%
Total	**78 537**	**100%**

Table 7.3. Total ML related to criminal activity investigations by Sate Police, SRS TCPD and CPCB (2018-2023)

Investigations of ML related to Criminal activity	Investigations	Percentage
State Police investigations (all crimes)	**1 419**	**83%**
ML stand-alone	813	47%
Various crimes investigated in regional departments	356	21%
Illegal activities with financial instruments	185	11%
Fraud, misappropriation	31	2%
Smuggling	9	1%
Sexual exploitation, including of children	5	0.3%
Human Trafficking	3	0.2%
Illegal operations with excise goods	3	0.2%
Counterfeiting and piracy of products	2	0.1%
Prohibited entrepreneurial activity	2	0.1%
Tax crime (excl. SRS)	2	0.1%
Illegal acquisition and use of data	2	0.1%
Murder	1	0.1%
Robbery	1	0.1%
Extortion	1	0.1%
Illegal acts with cultural objects	1	0.1%
Failure to act by a public official	1	0.1%
Corruption and bribery (excl. CPCB)	1	0.1%
SRS TCPD investigations (ML related to Tax crimes, fraud, cash smuggling)	**249**	**15%**
CPCB investigations (corruption cases)	**48**	**3%**
Total	**1 716**	**100%**

Totals include identification from three main LEAs, or 1 716 of the 1 756 ML investigations cited in the previous table above

383. A considerable number of Latvia's investigations are conducted on stand-alone ML. Of the 1 419 investigations conducted by the State Police, 813 (or nearly 60%) are for stand-alone ML. 112 cases, or around 6% of investigations come from cash controls at the borders. This relatively low percentage is due to the lower risk of cross-border cash smuggling, the COVID era, and the use of administrative measures for sums below EUR 35 000, which mitigates the need for mandatory investigations for every cross-border case (where there is no suspicion of underlying offences such as cash smuggling or ML). The remaining 336 are conducted by other LEAs, including principally the SRS, which initiated 249[85] criminal proceedings under the ML statute between 2018 and 2023. Although this proportion seems relatively small in comparison to the quantum of risk associated with tax evasion in Latvia in its second risk profile,[86] the first risk profile was dominant during the entire assessment period.

Table 7.4. Types of ML Investigations by the State Police

Investigations by the State Police	2018	2019	2020	2021	2022	2023	Total
ML stand-alone	80	134	157	156	217	69	**813**
ML linked to predicate offences	53	43	130	126	121	133	**606**
Total	**133**	**177**	**287**	**282**	**338**	**202**	**1 419**

384. As outlined in IO.1, Latvia has faced an evolving set of ML risks. Nevertheless, investigations are broadly matching the shape of this changing risk profile. Stand-alone ML investigations linked to Latvia's first risk profile dropped from 217 in 2022, to 69 in 2023. ML investigations from domestic and foreign predicate offences rose from 53 in 2019 to 133 in 2023.[87] The yearly number of ML investigations has declined due to the finalization of FIU's work on ML cases involving credit institutions under liquidation, recent sanctions, and border restrictions. This trend is also reflective of the declining overall numbers of predicate offenses. As the risk profile evolves, authorities will need to increasingly identify and investigate ML in alignment with domestic predicate offences (i.e. tax, fraud, smuggling, corruption, drug trafficking, and human trafficking).

Skills, Training and Tools

385. All relevant authorities have dedicated staff in place to investigate ML. Training of officers takes place regularly. Latvian authorities access information directly via automated systems and interface with foreign counterparts through Interpol, Europol, and other channels. Specialized authorities, like SRS TCPD among others, use databases such as cross-border currency reports, TLKAIS and SKLOIS,[88] and access registries such as the Account Register and the ER. LEAs also co-operate with the ARO for tracing assets domestically and internationally.

386. The ECED of the State Police counts over 80 specialised trained staff, including cybercrime analysts, to address complex ML cases and fulfils its mandate as a centre of knowledge, training and expertise for ML investigations. Currently, 22% of all posts are not filled across the Police Force, but because of prioritization, there do not appear to be issues in resourcing for ML offences. The State Police Cybercrime Enforcement Department was established to investigate complex cybercrime cases and predicate offences of ML committed in cyberspace, involving the use of digital technologies and online platforms. Regional branches of the State Police have also received training for the investigation of ML and regional State Police officers regularly investigate ML cases thanks to relevant trainings.

85. State police undertook two ML investigations into tax offences during this period, highlighting that the role of investigating tax offences under the ML statute would typically fall to the SRS.
86. The State Police is the main investigative LEA with the broadest range of criminal activities, while SRS investigates only tax crimes, an area highly regulated by administrative laws and penalties.
87. Statistics on ML investigations per predicate offence were not provided. However, the statistics on the number of prosecutions and their alignment with risks is discussed further below (see core issue 7.2).
88. TLKAIS: vehicle and container automatic identification system; SKLOIS: Information on arriving vessels.

387. The SRS TCPD does not have a separate unit for ML related to tax crimes and smuggling. All eight units are trained to investigate ML alongside predicate offences, using various information sources, including customs, tax information and revenue data, alongside financial intelligence, and the Black-Box system. They face challenges obtaining reliable information from some neighbouring countries, hindering cross-border smuggling investigations and related tax crimes. Russia's war against Ukraine and the consequent EU sanctions have also significantly increased the workload of Latvian authorities for enforcing these sanctions (SRS TCPD and State Security Service) and has displaced some of their capacities to investigate tax related offences and illicit movement of excise goods, including smuggling. To address this, the SRS TCPD has been allocated with additional staff during the last two years.[89]

388. For CPCB, ML investigation and parallel financial investigations into corruption are entrusted to 18 investigators and two directors, supported by 12 officers in the analytical department. Investigators regularly access case data in CPCB's record keeping system.

389. Co-operation among authorities is strong. Investigators use innovative tools like the Black-Box system (see IO.1 and IO.6 above), goAML, and OpCEN to identify leads. LEAs follow up with competent authorities and set up CCG meetings involving all relevant parties, including private sector entities like banks. Given the international aspect of ML cases, LEAs and the FIU seek co-operation through various channels, including Interpol, Europol, and ARO, to verify information and gather evidence. As noted in IO.2, Latvian authorities reported 12 ongoing JITs, a high number considering the risk and context.

Box 7.2. Identifying large scale ML using NPO – co-operation between authorities

Based on DCSSOC criminal intelligence and State Labour Inspectorate risk data, the State Police investigated an organized group of ten individuals exploiting vulnerable persons from January 2018 to July 2021. Under the guise of aid centres, they deceitfully recruited, transported, housed, and forced individuals to work, receiving over EUR 565 324 in compensation.

The FIU and State Police convened a CCG meeting, monitored transactions, and froze funds abroad using MLA.

Authorities seized two apartments, land, a new building, two luxurious watches, five vehicles, EUR 147 298 cash and EUR 38 206 deposited in FIs. Proceedings were also initiated against a legal person. The case, involving human trafficking and aggravated ML, was referred to the Economic Court on 22 May 2024, and is ongoing.

390. Investigating authorities receive strong support from the GPO, which has a specialized section for ML cases. This section accompanies LEAs in pre-trial investigations and provides expertise. Once an investigation is initiated, LEAs contact the GPO to supervise and guide investigators. The GPO appoints a supervising prosecutor within 48 hours and prioritizes[90] ML investigations. Authorities have shown considerable co-ordination and co-operation in pre-trial investigations of suspected ML cases.

7.2. Prosecuting and convicting different types of ML activity[91]

391. Latvian authorities are prosecuting and convicting different types of ML activity to a strong degree, with some weaknesses in the pursuit of legal persons and with the identification of persons or BOs for court convictions in major transnational ML schemes (aligned with their first risk profile).

Types of Prosecution and alignment with Risk

392. Prosecutors have actively pursued ML cases tied to the initial risk profile (stand-alone ML linked to banks under liquidation and foreign predicate offenses like corruption and fraud) and the second risk profile

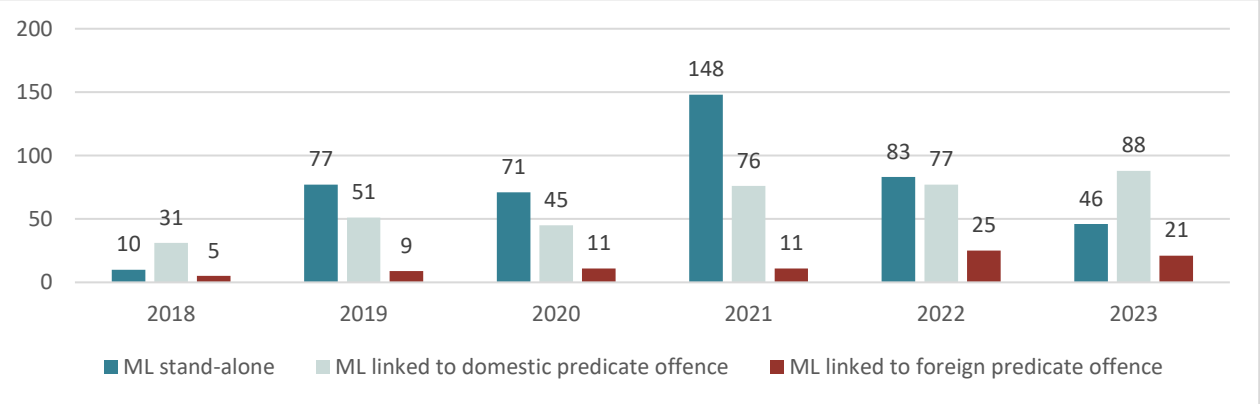
89. TCPD relies on OSINT, customs, tax information, and revenue data for investigations. They face challenges obtaining reliable information from some neighbouring countries, hindering cross-border smuggling investigations and related tax crimes.
90. This prioritisation is ensured through an order on the supervision of ML investigations.
91. See *Methodology*, IO.7, Note to Assessors 2 and related footnotes.

(domestic crimes). Since the previous MER (2013-2017), Latvia has steadily progressed in prosecuting and convicting individuals linked to both profiles. Despite numerous investigations, Latvia has achieved a limited number of convictions for complex, professional ML schemes. While Latvia successfully achieved convictions of professional facilitators in one of the now-defunct banks, it has not achieved convictions of the professional actors, or companies involved in these major laundering schemes. This is largely due to challenges in pursuing international ML schemes, especially when perpetrators operate from non-cooperative jurisdictions. Latvia has also prosecuted banks and their management for facilitating ML, but to a small extent.

393. In 2021, the Anti-Money Laundering Coordination Unit (AMLCU) was established within the Department of Criminal Justice of the GPO to provide guidance and close co-ordination to LEAs (such as State Police and others) for investigation of ML (see core issue 7.1 above). The AMLCU also issues Guidelines and methodological materials, training, co-ordination and expertise to other prosecutors, as well as investigators and judges. The investigators, prosecutors, judges, and representatives of other legal professions are trained in identification and recovery of criminally acquired property.

394. Latvia has steadily increased ML prosecutions, covering both stand-alone ML and ML related to domestic or foreign predicate offenses. Prosecutions followed Latvia's two risk periods, with stand-alone ML cases rising from 2018 but recently declining due to reduced risks from the first risk profile. Of all the ML cases being prosecuted during the years 2018-2021, 55-60% of them were stand-alone ML cases, which slightly decreased to 30% in 2023. As the table below highlights, domestic ML and ML linked to foreign predicates are growing as a proportion in recent years.

Figure 7.1. Breakdown of prosecution of persons for stand-alone ML and ML linked to domestic and foreign predicate offences



395. Latvia is broadly prosecuting ML in line with its risks. Overall, from 2019 to 2023, Latvia prosecuted 885 persons for ML. Stand-alone ML accounts for 49% of all prosecutions (see table below). Aside from the significant number of stand-alone offences, Latvia prosecutes ML tied to predicate offences committed in Latvia and abroad, such as fraud, drug trafficking, misuse of financial instruments, misappropriation (including bribery and corruption), and tax related offences. The table immediately below also showcases the cases sent by State Police by the estimated severity of the offences.

Table 7.5. Cases sent for prosecution by State Police with classification of ML offence (Section 195, CL)

	2018	2019	2020	2021	2022	2023	**Total**
Non-aggravated ML	8	10	18	32	25	16	**109**
Aggravated ML	3	13	21	50	46	32	**165**
Especially aggravated ML	19	27	27	24	25	23	**145**
Total:	30	50	66	106	96	71	**419**

Table 7.6. Prosecutions of persons for ML by predicate offence (natural and legal persons)

Prosecutions	Total	Percentage
ML stand-alone	**435**	**49%**
ML linked to foreign predicate offence	**82**	**9.3%**
ML linked to domestic predicate offence	**368**	**41.6%**
Fraud (Art. 177, 177.1)	86	9.7%
Tax Evasion (Art. 218)	64	7.2%
Financial Fraud (Art.193)	48	5.4%
Drug Trafficking	41	4.6%
Misappropriation (Art. 179)	30	3.4%
Illegal activities with excise goods	24	2.7%
Human trafficking	14	1.6%
Theft (Art. 175)	14	1.6%
Organised crime, racketeering (Art. 184)	9	1%
Abuse of Power (Art. 341)	9	1%
Environmental crime (Chapter XI)	8	1%
Corruption and bribery (Art. 320-323)	6	0.7%
Other	15	1.7%
Total	**885**	**100%**

Table 7.7. Prosecutions by ML type (incl. natural and legal persons)

	2018	**2019**	**2020**	**2021**	**2022**	**2023**	**Total**	**Percentage**
Self-laundering	31	51	58	78	82	74	374	42%
Third party ML (including professional)	15	86	69	157	103	81	511	58%
Total	46	137	127	235	185	155	885	100%

Trials and timely prosecution of ML

396. In 2021, Latvia established the Economic Affairs Court to expedite justice for economic crimes, including ML and corruption, and to review NCBC cases. Despite a steady increase in ML cases and rising rates of the adjudicated ML cases in courts yearly, Latvia has managed to maintain average adjudication times between 2018 and 2023. Though an increase is noted at the cassation level, not posing significant risks yet. However, authorities have dedicated sufficient resource to address delays.

Table 7.8. Average adjudication time for ML Cases (Sec. 195, CL) by court

	Average processing time in months					
	2018	**2019**	**2020**	**2021**	**2022**	**2023**
First instance	11.0	7.0	7.0	9.2	5.5	11.1
Appellate instance	8.8	12.2	6.3	3.4	2.3	8.6
Cassation instance	3.9	4.0	6.1	8.5	9.1	9.3

397. The case below highlights one of the major cases of the Economic Court in relation to a Bank under liquidation, and its owners.

Box 7.3. Professional, complex and stand-alone ML scheme involving senior bankers of a bank under liquidation in an organised crime group

Investigations into a bank under liquidation (Bank A) led to charges against eight senior bankers, including the owner and the bank itself, for facilitating a global laundromat scheme for high-risk foreign PEPs, shell companies, and clients in high-risk jurisdictions to commit ML in Latvia. Funds were transferred through accounts of various FIs in different jurisdictions opened for shell companies involved in a complex scheme. Employees of the financial service provider arranged the registration of shell companies and the opening of accounts with FIs. Large sums received at the bank originated from foreign accounts held by non-resident legal entities part of ML schemes. Many of the bank's customers were shell companies with declared non-resident BOs. Proceedings against the bank (a legal person) for aggravated ML were initiated.

In criminal proceedings, the prosecutors allege that the bank (as a legal person) and its employees used client settlement accounts and created offshore shell companies with the knowledge and intent to commit ML. Authorities also identified over EUR 414 million in alleged proceeds. The Prosecutors requested EIOs, MLAs were sent, and evidence was obtained from Luxembourg, Ukraine, Belarus, and the United Kingdom. The criminal case is in the Economic Court and evidence is being examined.

At least 584 other criminal proceedings were launched, mostly involving foreign clients and potential ML and other predicate offences like tax fraud and tax evasion. These schemes used similar structures to commit ML offences in Latvia.

398. Regarding legal tools to achieve higher effectiveness of prosecutions and convictions, Latvia has transposed the provisions of EU Directives (2018/1673), which requires that ML can be inferred from factual circumstances (see also R.3 in TC Annex). Unlike previous evaluations, Latvia now regularly prosecutes stand-alone ML without knowledge of the underlying predicate offences (in line with Sec. 195 CL).[92] According to Supreme Court decisions from 2024,[93] and the Supreme Court summary of the case law in ML cases, the criminal origin of the funds may also be proved by indicative or circumstantial evidence, as well as on the basis of the facts established in each particular case.[94] The case above, among others, demonstrates Latvia's progress in developing jurisprudence for third-party ML cases and stand-alone ML prosecutions. Whilst this approach by the highest judicial authority is reflected in the data and case studies, and an advanced interpretation on assessing evidence in ML-related criminal proceedings was applied in certain cases, judges presiding these cases did not demonstrate strong awareness on application of this jurisprudence.

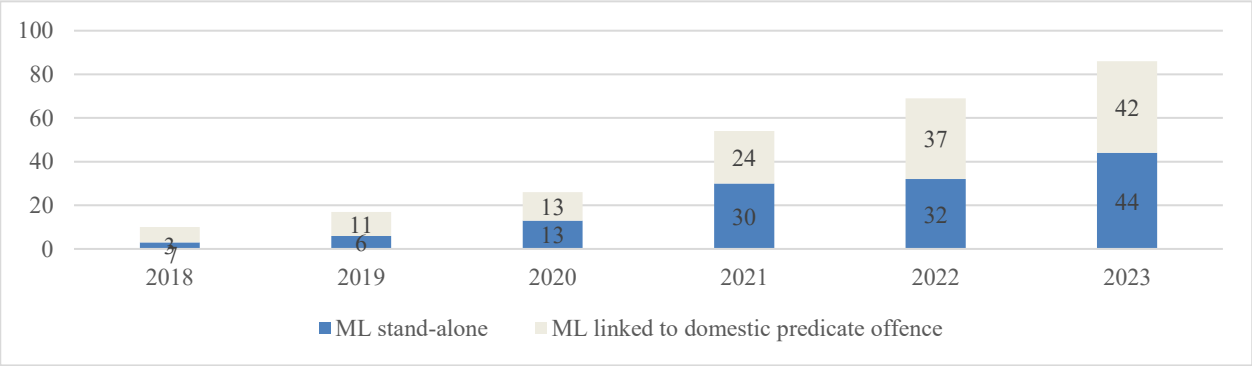
92. In the case of autonomous or stand-alone laundering, the fact that it is not ascertainable from which offence the laundered funds of the accused were obtained is not an obstacle to finding a person guilty of the criminal offence provided (Sec 195, Paragraph 3, CL) (Paragraph 10.2.4 of the Senate Decision of 29 February 2024 in Case No SKK23/2024).
93. Rendered in a case related to ML, the Court concluded that the fact that it is not known exactly from which criminal offense the financial means or other property used for money laundering were obtained does not prevent holding a person criminally liable.
94. The case-law of the Senate recognises, in criminal proceedings, circumstantial evidence to aid in proving the guilt of the accused alongside totality of evidence (so long as it does not raise a reasonable doubt of guilt). (Decision of the Senate of 13 May 2021 in the case No. SKK-89/2021, Paragraph 5.1).

Convictions have nevertheless achieved a significant rate of success, with an approximate conviction rate of 90% for ML cases when the prosecuted persons are identified in Latvia and are available to go to trial.[95]

Conviction for ML

399. Latvia achieved 262 ML convictions between 2018 and 2023, involving 380 natural and 10 legal persons, mostly resolved in the first instance court. This is a significant increase from the previous period (2013-2018), which had 33 convictions for 55 natural persons. Many convictions are for stand-alone ML prosecutions initiated in past years (see figure below). Additionally, 42 persons received "prosecution penalty orders" for lower-level ML offences, such as money muling, involving out-of-court settlements in exchange for admission of guilt.

Figure 7.2. Annual convictions for ML



400. The case study below highlights the Latvian authorities' co-ordination to achieve convictions for ML. The below case involves high-level corruption and the President of Latvijas Banka.

Box 7.4. Conviction for large scale ML from corruption

In 2018, CPCB investigated a 2012 bribery case involving the President of Latvijas Banka, supported by the FIU. Authorities uncovered a EUR 250 000 bribe disguised as a real estate investment and conducted seizure of properties. Authorities co-ordinated with authorities in Germany on the status of immunity of the person and sent requests abroad via international co-operation channels to identify proceeds (but nothing was identified abroad).

Two individuals – the bribe recipient and the member of the board (an official) of the legal person – were accused of committing ML (CL Section 195(3)). The trial lasted four years and involved a ruling from the European Court of Human Rights on the accused status' in the ECB. The case also received input from the Court of Justice of the EU.

First instance sentences:

- **Natural person 1**: 5 years' imprisonment, property confiscation (EUR 174 140 and USD 2 000).
- **Natural person 2 (President)**: 6 years' imprisonment, property confiscation (EUR 20 319; GBP 2 320; EUR 3 900; and three real estates valued at EUR 207 562).
- **Legal person**: EUR 3 500 000 fine, half of real estate confiscated (value EUR 120 072).

95. Over 400 of the earlier mentioned 885 prosecutions did not go to trial because the persons were not present in the territory of Latvia. In these cases, prosecutions were pursued to ensure a referral of suspected ML for NCBC.

The judgment is pending in the appellate court. On 20 December 2023, a court ruled on NCB confiscation of a real estate asset worth EUR 406 402. Half of the real estate was confiscated as criminally acquired property and the other half confiscated as a coercive measure.

401. Latvia has seen an increase in prosecutions and convictions due to cases uncovered by authorities, international partners, and the FIU. However, many major ML schemes remain unprosecuted because the perpetrators and BOs are often not in Latvia. For example, many of the 584 criminal proceedings related to a Latvian Bank under liquidation involve shell companies using Latvian banks for global laundromat schemes, but the accused cannot be prosecuted as they are not located in Latvia or remain unknown.[96] In such cases, investigators and prosecutors pursued NCBC (see IO.8 and Chapter 59, CL), securing criminal assets. This accounts for many of the 317 cases terminated after achieving NCBC. Latvia's inability to prosecute non-resident perpetrators or foreign shell companies stems from challenges in international co-operation involving certain jurisdictions, not operational deficiencies in Latvia's system.

Table 7.9. Rulings of first instance court on ML (2020-2023)

Status of ML investigation and adjudication by year:

Sec. 195 CL	2020	2021	2022	2023	Average	**Total**
ML investigations	344	340	398	235	329	**1 317**
Cases suspended	64	46	34	10	39	**154**
Cases terminated	39	216	256	187	175	**698**
Cases terminated after NCBC has been achieved	0	135	126	56	79	**317**
Cases prosecuted (charges brought against person)	73	133	110	84	100	**400**
Cases completed - sent to court	47	104	97	90	85	**338**

Note: Timeframe for the above cases is limited to 2020-2023 only (and, therefore, total number of investigations are not the same as tables above)

Box 7.5. Case Study Box: Conviction for ML over circumstantial evidence

On 7 December 2022, the Economic Affairs Court convicted two individuals for aggravated ML. Despite their denial, the court found that their testimony indicated awareness of the criminal origin of the funds. The court concluded that, based on the information and intended actions, the accused knew the funds were of criminal origin, proving their guilt beyond a reasonable doubt.

402. Convictions of legal persons are insufficient considering Latvia's exposure to professional ML schemes facilitated by and involving legal persons. In the five-year period, Latvia achieved just ten convictions against legal persons. While this is an improvement from the previous assessment period (2013-201), the relatively low number of prosecutions and convictions of legal persons (10) remains an issue. However, this deficiency is lessened to some extent by the liquidation of legal persons after the initiation of criminal proceedings (once a legal person is dissolved, there is no longer a legal person to which criminal sanctions or coercive measures can be applied). Nevertheless, the number of legal persons pursued appears low, given the significant number of legal persons involved in suspected ML cases.[97] To ensure an effective application of criminal sanctions (coercive measures) to legal persons, in 2022 the Parliament introduced

96. Often in non-co-operative jurisdictions or PEPs whose extradition or domestic investigation is sensitive or not possible.
97. As outlined by the FIU during the assessment, there were over 1 000 cases involving 5 or more legal persons and over 500 cases involving 10 or more legal persons that were disseminated to competent authorities. This suggests a considerable number of legal persons involved in suspected ML.

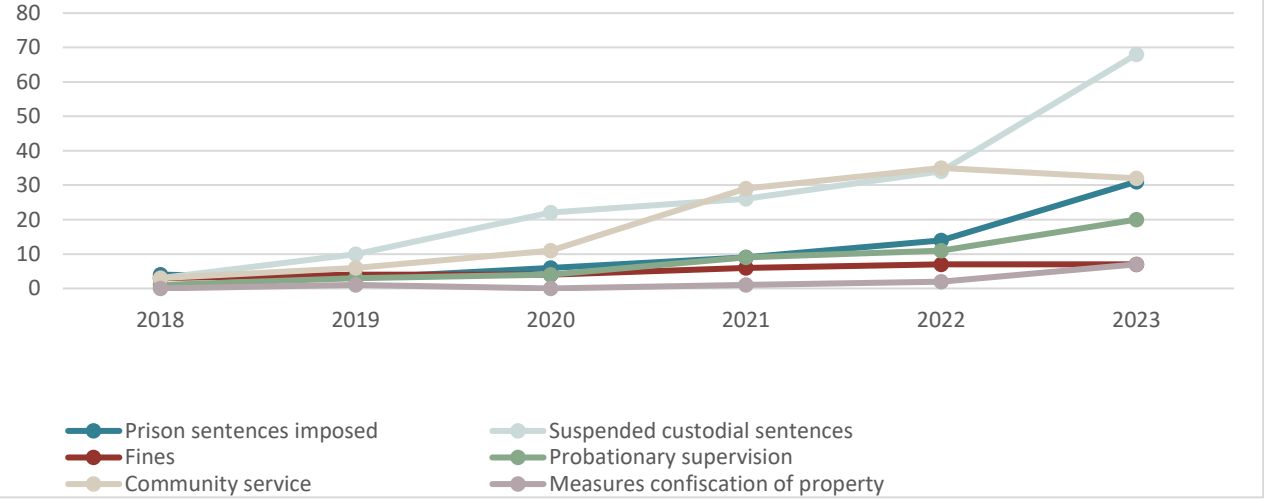
security measures which can be applied to legal persons during the pre-trial investigation. However, results have not yet been achieved.

7.3. Effectiveness, proportionality and dissuasiveness of sanctions

403. Latvia's custodial sanctions are broadly effective, proportionate and dissuasive. There are, however, some weaknesses in the pursuit of legal persons.

404. On average, the length of deprivation of liberty is 45 months (or just under 4 years). Sanctions are proportionate to other offences, and proportionate to the severity of the ML offence, with some persons serving community service and fines as a punishment for crimes such as acting as a money mule. As the chart below indicates, the number of instances of convictions involving prison terms and non-administrative sanctions has increased.

Figure 7.3. Number of penalties for ML against natural persons with a conviction



405. The number of fines imposed for ML remains broadly steady (see figure above). This appears to be in contradiction with the principle to apply monetary punishments for economic crimes instead of imprisonment. When these fines are applied, their amount seems proportionate and dissuasive. A community service as a punishment is increasingly used, with over 68 penalties involving community service in 2023. These penalties apply to non-aggravated ML and aggravated ML and mostly for money mules,[98] where it is proved to be effective and proportionate.

406. Penalties against legal persons include fines, liquidation, deprivation of right to carry out activities and confiscation. With just 10 convictions of legal persons, it is not possible to assess the effectiveness of this system. Fines totalled just over EUR 3 million, which highlights a relatively light approach to sanctions of legal persons, given Latvia's risk, context and materiality as a former regional financial centre where major ML laundromat schemes occurred (see table below).

98. Mostly young, unemployed students, who have no income and ability to pay.

Table 7.10. Convictions of legal persons

	2018	2019	2020	2021	2022	2023	**Total**
Number of convictions			1	2	3	4	**10**
Level of fine imposed (in EUR)			8 600	50 000	10 000	3 118 600	**3 187 200**
Liquidation					1		**1**
Deprivation of right to carry out activities				1			**1**
Deprivation of right to carry out activities (with prosecutor's penal order)					2		**2**
Confiscation					1	1	**2**
Other measures							**0**

7.4. Use of alternative measures

407. Latvian authorities apply other criminal justice measures in cases where a ML prosecution is not possible, for justifiable reasons. Such measures are fines for cross border cash non-declaration (below the threshold), penalties and prosecution for non-disclosure or false BO information, prosecutions for illegal activities with financial instruments and means of payment allowing the use of financial instrument, and going after violation of sanctions, fraud, bribery, tax crimes.

408. Latvian authorities have achieved several convictions of legal persons for other criminal offences in instances where ML may have occurred. For example, there were 77 convictions of legal persons for tax evasion (38); sanctions evasion (9); fraud (8); bribery (5); and other offences (17) from 2019 to June 2024. However, authorities should ensure the pursuit of ML in the future, as it is not clear to what extent an ML prosecution would have been possible.

409. Latvia includes confiscation of legally obtained property as punishment. The CL (Sec 36(2)) allows an additional penalty for ML convictions or as a coercive measure for legal persons. Though few cases applied this penalty, authorities should continue to use it under certain circumstances.

Chapter 8. Asset Recovery

The relevant Immediate Outcomes considered and assessed in this chapter is IO.8. The Recommendations relevant for the assessment of effectiveness under this chapter are R. 1, 4, 32 and elements of R. 15, 30, 31, 37, 38 and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Latvia pursues confiscation of proceeds, instrumentalities and property of equivalent value as a policy objective. Latvia has demonstrated its commitment to asset recovery through institutional reforms, which is also reflected in the country's national AML/CFT/CPF action plans and LEAs' guidelines.

b) Latvia effectively uses provisional measures to identify, trace, and freeze assets swiftly, which led to over EUR 3 billion in assets seized/frozen. Most of these assets are tied to a bank liquidation case and Latvia's first risk profile. During the assessment period, Latvia confiscated considerable amounts, having recovered over EUR 300 million, mainly under a non-conviction-based confiscation (NCBC) regime. Nonetheless, there is a considerable gap between the amount of assets seized/frozen and those confiscated, this being a result of a number of high-profile cases still pending a final decision by the judicial authorities.

c) Latvian authorities use asset recovery networks to identify and trace assets held abroad effectively. However, the confiscation and repatriation figures are not aligned with these efforts. This represents a minor shortcoming.

d) Latvia pursues undeclared or falsely declared cross-border currency and bearer negotiable instruments (BNI) movements to a large extent. This is mainly thanks to increasing numbers of investigations and the adoption of a threshold-based system of penalties and fines. With decreasing cross-border flows from higher-risk jurisdictions and increased identification and investigations, this change marks a substantial level of effectiveness.

e) Freezing and seizing of assets statistics reflect a broad alignment of Latvia's confiscation policy with the evolving risks. Confiscation results still reflect the first risk profile (regional financial centre) due to the lifecycle of criminal proceedings, which can take several years.

Key Recommended Action (KRA)

N/A

Other Recommended Actions

a) Authorities should address the gap between frozen/seized and confiscated assets as a key performance indicator. In order to do so, authorities should take appropriate actions, such as providing specific guidance and training for judicial authorities.

b) Latvian authorities should increase the confiscation figures on repatriation of assets held abroad in line with Latvia's risk profile to mirror their efforts of identifying and tracing.

c) Authorities should continue to monitor violations of cross-border cash flows under the EUR

35 000 threshold (where administrative sanctions apply) to prevent exploitation of this higher reporting threshold for criminal case referrals.

Overall conclusions on IO.8

Latvia prioritises asset recovery as a policy objective. All investigations and prosecutions into major proceeds-generating offences also focus on asset recovery. Although most assets are held in accounts, relevant authorities have demonstrated their ability to manage and dispose of assets and liquidate virtual assets, too.

LEAs carry out asset identification and tracing regularly in proceeds-generating offences. Freezing and seizing statistics show a well-functioning system of provisional measures. Latvia pursues confiscation of criminal proceeds, which relies on conviction and NCBC, enabling Latvian authorities to recover considerable amounts. Overall, Latvia has confiscated significant amounts of proceeds of crime and goods of equivalent value. This notwithstanding, majority of seized assets were still pending a judgement.

Latvia's SRS Customs Administration is implementing the EU Declaration system to a large extent, which has resulted in encouraging results for non-declared cash, both at the external and the internal borders. Authorities face challenges from low levels of co-operation with some neighbouring countries where cash may originate.

Results from provisional measures are aligned with the evolving risk profile of Latvia. The consistency of confiscation results still reflects Latvia's first risk profile and is yet to fully align with changing risks, which can be justified by the lifecycle of the criminal proceedings.

Latvia is rated as having a high level of effectiveness for IO.8.

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

410. Latvia prioritises the confiscation of proceeds of crime, as well as instrumentalities and property of equivalent value as a policy objective. Latvia's National Strategy and AML/CFT/CPF action plans specifically target asset recovery and confiscation. The 2020-2022 plan included objectives like collecting confiscation statistics, training, and improved pre-trial guidelines. In 2020 and 2021, MoJ conducted confidential reviews on the effectiveness of confiscation, which were used in 2022 to update the Handbook on Confiscation and Handling of Criminal Property, which provides guidance to investigators, prosecutors, and judges on CL and procedure for confiscation.

411. Asset recovery prioritization is evident at the operational level, with regular training for investigators, prosecutors and judges on asset seizure and confiscation, including cash controls at borders. The government has allocated necessary resources, leading to increased financial investigations and parallel financial investigations by LEAs, also by using international co-operation mechanisms, with the aim of identifying the proceeds of crime or instrumentalities or the laundering activities, including analysis of financial flows and assessment of unexplained wealth (extended confiscation).[99]

412. Latvia has also shown its commitment to asset recovery through institutional reforms, establishing a confiscation fund in 2018 and the Economic Affairs Court in March 2021, which is a specialised first instance court responsible for economic crimes, including ML and corruption with specialised judges. The Economic Affairs Court also reviews NCBC cases (see also IO.7).

99. Section 70.11 (2) (3) of the CL.

413. With its latest Action Plan for 2024-2026 focusing on training, strengthening cash controls at borders, and increasing court rulings on conviction-based confiscation, Latvia is well positioned to continue prioritising the identification and recovery of the proceeds of crime.

8.2. Confiscation of proceeds, instrumentalities, and property of equivalent value from foreign and domestic predicates, and proceeds located abroad

414. Latvia has achieved significant results in identifying, tracing, freezing, and seizing suspected proceeds of crime. Confiscation values (EUR 317 million in total) are considerable. Nevertheless, the amount of assets pending adjudication is significant, thus affecting final confiscation figures.

Provisional Measures

415. Latvia carries out provisional measures, identifying, freezing, and seizing to a large extent. As noted in IO.6 and IO.7, various agencies, including the FIU, State Police, ARO,[100] CPCB, SRS TCPD and the PO have the structures and tools in place to identify and trace assets and to carry out seizures. These actions prevent proceeds from circulating, disrupting criminal networks, and prevent proceeds of crime from being reintegrated.

416. LEAs effectively identify and seize suspected proceeds of crime early in investigations to prevent asset flight or dissipation. They conduct parallel financial investigations to trace financial flows from criminality to property and from suspicions of unexplained wealth to the origin of the funds used to acquire them. LEAs use information from credit institutions and public registers and conduct investigative activities (surveillance, searches, special investigative techniques) to identify assets.

417. All LEAs co-operate and seek information from the FIU and the Asset Recovery Office (ARO). The FIU supports tracing and identification of suspected proceeds of crime, instrumentalities and property of equivalent value located inside Latvia by providing LEAs with a broad overview of accounts, assets, transactions and analysis and conducts exchanges regarding intelligence on assets located abroad (see IO.6). The ARO typically conducts requests for asset tracing abroad using operational contact points across multiple agencies.

418. The FIU can temporarily freeze funds for 40 days, extendable by 45 days if assets subject to confiscation are identified. In exceptional cases, this period can be prolonged by up to 40 additional days with approval from the Prosecutor General.[101] The FIU can issue binding orders to REs to freeze funds if there are reasonable suspicions of criminal activity, including ML/TF/PF, based on reports, its own initiative, or requests from foreign authorized institutions.[102]

419. Authorities have the power to seize suspicious funds[103] during criminal proceedings for extended periods. In all cases where ML is investigated, assets are seized for up to 31 months maximum. By the end of this period, a criminal case or NCBC proceedings must be submitted to court to maintain the assets under seizure, otherwise seized assets should be released (in accordance with Chapter 59 of the CPL).

100. While located within the State Police, the ARO is worth mentioning separately here due to their differentiated role in the context of asset recovery.

101. In exceptional cases for the receipt of significant requested information, including from abroad, a possibility exists to prolong this time, not longer than for additional 40 days, with acceptance by the Prosecutor General or his or her specially authorised prosecutor.

102. This includes a) After receipt of the report of the subject of the Law on refraining from executing a transaction; b) Upon its own initiative; and c) upon a request of foreign authorised institutions referred to in Section 62, Paragraph one of this Law to freeze the funds (Sec 32.1(1) AML/CFT/CPF Law).

103. Sec.70 et seq. of the CL provides for measures to confiscate both directly and indirectly criminally acquired property, laundered property and instrumentalities of crime, regardless of whether the property is held by criminal defendants or third parties. This includes any economic benefit as a direct or indirect result of committing a criminal offence, as well as any economic benefit derived from such proceeds. If such property has been alienated, destroyed, concealed, or disguised, and its confiscation is not possible, confiscation of corresponding value may be applied (R.4).

420. Freezing and seizing statistics indicate a robust and well-functioning system of provisional measures. During the review period, FIU Latvia froze more than EUR 1.5 billion. Of note, FIU freezing actions account for most of the cases that involved banks under liquidation and the global laundromat schemes in Latvia (i.e., the first risk profile). Such stand-alone ML cases tied to credit institutions and Latvia's prior role as a regional financial centre made up well above 90% of all frozen sums. More specifically, between 2021 and 2023, FIU Latvia froze EUR 2.3 to EUR 5.7 million annually in domestic cases ("second risk profile" and "third risk profile), and between EUR 92.2 and EUR 427 million annually in all cases (including "first risk profile" cases – such as bank liquidations). Of the temporarily frozen assets by the FIU, almost all of them (98%) are eventually seized by the investigative authorities and the PO to secure confiscations where appropriate and possible. The consolidated figures are below:

Table 8.1. Freezing and seizing statistics (2018-2023)

	2018	2019	2020	2021	2022	2023	**Total**
Total Frozen by FIU (EUR)	92 211 661	348 503 269	427 883 210	202 525 662	356 942 812	92 235 277	**1 520 301 891**
Seized by LEA/Judicial Authority (EUR)	87 075 399	366 696 812	437 376 517	198 200 605	356 042 114	91 509 610	**1 536 901 056**

Note: Seizure figures are higher than freezing amounts as they may have occurred in a previous year

421. Since the last evaluation, Latvia's asset recovery efforts have increased dramatically. In total, authorities have seized over EUR 3.2 billion from 2018-2023 (see table below).[104] It is noteworthy that 1.3 billion of the 3.2 billion refers to shares in a now-defunct bank.[105]

422. Foreign predicate offences make up just 40% of all seizure cases (971 out of 2 418), but account for 94% (EUR 3 billion of EUR 3.22 billion) of all funds seized (2018-2023). Most of the funds from foreign predicate offences are tied to large bank accounts in Latvia, investigated during bank liquidations and suspected laundromat schemes.

Table 8.2. Value and number of seizures (2018-2023)

	Domestic Predicates		Foreign Predicates[106]		Total	
Year	Cases	Amounts Seized	Cases	Amounts seized	Amounts	Cases
2018	151	48 954 578	54	38 343 314	87 297 892	205
2019	225	40 155 961	125	293 058 727	333 214 689	350
2020	291	33 443 989	238	512 684 904	546 128 893	529
2021	275	15 426 753	174	1 530 745 580	1 546 172 334	449
2022	313	22 060 350	293	474 930 476	496 990 826	606
2023	192	19 538 653	87	192 829 622	212 368 276	279
Total	**1,447**	**179 580 287**	**971**	**3 042 592 625**	**3 222 172 912**	**2 418**

423. Seizures climbed from over EUR 333 million in 2019 to over EUR 1.5 billion in 2021 and nearly EUR 500 million in 2022 and then declined to around EUR 212 million in 2023 (see table further below). The recent decline in seizures is attributed to Latvia's shifting risk profile, where individual crimes generate less revenue, in addition to an overall drop in criminal activity (see IO.7). However, it is unclear how much of this decline is due to these factors, as estimates of proceeds from each crime type are unknown.

104. The previous period accounted for around EUR 189 million seized in a similar time frame.
105. This number represents the appraised value at the time of the freezing.
106. This includes ML deriving from foreign predicates.

Final Confiscation

424. Latvia has achieved strong results for final confiscation. Authorities have successfully confiscated close to EUR 317 million (see table below). When comparing figures to its previous MER, this figure represents a near three-fold increase[107] in the proceeds of crime recovered over a similar time period. This increased value of confiscations reflects the structural and institutional reforms to Latvia's asset recovery framework, and the substantial efforts to ensure that asset recovery is pursued in line with Latvia's risk and context.

425. Looking from seizures to confiscation, most of the seized assets that have undergone court adjudication have been ultimately confiscated. A smaller portion has been released. This success rate demonstrates effectiveness from both the investigative authorities and the judicial authorities in terms of investigation and finally proving the illegal origin of the assets.

426. Nevertheless, confiscations have not kept pace with the amounts seized, and at the time of the on-site visit, almost 90% of seized assets were still pending a judgement (EUR 3.2 billion seized vs EUR 317 million confiscated).[108] Although assets remained seized and secured, it is clear that there are moderate shortcomings that authorities can address to improve the overall rate of confiscation.

Table 8.3. Seizures compared to confiscations (2019-2023)

Year	2019	2020	2021	2022	2023	**Total**	**Average**
Seized Amount (EUR)	333 214 689	546 128 893	1 546 172 334	496 990 826	212 368 276	**3 134 875 020**	**626 975 004**
Confiscated Amount (EUR)	50 548 187	40 645 499	84 159 862	117 357 019	24 179 455	**316 890 025**	**63 378 005**

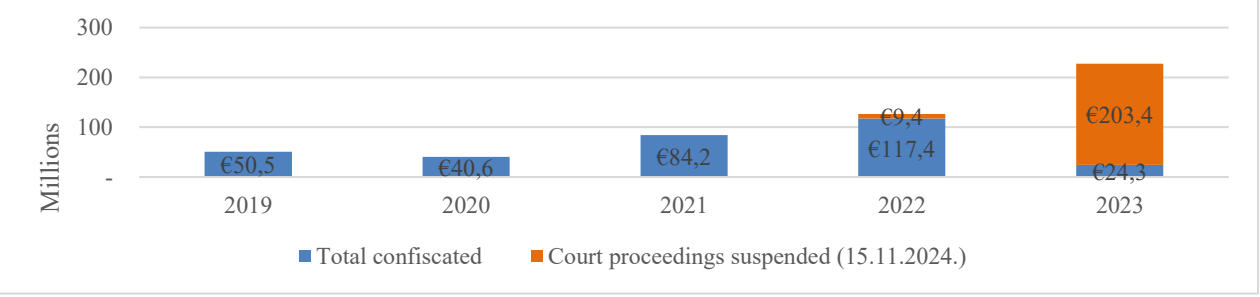
427. Part of the gap between confiscations and seizures can be attributed to legal delays and suspensions of major proceedings pending constitutional judicial decisions on NCBC regime that occurred from 2023 onwards (see discussion in paragraph below). Twenty-five cases challenging Latvia's constitutional principles remained at the time of the on-site visit.[109] While this issue does not reflect a decrease in enforcement efforts of LEAs, the suspension nonetheless impacted the overall volume of recoveries. The impact of these suspensions can be seen in the table below.

107. The previous period saw confiscations of around 105 million in a similar timeframe.

108. This rate includes the 1.3 billion in shares of a major bank liquidation from one single case. The value of these shares was estimated at the time of the seizure. Without considering this value, rate of seized assets pending adjudication drops to 82%.

109. Between 2019 and 2023, the Constitutional Court of Latvia initiated 31 cases under the Criminal Procedure and Criminal Law. Six cases resolved in Latvia's favour. The latest of these rulings involved five cases on the right of property owners to access case materials, referred to courts after the onsite visit of Latvia (which took place in November 2024). On 20 February 2025, the Constitutional Court published a judgement in the case in favour of Latvia, concluding that the legal provisions on the disclosure of case materials in NCB proceedings are compliant with the constitution. The remaining twenty-five cases at the time of the onsite included: Seven cases on the inability to appeal appellate court decisions when the court overturns a lower court's ruling and orders NCBC. (hearings schedule to begin March 2025); Two cases on the submission of evidence during appeal and whether there are violations to the right to a fair trial and effective defence. (hearings which began January 2025); Fourteen cases on the burden of proof placed on defendants, particularly for ML cases. (hearings scheduled which began February 2025). The first of the challenges have been broadly addressed by amendments to the CPL, and therefore only apply to past rulings. However, the remaining final two challenges above were continuing to move through the courts at the time of the onsite visit.

Figure 8.1. Confiscated assets and assets suspended in NCBC cases (EUR millions)



428. Although the suspended cases account for just 6% of the total confiscation cases submitted since the constitutional challenges occurred, they represent significant sums, accounting for over 85% of the amounts under adjudication in 2023 and 39% of the total amounts that have proceeded to court since 2019 (EUR 317 million confiscated vs EUR 203 million suspended). Despite the significant value of the suspensions, the constitutional court challenges had a moderate (rather than a major) impact on Latvia's overall asset recovery framework.

429. As outlined in the technical compliance annex, Latvia uses both conviction and NCBC (see R.4). The legal framework includes a presumption that, if the person involved cannot credibly explain the lawful origin of their assets, these assets may be presumed to be criminally acquired.[110] Consequently, in cases where the identity of the guilty person has not yet been determined or there is insufficient evidence to bring a possible suspect to criminal liability, or for objective reasons (e.g., the suspect has absconded or is abroad), the case cannot be transferred to court in the near future, it is only necessary to establish the illicit origin of the property without needing to prove an individual's guilt or a predicate offence. This allows for quicker and more focused decisions regarding property confiscation, streamlining the process and avoiding unnecessary delays in criminal trials.

430. NCBC has proven to be a valuable mechanism for resolving property-related issues promptly, especially given Latvia's context and risks, with numerous cases involving foreign predicates and assets laundered in now-defunct banks. NCBC accounted for 73% of all cases where confiscation was applied and 98% of all assets recovered from 2018 to 2023. Overall, first-instance decisions on NCBCs are rarely changed, with only a few exceptions not exceeding 10%.

431. As Latvia's prosecutors pursue more cases tied to asset seizures from the second risk profile, we are now seeing a greater number of conviction-based confiscation cases to proceed (but with fewer funds confiscated overall from conviction-based confiscations).

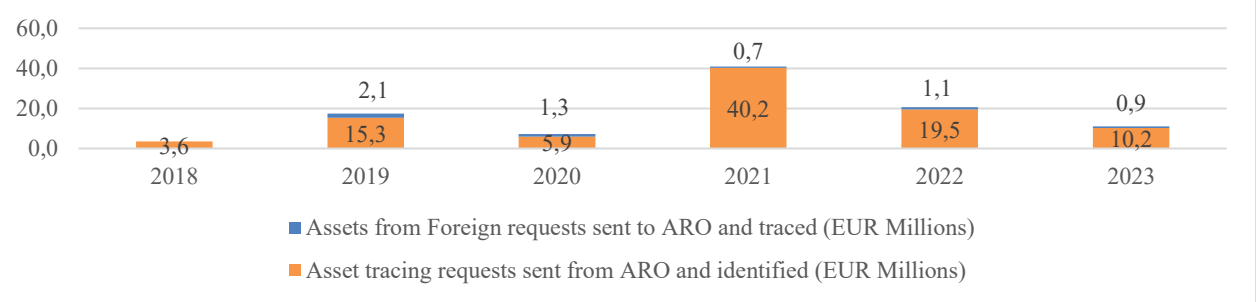
Proceeds moved abroad

432. The ARO is the dedicated authority for seeking criminal intelligence for operational authorities and conducting unexplained wealth assessments for assets abroad. In instances of suspected proceeds of crime located abroad, Latvia relies on a well-established framework of international co-operation to identify and request seizing of assets. LEAs regularly contact the ARO and the FIU to trace and identify assets located abroad. The ARO has an international co-operation handbook with contact information of relevant counterparts and is an active member of the CARIN within the ARIN Network. It regularly participates in tracing and seizing requests. Latvia traced nearly EUR 100 million in assets to foreign jurisdiction (see table below and IO.2).

110. Section 126(6) of the CPL states that: "… *the criminal origin of the property shall be considered proven if … that property is, most likely, of criminal rather than lawful origin*."

Figure 8.2. ARO asset tracing[111]

Total amounts (in EUR millions) traced in international asset tracing efforts



433. Of the near EUR 100 million in assets traced abroad, Latvian authorities have sent 126 seizure requests abroad totalling EUR 19.1 million. They have successfully achieved the final confiscation of just EUR 1.3 million in five cases. As also noted under IO.2, Latvia's actions on tracing and identifying assets located abroad are not always followed by seizure, which in turn is not always followed by confiscation (and repatriation or sharing) requests. This demonstrates a minor deficiency in Latvia's application of its asset recovery regime as the risk profile of Latvia suggests most illicit proceeds are held domestically.[112]

434. It is worth noting that assets traced from foreign LEA requests totalled only EUR 6 million. Despite few requests from counterparts, Latvia proactively traces suspected proceeds of foreign predicates domestically and engaged with foreign counterparts on foreign account holders in relation to these cases (see also IO.2).

Managing seized assets, sharing and restitution

435. Most Latvia's seized assets have been in the form of frozen funds located in bank accounts. In these instances, the assets are effectively seized and maintained through mechanisms that are robust, preventing tipping-off and guaranteeing a secure maintenance of the frozen accounts. The State Provision Agency manages and disposes of seized, frozen, or confiscated property, including converting seized virtual currencies to cash. The Provision Agency transfers funds from the sale of assets to an escrow account in the State Treasury until the final decision in the criminal case. Modest sums are disposed of and realized by the State Provision Agency (see table below).

111. Assets traced in national cases means that those are domestic investigations in which ARO has been asked to trace assets abroad. International cases refer to the foreign requests to trace assets in Latvia. Previously until 2020, AROs only requested information on assets, but now there are also requests on the ownership of accounts.

112. The low final confiscation amounts may also be due to difficulties in co-ordination for international co-operation on asset recovery, particularly given low levels of co-operation from some neighbouring countries and from various offshore financial sectors where assets may be located.

Table 8.4. Sums of disposed property and realised virtual currency

	2018	2019	2020	2021	2022	2023	total
Proceeds from the disposal of property	137 191	135 044	68 522	124 861	109 284	352 037	**926 939**
Proceeds from the realisation of virtual currency	-	-	-	-	420 325	1 455 716	**1 876 041**
Sums returned to victims (2019-2023)	-	116 097	18 213 289	285 806	8 185	38 682	**18 662 059**
Other property returned (2019-2023)	-	1 property, 3 vehicles	1 property, 1 vehicle	2 properties	10 vehicles, 74 sheep	-	-

436. Restitution to victims is being followed as a policy and all implicated authorities share this view. According to Section 70.11(4) of the CL, criminally acquired property shall be confiscated if it is not to be returned to the owner or lawful possessor. The procedure for restitution of property is regulated in Section 357 of the CPL. From 2019 to 2023, over EUR 18 million in sums and additional property was restituted to victims (see table above).

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

437. Latvia is confiscating falsely and undeclared cash to a large extent. Thanks to additional resources and legal and regulatory reforms, authorities are targeting and identifying more cases at the border, which highlights important progress for interdicting currency/BNI at the borders.

438. The SRS Customs Administration officers carry out cash controls at the external and internal (EU) borders (declaration and disclosure, respectively). Latvia has borders with three EU Member States (Estonia, Lithuania, and Sweden) as well as with Belarus and the Russian Federation. The country has one major international airport (Riga) and about nine sea harbours/ports.

439. Cash declarations must be made above EUR 10 000. Latvia applies a declaration system at external borders and a disclosure system for internal (EU) travellers and packages. As regards the declaration of cash entering or leaving the EU's external borders, Regulation (EU) 2018/1672 of the European Parliament and of the Council applies (see R.32). For amounts under EUR 35 000[113] and when there is no suspicion of underlying offences such as cash smuggling or ML, authorities apply an administrative process and penalty worth up to 20% of the undeclared amount. For amounts more than this and for all amounts that are suspected of being proceeds of crime (or part of a broader smuggling or ML scheme), criminal liability applies (Sec. 195, CL). In total, there are 179 cases a year where the administrative sanctions are used for these amounts between EUR 10 000 and EUR 35 000. These cases led to administrative fines worth EUR 340 000 over the period assessed (see table below).

440. The initiation of criminal proceedings, and the confiscation of sums at the border shows an improvement over the last period (2013-2017) where authorities initiated no criminal proceedings or confiscations. This improvement has also occurred at a time when the risk from cross-border cash smuggling has decreased, with the near closure of several border crossings with the Russian Federation and Belarus (since 2020), and as Latvia has transitioned away from its role as a regional financial centre. Between 2018-2023, Latvian authorities received nearly 5 500 cash declarations, averaging 909 per year, with a drop during COVID-19 (2020-2022). In 2023, this increased to over 1 400. Authorities detected 256 undeclared cash declarations totalling EUR 9.5 million (around EUR 1.6 million per year). Over half (140) led to criminal proceedings for ML or non-declaration, resulting in 38 prosecutions and 8 confiscation orders worth EUR 1.67 million.

113. The amount corresponds to the amount of 50 times the minimum monthly wage of any given year.

Table 8.5. Annual declaration numbers and breaches (2018-2023)

	2018	2019	2020	2021	2022	2023	total
Number of declarations/disclosures submitted	885	985	467	531	1 166	1 417	**5 451**
Number of false declaring	29	45	16	38	51	77	**256**
Number of cases where sanctions applied* (administrative violations)	36	27	3	12	28	66	**172**
Number of initiated criminal proceedings for ML and/or non-declaration or false declaration	7	47	20	28	27	11	**140**
Number of sent criminal proceedings for initiation of criminal prosecution for legalization of cash and/or non-declaration or false declaration	-	5	5	4	13	11	**38**
Number of cases where confiscation applied (by TCPB)	-	-	2	2	2	2	**8**

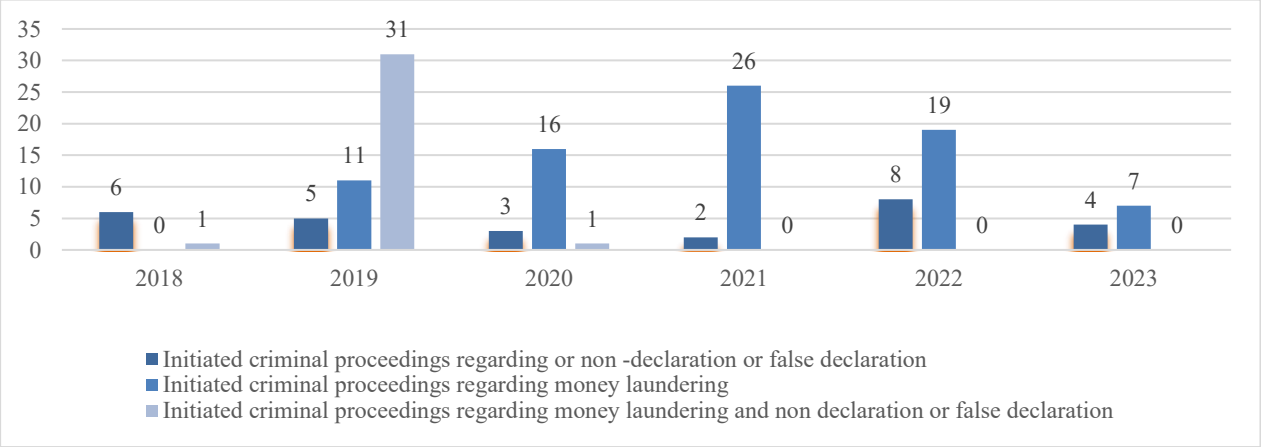
Table 8.6. Annual value of disclosures and confiscations for cross-border currency (EUR, 2018-2023)

Year	2018	2019	2020	2021	2022	2023	total
Annual value of declared/disclosed assets in EUR	222 241 638	162 784 412	58 570 516	55 684 221	79 903 489	41 247 680	**620 431 956**
Annual value of undeclared/falsely declared assets in EUR	522 685	2 570 366	530 174	2 454 866	1 780 934	1 613 244	**9 472 269**
Annual value of fines in EUR	30 690	40 760	6 696	42 952	78 258	141 139	**340 495**
Annual value of confiscation orders in EUR (by TCPB)	-	-	42 538	271 934	116 915	1 241 822	**1 673 208**

441. In most cases, criminal proceedings initiated for moving cash across the border are for undeclared cash. These often involve citizens from neighbouring countries. Latvia's legal framework does not require identification of a predicate offence. The number of administrative violations increased and consequently the total amount of fines imposed increased, too. However, the number of criminal prosecutions decreased compared to previous years. One factor that hinders effectiveness is that most of the possible predicate crimes and possible ML schemes take place in some neighbouring countries, where it is currently difficult to receive trusted information and in timely manner from those countries. As it is challenging to investigate the predicate offense that has occurred in these countries, cash movements are criminally investigated as stand-alone ML.

442. In response to undeclared assets and suspicions at the border, SRS TCPD initiated 140 criminal proceedings for non-declaration or false declaration of cash, of which 38 were sent to PO for prosecution and ten of these were for ML. In eight criminal proceedings, the court declared the seized funds to be the proceeds of crime and ordered the confiscation of the cash, totalling EUR 1 673 208.

Figure 8.3. Initiated criminal proceedings regarding ML and/or non-declaration or false declaration



443. Overall, Latvia has implemented the EU framework to register cross-border cash and BNI declarations for external borders to a large extent. This is now starting to yield some criminal investigations into cross-border smuggling, and some limited number of ML investigations, with some confiscations. Noting that authorities may at any time trigger an investigation of suspected ML and criminal offences for non-declaration, authorities should nevertheless continue to systematically monitor threshold violations that fall under EUR 35 000 to carefully to ensure that cash smuggling is not occurring at or near these threshold amounts.

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

444. The amounts confiscated over the past years in Latvia highlight consistency with national ML/TF policy and identified risks. Latvia is pursuing illegal funds in Latvian banks under liquidation and prioritises the follow-the-money approach. The authorities are actively freezing, seizing, and confiscating illegal property, especially bank account assets, which resulted in some high-profile cases with considerable amounts of confiscated illegal property. Nevertheless, given the lifecycle of criminal proceedings, confiscation figures still reflect Latvia's first risk profile (regional financial centre) which prevailed during the assessment period and are only somewhat aligned with Latvia's changing risk profile (confiscations in relation to recent seizures may take some time to materialise). Still, the results achieved in freezing and seizing assets related to the second risk profile are encouraging.

445. Looking first at freezing statistics relative to risk, these figures show a shift that mirrors Latvia's evolution from the first risk-profile (regional financial centre) towards the second risk profile with increasing shares of predicate offences such as fraud, tax crimes, and other offences (tied to the second risk profile) and fewer stand-alone cases (tied to the first risk-profile) in the freezing statistics.

Table 8.7 Annual Breakdown of Seizure Cases (2018-2023)

	2018	2019	2020	2021	2022	2023
Other predicates	39%	46%	38%	56%	41%	58%
ML	61%	54%	62%	44%	59%	42%

Table 8.8. Seizure cases and value by predicate offence (2018-2023)

Predicate	Total seizure cases	Cases as % of total	total assets seized	Assets as % of total
ML	1 849	54%	3 097 014 396	94%
Drug related offences	547	16%	7 433 974	0.2%
Tax crimes	326	10%	15 503 812	0.5%
Illegal activities with excise goods	310	9%	5 643 992	0.2%
Fraud	239	7%	92 764 192	2.8%
Corruption related offences	90	3%	78 762 497	2.4%
Smuggling	64	2%	1 621 270	0.05%
Total	**3 425**	**100%**	**3 298 744 133**	**100%**

446. However, looking at the breakdown of final confiscations, these figures do not yet mirror Latvia's changing risk profile to the same extent as the freezing and seizing statistics. As the table below shows, around 83% of all confiscated funds are tied to stand-alone ML, with the remaining connected to fraud (7.4%), corruption (3.4%), forgery (2.2%), tax evasion (1.9%) and sanctions violations (1.7%) and other offences (less than 1%). Given the quantum of value tied to Latvia's first risk profile, it is not clear to what extent Latvia is conducting confiscations aligned with its second risk profile (e.g. fraud, tax evasion, smuggling, etc.).

Table 8.9. Confiscation figures by predicate offence (2018-2023)

Predicate offence	percentage
ML Stand-alone	82.9%
Fraud	7.4%
corruption (bribery, abuse of position, misappropriation, etc.)	3.4%
Forgery of a Document	2.2%
Tax evasion	1.9%
Sanctions violation	1.7%
Illegal production, sale, storage of Alcohol and Tobacco Products	0.2%
Sexual violence	0.1%
Extortion	0.1%
Illicit trafficking in narcotic drugs and psychotropic substances	0.1%
Smuggling, Robbery, Theft	0.0%
Other	<1%
Total	**100.0%**

Note: Figures under 1% are selected among a wider range of crime, whose total is less than 1%.

Table 8.10. Confiscation cases by predicate offence

Predicate offence	percentage
ML Stand-alone	45%
Illicit trafficking in narcotic drugs and psychotropic substances	17%
Fraud, theft, robbery, misappropriation	10%
Tax related crimes (tax evasion, tax fraud, etc.)	9%
Illegal production, sale, storage of alcohol and tobacco products, including smuggling	6%
Other (THB, corruption related crimes, etc.)	13%
Total	**100%**

447. With the overwhelming percentage of confiscations tied to "stand-alone ML" and few figures attached to other offences such as smuggling, tax crime, fraud and others, it is clear that Latvia has confiscated assets in line with risks associated with major ML schemes and global laundromat schemes located in Latvia (their first risk profile), but it is less clear to what extent other major proceeds generating offences (particularly those in Latvia's second risk profile) are subject to confiscation. However, considering the freezing and seizing results so far, Latvia shows consistency in pursuing seizures in line with ML/TF risks and policies.

Chapter 9. Terrorist Financing Investigations and Prosecutions

The relevant Immediate Outcomes considered and assessed in this chapter is IO.9 The Recommendations relevant for the assessment of effectiveness under this chapter are R. 5, 30, 31 and 39 and elements of R. 1, 2, 15, 32, 37 and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Latvia has a sound legal and institutional frameworks for combating TF, with authorities having a good understanding of the country's risk profile. There have been few cases of identification of possible TF, based on the FIU and the State Security Service intelligence. One investigation was initiated, which is consistent with country's risk profile. Co-operation between competent authorities is effective and timely, and it is further strengthened through the work of a dedicated CFT Task Force.

b) Given the lack of TF prosecution and conviction, it is not possible to assess whether sanctions or measures applied for TF offences would be effective, proportionate, and dissuasive. However, there are Guidelines for prosecutors on sanctioning policy which serve them as a basis for demanding harsher penalties from the courts in potential TF cases.

c) The 2021-2026 Counter-terrorism strategy is an overarching strategy which also addresses TF issues. Given the low number of TF investigations and no TF prosecutions so far, it is difficult to assess to what extent the findings and lessons learnt from these are considered and used in the formulation of national counter-terrorism strategies.

d) Latvia has several measures to disrupt TF activities when it is not practicable to secure a TF conviction. These measures have effectively been applied in practice.

Key Recommended Actions (KRA)

N/A

Other Recommended Actions

a) Latvia should use any future TF cases (whether investigation, prosecution or conviction) in the formulation of national counter-terrorism strategies.

b) Latvia should ensure the implementation of the Guidelines on Sanctioning in Criminal Proceedings Related to Threats to State Security and raise awareness among judges and prosecutors with the aim to harmonize prosecutor's and courts' practice on sentencing in TF cases, if such cases occur.

Overall conclusions on IO.9

Latvia faces low terrorism and TF risks, as demonstrated by thorough risk assessments and a well-substantiated understanding shown by the authorities during the assessment period. The country benefits from a solid legal and institutional framework, supported by highly skilled professionals and strong co-operation among key stakeholders. Latvia has established several task forces to facilitate TF identification and investigation. These structures enable the effective identification and investigation of TF activities and prompt exchange of information.

Throughout the review period, several instances of potential TF-related suspicions were identified and properly analysed. One TF investigation was initiated, which was ultimately closed due to insufficient evidence of TF. Overall, in all cases, competent authorities applied appropriate measures to detect and investigate TF activities. The absence of TF prosecutions or convictions appears consistent with the country's overall TF risk profile.

There is an overarching counterterrorism strategy, addressing the issue of TF. Nevertheless, given that there was only one TF investigation and no prosecution, it was not possible to assess the extent to which they were used in forming a strategy. While it is difficult to assess the effectiveness, proportionality, and dissuasiveness of sanctions for TF offences, it is worth noting that authorities have issued guidelines to ensure proper sanctioning in criminal proceedings, though these guidelines have yet to demonstrate that they affect final courts' decisions. Finally, Latvia has demonstrated its ability to implement alternative measures to disrupt potential TF activities, when a formal conviction for TF cannot be achieved.

Latvia is rated as having a substantial level of effectiveness for IO.9.

448. In the previous mutual evaluation, Latvia demonstrated a moderate level of effectiveness in combating TF and major deficiencies were identified in its understanding of TF risks. That said, during the period under review by this MER, Latvia has undertaken several initiatives to enhance its TF risk understanding and address the previously identified deficiencies. As discussed in IO.1, terrorism and TF risks are assessed as low, based on variety of data, information and contextual issues analysed and evaluated through regular NRA processes.

449. As noted above, 2018 MER recommended to Latvia to conduct a risk assessment focused on TF vulnerabilities inherent to its role as a regional financial centre, and to enhance interagency awareness of the then TF investigations *which could be achieved by a common platform housing current information on terrorism-related investigations and information*. These recommended actions were translated into concrete measures – TF risks were reassessed (see IO.1) and a CFT task force was established. In addition, the Specially Authorised Prosecutors' Division was assigned as the competent division for the prosecution of TF and other terrorism related cases. The division is part of Criminal Justice Department of the GPO.

450. There is a sound legal and institutional framework for combating TF and other terrorism-related offences. Authorities are well-trained and knowledgeable about TF trends and methods, with a strong understanding of the country's risk profile. The FIU and the State Security Service are competent authorities to identify TF cases, while the State Security Service is the only authority in charge of investigating TF cases. There is a Specially Authorised Prosecutor's Division of the GPO which is competent to prosecute TF and other terrorism related cases.

9.1. TF activity identified and investigated

9.1.1. Identification and investigation of TF activity

451. In Latvia, different sources of information are used to identify and investigate potential TF cases and the authorities, during the assessment period, have undertaken a number of initiatives and measures in order

to improve the understanding and the interpretation of TF offences. Several task forces and WGs have been created to improve and strengthen the system of TF identification and investigation.

452. The CFT Task Force was established in June 2024. Whilst its effectiveness at the operational level could not be fully assessed primarily due to its recent establishment, it structure, including the modus operandi it has put in place, present a useful mechanism for the identification of possible TF cases (see IO.1).

453. On an operational level, the Terrorist Financing Investigation Co-ordination WG (consisting of State Security Service, FIU, PO, SRS TCPD, State Police and Latvijas Banka), was created in December 2019 as a subgroup of the Council of Experts of the Counter-terrorism Centre. This WG serves as a solid platform to share information relevant for TF identifications and investigations.

454. Various sources are used to identify potential TF cases. These include FIU's financial intelligence (stemming from STRs or other sources), information gathered during the process of the NPOs' supervision, open sources, State Security Service's own intelligence, information and requests received from foreign counterparts (formal and informal), criminal investigations related to terrorism, information from supervisory authorities, strategic and tactical analysis (including those in relation to cross-border financial flows to and from high risk jurisdictions), information on terrorism-related TFS hits, and other.

455. It is also possible to identify and initiate a TF case through specific measures applied by State Security Service which concern radicalised persons. These measures are carried out on a regular basis with the aim to prevent terrorism and the threat of its financing. This is done through preventive screening of individuals where there is a suspicion about their possible interest in terrorism or terrorism related ideologies. In practical terms, the process applied by the State Security Service includes the use of the Black-Box to determine whether the FIU Latvia has any information at its disposal on a suspect/radicalised person. If the Black-Box provides a positive match and confirms that the FIU has information about a suspect, the State Security Service then requests from the FIU further information and financial profiling of a suspect, including his/her connections to other natural and legal persons. The current practice of using Black-Box in terrorism related cases proves the ability of State Security Service to identify or contribute to the identification of a potential TF activity.

456. Additionally, the FIU of Latvia takes active part in two international WGs: the Counter Terrorist Financing Taskforce – Israel (CTFTI) and the Counter ISIS Finance Group (CIFG). Through its participation in these groups, FIU Latvia gains crucial insights into global TF trends and investigative methods, significantly improving its ability to detect and combat TF more effectively.

457. To improve the detection of TF cases, in 2019 the FIU, in close collaboration with the State Security Service, issued guidelines on CFT/CPF for REs and SCAs. These guidelines were revised in 2024 outlining current trends and developments in Europe and Latvia and offering comprehensive information on TF indicators. In addition, the State Security Service has developed and updated Guidelines on Investigating TF, approved by the GPO in July 2024. The guidelines outline the concept of TF, its legal definition, and provide detailed information on the investigation process, including when to initiate an investigation and steps to take at the initial stage. They emphasise the use of circumstantial evidence and clarify that linking TF to a terrorist attack is not required. The guidelines also address the importance of seeking international co-operation in TF investigations. They serve as a practical tool for investigators and prosecutors, reflecting the latest trends and best practices in TF prevention and investigation. The AT considers that, despite the fact that the TF risk is low and there is an insignificant number of TF cases, the authorities are equipped with knowledge, tools and mechanism to timely and proactively tackle any possible TF case.

458. There were a few instances where possible TF activities were identified, based on the intelligence from the FIU and the State Security Service. One of these cases led to an investigation (see box 4.3), whilst for others the authorities advised that they had not found sufficient evidence of TF to proceed with investigations.

459. During the review period, the FIU received 30 TF-related STRs. Each STR was analysed with urgency, using various databases and information sources to verify details swiftly (see box 4.1). In cases where foreign

links were identified, information from foreign counterparts was sought. In addition, the FIU received 23 foreign requests, and 21 spontaneous disseminations reports related to TF suspicion, which were analysed in the context of Latvia. In only 12 of these cases, links to Latvia were established. In all FIU cases, the information was thoroughly assessed, using analytical tools and various databases – cases were either disseminated to LEAs or foreign FIUs or archived if TF suspicions were not confirmed (for issues related to the FIU performance, please see IO.6).

460. Overall, the FIU disseminated 15 intelligence reports to the State Security Service and foreign FIUs following the receipt of TF-related STRs. Further to that, in 15 operational cases the FIU verified potential TF-related information by requesting further details from REs, foreign FIUs, or the State Security Service. Based on the requests and spontaneous dissemination reports received by the FIU concerning potential TF activities, 8 additional intelligence reports were disseminated to the State Security Service. As it is demonstrated by the case example (see box 4.1), it is evident that the FIU takes appropriate measures to identify potential TF suspicion and promptly disseminates the case to the LEA. Furthermore, the State Security Service, when conducting preliminary inquiries, demonstrates a high level of expertise and thoroughness in its work, ensuring that all relevant information is carefully assessed and acted upon.

Box 0.1. TF STR dissemination to the State Security Service

In November 2019, the FIU Latvia received a TF-related STR regarding a Latvian citizen who applied for a EUR 8 000 loan, claiming it was for apartment repairs. The citizen had already received loans from other institutions and transferred the funds abroad. When asked, the Latvian citizen explained that the loan would be sent to a Nigerian citizen in Country A, allegedly to help the person travel to Syria. Between May and September 2019, the Latvian citizen sent EUR 12 943 to an account held by the Nigerian citizen in Country A. In order to verify information, the FIU sent a request to the Country's A FIU seeking banking information of the Nigerian citizen. The FIU disseminated the analysis carried out in this case together with the information received from the foreign counterparts. The State Security Service conducted an in-depth analysis during the pre-investigation stage and questioned the Latvian citizen. It was established that the citizen of Latvia had become the victim of financial fraud, and no indications of TF activities were identified.

461. In cases where STRs were not disseminated to LEAs, this was due to insufficient evidence of TF. The FIU determined that this was not a matter of STR quality but rather the result of requiring additional information, which, once obtained, confirmed the absence of TF grounds (see box 4.2). This process highlights Latvia's commitment in combating TF, showcasing the FIU's effectiveness in handling and sharing intelligence related to TF risks.

Box 9.2. Analysis of TF STR without making further dissemination

In November 2022, FIU Latvia received a TF-related STR concerning a Latvian resident born in a country ISIS-operated. Between January 2021 and October 2022, this individual made 50 cash deposits in the total amount of EUR 18 805 into an account at a Latvian credit institution.

Additionally, between August 2022 and September 2022, the resident received 15 transfers amounting to EUR 9 440 from a non-EU citizen–some of which were sent immediately after the sender deposited cash into their own account. Similar transfers were also received from several Latvian citizens. The Latvian resident then transferred the funds further to his account in a foreign credit institution and occasionally used a foreign payment service provider.

When asked, the Latvian resident mentioned another foreign payment service provider but was hesitant to provide his foreign account statement. FIU Latvia requested details from the foreign counterparts about the transactions conducted through the foreign payment service provider and analysed the submitted data alongside information from its databases. The analysis revealed that the Latvian resident was involved in several criminal cases relating to illegal immigration services. However, no links to TF were found, and as a result, the FIU did not proceed with

a TF-related dissemination.

462. The authorities had one TF investigation during the assessment period, which was terminated due to the lack of evidence (see box 4.3). Looking solely at this investigation, and the way the investigative techniques were applied, it could be concluded that all relevant facts of the case were properly considered.

Box 9.3. TF investigation

In 2021 during the follow-up and monitoring activities of data, the State Security Service discovered that in 2015, a Latvian resident transferred in total EUR 3 757 to a person who was charged with TF and was listed in Country A. After collecting data and making an analysis, a criminal investigation was launched concerning possible TF activities. During the course of the investigation, information was sought from Country A, however, no information was provided regarding the suspicion of beneficiary in TF.

The authorities undertook several investigative measures, including a search of the Latvian resident's place of residence. It was discovered that, at the time of the search, the Latvian resident was in possession of terrorist propaganda materials. However, these were fairly recent and no terrorist propaganda materials from 2015 or other indications of TF or radicalisation in 2015 were discovered. The criminal investigation was terminated, since there was no evidence that the Latvian resident had transferred funds with the intention of financing terrorism or that the Latvian resident had been aware that the recipient of funds was involved in TF or terrorism.

463. Apart from analysing this case, the AT has held in-depth discussions on TF identification and observed that there is a strong and effective level of co-operation between the FIU, the State Security Service, and prosecutors in identifying potential TF cases, demonstrating a well-coordinated and collaborative approach. There are adequate necessary tools and guidelines on how to conduct TF probes and what evidence should be collected, including ones from foreign jurisdictions. In addition, measures applied after a TF investigation were terminated, again confirming the competent authorities' ability to properly respond to possible challenges at any stage of a TF case.

9.1.2. Investigations identifying the specific role of terrorist financier

464. The authorities have demonstrated a versatile understanding of various specific roles that can be played by terrorist financiers. Despite there being only one criminal investigation into TF, the AT based its conclusions on two key sources; (i) the outcomes of investigations conducted by the State Security Service in terrorism-related cases, and (ii) discussions held with the relevant interlocutors.

465. There were nine criminal cases involving terrorism-related offences during the assessment period. In seven of these cases, parallel financial investigations into possible TF were conducted. As for the two cases where parallel financial investigation was not conducted, one of the cases was terminated at an early stage, and the other one did not include any suspicion on TF. As a result of the terrorism related investigations, seven cases were referred to the court, out of which four have been heard at the first instance.

466. With regard to the way parallel financial investigations into potential TF are carried out, it appears that FIU intelligence is critical for commencing such investigations. In all provided case examples of investigation of TF and terrorism-related offences, the State Security Service had required financial information from the FIU.

467. This notwithstanding, as part of their scrutiny of potential TF activity, the State Security Service is systematically conducting parallel financial investigations which serves as a good base to identify different roles that potential terrorist financiers could have. Whilst the key milestones of TF investigations are touched upon in the State Security Service's guidelines, as discussed above, a wide range of operational tools, tactics and information are at the State Security Service's disposal when investigating TF. Discussions held on-site confirm the State Security Service's awareness and ability to identify different roles performed by terrorist

financiers. Parallel financial investigations by the State Security Service take the form of general and special operational activities provided by the Operational Activities Law. These activities include investigatory inquiries to credit and FIs, investigatory acquisition, investigatory monitoring of transactions in an account of a client of the credit institution or financial institution, which may be performed during the operational phase. Application of these means is possible only upon approval by the Supreme Court. The practice from terrorism related investigations has proven that Supreme Court decisions on these matters are timely, and a wide range of financial information regarding the subject person, as well as persons involved in financial transactions, are thus gathered in the course of these investigations.

468. Furthermore, internal guidelines on conducting financial investigations further bolster these efforts, providing structured directions to authorities.

9.2. Prosecuting and convicting different types of TF

469. In Latvia, there is a Specially Authorised Prosecutors' Division within the GPO which is competent for the prosecution of terrorism and TF cases. There are six prosecutors in the division who demonstrated a good understanding of TF offences and expertise in dealing with such cases. Besides, they have all sufficient powers enabling them to collect lawful evidence suitable to corroborate TF offence before the court.

470. Prosecutors are involved in TF cases from the early stage of the identification, providing case-specific guidelines to the State Security Service in order to secure evidence properly and timely. As explained in the previous core issue, the prosecutors guided and approved general guidelines on TF investigation which are to be applied and followed by the State Security Service.

471. There has been no prosecution nor conviction for TF offence in Latvia and therefore no occasion for the prosecutors and courts to develop case law on the evidence needed to secure TF conviction. Notwithstanding, the authorities demonstrated that there is well established understanding that objective factual circumstances would be used to prove the intent and knowledge of the perpetrator of a TF offence. To corroborate their arguments, the authorities confirmed that the jurisprudence on assessing circumstantial evidence, as established by the Supreme Court, would be applied in TF cases equally. Nonetheless, the Supreme Court decision discussed an ML case and assessment of circumstantial evidence thereof, but the principle it emphasised states that in criminal proceedings *indicative or circumstantial evidence may also be used to confirm the existence or non-existence of the facts to be proved, which, by means of related facts, gives rise to an inference of the facts to be proved, and it is not decisive which evidence – direct or indicative or circumstantial – is used to prove the guilt of the accused, but what matters is whether the totality of the evidence does not raise a reasonable doubt as to guilt* (Paragraph 5.1 of the decision of the Senate of 13 May 2021 in Case No SKK-89/2021). As a consequence, judicial and prosecutorial authorities would apply these principles in potential TF case trials. This understanding is further embodied into the guidelines on TF investigation, which also emphasise the importance of using objective factual circumstances when proving intent and knowledge by the perpetrator of a TF offence.

9.3. Effectiveness, proportionality and dissuasiveness of sanctions

472. In the absence of TF convictions, it is not possible to assess whether the criminal sanctions applied in practice are effective, proportionate, and dissuasive.

473. However, in order to assess the effectiveness, the AT considered sanctions imposed in terrorism related cases and sanctioning policy adopted by the authorities, which would be expected to be applied in TF criminal cases. Reasoning for this is further explained below.

474. The GPO issued updated Guidelines on Sanctioning in Criminal Proceedings Related to Threats to State Security (referred to as the "Guidelines on Sanctioning"). According to these guidelines, for criminal offenses that threaten national security (including terrorism and TF offences), prosecutors are required to recommend specific sentencing measures to the court, as follows: (i) If no mitigating circumstances are present- a sentence exceeding half of the maximum custodial penalty prescribed by the relevant section of

the Special Part of the Criminal Law; (ii) If one or more mitigating circumstances are present: a sentence of no less than half of the maximum custodial penalty prescribed by the relevant section of the Special Part of the CL; (iii) In cases of recidivism or multiple aggravating circumstances: the maximum custodial penalty prescribed by the relevant section of the Special Part of the CL. Furthermore, the Guidelines on Sanctioning provide for the possibility for the Chief Prosecutor of the Criminal Justice Department of the GPO, based on the arguments provided by the competent prosecutor, to agree with the prosecutor's reasoning about the need to apply a different type or measure of punishment.

475. The AT finds that these guidelines would be beneficial for ensuring that sentences in TF cases are dissuasive and proportionate. Whilst prosecutors systematically follow the requirements of the guidance and suggest harsher penalties when presenting terrorism related indictments before the court, sentencing by judges in terrorism-related convictions did not reinforce prosecutors' approach as expressed in the Guidelines. For example, a criminal case was recently concluded at the first instance with the penalty of 2 years and 2 months of deprivation of liberty for the offence of self-training for terrorism, whilst the CL foresees a maximum penalty of seven years for this offence. Although it is not up to the AT to comment a criminal sanction in individual cases, it can however conclude that the impact of the Guidelines and their application by prosecutors have so far had limited effect on final courts' decision(s) regarding sentences.

9.4. National counter-terrorism strategies and activities

Formulating national counter-terrorism strategies and activities, as well as sharing and using information and intelligence to support national counter-terrorism purposes and activities

476. In November 2021, Latvia adopted an overarching 2021-2026 Counter-terrorism strategy, also addressing TF issues. The strategy includes a chapter on TF that outlines the country's legal framework for CFT and co-operation between the FIU and the State Security Service in TF cases. Given that there was only one TF investigation and no TF prosecutions so far, the AT was not able to assess to what extent the findings and lessons learnt from these are considered and used in the formulation of national counter-terrorism strategies.

477. It is also important to note, under this core issue that, cognisant of the importance of having an up-to-date assessment and mitigation of TF risks, and as noted under the core issue 9.1, Latvia established a specialised CFT Task Force, competencies and activities of which are presented under IO.1. State Security Service has also developed two CFT strategies which are based on the findings of NRAs and are focused on mitigation measures on the specific TF risks.

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

478. In Latvia, various alternative measures can be applied when securing TF conviction is not practicable, including monitoring of high-risk individuals and application of limitations to them, as well as pursuing other terrorism-related offences.

479. Given the country's low TF risk, there have been few instances where these measures were needed. Nevertheless, one example illustrates how the authorities effectively understand and implement relevant TF disruptive measures: a detainee from another country, who had become radicalised during his time in prison, virtually married a Latvian national thus formally fulfilling a requirement to become a Latvian resident. This notwithstanding, the authorities did not permit him residence given his profile and the assumed threat he may pose in relation to terrorism and TF. Based on this, a decision was made to deport him to his country of origin. This case demonstrates positive and proactive approach by the authorities in addressing potential TF.

Chapter 10. Terrorist Financing Preventive Measures and Financial Sanctions

The relevant Immediate Outcomes considered and assessed in this chapter is IO.10. The Recommendations relevant for the assessment of effectiveness under this chapter are R. 1, 4, 6 and 8 and elements of R.14, 15, 16, 26, 30, 31, 32, 35, 37, 38 and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Latvia implements TFS for TF without delay through directly applicable EU regulations, Law on Sanctions, and CoM Reg. No. 184, ensuring immediate compliance with United Nations Security Council Resolutions (UNSCRs). From the moment of adoption, the UN sanctions are directly applicable in Latvia.

b) The MFA co-ordinates the designation and delisting process. It publishes updates on new designations and amendments on its website and communicates them via email to relevant supervisory authorities, which then notify REs respectively.

c) In April 2024, the FIU Latvia assumed the role of the national authority for sanctions implementation, enhancing co-ordination and efficiency in applying TFS for TF. However, the implementation of this additional function remains too recent to allow a comprehensive assessment of its long-term impact.

d) Latvia's flexible application of TFS extends beyond formal ownership to actual control, ensuring sanctions remain effective against attempts to circumvent them through complex ownership arrangements. Although, no individuals or entities have been designated, nor funds frozen under UNSCR TFS for TF, Latvian REs have successfully frozen assets under other sanctions regimes, demonstrating their capability to implement UNSCR TFS requirements if needed.

e) Latvian authorities have conducted a risk assessment of the NPO sector, with a primary focus on fundraising activities. While the assessment concludes that the overall TF risk is low, the methodology places limited emphasis on the disbursement of funds, leaving disbursing-only NPOs outside the scope of risk classification, creating a gap in proactive scrutiny and tailored mitigation. However, this limitation is mitigated in practice by the systematic review of all financial flows to high-risk jurisdictions—regardless of an NPO's assessed risk. Latvia applies targeted mitigation measures to NPOs at heightened risk of TF, including outreach, risk-based engagement, and ongoing monitoring, in line with its overall low TF risk profile.

f) REs including FIs and DNFBPs, are generally well-informed of TFS obligations. FIs, VASPs utilize commercial screening tools for real-time and ongoing screening of clients, while DNFBPs mostly rely on the FIU's online resources. However, while extensive outreach and training activities have been conducted by FIU Latvia and other competent authorities in response to EU sanctions, understanding of UNSCR-specific TFS obligations among some DNFBPs (particularly the legal sector) is developed to a lesser extent.

g) Competent authorities provide guidance and SCAs conduct inspections regarding TFS compliance as part of broader AML/CFT initiatives. The inspections identified only minor breaches, and appropriate corrective measures have been applied.

Key Recommended Actions (KRA)

N/A

Other Recommended Actions

a) Latvian supervisory authorities should continue to ensure that inspections of REs, particularly for higher-risk sectors and entities, focus on TFS compliance at sufficient frequency and depth. Supervisory authorities should continue to ensure that breaches, even minor ones, are consistently identified, documented, and addressed with proportionate and dissuasive sanctions to strengthen compliance behaviour.

b) Continue delivering targeted training and outreach programmes for REs, particularly the legal sector. This should include detailed guidance on identifying and managing risks associated with TF and emphasize the distinction between obligations under UNSCR, EU, and national sanctions regimes.

c) Consider revising the methodology for assessing NPO risks to include a greater focus on the disbursement of funds, in addition to fundraising activities. Conduct periodic reviews of NPO activities and financial flows to ensure alignment with the FATF definition and mitigate potential vulnerabilities to TF abuse.

d) Latvia has identified individuals or entities for designation under non-UNSCR sanctions regimes. Authorities should consider reviewing and enhancing processes for identifying potential designees and freezing assets in line with UNSCR requirements to ensure that all opportunities for designation are exploited, should these arise in the future.

Overall conclusions on IO.10

Latvia has established a solid legal and institutional framework for implementing TFS related to TF. While no designations or asset freezes have occurred under relevant UNSCRs- consistent with the country's low risk exposure- Latvia has demonstrated the operational capability to act effectively when required. The recent designation of FIU Latvia as the sole competent authority for sanctions implementation is expected to enhance system-wide co-ordination, however, this institutional change was afforded limited weight in the assessment, as the framework in place prior to the reform was already functioning effectively.

Latvia has conducted TF risk assessment of the NPO sector and implements risk-based monitoring measures to prevent TF abuse, though further refinement of the risk assessment methodology to include disbursement-only entities- and thereby strengthen its initial risk classification and proactive scrutiny- would close the remaining gap.

Implementation of TF- related TFS obligations within the financial sector is strong. FIs and VASPs show high levels of awareness and compliance with TFS obligations, technical capacity, and are subject to effective supervision. While DNFBPs meet core screening requirements, gaps remain- accountants continue to exhibit a high number of TFS shortcomings and independent legal service providers display less-mature TFS awareness and procedures. Due to the exposure of DNFBPs to TF typologies, the identified shortcomings have been given greater weight in the TF context.

Latvia is rated as having a substantial level of effectiveness for IO.10.

480. Latvia's 2018 MER identified several gaps in the country's TFS regime under Immediate Outcome 10. The findings highlighted the need to clarify competent authorities' responsibilities, enable permanent freezing orders, and integrate TFS obligations into supervisors' inspection programmes with adequate resources. Latvia was also encouraged to address TF TFS evasion risks in risk assessments, enhance outreach and training for REs, and adopt a risk-based approach (RBA) to monitoring NPOs, guided by broader TF risk assessments.

481. Since 2018, Latvia reviewed and amended key legislation, including Law on Sanctions and AML/CFT/CPF Law, and CoM adopted new regulations on the implementation of sanctions to ensure that TFS are implemented directly, fully and without delay. A SCC was established as the key co-ordination mechanism, bringing together public sector, private sector and NPOs. Latvia incorporated TFS obligations into supervisors' inspection programmes with necessary resources allocated. Both NRAs conducted in the reporting period, identified TF TFS evasion risks highlighting greater exposure to non-TF/PF-related sanctions evasion. Outreach and training efforts were expanded, with comprehensive guidelines and training sessions for REs. Latvia also implemented an RBA to monitor NPOs, identifying high-risk entities and updating recommendations for BO identification and transaction assessments. Further reforms and country's actions will be discussed in the following chapters of this Immediate Outcome.

10.1. Implementation of TF-related targeted financial sanctions without delay

482. Latvia implements TF-related TFS through the directly applicable EU regulations, Law on Sanctions and CoM Reg. No. 184. The Law on Sanctions provides for the direct and immediate implementation of all UNSCRs (including UNSCR 1373, 1267/1989 and its successor resolutions) together with the procedures provided for therein, which become binding from the moment of their adoption and ensures that TFS are implemented without delay by all natural and legal persons in Latvia.

483. All UNSCRs including changes thereto have legal effect in Latvia immediately and automatically, regardless of whether a notice has been published. Nevertheless, to raise awareness of the private sector and general public, Latvia employs a comprehensive and structured approach to communicating new or amended sanctions designations to FIs, VASPs, DNFBPs, and the public.

484. Latvia has a structured system for the communication of UNSCR-related TFS designations to relevant competent authorities and REs. Designations are disseminated without delay following UN notification, using the multiple channels: the MFA website, the Official Gazette, and the FIU Latvia's sanctions search engine, which hosts a unified database of UNSCR, EU, and national sanctions. Updated at least twice daily and publicly accessible, the FIU search engine averaged 2,290 monthly users between April and October 2024. This multi-channel approach ensures that communication reaches a broad range of REs.

485. Proactive communication is supported by a MFA's subscription-based email alert system (approx. 590 subscribers)- used to disseminate listings, de-listings, and updates immediately upon notification- and sectoral outreach by FIU Latvia, including training, guidance, and use of media. Supervisory authorities are expected to cascade designation information to the REs they oversee. Latvijas Banka and the LCSN have automated onward communication systems, enabling real-time dissemination of updates to their REs. Other supervisory authorities use manual processes in line with their internal procedures, which ensure that REs receive relevant information without undue delay.

486. The MFA serves as the co-ordinating body responsible for proposing of persons or entities for designation and their removal under sanctions regimes, as decided and approved by the CoM. The designation process involves consultations with relevant state security institutions and the FIU Latvia, and the compilation of evidence to support proposals, which are submitted to the appropriate bodies for further consideration.

487. Latvia has not identified individuals or entities to propose any designations to the UN Security Council Committees pursuant to UNSCR 1267/1989 and 1988, nor has it individually initiated designation pursuant to UNSCR 1373 at the domestic level and at the EU level, which is consistent with Latvia's low

TF risk level. The authorities met onsite were able to explain the process for proposing a terrorism designation and the criteria considered when assessing such proposals from foreign counterparts, demonstrating that the relevant procedures are likely to be implemented in practice when needed.

488. Latvia has demonstrated the capacity to implement UN TFS through its active participation in EU sanctions regimes, including co-sponsorship of TF-related listings. The same institutional framework, designated authorities, and co-ordination mechanisms are used for both EU and UN sanctions regimes, including TFS. This reflects Latvia's operational readiness to take action under UNSCR 1373, should the need arise.

489. Latvia has progressively strengthened its sanctions implementation framework through a structured sequence of reforms. For the majority of reporting period (until early 2024), sanctions were implemented through a decentralized system involving 12 competent authorities, with overall co-ordination by the MFA as the policy maker. This model was supported by key institutional developments such as the creation of the Sanctions Division within the MFA and the establishment of the SCC, which facilitates inter-agency consultation, trend analysis, and policy co-ordination. In response to the increasing complexity and volume of sanctions- particularly following the Russia's invasion of Ukraine in 2022- Latvia introduced significant operational and analytical enhancements across multiple authorities and reinforced co-operation using CCG in TFS matters. The reform process culminated in April 2024, with the designation of FIU Latvia as the national competent authority for the implementation of all international, EU, and national sanctions, supported by dedicated staffing and budgetary resources. These developments reflect Latvia's adaptive and risk-responsive approach to sanctions governance.

490. The FIU Latvia now oversees all aspects of sanctions implementation, including maintaining the online sanctions search engine for designated persons, processing exemptions (derogations), issuing binding decisions to freeze or unfreeze assets, and providing detailed guidance and training to REs. However, this change was only initiated towards the end of the reporting period (April 2024) making a full assessment of its effectiveness over the longer term difficult.

491. Latvia has not received any request from foreign states for designation of persons or entities within the UN TFS framework within the reporting period. It also has not had any case where it was necessary to consider initiating delisting of persons or entities. Had it received a request, there is a clearly established delisting procedures with MFA as designated contact point for forwarding without delay the delisting applications to the relevant UN bodies (1988 Committee or the Ombudsman). The MFA's "Information material (guidelines) for the effective implementation of sanctions in Latvia" offers additional detailed explanation on the applicable delisting procedure.

10.2. Identification and deprivation of terrorist funds or other assets

492. Latvia has demonstrated that overall, the system in place would allow to freeze and deprive of TF assets and instrumentalities when identified within the scope of the UN TFS.

493. Latvia has not identified any designated individual or entity under UNSCR-related TFS for TF, nor have funds been frozen under this framework, which is consistent with the low TF risk profile of the country. However, Latvian authorities and REs have effectively implemented TFS under EU regimes- freezing significant amount of funds and other assets under the Russian Federation linked EU sanctions, by involving the same institutional actors- namely, the FIU, MFA and supervisory authorities and operational processes used for implementing UN TFS, demonstrating Latvia's capability to respond effectively if TF-related designations arise.

494. The majority of frozen funds and assets in Latvia in the reporting period belong to legal persons owned or controlled by designated persons under the Russian Federation and Belarus linked EU sanctions (159 out of 176), evidencing strong identification and screening practices by FIs and other REs, including through complex ownership structures. While engagement with authorities on TF-specific cases was limited, REs showed awareness of their obligations under the TFS regime and used automated screening tools, routinely

identifying and reviewing false positives. These measures reflect a functional framework and operational capacity.

10.3. Targeted application of focused and proportionate mitigation measures to at-risk non-profit organisations

495. Latvia assessed the risks associated with NPOs[114] as part of its NRAs published in 2020 and 2023. These assessments identified certain NPOs as having heightened TF risks. These include NPOs operating in or delivering services to high-risk jurisdictions, those focused on international activities such as promoting cultural diversity, humanitarian aid, or human rights, those with unspecified or vague fields of activity that engage with high-risk jurisdictions, and those whose representative (BO, board members or executives) are residents of high TF risk countries. Nonetheless the overall risk rating for NPOs remains low, since less than 1% of NPO transactions in Latvia involve NPOs with a heightened TF risk, with most transactions occurring domestically and no links identified to individuals from conflict zones.

496. Further to the NRA2, FIU Latvia performed a strategic analysis of 2 084 NPOs that primarily rely on donations or gifts and identified 27 NPOs at heightened TF risk. The assessment incorporated a range of risk indicators, including foreign fundraising sources, links to high-risk jurisdictions, unspecified or vague operational purposes, and absence of Latvian bank account. All identified NPOs at heightened risk of TF hold accounts in Latvian credit institutions, which is treated as risk mitigating measure.

497. However, the scope of the risk assessment focuses predominantly on NPOs that raise funds and does not include organizations that only disburse funds, as required by FATF definition under R.8. While Latvian authorities argue that such entities are likely to be detected through other mechanisms—such as cross-border payment monitoring of all NPOs' transactions—this tool operates reactively and is not integrated into the initial risk classification methodology. This results in a minor limitation as disbursing-only NPOs remain outside the scope of the initial risk classification and may not be subject to the same level of proactive scrutiny or tailored mitigation.

498. To further address identified risks, Latvian authorities have conducted targeted outreach to the identified higher-risk NPOs through the dissemination of an informative leaflet and a dedicated seminar on TF typologies, raising awareness about their potential exposure to TF abuse and encouraging stronger risk mitigation practices. In interviews with a selected cross-section of NPOs it was clear that this outreach has resulted in good understanding of the risks of TF abuse across the NPO community. Moreover, Latvia established the inter-institutional CFT Task Force[115] responsible for analysing cross-border payments to high-risk TF jurisdictions, identifying legal entities with BOs from high-risk TF jurisdictions, and applying risk-based mitigation measures in line with identified TF risks.

499. All Latvian NPOs are required to register with the ER and to adhere to transparency and reporting standards, with Public Benefit Organizations (PBOs) facing even more stringent requirements due to their tax advantages. The SRS acts as the primary authority overseeing NPOs for tax-related matters and conducts targeted audits of associations and foundations, including PBOs. To ensure compliance, PBOs must provide detailed reports covering donors, donation amounts, expenditures, balance sheets, and other pertinent data, as part of their enhanced disclosure obligations under SRS supervision. While these broad governance and transparency measures are not TF-specific, they contribute to the overall mitigation of TF risk by improving sectoral transparency and enabling detection of unusual financial patterns. The authorities maintain a risk-based and proportionate approach, ensuring that these measures do not unduly disrupt legitimate NPO activities. Targeted TF-specific measures are applied only where elevated risk is identified through strategic analysis.

114. As of the end of 2022 a total of 27 004 NPOs were registered in Latvia. The most frequently registered form of NPOs was associations, followed by foundations, religious organisations and other forms of NPOs.
115. See IO.1 describing CFT Task Force.

500. Outreach to NPOs has included published analyses of TF risks (NRA1, NRA2), publicly available guidance, and recognized best practices. NPOs have benefited from seminars, workshops, and interactive sessions organized by umbrella organization, financial industry associations, and regulatory bodies, all aiming to foster transparency, good governance, and ethical funding. These co-ordinated efforts have ensured that NPOs possess both the knowledge and practical tools to identify, understand, and mitigate TF vulnerabilities, which was confirmed by the NPOs met onsite.

501. The NPOs met onsite were aware of the potential TF threats to which they might be exposed. They demonstrated a good understanding of the measures required to protect themselves from TF abuse, with the most prevalent being the screening and verification of partner NPOs. It is common practice among NPOs to rely on publicly available databases, such as the FIU's sanctions search engine, for screening against sanctions.

502. Latvia applies an RBA to monitoring NPOs, co-ordinated by the SRS and FIU Latvia. The SRS maintains a biannual NPO Risk List based on indicators such as foreign donations, cash-intensive transactions, links to foreign officials, unusual loan or real estate activities, and absence of Latvian bank accounts. NPOs exceeding a 30-point risk threshold undergo off-site reviews and possible escalation. Consequently, the SRS conducted 198 assessments in 2021, 42 in 2022, 103 in 2023, and 209 in the first half of 2024, resulting in 13 referrals to FIU Latvia and 14 referrals to the SRS TCPD (2021–2023). In parallel, FIU Latvia identified 27 NPOs at heightened TF risk, based on their cross-border activities and financial flows. Following this, the SRS carried out supervisory inspections of all 27, and the State Security Service prioritized them in its own risk matrix for ongoing monitoring. Although Latvia's overall TF risk for NPOs remains low, these measures effectively prioritise scrutiny of higher-risk entities while proportionately applying broader governance requirements, avoiding unnecessary disruption to legitimate NPO activities.

10.4. FIs, VASPs and DNFBPs understanding of and compliance with obligations

10.4.1. FIs and VASPs

503. REs, including FIs and VASPs, demonstrate a solid understanding of their TFS obligations and the requirement to freeze the assets of designated individuals or entities. Larger FIs and VASPs primarily use automated screening tools, which are kept up to date with the latest UNSCR listings. Smaller FIs commonly rely on the FIU Latvia's online resources, such as the sanctions search engine, and commercial screening tools for compliance. These tools facilitate the identification of sanctioned persons or entities under UNSCRs, EU, and national sanctions regimes. Notably, REs do not differentiate between TFS related to TF and PF, applying screening and compliance measures uniformly across all sanctions' regimes.

504. All credit institutions and other major FIs have dedicated sanctions officers responsible for assessing TF risks and implementing controls to ensure compliance with TFS relating to TF and PF. The entities met onsite had clear procedures and sufficient resources to manage potential matches and discard false positives.

505. The intensity of TFS checks varies based on the size, risk exposure, and operational scope of the entity. Larger FIs and VASPs typically implement advanced, real-time screening systems, ensuring continuous compliance during client onboarding and throughout the customer relationship. Smaller entities, while maintaining compliance, may rely on periodic or manual checks. SCAs provide guidance and oversight to ensure these entities meet their obligations effectively.

506. FIs employ ongoing, risk-based transaction monitoring systems and scenario-based alerts, including measures for high-risk jurisdictions. Internal policies and controls enable the timely identification, assessment, and reporting of suspicious transactions. While instances of TF-related suspicious transactions have been limited in the reporting period, monitoring efforts have also detected potential non-compliance with EU sanctions requirements.

10.4.2. DNFBPs

507. DNFBPs generally demonstrate a good awareness of risks and the importance of TFS compliance, particularly in higher-risk sectors identified in Latvia's NRAs. DNFBPs subject clients to screening during onboarding or before conducting transactions and perform periodic reviews based on identified risks.

508. The following case demonstrates that the systems, processes, and guidance in place for implementing EU TFS measures—such as due diligence by private sector actors and prompt STR reporting—are functioning effectively and would also be well-positioned to identify and address potential breaches of UNSCR sanctions. The detection of a dual-listed individual highlights the interoperability of sanction screening mechanisms across both EU and UNSCR frameworks.

Box 10.1. Qualitative accountant's STR on possible TFS case

Person A, listed on both the EU TFS list and UNSCR 1267 (connected with Al-Qaeda and Islamic Jihad Union), manipulated Person B, a self-employed female entrepreneur in Latvia, into sending him money under the guise of a romantic relationship.

When Person B's accountant conducted a due diligence check, they discovered Person A's designation under EU sanctions and refused the transfer. The accountant then filed an STR with the State Security Service, which interviewed Person B and explained the sanctions implications and potential legal consequences.

509. DNFBPs, depending on factors such as their activity type, size, and client base, implement sanctions screening mechanisms tailored to their specific risk exposure. They may use automated screening tools or perform manual screening for TFS compliance. When conducting manual checks, DNFBPs rely extensively on the FIU Latvia sanctions search engine, along with commercial databases and other publicly available resources, including the UN sanctions search form, the EU Sanctions Map, and other public databases.

510. Entities met onsite lacked sufficient experience with genuine TFS hits related to TF, primarily dealing with false positives flagged by their internal systems. Despite their lower exposure to sanctions risk compared to more material sectors, they were aware of their obligation to immediately freeze accounts in the event of a positive match, with most indicating they would also notify the FIU.

511. During the reporting period, STR reporting from the legal sector was low. Sworn advocates submitted only seven STRs in total, while no STRs were submitted by other legal professionals. These figures include STRs related to TFS and sanctions evasion. Given the sector's potential exposure to higher-risk activities—such as involvement in complex financial or property transactions—this minimal level of reporting raises concerns about the legal profession's understanding of its obligations in relation to TFS. While FIU Latvia notes that the lower volume of STRs from independent legal service providers aligns with their relatively low risk exposure, the near absence of reporting nonetheless suggests a need for strengthened outreach, supervision, and guidance to ensure that TFS-related risks are appropriately identified and addressed across the sector.

10.5. Competent authorities monitoring and ensuring compliance with TF-related targeted financial sanctions

10.5.1. FIs and VASPs

512. SCAs provide guidance and conduct inspections on compliance with TFS as part of their broader AML/CFT/CPF frameworks. Supervisory activities are risk-based, focusing resources on higher-risk FIs and VASPs. Guidance materials and training sessions are regularly delivered to support compliance and address sector-specific vulnerabilities.

513. Latvijas Banka's 2023 thematic review covered sanctions-screening systems at 22 institutions (13 banks, 5 investment firms, 3 payment/e-money firms, 1 pension fund), testing 45 in-house and third-party screening tools against 10 000 control and manipulated entries from UN, EU, OFAC, and other relevant sanctions lists. The assessment tested both customer and transaction screening processes, focusing on technical detection capacity, including the quality and quantity of generated alerts and false positives. While the majority of systems were found to operate effectively, some institutions showed deficiencies, particularly in responding to manipulated entries, documentation of screening outcomes, and timeliness of list integration. Following the review, Latvijas Banka issued updated guidelines in April 2024 and required remediation plans for the institutions concerned.

514. Inspections conducted by SCAs indicate that most FIs and VASPs are generally compliant with TFS obligations. These entities utilize advanced tools, including the FIU Latvia's sanctions search engine, and commercial screening tools, for client screening during onboarding and on an ongoing basis. Between 2019 and 2023, Latvijas Banka imposed 11 financial penalties on credit institutions, totalling EUR 16.3 million, for breaches related to AML and TFS obligations, including a EUR 1.12 million fine for failing to freeze the assets of a sanctioned individual. Enforcement measures also included written warnings, onboarding restrictions, and in one instance, withdrawal of an operating licence. For non-bank FIs, supervisory, supervisory action was taken proportionally, including fines and supervisory follow-ups based on individual risk exposure. Generally, breaches identified are typically minor, such as delays in updating screening systems or incomplete records.

10.5.2. DNFBPs

515. DNFBPs' supervisors integrate sanctions compliance checks into broader AML/CFT supervision. However, to date, no sanctions or remedial measures have been applied to any DNFBP for breaches or failures related to UNSCR TFS obligations.

516. The SRS, as the primary supervisor for DNFBPs, conducts frequent on-site inspections, particularly for higher-risk sectors such as real estate agents, and accountants. These inspections are supplemented by targeted outreach and training programmes, which improve understanding of TFS obligations. The SRS uses a consultative "consult-first" approach for minor compliance issues, fostering engagement with supervised entities while addressing non-compliance effectively. Nevertheless, inspection findings show accountants still account for a large proportion of TFS -related shortcomings compared to other DNFBPs.

517. The LCSA has not adopted a comprehensive risk-based approach to TFS compliance supervision. The LCSA's institutional risk assessment is limited to the type of activity performed by sworn advocates, overlooking other key risk factors such as client profiles and transaction patterns. However, given the low TF risk and limited materiality of this sector for sanctions evasion, this narrow focus has not adversely affected overall TFS implementation.

518. Sanctions screening, as well as other aspects relevant to both TFS compliance and the overall AML/CFT/CPF compliance (such as risk understanding, application of internal control systems, identification of the BO, customer due diligence and (where applicable) transaction monitoring) are equally part of the scope of the SCAs non-thematic supervisory actions (most notably full-scope onsite inspections).

519. Internal inspection procedures at the SRS and other SCAs, with the exception of LCSA, outline risk-based supervision practices. Significant resources are devoted by SCAs as well as the FIU Latvia to regularly increase the awareness and competence of the REs, as well as other involved stakeholders on TF and TFS matters. All SCAs that supervise DNFBPs carry out inspections, targeted training and other supervisory activities in order to ensure that DNFBPs comply with and understand their TFS obligations.

520. However, outreach and training on TFS have largely focused on EU sanctions introduced in response to Russia's war against Ukraine. Although FIU Latvia has assumed responsibility for all sanctions implementation and introduced guidance, UNSCR-specific TFS obligations have not been systematically prioritised in DNFBP-focused outreach.

Chapter 11. Proliferation Financing Financial Sanctions

The relevant Immediate Outcomes considered and assessed in this chapter is IO.11. The Recommendations relevant for the assessment of effectiveness under this chapter are R. 7 and elements of R.1, 2 and 15.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Latvia implements TFS for PF without delay through directly applicable EU regulations, Law on Sanctions, and CoM Reg. No. 184, ensuring immediate compliance with United Nations Security Council Resolutions (UNSCRs). From the moment of adoption, the UN sanctions are directly applicable in Latvia.

b) The MFA co-ordinates the designation and delisting process. It publishes updates on new designations and amendments on its website and communicates them via email to relevant supervisory authorities, which then notify REs respectively.

c) In April 2024, the FIU Latvia assumed the role of the national authority for sanctions implementation, enhancing co-ordination and efficiency in applying TFS for PF. However, the implementation of this additional function remains too recent to allow a comprehensive assessment of its long-term impact.

d) Latvia's flexible application of TFS extends beyond formal ownership to actual control, ensuring sanctions remain effective against attempts to circumvent them through complex ownership arrangements. Although, no individuals or entities have been designated, nor funds frozen under UNSCR TFS for PF, Latvian REs have successfully frozen assets under other sanctions regimes, demonstrating their capability to implement UNSCR TFS requirements if needed.

e) REs including FIs and DNFBPs, are generally well-informed of TFS obligations. FIs, VASPs utilize commercial screening tools for real-time and ongoing screening of clients, while DNFBPs mostly rely on the FIU's online resources. However, while extensive outreach and training activities have been conducted by FIU Latvia and other competent authorities in response to EU sanctions, understanding of UNSCR-specific TFS obligations among some DNFBPs (particularly the legal sector) is developed to a lesser extent.

f) Competent authorities provide guidance and SCAs conduct inspections regarding TFS compliance as part of broader AML/CFT initiatives. The inspections identified only minor breaches, and appropriate corrective measures have been applied.

g) Latvian authorities have assessed PF risks comprehensively, incorporating geographical and sectoral factors, such as goods of strategic significance. They have concluded that the PF risk associated with UNSCR TFS alone is low but acknowledge higher risks from other contexts.

Key Recommended Actions (KRA)

N/A

Other Recommended Actions

a) Latvian supervisory authorities should continue to ensure that inspections of REs, particularly for higher-risk sectors and entities, focus on TFS compliance at sufficient frequency and depth. Supervisory authorities should continue to ensure that breaches, even minor ones, are consistently identified, documented, and addressed with proportionate and dissuasive sanctions to strengthen compliance behaviour.

b) Continue delivering targeted training and outreach programmes for REs, particularly the legal sector. This should include detailed guidance on identifying and managing risks associated with PF and emphasize the distinction between obligations under UNSCR, EU, and national sanctions regimes.

Overall conclusion on IO.11

Latvia has a robust legal framework for implementing PF-related TFS without delay. National PF risk assessments are well-developed and incorporate both geographical and sector-specific considerations, including trade in GSS, such as dual-use and military goods. Co-ordination among competent authorities is effective, particularly through the Committee for Control of GSS, which provides oversight of proliferation-related risks. While there are no detected breaches or designations under UNSCRs 1718/2231, these outcomes are consistent with Latvia's exposure and risk profile. The recent designation of FIU Latvia as the sole competent authority for sanctions implementation is expected to enhance system-wide co-ordination, however, this institutional change was afforded limited weight in the assessment, as the framework in place prior to the reform was already functioning effectively.

PF-related TFS are implemented without delay, and REs—including FIs and VASPs—demonstrate strong understanding and compliance with TFS obligations, supported by advanced screening and monitoring systems to detect and freeze assets of designated persons. Latvian authorities have also demonstrated the ability to identify and freeze assets effectively through the implementation of EU sanctions - particularly those related to the Russian Federation and Belarus - using the same institutional structures and operational processes that would apply to PF-related TFS under UNSCRs. These are reflective of the country's operational readiness, including: (i) timely inter-agency co-ordination; (ii) mechanisms for prompt communication of new or amended designations to REs; and (iii) detection of complex ownership structures by FIs, and their ability to uncover attempts to conceal beneficial ownership or controlling interest in order to evade sanctions.

While the financial sector performs strongly, implementation among DNFBPs remains uneven. Independent legal service providers, in particular, show less-mature TFS processes than those observed in the financial sector, however their materiality in the PF context is low and these shortcomings are weighted as minor. While there are no detected breaches or designations under UNSCRs 1718/2231, these outcomes are consistent with Latvia's exposure and risk profile

Latvia is rated as having a high level of effectiveness for IO.11.

11.1. Competent authorities co-operation and co-ordination to combat PF financing

521. The 2018 MER identified several areas where Latvia needed to strengthen its legal and regulatory framework to ensure effective implementation of TFS, particularly concerning PF. Recommended actions included reviewing and amending the legal framework governing TFS implementation, enhancing the identification and prevention of sanctions evasion by empowering the relevant authority to issue binding

regulations on TFS, and improving supervision of compliance with PF-related TFS. Latvia was also advised to enhance outreach efforts to REs to better detect potential PF activities and improve co-ordination in sanctions enforcement.

522. Since 2018, Latvia has made significant progress in strengthening its sanctions compliance framework, particularly through amendments to the Law on Sanctions. Key measures include the establishment of clear reporting mechanisms, permanent freezing of funds without prior notice, and an enhanced regulatory environment to prevent sanctions evasion. Latvijas Banka (previously FCMC) has been empowered to issue binding regulations, while key agencies, including the FIU, have been incorporated into the SCC to ensure effective enforcement and co-ordination. Latvia's commitment to transparency in legal persons and ongoing training programmes further enhances its capacity to detect and prevent sanctions violations, including PF.

11.1.1. Co-operation and co-ordination to develop and implement policy

523. Latvia has established a comprehensive inter-agency co-operation framework to combat PF, with clearly defined co-ordination mechanisms at both the policy and operational levels. The Committee for the Control of Goods of Strategic Significance (GSS Committee)[116] plays a central role in overseeing export control and dual-use goods regimes that intersect with PF risks. It brings together the MFA, FIU Latvia, SRS, Ministry of Defence, and meets regularly to assess the impact of international sanctions and update national control lists. The FSDB[117] provides high-level strategic oversight, ensuring that Latvia's PF policy objectives remain aligned with national priorities and its international obligations. Both bodies were instrumental in drafting and guiding the recent amendments to the Law on Sanctions, and in shaping Latvia's implementation of TFS to mitigate PF risks.

524. Latvia's policy-level co-ordination has been key to mapping PF risks, notably during development of the NRA2 PF chapter. Led by FIU Latvia with input from SRS, the GSS Committee and Latvijas Banka, this effort analysed cross-border transaction flows, dual-use goods classification trends and identified priority threat actors. The SCC—chaired by the MFA—aligned policy priorities across agencies and integrated EU Dual-Use Regulation requirements and FATF guidance. These co-ordination structures are reinforced by standing WGs and operational platforms that facilitate rapid information-sharing and joint implementation. Importantly, authorities incorporate private-sector insights—engaging banks, logistics firms and others through structured SCC consultations—so that operational feedback continuously informs policy. Together, these mechanisms keep Latvia's PF policy and practice tightly synchronized.

11.1.2. Co-operation and, where appropriate, co-ordination for operational purposes

525. Operational co-operation between the FIU Latvia, the SRS, LEAs and the SRS Customs Board, and other relevant authorities is well-established through Co-operation and Coordination Group (CCG) format. CCG is a flexible and multi-purpose co-operation mechanism which supports operational and strategic exchange between state authorities, including LEAs and SCAs. It enables information-sharing on suspicious transactions and goods related to proliferation. Joint operational task forces, including SRS Customs Department, State Security Service, SRS TCPD and the State Police, effectively target PF-related risks, particularly in high-risk sectors such as transportation and logistics. Authorities also engage with private sector stakeholders to enhance awareness and compliance. Although the CCG has not yet encountered PF-related TFS cases (reflecting Latvia's medium low PF risk profile, with the prevalent threats arising from trade related sanctions rather than TFS), it has encountered trade related sanctions cases, and it is recognized as the appropriate mechanism should PF-related operational co-operation be required.

116. The Committee for Control of GSS provides a forum for an interagency co-operation and co-ordination bringing together expertise from number of Latvian authorities: MFA, Ministry of Economy, MoF, Ministry of Health, Ministry of Defence, State Environmental Service, State Police, State Security Service, Constitution Protection Bureau, SRS, FIU Latvia, Latvijas Banka. The Committee is chaired by the State Secretary of the MFA.

117. See IO.1.

526. In July 2024, FIU Latvia, in co-operation with the State Security Service, issued updated guidelines on "Prevention of TF and PF." These guidelines—distinct from existing indicators on sanctions circumvention—specifically address PF risks and controls and are tailored to the Latvian context. They incorporate international typologies, domestic and cross-border risk indicators, and anonymised case examples to help REs and supervisory authorities better understand PF threats and apply proportionate mitigating measures. The issuance of these guidelines is expected to enhance the practical implementation of PF-related obligations across both FIs and DNFBPs, by improving their ability to identify red flags, apply screening controls, and escalate suspicious activity.

11.2. Understanding and mitigating the risk of breach, non-implementation or evasion of PF-related targeted financial sanctions

527. Latvian authorities have conducted comprehensive assessments of PF risks, incorporating geographical and sectorial vulnerabilities. These assessments focus particularly on the movement and control of GSS, including dual-use and military goods, and reflect Latvia's recognition that its role as a regional logistics and transit hub increases exposure to PF-related activity. However, authorities stated during the onsite that, if the assessment were limited strictly to the scope of UNSCR-related TFS the assessed PF risk would be low. This view is based on several factors, including the absence of any designated persons or entities under UNSCR PF-related sanctions holding assets or operating in Latvia, and the absence of related STRs or international information requests. Authorities also highlighted the extensive use of automated screening systems in the financial sector, the functionality of the FIU Latvia's centralised sanctions search engine, and the lack of practical exposure to jurisdictions like DPRK.

528. The AT considers this assessment to be reasonable and supported by current exposure levels, particularly in the financial sector. However, continued attention to system testing, DNFBP supervision, and cross-sector outreach is warranted to ensure that the framework remains responsive should UNSCR-related exposure increase.

529. To address sector-specific risks, Latvia has implemented strict licensing and oversight mechanisms for GSS, including dual-use items and military-related materials that could contribute to weapons of mass destruction (WMD) programmes. The Committee for the Control of GSS evaluates all applications for export, import, and transit of such goods. Applications are assessed against domestic controls, EU dual-use regulations, and relevant UNSCRs related to PF. In 2022, 183 licences were denied, demonstrating a proactive and risk-sensitive approach to mitigating PF risks by preventing the movement of goods with potential proliferation applications. These controls represent a key element in Latvia's strategy to combat PF by addressing the material dimension of proliferation pathways.

530. In the NRA2 Latvian authorities assessed the risks of violation and circumvention of TFS (under all applicable sanctions regimes) as medium, with trade-based sanctions breaches rated as medium high/high. The increase in risk level is attributed to the broad scope of EU sanctions imposed on the Russian Federation in 2022, Latvia' geographical location bordering the Russian Federation and Belarus, and its historical economic relations with the Russian Federation. To address these risks, Latvia has prioritized sanctions implementation, enforcement, and supervision, established new co-operation mechanisms, centralized sanctions implementation under FIU Latvia, and allocated significant additional resources, demonstrating its capacity to adopt an RBA and respond swiftly to evolving risks.

11.3. Implementation of PF-related targeted financial sanctions without delay

531. Latvia implements PF-related TFS without delay. Latvia relies on both, domestic (Law on Sanctions and CoM Reg. No. 184) and EU legislative frameworks. The framework ensures that UNSCRs on PF are implemented directly and immediately upon adoption by the UN, making the measures binding on all natural and legal persons.

532. Considering that the Law on Sanctions applies equally to TF and PF related UN TFS, the institutional framework and the powers are identical to what is described under IO.10. The MFA is a co-ordinating body for implementation of sanction regimes and the FIU Latvia is national competent authority for implementation of financial sanctions, and as such has the power to freeze the funds and economic resources of sanctioned persons autonomously.

533. Like for TF-related sanctions, designations and amendments to the UN TFS on PF are communicated to REs without delay via multiple channels—the MFA website, the FIU Latvia sanctions search engine, and the Official Gazette—and are automatically pushed through supervisory authorities' onward-communication systems. Latvia also maintains a subscription-based email alert to ensure that all REs receive updates in real time. Further details regarding communication of designations are described under IO.10.

11.4. Identification of assets and funds held by designated persons/entities/those acting on their behalf and prohibitions

11.4.1. Identifying funds or assets held by designated persons/entities/persons acting on their behalf or at their direction

534. During the reporting period, there were no funds or assets frozen in Latvia pursuant to UN designations related to PF, which is consistent with Latvia's PF risk profile. The FIU Latvia has not received any requests or spontaneous reports from foreign FIUs related to PF, and only one STR where credit institution suspected PF has been reported.

535. While no assets have been frozen under PF-related UNSCRs, Latvia's system demonstrates that immediate identification and freezing of funds is ensured through implementation of TFS under the EU sanctions, mainly on the Russian Federation and Belarus-related sanctions. Latvia has successfully frozen significant amounts of funds and assets linked to EU sanctions. As of June 11, 2024, Latvia has frozen funds and assets linked to 176 sanctioned persons (17 directly designated and 159 owned or controlled by designated persons), totalling about EUR 109 million.[118]

536. Throughout the assessment period, Latvia's licensing system for sanctions derogations- including those potentially related to UNSCR PF-related financial sanctions, transitioned from a multi-authority model into a centralised framework under the FIU Latvia. Effective April 2024, FIU Latvia became the sole competent authority for evaluating and issuing licences to use frozen assets under international and national sanctions regimes. While over 130 licenses were issued by various authorities prior to the reform, the FIU's effectiveness under its new mandate remains to be fully assessed. The reform is directly relevant to PF, as derogation mechanisms—such as humanitarian exemptions—must ensure that frozen funds are not misused to support entities engaged in proliferation activity. FIU Latvia now assesses all licence applications against UNSCR obligations, EU and national sanctions criteria, and monitors compliance with any usage conditions. Further data on licence turnaround times, approval rates, and post-licence monitoring—and targeted testing of these procedures—will be necessary to determine whether centralization strengthens Latvia's ability to detect and prevent the misuse of sanctioned assets for proliferation purposes.

537. Latvia has developed a multi-pronged system to ensure that accurate, up-to-date basic and BO information on legal persons is readily accessible. This framework starts with mandatory BO disclosure at the moment of registration with the ER and continues through ongoing verification mechanisms. Public and online access to the ER database, combined with free-of-charge availability, ensures that both the public and relevant authorities—such as the FIU Latvia, LEAs and SCAs—can quickly retrieve comprehensive data. In practice, authorities supplement this official information with multiple external private databases, enabling

118. Given that the value of frozen assets (e.g. bonds, securities) is variable and the funds are frozen in different currencies, the value of assets frozen in Latvia is approximate. By June 2024, the total value of other types of assets frozen in Latvia was approximately EUR 310 million. These other assets frozen included a range of economic resources, including both tangible assets (such as vehicles, real estate), as well as intangible assets (such as voting rights arising from frozen capital shares, and trademarks).

cross-checking and deeper analysis of potentially complex or opaque ownership structures, including those involving foreign elements. These measures significantly enhance the capacity of authorities to detect and investigate potential front companies and prevent misuse of Latvian legal entities for PF, and respond effectively to offences or breaches related to UNSCRs on PF.

11.4.2. Prohibiting financial transactions related to proliferation

538. FIs, VASPs, and DNFBPs are required to freeze assets and prohibit transactions related to designated persons or entities. Supervisory authorities actively monitor compliance, ensuring that FIs apply robust measures to prevent PF-related financial transactions.

539. Latvia applies TFS flexibly and thoroughly, looking beyond formal ownership to actual control. If a designated person appears to have merely shifted shares to close partners while still exerting influence, Latvian authorities and FIs continue freezing assets linked to those subsidiaries. This approach ensures that sanctions remain effective against attempts to circumvent them through complex ownership arrangements. This practice has been grounded in numerous case examples presented to the AT, including the case detailed below, which - although based on EU sanctions – illustrates the same practical mechanisms and operational readiness that would be needed in a PF context: collaboration between FIs, public-register authorities, and FIU Latvia, and the ability to determine who has direct control of a customer (including through complex structures such as foreign-registered trusts) and freeze assets without delay. The same legal basis, institutional co-ordination, and procedural mechanisms would apply to PF-related TFS under UNSCRs.

Box 11.1. Example of effective identification of legal person controlled by designated person, ensuring freezing of funds and other assets without delay

FIs and public-register authorities reported to FIU Latvia that LLC ABC's assets—bank balances, insurance premiums, capital shares, two Riga properties, and ten vehicles—had been frozen once its indirect owner, D.A., was EU-designated.

The day after D.A.'s designation, it emerged that 52% of D.A.'s shares in the non-EU parent company OOO LMN had been sold to A.B. and A.C., long-time senior employees of D.A.'s firms, with no evidence they could legitimately afford the purchase. FIU Latvia determined these transfers were a façade to reduce D.A.'s reported stake below 50% and evade TFS measures. Consequently, FIU Latvia concluded that D.A. still controlled LLC ABC and properly froze all its assets under the sanctions regulations.

540. Latvia's enforcement framework builds on a system of proactive reporting, analytical follow-up, and robust inter-agency co-operation. One of the cases presented- effective action against a sanctions breach involving the export of luxury goods- demonstrated the system's capacity to detect and disrupt illicit trade involving restricted items. While the case concerned sectoral EU sanctions and did not involve a designated individual or entity under UNSCR PF-related sanctions, it nonetheless illustrated how Latvia's enforcement mechanisms- particularly customs controls and law enforcement co-ordination- can address scenarios that are analogous to proliferation threats, such as the transit of GSS through Latvian territory. This type of enforcement infrastructure is relevant to R.7, as it could be applied in cases where designated persons or entities attempt to move funds or other assets through trade or financial channels, particularly in evasion contexts. Since 2022, LEAs have initiated a growing number of criminal proceedings for sanctions violations, indicating heightened enforcement capability and responsiveness to PF-related vulnerabilities, even where direct links to designated parties have not yet been identified.

11.5. FIs, VASPs and DNFBPs understanding of and compliance with obligations

11.5.1. FIs and VASPs

541. Overall, the framework as already analysed in detail under IO.10 applies also here. Hence the strengths and weaknesses of the system identified are the same.

542. FIs and VASPs demonstrate a good level of understanding of PF-related TFS obligations. FIs conduct real-time and ongoing screening of clients and transactions using advanced systems that allow to detect PF-related evasion by integrating customer profiling, locational information, and sectoral characteristics into transactional screening criteria. However, smaller entities may require additional support and guidance to ensure consistent compliance across the sector. VASPs have evolved from using basic, free transaction monitoring tools to more sophisticated commercial providers, improving their ability to detect suspicious transactions patterns (e.g., use of mixers, darknet sources).

543. Most FIs and VASPs rely on commercial automated software to screen against TFS lists. Customer information is reviewed against these TFS-related lists during the onboarding process and periodically, based on a pre-defined frequency that aligns with the client's risk profile or updates to their CDD data. Additionally, checks are conducted during occasional transactions or ad-hoc when changes to sanctions lists are announced. The level of scrutiny of checks is correlated with the size and scope of activities of the given entity.

544. Entities met onsite were aware of the obligation to file sanctions compliance reports to the FIU in case of the need to report asset-freezing under the UN sanctions regimes. Although no funds have been frozen based un UNSCRs, which is consistent with the national low risk for violation of TFS on PF, FIs and other REs regularly report to FIU Latvia freezing of funds under EU sanctions, in particular the Russian Federation-related EU sanctions. As part of the NRA2, an analysis of the STRs received from 2020 to 2022 found that the low number of PF-related STRs aligns with Latvia's assessed PF risk and threat.

545. SCAs, in carrying out their supervisory functions, have not identified any examples of un-reported PF-related activities or transactions, nor any instances of non-compliance with EU sanctions measures relevant to PF. Furthermore, an analysis of STRs received by FIU Latvia has not identified any STRs containing PF-related suspicions, but which have not been properly reported as PF-related STRs.

546. During the assessment period, cross-border financial flows with jurisdictions previously identified as posing heightened financial crime or sanctions evasion risks—such as certain CIS countries and offshore financial centres—decreased significantly, by 89% and 93% year-on-year, respectively. This trend reflects ongoing de-risking measures by Latvian FIs and supervisory action to reduce exposure to high-risk or non-transparent jurisdictions, as outlined in Latvia's NRA2. While the CIS region as a whole is not assessed to pose a specific PF threat, the NRA notes that financial flows to certain CIS countries increased during 2022 and may indicate attempted circumvention of sanctions.[119] The significant reduction in such flows since then has lowered the likelihood that Latvian financial channels are being used to facilitate complex PF-related transaction chains. Notably, no cross-border financial flows involving the DPRK[120] were recorded during the reporting period.

11.5.2. DNFBPs

547. DNFBPs have strengthened their TFS compliance- particularly in screening clients and transactions against sanctions lists- but their overall understanding remains less mature than that of financial sector. While

119. NRA Paragraph 1.5.13 – noting increased payment flows to certain CIS jurisdictions in Q2 2022 potentially related to sanctions circumvention activity.

120. As of 18 October 2023, TFS set out in UNSCR 2231 related to Iran ceased to apply. However, as they were in force for the majority of assessment period it should be indicated that there were no cross-border flows to or from Iran recorded for that period.

these entities meet the general requirement to conduct screening against sanctions list, there is room for further enhancement in structuring their processes regarding scope and frequency of screenings.

548. DNFBPs rely on various official resources for sanctions screening, including FIU's website, EU/UN Sanctions Map and other available databases. They verify that neither their client, nor the BOs are on UN or EU sanctions lists. Entities met onsite were aware of their obligation to report to FIU Latvia and to terminate the relationship once they identify that client is a sanctioned person, or it is providing services or goods to a sanctioned person.

549. DNFBPs, particularly in higher-risk sectors such as real estate and legal services, have benefited from targeted training and outreach delivered by SCAs and FIU Latvia to enhance understanding of their obligations related to PF and TFS. These efforts have contributed to increased general awareness across the DNFBP sector. However, while some DNFBPs have submitted STRs concerning suspected sanctions circumvention, overall reporting volumes remain low, particularly from the legal sector. This limits the ability to fully assess the extent to which awareness is being translated into operational practice. Nevertheless, substantial asset freezes under TFS and only minor internal control issues identified during SCA inspections indicate some effective implementation within the sector.

550. While a small number of DNFBPs submitted STRs and reports related to EU TFS obligations, no DNFBPs submitted STRs or freezing reports relating to UNSCR TFS obligations concerning PF during the reporting period. This is broadly in line with Latvia's assessed low exposure to such risks, although the limited level of reporting from sectors with potential exposure, such as legal professionals, suggests a need for continued outreach and supervisory attention to ensure risks are adequately understood and addressed.

11.6. Competent authorities monitoring and ensuring compliance with PF-related targeted financial sanctions

11.6.1. FIs and VASPs

551. Latvia's supervisory framework integrates PF risk considerations into a broader AML/CFT/CPF compliance regime. SCAs do not distinguish between PF and TF related TFS for the purpose of their supervisory activities thus analysis and conclusions presented under IO.10 equally apply to PF-related TFS. No breaches of UNSCR-related PF TFS obligations were identified during the reporting period, including any cases of non-implementation or evasion.[121]

552. Supervisory authorities, including Latvijas Banka (previously FCMC) and SRS, conduct regular inspections of FIs and VASPs to ensure compliance with PF-related TFS obligations. SCAs use a risk-based approach, conducting both on-site and off-site inspections that reflect entities' risk profiles. While not tailored exclusively to PF, these inspections include assessments of internal controls, sanctions screening practices, and the entities' ability to detect and respond to potential sanctions violations, including in relation to TFS for PF.

553. Breaches identified are typically minor and are addressed through corrective measures. However, authorities aim to increase the use of dissuasive sanctions for more significant violations.

554. SCAs undertake extensive outreach, guidance, and training efforts. These initiatives, including specialized seminars, training sessions, and the publication of risk assessments, foster greater sector-wide awareness of PF-related TFS obligations.

121. In line with R.1, this refers specifically to the assessed risk of non-implementation or evasion of UNSCR-mandated TFS related to proliferation financing, such as attempts by designated persons or entities to circumvent freezing obligations.

11.6.2. DNFBPs

555. The SRS, as the primary DNFBP supervisor, focuses on high-risk sectors through frequent inspections and targeted guidance. For example, the SRS has developed the "Guidelines for the subjects of the AML/CFT/CPF Law to be supervised by the SRS".

556. Despite conducting a large number of full-scope inspections annually, SRS has not identified specific PF breaches. Instead, it focuses on general AML/CFT/CPF compliance, offering guidance, consultation, and when necessary, sanctions—though none specifically for PF TFS violations to date. In addition, agencies (including the FIU Latvia) deliver training events designed to educate REs (and other key stakeholders) of the AML/CFT/CPF Law and the risks of ML/TF/PF. These events have included those specifically dedicated to PF risks.

557. The SRS engages in ongoing outreach and guidance through multiple channels: video seminars, e-learning platforms, and the Electronic Declaration System (EDS). Annual training materials are prepared and published, ensuring that entities have up-to-date instructions and best practices.

558. Outreach and training on TFS have primarily focused on EU sanctions introduced in response to Russia's war against Ukraine. While this focus reflects Latvia's risk context and the practical relevance of EU sanctions- which also encompass proliferation-related elements- UNSCR-specific obligations have not been systematically prioritised in outreach to DNFBPs. However, this is considered proportionate to the country's assessed PF risk and the comparatively lower exposure of DNFBPs to PF TFS.

Annex A. Technical compliance

This section provides detailed analysis of the level of compliance with the FATF 40 Recommendations in their numerical order. It does not include descriptive text on the country situation or risks and is limited to the analysis of technical criteria for each Recommendation. It should be read in conjunction with the Mutual Evaluation Report.

This analysis of technical compliance covers: (i) Recommendations where the country has made legal, regulatory or operational framework changes since its last mutual evaluation (dated July 2018, MER 2018) or FUR with technical compliance re-ratings (dated December 2019, FUR 2019) - R.3, R.5, R.29-R.33 and R.38; and (ii) Recommendations where there has been a change in the FATF Standards for which the country has not previously been assessed - R.1, R.2, R.8, R.15, R.24, and R.25. The latter Recommendations are identified with the Recommendation heading in green text.

For Recommendations not under review, where legal, regulatory or operational framework changes introduced by the Latvian authorities were not material, no additional analysis has been conducted and pre-existing information from the country's most recent assessments with technical compliance re-ratings has been compiled for inclusion in this annex. Recommendations that draw solely on MER 2018 are: R.4, R.9, R.11-14, R.16, R.17, R.19, R.20, R.23, R.27, and R.34-37. Recommendations which additionally refer to FUR 2019 are: R.6, R.7, R.10, R.18, R.21, R.22, R.26, R.28, R.39 and R.40.

To ensure a consistent and coherent approach to EU Supranational Measures, the common text adopted by the February 2025 FATF Plenary has been incorporated into this annex for: R.6, R.7, R.31, R.32, R.38 and R.40.

Recommendation 1 – Assessing risks and applying a risk-based approach

Note: The country's submission was made before the July 2024 update to the Methodology was published, therefore the analysis does not follow the order and numbering of the July 2024 version on R.1 criteria.

Latvia was rated compliant in the 2018 MER, as no deficiencies were identified.

Recommendation 1 has undergone specific changes, also in terms of requirements by the revised Methodology. In view of that, three new criteria were added to address PF risk assessment and these risks' mitigation requirements (1.4a; 1.9a and 1.13). Latvian AML/CFT/CPF legislation has also undergone changes and now addresses the need to have the PF risk assessment alongside these for ML and TF. The first PF risk assessment (carried out together with the TF risks assessments) was finalised and published in 2019. Latvia has also developed a Guidance for PF risk assessment, to facilitate the process.

Since the 2018 MER, Latvia carried out a number of risk assessments – those at the national level and for specific sectors. The most recent NRA, which covers the period 2020 – 2022, was published in November 2023.

Criterion 1.1 – Section 51(1).14 of the AML/CFT/CPF Law requires the FIU to organise and carry out ML/TF/PF risk assessment(s) and the development of NRA. Latvia has completed a wide range of assessments to identify, assess and understand ML/TF risks. This includes NRA1 and NRA2 as well as sectoral risks assessments for all sectors (most recent versions 2023) and annual assessments in areas such as emerging technologies. The FIU also issued (in 2019) the Guidelines for Assessment of Risks of ML, TF, and PF which detail various procedural aspects on how risk assessments are to be carried out, as well as a clear communication strategy for risk assessments covering AML/CFT/CPF areas.

Being a part of the EU, Latvia also benefits from supranational ML/TF risk assessment carried out at the EU level, which mostly concerns the risks arising from EU's internal market and to cross-border activities in Member States.

Overall, the risks assessment processes in Latvia cover a broad range of areas targeting country's key ML/TF/PF threats and vulnerabilities. The analysis presented in the NRAs are comprehensive and detailed

enough, with reasonable and well-grounded conclusions. The authorities used the World Bank methodology for assessing the risks and have adapted it to their assessments' specific needs.

Criterion 1.2 – FIU Latvia is the responsible body for the co-ordination of actions to assess risks (Section 51 (14) of the AML/CFT/CPF Law). As noted above, the "Guidelines for Assessment of ML/TF/PF Risks" detail the process and obligations of all institutions relevant to the assessment process. The FSDB,[122] which is chaired by the Prime Minister, is the co-ordinating authority responsible for improving co-operation between the competent authorities and the private sector in the prevention of ML/TF/PF (Section 61 of the AML/CFT/CPF Law).

Criterion 1.3 – Latvia keeps risks assessments up to date through conducting an NRA every three years (as noted above the most recent one was published in 2023), periodical sectoral risks assessments, annual assessments of higher risk or emerging threat areas such as new technologies. The AML/CFT/CPF Action Plan (published 2018 adopted by the Government Order No 512), mandates that the next NRA will be published in 2026. Implementation of two consecutive rounds of NRA in the reporting period indicates Latvia's commitment to keep these assessments up-to-date.

Criterion 1.4 – Latvia has a mechanism in place to ensure that the NRA findings are channelled to the competent authorities, SRBs and REs. Latvia publishes its NRA online, making them freely available. According to AML/CFT/CPF Action Plan for 2023-2025 which was adopted by the Government on 13 December 2022 the FIU Latvia is responsible for providing awareness raising, information and training to the competent authorities, REs and SRBs.

Criterion 1.4a –

a) Latvia began formally assessing the PF risks in 2020 with the first National Terrorism Financing and Proliferation Financing Risk Assessment Report, which covered the period from 2017 to 2018. In the NRA1 and in the latest NRA2 PF risks have been identified and assessed as part of the NRA. Latvia's assessment of PF risks goes beyond those relating to Recommendation 7.

b), c) and d) the same requirements here apply as for criteria 1.2 and 1.3 – the mechanisms and requirements are equal for ML/TF and PF risk assessments.

Criterion 1.5 – Latvian authorities apply a risk-based approach to allocating resources, based on their understanding of the risk as articulated in their NRAs. AML/CFT/CPF Action Plan articulates the actions to be taken as a result of the findings of the NRAs. As already noted, the AML/CFT/CPF Action Plan is approved by the Government and, as such, implicitly addresses the issues on resources needs and other measures to prevent ML/TF/PF. In other words, the AML/CFT/CPF Action Plan, being a Government document/decision informs budgets allocations, with individual institutions responsible for delivery. Reporting on progress made semi-annually is mandatory by these institutions to the MoI. Report on results of the implementation of the AML/CFT/CPF Action Plan are also submitted to the FSDB for their review.

Criterion 1.6 – Latvian does not exempt any sectors from AML/CFT obligations.

Criterion 1.7 – FIs and DNFBPs are required to apply EDD when establishing and maintaining a business relationship or executing an occasional transaction with the customer, if an increased ML/TF/PF risk exists (Sec.22(2)(5) AML/CFT/CPF Law). FIs and DNFBPs are required to conduct and document the assessment of the ML/TF/PF risks in order to identify, assess, understand, and manage the ML/TF/PF risks. They are required to include information from NRAs, SNRA and sectors risk assessment in their risk assessments (Sec.6 of the AML/CFT/CPF Law).

Further to these, Paragraph 6 of the FCMC Regulation No 5 defines that, while performing assessment of the risks inherent for their customers, developing a framework for quantifying the client's risk and determining the appropriate due diligence measures, findings of both the NRA and risk assessment performed by the EC must be considered by the covered FIs.

122. The FSBD is composed of the following authorities: Prime Minister and ministers of the Government, heads of SCAs and associations related to the financial sector, the Head of FIU, General Prosecutor, and other authorities as may be relevant (upon invitation officials and employees of other State authorities, and representatives of the interested parties may participate). Central to the responsibilities of the FSDB is the formulation and enforcement of policies and strategies aimed at bolstering the financial sector's growth and stability.

Criterion 1.8 – Section 26 of the AML/CFT/CPF Law identifies cases when simplified CDD can be performed – if there is a low risk of ML/TF/PF which is not in contradiction with a risk assessment, including the NRA, and if measures have been taken to determine, assess and understand the ML/TF/PF risks inherent to own activities and the customer, than simplified measures could be applied. The AML/CFT/CPF Law also specifies certain exceptions, when simplified CDD is not applicable. These concern the cases where, on the basis of the risk assessment, the RE detects, or there is information at its disposal regarding ML/TF/PF, or an attempt to carry out such actions, or an increased risk of such actions, including if the risk increasing factors, as referred in the AML/CFT/CPF Law, are present. Simplified CDD shall also not be applied with respect to a customer who performs economic activity in high-risk third countries.

When applying simplified CDD, REs shall obtain and document information attesting to the conformity of the customer with the exemptions as referred in the AML/CFT/CPF Law, and after establishment of a business relationship shall supervise them.

Criterion 1.9 – Supervisors and SRBs are required to ensure that FIs and DNFBPs are implementing their obligations under the AML/CFT/CPF Law (Section 45 of the AML/CFT/CPF Law), including the requirements of Rec 1. *Reference is made to the analysis of relevant criteria 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.*

Criterion 1.9a – Latvia's understanding of risk, mitigation of risk and allocation of resources for PF is part of its overall AML/CFT/CPF risk assessment and action plan processes (see criterion 1.5).

(a) Latvia does not have in place any exemptions.

(b) FIs and DNFBPs are required to apply EDD when establishing and maintaining a business relationship or executing an occasional transaction with the customer, if an increased PF risk exists (s.22(2)(5) AML/CFT/CPF Law). FIs and DNFBPs are required to conduct and document the assessment of the PF risks in order to identify, assess, understand, and manage the PF risks. They are required to include information from NRAs, SNRA and sectors risk assessment in their risks assessment (Sec.6 AML/CFT/CPF Law).

(c) Section 26 of the AML/CFT/CPF Law identifies cases when simplified CDD can be performed, for example where steps have been taken to determine, assess and understand the PF risks inherent to own activities and the customer which have identified a low risk of PF which is not in contradiction with a risk assessment such as the NRA (see also criterion 1.8). Reference is made to R.7 for further details regarding implementation of PF TFS to all natural and legal persons in Latvia.

(d) Supervisors and SRBs are required to ensure that FIs and DNFBPs are implementing their obligations under the AML/CFT/CPF Law (Section 45 of the AML/CFT/CPF Law), including the requirements of R.1.

Criterion 1.10 – FIs and DNFBPs are required to identify, assess and understand the ML/TF risks associated with their own activities and customers (Sec.6(1)(2) AML/CFT/CPF Law). This includes being required to:

(a) document their risk assessments (Sec. 6(1) AML/CFT/CPF Law)

(b) consider relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied. Sec.6(1^2) of AML/CFT/CPF 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/CPF internal control system.

(c) Regularly review and update their assessments (Sec.8 (1) of the AML/CFT/CPF Law).

(d) Submit their risk assessments to supervisors upon request (Sec.47 (1) (2) of the AML/CFT/CPF Law).

Criterion 1.11 – (a) FIs and DNFBPs are required to have policies, controls and procedures, which are approved by senior management, to enable them to manage and mitigate the risks that have been identified (Sec. 6(1) AML/CFT/CPF Law).

(b) FIs and DNFBPs are required to assess the efficiency of the operation of the internal controls, including by reviewing and updating the ML/TF/PF risk assessment at least every 18 months and, if

necessary, to implement measures for improving the efficiency of the controls (Sec.8(2) and 8(3) of the AML/CFT/CPF Law).

(c) FIs and DNFBPs are required to apply EDD to manage and mitigate higher risks (Sec.22 (2)5 of the AML/CFT/CPF Law).

Criterion 1.12 – Latvia allows simplified due diligence (SDD) measures if lower risks are identified (Sec.26 of the AML/CFT/CPF Law). SDD is not permitted where a ML/TF risk has been identified (see criterion 1.9).

Criterion 1.13 – Please see criterions 1.9, 1.9a, 1.10 and 1.11 – the same measures cover ML/TF and PF as per the AML/CFT/CPF Law.

Weighting and Conclusion

Recommendation 1 is rated compliant.

Recommendation 2 - National Co-operation and Co-ordination

In the 2018 MER, Latvia was rated largely compliant with Recommendation 2 The assessment found that co-operation and, where applicable, co-ordination mechanisms to combat the financing of proliferation of WMD are not clearly defined in the Latvian institutional system. Other than that, no deficiencies were identified.

Recommendation 2 was revised to address the CPF related issues with regard to co-operation and co-ordination – i.e., to put them fully in line with the requirements covering AML and CFT.

Since Latvia's 2019 FUR there have been amendments to the AML/CFT/CPF Law to specify the co-operation of the FIU Latvia and MoF with the SCAs and to institutionalise the Co-operation Platform for SCAs (Section 55.12).

Criterion 2.1 – Latvia develops and implements national AML/CFT/CPF policies which are based on the risks identified. The National Strategy for the Prevention and Combating of Financial Crimes has been approved in 2023 by the FSDB, based on the risks identified in NRA2. In April 2024 Latvia adopted the National Strategy the AML/CFT/CPF Action Plan for 2024 – 2026. The AML/CFT/CPF action plans are regularly reviewed and updated based on the risks identified in NRAs by the FSDB, both at a policy and operational level.

Criterion 2.2 – The FSDB is a co-ordinating body that aims to co-ordinate and improve co-operation between the public agencies (as well as the private sectors) for AML/CFT/CPF (Government Regulation No 233 "By-laws of the FSDB"77). As already noted under R.1, the main tasks of the FSDB in the area of prevention and combating of ML/TF/PF are to co-ordinate co-operation between public institutions and the private sector in AML/CFT/CPF, including the achievement of the objectives set out in the national AML/CFT/CPF policy and strategy, and to facilitate co-operation with relevant foreign public and private institutions responsible for financial sector development in the area of AML/CFT/CPF.

Additionally, Latvia also has in place an Advisory Board which is underpinned by statutory authority (Section 59 of the AML/CFT/CPF Law) which is responsible for exchanging information on ML/TF/PF risks, trends, and cases. The Advisory Board is led by the Head of the FIU and the membership includes representatives of the MoI; Ministry for Justice; Latvijas Banka; the Finance Latvia Association, the Latvian Insurers Association; the Latvian Association of Sworn Auditors; the Council of Sworn Notaries of Latvia; the LCSA; the Supreme Court; and the Prosecutor General.

Specifically for the TF, the Counterterrorism Centre Expert Advisory Council was established in 2019 to: (1) improve co-operation and co-ordination between authorities to prevent TF cases; (2) analyse identified TF cases and identify new indications of TF; (3) provide recommendations to the supervisory and control institutions and the REs under the AML/CFT/CPF Law to prevent TF more effectively.

Criterion 2.3 – FIU Latvia is the authority designated by the AML/CFT/CPF Law (Sections 51(17) and 55) with responsibility for co-ordinating efforts to address ML/TF/PF risks at the operational and policy level. Nationally the FSDB, chaired by the Prime Minister, is legally designated as the co-ordinating

authority with the objective to improve the co-operation between state authorities and the private sector in the prevention of ML/TF/PF (Section 61 of the AML/CFT/CPF Law).

Criterion 2.4 – Latvia has in place a range of mechanisms to facilitate operational co-operation, and co-ordination, as well as sharing of information between competent authorities for operational purposes related to AML, CFT and CPF.

Latvia's FIU co-ordinates the co-operation between the bodies performing operational activities, investigating institutions, as well as the REs by convening a CCG (Section 55(2) AML/CFT/CPF Law). Additionally, the FIU has introduced the OpCEN initiative, which allows the LEAs, as well as the PO to co-operate within criminal investigations to strengthen the effectiveness of co-operation, information analysis and exchange between the FIU and LEAs. As mentioned in Criterion 2.2, the Counterterrorism Centre Expert Advisory Council has responsibility for co-operation and co-ordination between authorities in relation to TF investigations.

Criterion 2.5 – The rules governing data protection do not inhibit any of the AML/CFT requirements (Section 5^2 of the AML/CFT/CPF Law).

AML/CFT/CPF Law provides for general conditions for the processing of personal data, for purpose of the AML/CFT/CPF measures being applied (Section 5^2 of the AML/CFT/CPF Law) noting their use to be 'in the interests of the society.' Specific restrictions on use of such data are also provided by the AML/CFT/CPF Law – Section 41.

Section 27 (1) of the Personal Data Processing Law provides that a data subject does not have the right to receive the information specified in Section 15 of the Data Regulation if it is prohibited to disclose such information in accordance with the laws and regulations regarding national security, national protection, public safety and CL, as well as for the purpose of ensuring public financial interests in the areas of tax protection, prevention of ML/TF or of ensuring of supervision of financial market participants and functioning of guarantee systems thereof, application of regulation and macroeconomic analysis.

Considering that the EU General Data Protection Regulation (GDPR) is directly applicable in Latvia (as it is in all EU MS), the Data Protection Advisory Support Council was established by the MoJ to promote the application of the principles of common understanding and good governance in the implementation of the GDPR. In addition, the Government Regulation No 606 "Rules of Procedures of the Cabinet" requires consent from the Data State Inspectorate of Republic of Latvia for any draft legislation that relates to personal data. In parallel to these legislative provisions, the MoJ is also responsible for developing, organising and co-ordinating the policy on data protection, including in relation to AML/CFT/CPF (Clause 4 of the 16 August 2017 Government Regulation No 474 "By-laws of the Ministry of Justice"). While data protection authorities are not directly included in the FSDB, the MoJ, as one of its permanent members, ensures that data protection principles are incorporated into the drafting of legislation, in line with its responsibilities.

Overall, the measures listed above respond to the requirements of this criterion and confirm that there is a sound basis for co-operation and, where appropriate, co-ordination, between the relevant authorities to ensure the compatibility of AML/CFT/CPF requirements with Data Protection and Privacy rules.

Weighting and Conclusion

Recommendation 2 is rated compliant.

Recommendation 3 - Money laundering offence

Latvia was rated largely compliant in the 2018 MER because of deficiencies in the scope of inclusion of designated offences, notably participation in an OCG, which was not designated, and collection of funds for TF. While Latvia has reformed elements of its laws to include TF as a predicate offence, it has not amended its laws to include participation in an OCG as a separate offence or an offence based on conspiracy. Several minor deficiencies in regard to proportionality and dissuasiveness of sanctions in certain cases remains.

Criterion 3.1 – ML is criminalised on the basis of the Vienna Convention and the Palermo convention. It is defined in Sec.5 AML/CFT/CFT Law of Latvia and criminalised by Section 195 of the CL.

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 and

terrorism-related offences, except participation in an OCG as a separate offence or an offence based on conspiracy. The liability for offences committed by an organised group is stipulated as a qualifying (or aggravating) element. This requires the commission of a certain criminal offence.

Criterion 3.3 – This criterion is not applicable as Latvia is not applying a threshold approach.

Criterion 3.4 – The ML offence extends to any type of property that directly or indirectly represents the proceeds of crime, regardless of its value. Latvia defines "criminally acquired financial resources or other property" and "proceeds of crime" as any economic benefit or funds which has come into the ownership or possession of a person as a direct or indirect result of committing a criminal offence (Sec. 70 and 195 CL, Sec. 4 and 5 AML/CFT/CPF Law). The term "funds" includes every financial resources or other corporeal or incorporeal, movable or immovable property, including legal documents or instruments evidencing title or interest in such assets.

Criterion 3.5 – When proving that the property is the proceeds of crime, it is not necessary that a person be convicted of the predicate offence. Latvia's criminal procedures state that in order to prove the laundering of proceeds from crime, there is no need to establish the specific predicate criminal offence (CPL Section 124 (7)). A person can be found guilty of ML if they are aware that the funds in question are proceeds of crime, regardless of whether it has been established from which offence the proceeds of crime were derived (Sec.5(2) AML/CFT/CPF Law).

Criterion 3.6 – Sec.5(2) AML/CFT/CPF Law establishes jurisdiction to prosecute ML if the predicate offence has occurred in another country, and if it constitutes an offence in that country. The requirement of dual criminality for a predicate offence has been excluded.

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.

Criterion 3.8 – It is possible for the intent and knowledge required to prove the ML offence to be inferred from objective factual circumstances. The Supreme Court of Latvia recognises that circumstantial evidence may also be used to confirm the existence of the facts to be proved. The authorities have provided examples of case-law by the Supreme Court according to which the nature of the intent was based on the circumstances of the crime committed and the subjective element of the offence was established by the persons' actions (Supreme Court of Latvia, SKK - 683/2007, criminal case No 11390091505 and SKK - 23/2024, criminal case No 12507000607).

Criterion 3.9 – Every form of the ML offence remains punishable. The basic ML offence remains punishable for a term not exceeding four years (Sec.195(1) CL) and in cases where the act is committed by a group of persons according to a prior agreement, up to five years (Sec. 193 (2). If the ML offence is committed on a large scale or by an organised group, the term of imprisonment ranges from three to twelve years (Sec.195(3)), 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 (paragraphs 1 and 2) provides for the possibility to impose fines or other forms of punishment (e.g. temporary deprivation of liberty, community service). The range of sentences for ML appears proportionate and equivalent to other financial offences under the CL.

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. This difference exists because a legal person cannot possess the requisite mental state to be criminally liable, although no fundamental principle of domestic law was cited to that effect. However, this does not alter the fact that the "coercive measures" against legal persons have their basis in CL, 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 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.

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 five to hundred thousand minimum monthly wages in Latvia (Sec.70.[6] CL). As the minimum monthly wage was EUR 700 per month in Latvia in 2024, this equalled a range of fines from EUR 3 500 to EUR 70 million. This range, together with the other available coercive measures (in particular the possible liquidation of the legal person), allows for proportionate and dissuasive penalties.

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.

Weighting and Conclusion

Latvia has undertaken several reforms to amend laws to address most gaps in regard to the ML offence. However, the required elements to establish participation in an OCG as a predicate offence are not fully met and require the commission of another crime. **R.3 is rated largely compliant.**

Recommendation 4 - Confiscation and provisional measures

In the 2018 MER, Latvia was rated compliant in relation to confiscation and provisional measures. Latvia has since revised some amendments to its legal framework (e.g. providing an *expressis verbis* definition of "indirectly criminally acquired property" (Section 70.11 (2) of the CL) that clarify its legal provisions but do not affect their levels of compliance. In additions, legal framework was amended in order to introduce a management of seized virtual currencies.

Criterion 4.1 – Latvia has a broad set of legal powers to deprive criminals of their proceeds or instrumentalities. Provisions of the CL (Sec.70.[10] et seq.) provide for measures to confiscate directly and indirectly criminally acquired property, laundered property and instrumentalities of crime, regardless of whether the property is held by criminal defendants or third parties. This includes any economic benefit as a direct or indirect result of committing a criminal offence, as well as any economic benefit derived from such proceeds. In addition, these sections of Latvia's CL include provisions that enable some forms of confiscation without conviction in such instances that property is not proportionate and justified to the legitimate income of a person and when this person is related to criminal activities, criminal or terrorist organisation. Moreover, Sec.4 (1) AML/CFT/CPF Law defines "proceeds of crime", the funds that belong or are controlled by persons related to TF, terrorist acts or terrorist organisations.

If such property has been alienated, destroyed, concealed, or disguised, and its confiscation is not possible, Sec.70[14] CL allows for the confiscation of corresponding value.

Latvia's CPL provides for a limited version of NCBC as the requirement to prove the legality of origin applies only to persons already involved in criminal proceedings (Ch 59, CPL and Sec.125, CPL) or a person who belongs to a group of specifically defined persons (among others, members and supporters of OCGs, persons engaged in terrorist activities or maintaining permanent relations with a person who is involved in terrorist activities, Sec.70.[11] CL).

Criterion 4.2 – a) Investigation institutions have investigative powers and are able to identify, trace and initiate seizing of property that is subject to confiscation (Sec.190 CPL), as well as to evaluate it (if need by a specialist, Sec. 364 CPL).

b) In order to prevent any transfer or disposal of such property, 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 et seq. CPL. A decision to freeze property 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 frozen/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) The LEAs can perform any of the investigative actions or special investigative techniques provided in Chapter 10 and 11 of the CPL, including interrogation, questioning, search, removal, requests for objects and documents, etc. as well as use instruments of international co-operation provided in the Part C of the CPL. Sec.215 CPL provides for special investigative measures in this respect.

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.

Criterion 4.4 – Latvia has mechanisms and designated authorities for managing seized, frozen or confiscated property. Latvia regulates in detail different forms of executing confiscated property, including virtual currencies. Latvia also has mechanisms for the disposal of seized property, when necessary, for instance in circumstances when the long-term storage of seized property is not possible or causes losses for the State. Seized virtual currencies are disposed of (i.e. converted to cash) as a matter of course during proceedings (Sec 365, CPL and CoM Reg. No. 1025 "Regulations Regarding Actions with Material Evidence and Seized Property"). 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.

Weighting and Conclusion

R.4 is rated as compliant.

Recommendation 5 – Terrorist financing offence

Latvia was rated as largely compliant for Recommendation 5 in the 2018 MER. The principal deficiency identified was that the TF offence did not cover indirect transfers, the direct and indirect provision of funds, or the direct and indirect collection of funds.

As for the legislative changes in the country, in 2018, the CL was amended to include a new Chapter on "Terrorism-related offences", which introduced new offences, thereby criminalising the activities provided for in the Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism and the Directive of the European Parliament and of the Council on combating terrorism and replacing Council Framework Decision 2002/475/JHA on combating terrorism. Amendments have also been made to the AML/CFT/CPF Law Section 5 (3) and (4). These amendments were introduced following the recommendations of the 5th round MONEYVAL MER, addressing direct or indirect collection or transfer at the disposal of a terrorist group or an individual terrorist of financial funds or property acquired by any means. Amendments to Section 5 (3) of the AML/CFT/CPF Law expanded the definition of TF with travel for the purpose of terrorism and provision or receipt of terrorist training.

Criterion 5.1 – TF offence is criminalised in Sec. 79.[1] of the CL and the definition of TF is set out in Sec. 5 (3), (4) of the AML/CFT/CPF Law, which are in line with the UN TF Convention. There is no specific provision in CL making reference to the TF definition in the AML/CFT/CPF Law, but Latvian well-established jurisprudence confirms that *lex specialis*-definition of TF in AML/CFT/CPF Law complements incrimination in CL. The definition of the TF encompasses direct or indirect collection or transfer of financial funds or other property acquired by any form with the view to use them or by knowing that they will be used

to carry out one or several activities. Legislation further provides a list of activities that can be financed within the scope of TF offence including terrorism and all offences from Annex of the TF Convention. The definition of the TF offence contains a clear act and knowledge requirement, from which it is clear that the element of wilfulness can be inferred.

Criterion 5.2 – TF offence as defined in AML/CFT/CPF Law (Sec. 5 (3) and (4)) extends to direct or indirect (a) collection or transfer of funds or property acquired by any mean with the aim to use them or by knowing that they will be used to carry out terrorist activity; (b) collection or transfer at the disposal of a terrorist group or an individual terrorist of financial funds or property acquired by any means. The latter incrimination appears to be broad enough to cover both mental elements of the offender required by the standard: unlawful intention and/or knowledge that the funds are used or should be used by individual terrorist or terrorist organisation.

A link to a specific terrorist act or acts is not required.

Criterion 5.2bis – The definition of a TF offence in Sec. 5 (11 and 13) of the AML/CFT/CPF Law includes the financing of the travel of individuals "for the purpose of terrorism" and financing of training of a person for terrorist purposes. In addition, the CL provides criminal liability for financing the recruiting, training, receiving of training for terrorist purposes (Sections 79.^{2}, 79.^{4}, 79.^{5}) and for providing funds for persons travelling for terrorist purposes.

Criterion 5.3 – The definition of TF offence covers "funds or other property acquired in any manner" and does not differentiate between legitimate and illegitimately sourced funds. According to the Sec. 1(1) AML/CFT/CPF Law funds are defined as "financial resources or other corporeal or incorporeal, movable or immovable property." The AML/CFT/CPF Law further provides the definition of "financial resources" as financial instruments or means of payment held by a person, documents (in hard copy or electronic form) in the ownership or possession of a person that give the right to gain benefit from them, as well as precious metals in the ownership or possession of a person. Authorities advised that the Commentaries to the CL explains that "funds or other property" can be money or any type of material value of any nature. Overall, it can be concluded that definition of funds appears to encompass "assets of every kind" as required by the FATF glossary.

Criterion 5.4 – The definition of TF offence does not require that the funds or other assets were used to carry out terrorist act (or attempt), nor a requirement for a link to be established to a specific terrorist act.

Criterion 5.5 – The AT acknowledges that Sec. 8 of CL requires establishment of the mental state of the person in relation to objective elements of the criminal offence. The criminal offence is committed in instances when the offender is aware of the harm caused by the offence and has knowingly committed it. While this provision details the nature and degree of *mens rea*, it does not establish the method to corroborate the mental element, i.e., if it is possible to prove intent (intentional or negligent) using objective, factual circumstances. In their response to this query the authorities provided several cases/convictions where the courts used circumstantial evidence to prove intent by a perpetrator. Whilst these were not TF related cases (some of the examples include standalone ML prosecutions), the principles applied and the way courts inferred knowledge (*mens rea*) from objective, factual circumstances, confirmed that the requirements of this criterion are applied in practice.

Criterion 5.6 – The CL provides sanctions applicable for TF offence such as life imprisonment or incarceration ranging from 8 up to 20 years of imprisonment. For the large-scale TF offence beside life imprisonment the court may order incarceration ranging from 10 up to 20 years of imprisonment. The legislation further defines large-scale TF offence as the offence where the total value of the property which was the object of the offence was not less than the total of fifty minimum monthly wages specified in the Republic of Latvia at that time (the current minimum monthly wage in Latvia is EUR 740). Therefore, it can be concluded that sanctions available for TF offence are proportionate and dissuasive.

Criterion 5.7 – The criminal liability of legal persons is established under Section 70 of CL. In Latvia, legal person can be liable if the offence is committed by natural person in the interests or for the benefit of legal person. Such liability is without prejudice to the criminal liability of natural person. Legal persons can also be held liable when there is insufficient supervision or control, when a natural person acts individually or as a member of the collegial authority of the relevant legal person. Nevertheless, liability of legal persons can be established only in cases where a crime is committed in the interest or for the benefit of legal persons

which narrows its application for TF, given that TF offences do not necessarily include these elements ('for the benefit' or 'in the interest'), and thus limits the liability of legal persons for TF.

There is a wide range of sanctions that can apply to the convicted legal person such as: (i) liquidation; (ii) restriction of rights; (iii) confiscation of property; (iv) fines. The range of fines that can be imposed varies depending on the classification of the crime. As TF offence is classified as especially serious crime, fines range between EUR 21 000 to 70 million. It can be concluded that these sanctions are proportionate and dissuasive.

Criterion 5.8 – Ancillary offences are set out in the general part of CL and are applicable for all criminal offences, including TF. Sections 15, 19 and 20 of the CL cover: attempt to commit criminal offence, participation as an accomplice, organising or directing others to commit the offence. Contribution to the commission of TF offence by a group of persons acting with a common purpose is partly covered by Sec.21 of CL. Nevertheless, this provision 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 this criterion.

Criterion 5.9 – Latvia has criminalised ML using an "all crimes" approach and thus the TF offence is designated as a ML predicate offence.

Criterion 5.10 – Incrimination of TF offence does not make any distinction regarding the place where the terrorist(s)/terrorist group(s) is located, or the terrorist act(s) occurred/will occur. Moreover, Sec. 4 of CL explicitly provides for extraterritorial jurisdiction for both Latvian citizens and foreigners.

Weighting and Conclusion

Whereas Latvia has a sound CL coverage of all elements of the TF offence, moderate deficiencies/limitations are identified in relation to the liability of legal persons for TF offence (c.5.7); and with regard to committing an offence within an "organised group" which requires a previous agreement with divided responsibilities (c.5.8). **Recommendation 5 is rated as largely compliant.**

Recommendation 6 – Targeted financial sanctions related to terrorism and terrorist financing

In the 2018 MER, Latvia was rated partially compliant with R.6, and following the 2019 FUR upgraded to largely compliant by addressing the major deficiencies. However, some shortcomings remained including: (i) 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); (ii) freezing obligation did not extend to all required categories of funds or other assets; (iii) the procedures did not explicitly mandate compliance with de-listing or freezing actions (iv) there is no definition of circumstances that must apply before authorising access to frozen funds or assets.

Latvia implements TF TFS through EU decisions and regulations, complemented by domestic legislation.[123]

Criterion 6.1 – (a) Under the Law on Sanctions, the CoM proposes, upon its own initiative or upon a proposal of the MFA or National Security Council the imposition of international sanctions (Sec. 3^1(1)). According to the procedure for the proposition of international sanctions, the CoM is the competent authority to take the decision on the proposition of international sanctions, which is submitted to the relevant international organisation by the MFA without delay. (Par. 4 and 6, CoM Reg. No. 184). The Law on Sanctions also states that the MFA is the competent authority for co-ordination regarding the imposition of sanctions in Latvia, including in communication with international organisations and foreign competent authorities (Law on Sanctions, Sec. 12(3)).

(b) Latvia has introduced mechanisms for identifying targets for designation based on criteria set by UNSCRs 1267/1989, 1988 and designating persons or entities that meet relevant criteria in line with the FATF

123. At EU level UNSCR 1267/1989 (on Al Qaida) are implemented through Council Decision 2016/1693/CFSP and EU Regulation 881/2002; UNSCR 1988 (on Taliban) – through Council Decision 2011/486/CFSP and EU Regulation 753/2011; and the UNSCR 1373 - through Council Common Position (CP) 2001/931/CFSP and EU Regulation 2580/2001.

standard.

(c) As the designation procedure in the Latvian legal system is an administrative process, the authorities apply an evidentiary standard of proof of "reasonable grounds" or "reasonable basis" when deciding whether to propose designations to the UN or make a national designation. There is nothing in the legislation provided that requires designation proposals to be conditional on the existence of criminal proceedings.

(d) Through a combination of Section 3 of the Law on Sanctions and CoM Reg. No. 184, procedures adopted by the UN would be followed and standard forms used when proposing a designation to the relevant UN Committee.

(e) Authorities are required to provide all information to allow the identification of individuals and entities being proposed for designations (Par. 7 & 8 of the CoM Reg. No. 184).

Criterion 6.2 – (a) At the EU level, the EU Council (through the Council's Working Party on the Application of Specific Measures to Combat Terrorism (COMET WP)) is responsible for designating persons or entities that meet the criteria set forth in UNSCR 1373. Designations are considered based on proposals submitted by EU Member States or third states. (EU Regulation 2580/2001, art.2(3); Common Position 2001/931/CFSP, art.1(4)). Relevant designations of EU internals (i.e., natural persons who have their roots, main activities, and objectives within the EU) only trigger enhanced police and judicial co-operation. (CP 2001/931/CFSP footnote 1 of Annex 1).

The CoM has responsibility for designating persons or entities that meet the respective UNSCR 1373 designation criteria. MFA is responsible for receiving third party request and the CoM shall take a decision in response to this request (Par. 27, CoM Reg. No. 184). The Law on Sanctions does not preclude introducing sanctions on an EU natural or legal person.

(b) At the EU level, proposals for listings are made by member states (for proposals based on decisions taken by their own competent authorities), or by member states or the High Representative for Foreign Affairs and Security Policy (HR) for proposals on the basis of decision(s) by third States' competent authorities. The EU (through COMET WP) applies designation criteria consistent with the designation criteria of UNSCR 1373 (CP 2001/931/CFSP, art.1(2) & (4); Council Regulation 2580/2001, art.2(3), COMET WP mandate, practical arrangements and working methods 10826/1/07 REV`1).

Latvia has introduced mechanisms for identifying targets for designation based on criteria set by UNSCRs 1373 and designating persons or entities that meet relevant criteria in line with the FATF standard.

(c) At the EU level, the European External Action Service or relevant member state (acting as intermediary) when receiving a request for designation from a non-EU country, will carry out a first basic scrutiny of the proposal and gather relevant information, including requesting additional information from the requesting country, in particular with regard to and respect for fundamental rights. (CP 2001/931/CFSP, art. 1(2) and (4), as well as COMET WP mandate, practical arrangements and working methods). If an EU country requests an EU designation, the compliance with due process is assumed when the EU reviews such requests. COMET WP has 15 days to review the proposal, this timeframe can be shortened in exceptional cases. (doc.14612/1/16 REV 1 on establishment of COMET WP, Annex II, arts.8-9). At national level, paragraphs 27-29 of the CoM Reg. No. 184 set out a mechanism for responding to foreign country request. Requests for designation under Latvia's national sanctions regime can be determined on a prompt basis by virtue of Rules of Procedures of the CoM.

(d) At the EU level, when deciding on a proposal, COMET WP decides on the basis of a decision (and the information/material supporting that decision) by a competent national body, irrespective of criminal proceedings (CP 2001/931/CFSP, art.1(4)).

At the national level, as the designation procedure in the Latvian legal system is an administrative process, the authorities apply an evidentiary standard of proof of "reasonable grounds" or "reasonable basis" when deciding whether to propose designations to the UN or make a national designation. There is nothing in the legislation provided that requires designation proposals to be conditional on the existence of criminal proceedings.

(e) There is no EU procedure or requirements regarding the provision of identifying or supporting information with respect to requesting non-EU countries to give effect to EU designations. Information to

support designation may be shared with non-EU members upon request provided EU Member States agree.

At the national level, UNSCRs on sanctions are directly applicable in Latvia (Sec 11 (1) of the Law on Sanctions), and UNSCR 1373 requires full co-operation to be provided, including when requesting another country to give effect to action initiated in Latvia under a freezing.

Criterion 6.3 – (a) At the EU level, all member states are required to provide each other with all available relevant information to identify persons meeting the criteria for designation (CP 2001/931/CFSP, art.4; EU Regulation 2580/2001, art.8; EU Regulation 881/2002, art.8).

At national level, Latvia cites Section 12(2^2) of the Law on Sanctions, which provides for information sharing between MFA and the FIU, as well as Section 13 of the Law on Sanctions, which provides that supervisory 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". LEAs, such as the State Security Service and the State Police, including the ECED, have the authority to employ the range of investigative tools and methods as described under R.31.

(b) At the EU level, designations take place without prior notice (EU Regulation 1286/2009, preamble paragraph 5).

At national level, no provision of the Law on Sanctions or other law requires that notice should be given to a party prior to a designation.

Criterion 6.4 – At the EU level, implementation of TFS, pursuant to UNSCRs 1267/1989 and 1988, does not occur "without delay."[124]

At national level, according to Sec.11(1) of Law on Sanctions, sanctions imposed by the UNSCRs are binding and directly applicable in the Republic of Latvia.

At EU level, for TFS under the UNSCR 1373 mechanism, these measures are implemented without delay, except in respect of EU internals. New designations are published on the day they are adopted and enter into force the same day. Once the decision to freeze has been taken, EU Regulation 2580/2001 is immediately applicable within all EU Member States. Designations under UNSCR 1373 made by Latvia upon its own motion or in response to a request by another country are also applicable without delay, pursuant to Section 11(3) of the Law on Sanctions. This section stipulates that designations are to be made by a CoM order which shall come into force immediately at the moment it is signed (FUR 2019, paragraph 9).

Criterion 6.5 – (a) At the EU level, for 1373 designations, there is no requirement to freeze assets of listed individuals that are EU internals Listed EU internals are only subject to increased police and judicial co-operation among members (CP 2001/931/CFSP footnote 1 of Annex 1). Under UNSCRs 1267/1989, 1988, 1373 all natural and legal persons within or associated with the EU are required to freeze without prior notice and delay the funds or other assets of designated persons and entities. (EU Regulation 753/2011, arts.3, 14; EU Regulation 881/2002, arts.2(1), 11; EU Regulation 2580/2001, arts.2(1)(a), and 10).

At national level, all natural and legal persons are obligated to freeze funds and economic resources in accordance with international and national sanctions that provide for such freezing (CoM Reg. No. 184, Par. 14-15). Moreover, permanent freezing orders can be made without a judicial order.

(b) At the EU level, freezing actions for UNSCRs 1267/1989 and 1988 extend to all funds and economic resources belonging to, owned, held or controlled, either directly or indirectly, by a designated person or entity, or by a third party acting on their behalf or at their direction. This extends to interest, dividends or other income or value accruing from or generated by assets (EU Regulation 881/2002, arts.1(1), 2; EU Regulation 753/2011, arts.1(a), 3). This does not explicitly cover jointly-owned assets, although this interpretation is taken in non-binding EU Best Practices on sanctions implementation (EC document 8519/18, paragraphs 34-35).

Under the EU mechanism on UNSCR 1373, the freezing obligation applies to all funds, other financial assets and economic resources belonging to, or owned or held by the designated person or entity (EU Regulation 2580/2001, arts.1(1), 2(1)). There is no explicit reference to funds or assets controlled by, indirectly owned

124. This is due to the time taken to consult between European Commission departments and the translation of Commission or Council Implementing Regulations containing the designation into all official EU languages. Though expedited procedures allow for implementation within 72 hours where possible, this does not meet the requirement of "without delay".

by, derived from assets owned by, or owned by a person acting at the direction of a designated person or entity. However, this gap is largely addressed by the EC's ability to designate any legal person or entity controlled by, or any natural or legal person acting on behalf of, a designated person or entity (EU Regulation 2580/2001, art.2(3) (iii) and (iv)). As above, the notion of joint-ownership is not explicitly covered, although this interpretation is taken in non-binding EU Best Practices (EC document 8518/18, paragraphs 35).

At national level, the Law on Sanctions states that all persons, whether natural or legal, are required to implement freezing obligations and the freezing obligation covers all the criteria mentioned under criterion 6.5(b)(i) to (iv). However, since the Law on Sanctions does not include a definition for "funds and financial instruments", it is not clear that it will allow all "funds or other assets" to be frozen. To the extent that sanctions are applied in Latvia through EU designations, these will however extend to "funds or other assets" covered through separate statutory instruments.

(c) At the EU level, natural and legal persons are prohibited from making funds, other assets or economic resources available unless authorised by a national competent authority (EC Regulation 881/2002, art.2(2), (3); EU Regulation 753/2011, art.3(2); EU Regulation 2580/2001, art.2(1)(b)). The EU UNSCR 1373 mechanism explicitly extends to the provision of financial services (EU Regulation 2580/2001, art.2(2)). While there is no similar explicit prohibition in the EU UNSCR 1267/1989 and 1988 mechanism, this is covered by the broad definition of funds and other assets *(economic resources*) and the prohibition to make available assets that can be used to obtain such services (EU Regulation 881/2002, art.1(2); EU Regulation 753/2011, art.1(c)). However, deficiencies in respect of freezing obligations noted under c.6.5(a) for EU internals applies to this criterion.

At national level, there is no explicit reference to "other services" (in the context of financial services). Accordingly, it is not clear that the provision of such services would be prohibited.

(d) At the EU level, information on EU designations is published in the Official Journal of the EU and included in the EU's Financial Sanctions Database the next working day (which includes a newsletter service to which FIs and DNFBPs can subscribe), though there may be delays to updates via the newsletter service notably in case of designations on Fridays or over the weekend. Guidance in relation to EU sanctions is published on the website of the European Commission.

At national level, the MFA has launched a sanctions webpage, consistent with its responsibility in CoM Reg. No. 184 to publish information on international and national sanctions in force. Additionally, pursuant to Sec.4(4) AML/CFT/CPF Law and CoM Reg. No. 184, the FIU maintains current lists of persons subject to national and international sanctions. Both the FIU and Latvijas Banka have provided guidance on sanctions to the REs on multiple occasions.

(e) At the EU level, all natural and legal persons (incl. FIs and DNFBPs) are required to report any information which would facilitate compliance with TFS obligations to their respective national competent authorities. This requirement does not explicitly extend to reporting attempted transactions, although this is covered by the requirement to report "any information which would facilitate compliance" with the relevant Regulations. The scope gap in obligations in respect of 1373 designations (EU internals) also applies to this criterion. (EU Regulation 753/2011, art.8; EU Regulation 881/2002, art.5(1); EU Regulation 2580/2001, art.4).

At national level, both the AML/CFT/CPF Law and the Law on Sanctions now include an obligation to report assets frozen or action taken in respect of sanctions to the State Security Service.

(f) At the EU level, for 1267/1989, 1988 and 1373 designations, third parties acting in good faith are protected (EU Regulation 753/2011, amended by EU Regulation 1286/2009, and 2016/1686 art. 12 and 13, art.6 and 7; EU Regulation 881/2002, art.6; EU Regulation 2580/2001, art.6).

At the national level, under Sec.40(3) AML/CFT/CPF 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.

Criterion 6.6 – (a) At the EU level, for designations under the 1267/1989 and 1988 mechanisms, there are procedures to submit de-listing requests to the relevant UN Sanctions Committee in line with Committee procedures (EU Regulation 881/2002, art.7c; EU Regulation 753/2011, art.11(4)). EU measures imposing targeted financial sanctions pursuant to 1267/1989 and 1988may be challenged by instituting proceedings

before the EU Court of Justice (art.263, par.4 and art.275, par.2 of the Treaty on the Functioning of the EU for challenging EU regulations or Council Decisions (CFSP)).

At national level, the de-listing procedures have been introduced that are publicly known (CoM Reg. No. 184, Par.36-37).

(b) At the EU level, de-listing procedures are available for designations under the 1373 mechanism under EU Regulation 2580/2001.

At national level, Sec.14(2) Law on Sanctions provides that the CoM 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 CoM must revise the national sanctions list at least annually and, if necessary, amend or partially or completely revoke it. When considering a de-listing under the national sanctions regime, the same evidentiary standard and other criteria are taken into account.

(c) At the EU level, a person or entities designated under the 1373 mechanism can write to the EU Council to have the designation reviewed by COMET WP (CP 2001/931/CFSP) or may institute a proceeding before the EU Court of Justice (Treaty on the Functioning of the EU, arts.263(4), 275(2)).

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) At the EU level, persons designated under UNSCR 1267 etc. and 1988 are informed of applicable de-listing procedures, which include the availability of the focal point (for designations under UNSCR 1989) and the UN Office of the ombudsperson (for UNSCR 1267/1989 designations). (EU Regulation 881/2002, art.7(a); EU Regulation 753/2011, art.11(4)).

For measures at the national level, see c.6.6(a).

(f) At the EU level, procedures for unfreezing funds due to cases of mistaken identity are in place (EC document 8519/18, paragraphs 8-17, 37).

At national level, there is a procedure to be followed in a case of mistaken identity.

(g) At the EU level, de-listings are communicated via publication of updated lists in the EU official journal and notifications within the EU sanctions database for subscribers. Guidance mentioned under c.6.5.d) also contains information on the obligations to respect a de-listing action.

At national level, the mechanism used for communication of designations is the same as for de-listings (Law on Sanctions, Sec.11). With respect to guidance on de-listing and unfreezing the same procedures apply as mentioned under 6.5(d). However, the procedures do not appear to explicitly highlight an obligation to respect de-listing or freezing actions.

Criterion 6.7 – At the EU level, the regulations imposing TFS obligations contain measures for national competent authorities to authorise access to frozen funds, where necessary for basic expenses or the payment of certain expenses in line with UNSCR 1452 (EU Regulation 881/2002, art.2a; EU Regulation 753/2011, art.5; EU Regulation 2580/2001, arts.5, 6). At national level, access to funds frozen is provided under CoM Reg. No. 184. However, the Regulation does not define the circumstances which must apply before authorising access to frozen funds or assets.

Weighting and Conclusion

The legal basis for implementing TF-related TFS is in place to ensure freezing without delay. However, there are some uncertainties and gaps, such as there is no explicit reference to "other services" accordingly, it is not clear that the provision of such services would be prohibited, the procedures do not appear to explicitly highlight an obligation to respect de-listing, as well as it is not defined which circumstances must apply before authorising access to frozen funds or assets. **R.6 is rated largely compliant.**

Recommendation 7 – Targeted financial sanctions related to proliferation

In its 2018 MER Latvia was rated partially compliant with R.7 and following the 2019 FUR, Latvia was re-rated to largely compliant by addressing the major deficiencies. The uncertainties and gaps described under R.6 were also relevant to R.7.

As of 18 October 2023, TFS set out in UNSCR 2231 related to Iran have ceased to apply. This directly impacts the scope of FATF Recommendations on proliferation financing and our related assessment work. As UNSCR 2231 is the legal basis for some elements of R.7, the scope of those requirements on proliferation financing has also changed. After 18 October 2023, R.7 no longer requires countries to apply TFS to individuals and entities designated under UNSCR 2231.

Latvia implements PF TFS through EU decisions and regulations, complemented by domestic legislation.[125]

Criterion 7.1 – At the EU level, implementation of TFS, pursuant to UNSCR 1718, does not occur "without delay." This is due to the time taken to consult between European Commission departments and the translation of Commission or Council Implementing Regulations containing the designation into all official EU languages. At national level, on the basis of Section 11(1) of Law on Sanctions, sanctions imposed by the UNSCRs are binding and directly applicable in the Republic of Latvia.

Criterion 7.2 – The competent authority responsible for implementing and enforcing the relevant UNSCRs is the FIU (Law on Sanctions, Sec.12.[1](1)).

(a) At the EU level, all natural and legal persons within the EU are required to freeze the funds or other assets of designated persons or entities as soon as a designation is published, i.e. without prior notice (EU Regulation 2017/1509, art.1and 2). Though delays in implementation apply as described under c.7.1.

At national level, the Law on Sanctions (Sec. 5) states that all persons, natural or legal, are subject to freezing obligations. The scope of persons obligated to comply with TFS obligations has been broadened by including a clear reference to PF.

(b) At the EU level, freezing actions for UNSCR 1718 extend to all funds and economic resources belonging to, owned, held or controlled, either directly or indirectly, by a designated person or entity, and includes assets generated from such funds. (EU Regulation 2017/1509, art. 1 and 34).

This does not explicitly cover jointly-owned assets, although this interpretation is taken in non-binding EU Best Practices on sanctions implementation (EC document 8519/18, paragraph 34-35).

While the definition does not explicitly cover funds or assets of persons acting on behalf or at the direction of a designated person or entity, this is largely captured by the coverage of funds 'controlled' by the designated person (paragraph 55b. of the Guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy).

At national level, as described in c.6.5(b), there is no definition for "financial resources and financial instruments", thus it is not fully clear that it will allow all "funds or other assets" to be frozen.

(c) At the EU level, EU nationals and natural and legal persons within the EU are prohibited from making funds and other assets available unless otherwise authorised or notified in compliance with the relevant UNSCRs (EU regulation 2017/1509, art.34(3)). Regulations apply to any natural or legal person, entity, body or group in respect of any business done in whole or in part within the EU. At national level, please see the analysis under c.6.5(c).

(d) At the EU level, the same mechanism to communicate PF TFS is used as for TF TFS (see c.6.5(d)).

At national level, see the analysis for c.6.5(d).

(e) At the EU level, all natural and legal persons (incl. FIs and DNFBPs) are required to report any information which would facilitate compliance with TFS obligations. (EU Regulation 2017/1509, art. 50). This requirement does not explicitly extend to reporting attempted transactions, although this is covered by the requirement to report "any information which would facilitate compliance" with the relevant Regulations.

At national level, please see the analysis under 6.5 (e).

(f) At the EU level, protections are in place for third parties acting in good faith (EU Regulation 2017/1509, art.54).

At national level, please see the analysis under 6.5(f).

125. At the EU level, UNSCR 1718 (2006) on DPRK and its successor resolutions are implemented through CFSP 2016/849 and Council Regulation 2017/1509.

Criterion 7.3 – Section 13 of the Law on Sanctions empowers supervisors to monitor and ensure compliance by FIs and DNFBPs. Moreover, a clear procedure has been established for sanctioning powers.

Criterion 7.4 – (a) At the EU level, listed persons are informed of their ability to petition the UN Focal Point or their own government for de-listing, through the EU Best Practices document for the effective implementation of restrictive measures (page 11, paragraph 23).

At national level, see analysis under c.6.6(a).

(b) At the EU level, procedures for unfreezing funds due to cases of mistaken identity are the same as those described under c.6.6(f).

At national level, see the analysis under c.6.6(f).

(c) At the EU level, the regulation imposing TFS obligations under UNSCR 1718 contains measures for national competent authorities to authorise access to frozen funds or other assets under the conditions set out in UNSCR 1718. (EU Regulation 2017/1509, art. 35-36).

At national level, see the analysis under c.6.7.

(d) At the EU level, de-listings are communicated via publication of updated lists in the EU official journal and notifications within the EU sanctions database for subscribers. Guidance mentioned under c7.2(d) also contains information on the obligations to respect a de-listing action.

At national level, see the analysis under c.6.6(g).

Criterion 7.5 – (a) At the EU level, regulations permit the addition of interests or other sums due on those accounts or payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of this resolution, provided that these amounts are also subject to freezing measures. (EC Regulation 2017/1509, art. 34(9)). At national level, there are no provisions to meet the requirements of this sub-criterion.

(b) This sub-criterion is not applicable, as the TFS elements of UNSCR 2231 expired on 18 October 2023. Therefore, this analysis did not assess the implementation of UNSCR 2231.

Weighting and Conclusion

The legal basis for implementing-PF related TFS is in place to ensure freezing without delay. There are some uncertainties and gaps as discussed under R.6 and there is no definition for "financial resources and financial instruments", thus it is not clear that it will allow all "funds or other assets" to be frozen. **R.7 is rated largely compliant.**

Recommendation 8 – Non-profit organisations

In its 2018 MER, Latvia was rated partially compliant with R.8 and by addressing the majority of deficiencies re-rated to largely compliant in the 2019 FUR. Since then, R.8 has undergone specific changes to clarify requirements under the FATF Standards regarding NPOs and the following criteria have been amended: c.8.1, 8.2(b)-(d), 8.3, 8.4(a) and 8.5(c).

Since the 2018 MER, Latvia has conducted several risk assessments of the NPO sector as part of two NRAs (NRA1 and NRA2) and in strategic analysis of TF risk of NPOs. Following the most recent NRA2, an inter-institutional CFT Task Force has been created with a task to monitor and analyse NPO risks associated with TF.

Criterion 8.1 – a) According to the current regulatory framework in Latvia, there are different types of NPOs: associations, foundations, and religious organisations. Latvia has identified the subset of organisations that fall within the FATF definition of NPO to some extent. The identification was based on the information about NPOs transactions and information about NPO activities as registered with the ER (where applicable). The methodology used for the identification of the subset of NPOs focused predominantly on activities of raising/collection of funds, and only in the second phase on the disbursement of funds by those NPOs to higher risk countries, thus limiting the identification of NPOs solely on the activity of raising/collection rather than disbursement. However, in addition to this, authorities are conducting ongoing monitoring with regard to all NPOs with transactions to higher risk countries, which in turn let them

identify the NPOs who disburse funds. Though this additional exercise is limited to identification of only those who conduct transactions to higher risk countries, this allows to identify also the NPOs who disburse funds to some extent.

b) Latvia has conducted a risk assessment of the NPO sector. The outcomes of the assessment are reflected in several documents, including the NRA1 and NRA2, as well as in strategic analysis of TF risks of NPOs. These analytical documents provide thorough examination of possible trends of TF risks for NPOs by identifying the threats to the cross-border nature of transaction to high-risk countries, as well as to NPOs whose representatives (BO, members of the executive body, etc.) are residents of high TF risk countries or countries with low AML/CFT/CPF compliance requirements, or NPOs whose activities are linked to such countries. Based on this risk assessment 27 NPOs were assessed as having higher risk. It is evident that risk assessments are reviewed periodically (every three year for NRAs).

c) Based on the NRA1, as well as NRA2 the risk mitigating measures were identified and included in the AML/CFT/CPF Action Plans to ensure greater transparency in the NPO sector, while allowing for proper monitoring of the sector's TF risks, as well as organise training for the NPO sector on the requirements of the AML/CFT/CPF, including on the obligation to disclose BO information. Additionally, in 2020 the Civic Alliance of Latvia, one of the largest umbrella organisations for NPOs, has developed guidelines on ethical funding. Although intended as an internal control measure, partner organisations recognised their value in preventing financial risks. The guidelines outline procedures for assessing the acceptance of funding, criteria for identifying potential ethical risks, and transparency principles regarding the use of funds. They also highlight the importance of monitoring funding from countries identified as high-risk for TF and ensuring that funds are not directed to individuals associated with terrorism or its financing.

Criteria 8.2 – a) According to Section 52(3) of the Associations and Foundations Law, an association shall submit the annual accounts or parts thereof – accounts on income and expenditure or accounts on donations and gifts – to the SRS each year not later than by 31 March in accordance with the procedures provided for in the regulatory enactments regarding drawing up and submission of accounts. According to Section 102 of the Associations and Foundations Law the executive board shall prepare and submit the annual accounts of a foundation after the end of the accounting year in accordance with the provisions of Section 52 of this Law. Pursuant to Section 103 of the Associations and Foundations Law, persons, which make donations to a foundation, may at any time verify the activities of the foundation, as well as become acquainted with all documents, except for accounting records and information regarding other persons which have donated to the foundation. Under Section 15(5) of the Law on Religious Organisations, religious organisations must maintain accounting records, prepare reports, and pay taxes in accordance with the applicable legislation. By 31 March of the following year, each organisation must file—via the SRS's EDS—a copy of its annual statement signed by its management body, together with the audit commission's report or, where applicable, the sworn auditor's report (CoM Reg. No. 380, clause 94). To further promote transparency the ethical funding guidelines developed by the Civic Alliance of Latvia provide for the list of information to be published on NPO's website.

b) Latvia reported various initiatives aimed at raising awareness among NPOs and the donor community about TF risks, including the publication of the NRA1 and NRA2 on the FIU website. Outreach activities have been initiated, including an information event on TF risks for religious organisations and the distribution of an informative leaflet on TF vulnerabilities to NPOs with heightened TF risk. Additionally, informative leaflet on NPO risks and vulnerabilities of being abused for TF purposes is published on the FIU Latvia website, which is available for the donor community.

c) As mentioned under sub-criterion 8.1(c), in 2020 the Civic Alliance of Latvia developed guidelines for the ethical funding. These guidelines were included in the FATF best practices paper to combat the abuse of NPOs. A seminar was organised by the Finance Latvia Association in co-operation with the Civic Alliance of Latvia and FCMC in January 2021. This seminar was on the co-operation of credit institutions and associations on AML/CFT/CPF and on NPOs' understanding of the ML/TF/PF preventative measures.

d) The Associations and Foundations Law 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. Authorities advise that the SRS proactively encourages NPOs to have bank accounts, while the MoJ continuously works with religious organisations through information

campaigns. Moreover, there are publicly available guidelines on the FIU's webpage provided to the NPOs, as well as donor community encouraging the use of financial channels.

Criteria 8.3 – a) and b) Most measures detailed in sub-paragraph 7(b) of INR.8 apply to Latvian associations, foundations and religious organisations. Overall, regulatory measures are applied without having regard to the specific level of TF risks they face. Namely, all NPOs register in ER and obtain legal personality. The registration is required to open a bank account. Associations 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. Associations and foundations provide the ER with information on their objectives. The registration of religious organisations and their institutions and the content, submission and examination procedure of documents related to them are determined in Sections 8 - 10 of the Law on Religious Organisations. Submitted documents are assessed for compliance with Sections 18.13 and 13.14 of Law on the Register of Enterprises of the Republic of Latvia. Registration is granted only upon meeting these requirements. Regulation of the CoM Reg. No. 380 of 21 June 2022 "Regulations Regarding Annual Statements and the Conduct of Accounting in a Single-Entry System of Religious Organizations and their institutions" determines the procedure by which religious organisations keep accounts, as well as the content and delivery procedure of the reports of religious organisations. SRS conducts risk-based supervision with regard to NPOs identified as having higher risk. Moreover, in June 2024, the specialised CFT Task Force was established under the CCG legal framework to apply risk-based mitigation measures and co-ordinate the monitoring of NPOs that fall within the FATF definition and exhibit high TF risk, involving members from FIU Latvia, the State Security Service, Latvijas Banka, and the SRS. Outreach activities have been initiated by the FIU and State Security Service, including an information event on TF risks for religious organisations and the distribution of an informative leaflet on TF vulnerabilities to NPOs with heightened TF risk. Additionally, as of 1 July 2024, new regulations require associations and foundations to disclose their areas of activity in the SRS EDS, aiming to ensure alignment with their stated purposes and to provide a comprehensive sector overview.

Criteria 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 Associations and Foundations Law (Section 52 (3)), and CoM Reg. No. 439 of 2022 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 Section13(1)). The ER grants registration or re-registration upon receipt and "examination" of required information. If the ER receives information on the possible submission of false information, it refers the case to the State Police. The authorities further indicate that the State Security Service 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 (State Police) 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 filled 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). Based on new requirements in force since 1 July 2024, the association or foundation may be terminated based on SRS or ER decision (Associations and Foundations Law, Sec.56[1]). ER may terminate the activity if the board lacks representation rights for over two years or if the association cannot be reached at its legal address, and in both cases, the deficiencies are not remedied within six months of a written warning. The SRS can terminate the association if it fails to submit an annual report within three months after an administrative penalty, provided at least two years have passed since the offense. The activities of a religious organisation may be terminated by a court on various grounds: if its operations are in conflict with the Constitution, regulatory enactments or articles of association; if the religious organisation 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)) Section 272 of the CL imposes criminal liability for submitting false information to state institutions, including the ER, which notifies relevant authorities of any suspected violations under Section 4(4) of the Law on Register of Enterprises. According to Section 12 CL, a natural person who has committed a criminal

offence acting in the interests or on behalf of a legal person or as a result of insufficient supervision or control thereof is criminally liable. Therefore, if a person on behalf (or in the interests or as a result of insufficient supervision or control by NPO) of a NPO will commit a criminal offence, this person will be sanctioned in accordance with the CL. The administrative and criminal sanctions available for NPOs and persons acting on behalf of the NPO are considered effective, proportionate and dissuasive.

Criterion 8.5 – (a) Latvian authorities responsible for overseeing NPOs and TF 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). Pursuant to Sec.3(4) AML/CFT/CPF Law, the Register is obliged to report unusual and suspicious transactions, including suspicions of TF. The FIU can share information on suspected TF transactions of which it becomes aware, and the SRS can report suspicious transactions to the FIU. Similarly, the State Security Service are empowered to share information as appropriate with the FIU and SRS, as well as the State Police.

(b) The State Security Service as the lead agency for TF 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) Latvia ensures that necessary information is promptly shared with competent authorities through ongoing work of the Terrorist Financing Investigation Co-ordination Working Group created for the purpose of co-operation between investigative authorities. The group was created by decision of Council of experts of Counterterrorism Centre on 6 December 2019 as its subgroup. The institutions which form Terrorist Financing Investigation Co-ordination Working Group are State Security Service, FIU, PO, SRS, State Police and Latvijas Banka.

Criterion 8.6 – Latvia's FIU and LEAs maintain both formal and informal channels to share information on TF threats, including through Egmont channels (see also discussion in R.40).

Weighting and Conclusion

The authorities took steps in identifying the subset of NPOs falling under the FATF definition of the NPOs. However, this exercise did not fully address the requirements under c.8.1. which is considered as a minor deficiency. This conclusion takes into account additional mitigating activities conducted by the authorities, as well as compliance with all other criteria under R.8. R.8 **is rated as largely compliant.**

Recommendation 9 – Financial institution secrecy laws

In the 2018 MER, Latvia was rated compliant with R.9. Latvian authorities report that whilst some changes have been introduced relating to the exchange of information between FIs and competent authorities, none of them are material. Following a merger of the FCMC and Latvijas Banka references to the FCMC in the MER 2018 are replaced with Latvijas Banka.

Criterion 9.1 – FI secrecy laws do not inhibit the implementation of AML/CFT measures in Latvia, as evidenced below.

Access to information by competent authorities: Upon request, REs are required to submit to the FIU and Latvijas Banka information on CDD and payments (Sec. 37^1 and 37^2, AML/CFT/CPF Law). Credit institutions are required to provide non-disclosable information to a wide range of authorities, including the Latvijas Banka, the FIU, investigation authorities, the SRS (Sec. 63 Credit Institution Law). Similar requirements enabling access to information by request of supervisors.

Sharing of information between competent authorities domestically: All state and local government authorities have an obligation to provide information requested by the FIU for the implementation of its functions (Sec. 54 AML/CFT/CPF Law). Sec.55 of the AML/CFT/CPF Law specifies that the FIU shall provide information to pre-trial investigative institutions, the PO and the court, if such information is used to prove a criminal offence, including ML/TF. The SCAs are allowed to share restricted information with

State institutions responsible for prevention or investigation of ML/TF/PF and related criminal offences (Section 47[1] (6) AML/CFT/CPF Law).

Sharing of information between competent authorities internationally: the SCAs can exchange information for AML/CFT purposes with foreign supervisors (Sec. 46(1)(10) AML/CFT/CPF Law). The FIU Latvia may exchange information with foreign counterparts and may enter into agreements for that purpose (Sec. 62 AML/CFT/CPF Law). Similar provisions enabling exchange of information with foreign counterparts are set out in other sectorial laws.

Sharing of information between FIs: Information exchange between credit and FIs are regulated by Sec. 44 AML/CFT/CPF Law: they have the right to mutually exchange CDD information as well as information about the clients (terminated or refused business relationship). Credit institutions are not held liable (legal, civil liability) for the provision of such data. 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/CPF Law (Sec. 63(6) the Credit Institution Law).

Weighting and Conclusion

R.9 is rated compliant.

Recommendation 10 – Customer due diligence

In its 2018 MER, Latvia was rated partially compliant with R.10 based on the deficiencies relating to CDD renewal, EDD, prohibition to take certain actions when unable to fulfill CDD requirements, etc. The 2019 FUR concluded that most deficiencies have been addressed and, as a result, R.10 re-rated as largely compliant.

Criterion 10.1 – FIs are prohibited from opening and maintaining anonymous accounts and accounts in fictitious names (non-conforming to personal identification documents) and anonymous individual strong-boxes (Sec. 15 AML/CFT/CPF Law).

Criterion 10.2 – FIs are required to apply CDD in, inter alia, the following circumstances: (a) before establishing business relationship; (b) before conducting an occasional transaction (or several transactions that appear to be linked) amounting to EUR 15 000 or above; (c) for transfer of funds exceeding EUR 1 000, however, the Law is silent regarding CDD when transfer of funds is equal to EUR 1 000; (d) suspicion of ML/TF/PF or an attempt of such actions; (e) suspicion that the previously obtained CDD data is not true or appropriate (Sec. 11(1) AML/CFT/CPF Law).

Criterion 10.3 – FIs are required to identify and verify clients natural, legal persons and legal arrangements by obtaining specific identification data required at c.10.3 (Sec. 12-13 AML/CFT/CPF Law).

Criterion 10.4 – FIs are required to identify the person acting on behalf of the client natural person or legal person or legal arrangement by obtaining a document or a copy of relevant document that confirms the right to represent (Art. 12(5) and 13(1)(3) AML/CFT/CPF Law).

Criterion 10.5 – FIs are required to identify (ascertain) and verify BO (Sec. 11[1](1)(2) AML/CFT/CPF Law) and provides a list of documents FIs can choose to collect for identification purposes (Sec.18(3) of the same Law).

Criterion 10.6 – FIs are required to obtain and document information on the purpose and intended nature of business relationship (11(1) AML/CFT/CPF Law).

Criterion 10.7 – FIs are required to conduct monitoring and confirm that transactions are consistent with the previously obtained data about the client, its economic activity, risk profile and origin of funds; as well as regularly assess CDD information, data and documents based on risks; further to this, the AML/CFT/CPF Law sets out risk indicators for determining the extent and regularity of CDD review (Sec. 11[1](1)(4-5) and 11[1](2) AML/CFT/CPF Law).

Criterion 10.8 – FIs are required to verify shareholding structure and control of a legal person or arrangement (Sec. 11[1] AML/CFT/CPF Law).

Criterion 10.9 – To identify a legal person the following shall be requested by FIs: 1) documents confirming 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) incorporation documents (memorandum of incorporation, articles of association) and the persons authorised to represent the legal person, including names of the managing persons. Similar documents are required for the identification of a legal arrangement, however, there is no explicit requirement to obtain names of the persons holding senior manager positions of legal arrangements. (Sec.13(1) and 13(1^1) AML/CFT/CPF Law).

Criterion 10.10 – FIs are required to identify and verify the BO holding an ownership interest and in cases of indirect control – a person exercising control over entity (Sec. 18(1-2) AML/CFT/CPF Law). FIs are allowed to identify a person holding the position of the executive body as a BO if identification of the natural person directly or indirectly owning or controlling a legal person or arrangement is not possible. In this case FIs have to prove that all possible means to establish BO have been exhausted and any doubts that the legal person or legal arrangement has another BO have been excluded. This includes duly justifying and documenting the activities performed in establishing BO (Sec. 18(7) AML/CFT/CPF Law).

Criterion 10.11 – In case of legal arrangements, BO is defined as a natural person who owns or in whose interests a legal arrangement operates, or who directly or indirectly exercises control over it, including the settlor, the trustee (manager), the protector (if any), the beneficiary of such legal arrangement or, if the natural persons who are beneficiaries have not been determined yet, the group of persons in the interests of which a legal arrangement has been established or operates, and also another natural person who directly or indirectly exercises control over a legal arrangement (Sec.1(5)(b) AML/CFT/CPF Law).

Criterion 10.12 – In relation to life and investment linked insurance, FIs are required: take the name and surname of the natural person or the firm name of the legal person; obtain information on the beneficiary so to enable identification at the time of the payout. The AML/CFT/CPF Law is explicit that these measures should occur prior to the payout of the insurance indemnity (Art.11^1 (9) and (11) AML/CFT/CPF Law).

Criterion 10.13 – FIs are required to assess ML/TF/PF risks, including the risk inherent to the beneficiary of insurance policies and conduct enhanced CDD to determine the BO of the beneficiary of the insurance contract at the time of pay-out (Art.11^1 (9) AML/CFT/CPF Law).

Criterion 10.14 – In low-risk circumstances FIs are allowed to delay verification of the client's identity after the initial contact until the moment business relationship is established and prior to executing transaction (Sec. 11(3) AML/CFT/CPF Law).

Criterion 10.15 – FIs are required to have procedures in place setting out ML/TF mitigation measures and, inter alia, defining limitations on the amount, number or type of transactions.

Criterion 10.16 – FIs are required to regularly assess and update client CDD files on the basis of inherent risk and at least every 5 years. Scope and frequency of the CDD renewal should be determined on the basis of risk factors set out in the AML/CFT/CPF Law (Sec. 11^1 (1)(5) and 11^1 (2)).

Criterion 10.17 – FIs are required to apply EDD measures in increased ML/TF/PF risk circumstances (Sec.22 AML/CFT/CPF Law).

Criterion 10.18 – SDD is allowed when there is low risk of ML/TF/PF exception being increased risk (and/or information or attempt to conduct ML/TF) and when specific risk factors set out in the AML/CFT/CPF Law are present (Sec. 26 (1) and (8)).

Criterion 10.19 – FIs are not allowed to enter into a business relationship, open an account and are required to terminate the existing business relationship without delay if they are unable to fulfill CDD requirements; filing an STR should be considered in these circumstances (Sec. 28(2) AML/CFT/CPF Law).

Criterion 10.20 - If FIs suspect ML/TF/PF and there are grounds to believe that the application of further CDD measures may reveal these suspicions to the customer, they are permitted not to continue CDD, but to file a report to the FIU instead. In its report to the FIU, RE shall also explain as to why it was considered that further application of CDD measures would tip-off the client (Sec.11(6) AML/CFT/CPF Law).

Weighting and Conclusion

R.10 is rated largely compliant. Latvia meets all criteria except one. There is no explicit requirement to obtain names of the persons holding senior manager positions of legal arrangements.

Recommendation 11 – Record-keeping

In its 2018 MER, Latvia was rated largely compliant with Recommendation 11 due to shortcomings related to records of analyses by the REs.

Criterion 11.1 – REs are required to keep information on all transactions, be it domestic or international, for five years after termination of a business relationship or execution of an occasional transaction (Sec.37(2)(1) AML/CFT/CPF Law).

Criterion 11.2 – REs are required to keep all information acquired through CDD process, account information and correspondence with the client for a period of five years following the end of business relationships or execution of an occasional transaction (Sec. 37(2) AML/CFT/CPF Law). Results of analyses are not explicitly mentioned.

Criterion 11.3 – Whilst legal acts do not explicitly require transaction records to be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity (Sec.127 and 130 CPL), however, provide the notions of evidence and its admissibility in criminal proceedings. These, combined with the general accountancy requirements (see Sec. 7 of the Law on Accounting that requires transaction records to be 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) are broad enough to permit reconstruction of transactions.

Criterion 11.4 – REs are required to provide relevant CDD and payments' information (including documents thereof) to the supervisors or the FIU within the term specified in the request (Sec. 37^2 AML/CFT/CPF Law).

Weighting and Conclusion

R.11 is rated largely compliant. Latvia meets all criteria except one. Results of analyses are not explicitly mentioned among the documentation that is required to be kept.

Recommendation 12 – Politically exposed persons

In the 2018 MER, Latvia was rated largely compliant with R.12 due to twelve months' timeframe for derecognising PEP status after the cassation of PEP-related duties which was identified as a deficiency.

The definition of a PEP, its family members and close associates (Sec.18 AML/CFT/CPF Law) is in line with the FATF definition. 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 subject to higher ML risks thereafter (Sec.25(5) of the AML/CFT/CPF Law).

Criterion 12.1 – The AML/CFT/CPF Law requires REs in relation to PEPs: (a) when establishing a business relationship to determine, on a risk sensitive basis and using internal control system, whether the customer or the BO is a PEP or a family member or close associate of a PEP including when it becomes a PEP (Sec. 25(1-2)); (b) receive a consent from the senior management prior to commencing a business relationship (except for sole practitioners) (Sec.25(3)(1)); (c) apply risk-based measures to determine the source of wealth and source of funds of the customer or the BO who is a PEP (Sec.25(3)(2)); (d) carry out ongoing and enhanced monitoring (Sec.25(4) and 22(2)(3)).

Criterion 12.2 – The measures provided by the AML/CFT/CPF Law with regard to PEPs are equally applicable to foreign PEPs, as well as to the persons entrusted with a prominent public function by an international organisation, since all these categories of persons are covered by the PEP definition in Sec.1 of the AML/CFT/CPF Law.

Criterion 12.3 – All additional measures stipulated in the AML/CFT/CPF Law are equally applicable to the customers who are family members or close associates of a PEP.

Criterion 12.4 – Life insurance service providers and their intermediaries shall determine whether the beneficiary or BO is a PEP. This should occur not later than before the payout or transfer of the contract to another insurer. If higher risks are identified, enhanced CDD and monitoring, including senior management approval is required, as well as consideration of filing an STR with the FIU (11^1 (9-11), $25(2)^1$ AML/CFT/CPF Law).

Weighting and Conclusion

R.12 is rated largely compliant. Latvia meets all criteria, however, timeframe of 12 months for derecognising PEP status after cassation of its functions (provided there is no high risk) is considered a limitation.

Recommendation 13 – Correspondent banking

In its 2018 MER, Latvia was rated largely compliant with R.13 due to reasons that the definition of a shell bank appeared not to be fully in line with the FATF definition.

Criterion 13.1 – Credit institutions and other FIs, when establishing correspondent relationship, shall take the following measures in addition to regular CDD: (a) gather information on the respondent in order to fully understand the nature of the respondent's business; to obtain information on respondent's involvement in ML/TF/PF and any sanctions imposed; (b) assess the measures related to the prevention of ML/TF/PF taken by the respondent; (c) obtain approval from the board or the specially authorised member of the board prior to establishing new correspondent relationships; (d) document the respective responsibility of the respondent in the field of prevention of ML/TF (Sec. 24(1) AML/CFT/CPF Law).

Criterion 13.2 – Credit institutions and other FIs, when establishing correspondent banking relationships should ascertain that the respondent, which uses services that enable direct access to accounts of the correspondent, has verified the identity and applied enhanced CDD to the customers that access those accounts, and, upon request, is able to provide relevant CDD data (Sec. 24(1)(5) AML/CFT/CPF Law).

Criterion 13.3 – Transactions and business relationship of FIs with the shell banks are explicitly prohibited under the AML/CFT/CPF Law (Sec. 21 and 21^{1}). Further, a credit institution shall not enter into or shall terminate the correspondent banking relationship with a credit institution or other FI which is known to be engaged in business relationships with a shell bank. Definition of a shell bank has minor shortcomings.

Weighting and Conclusion

R.13 is rated largely compliant. Latvia meets all criteria except one. Definition of a shell bank has minor shortcomings.

Recommendation 14 – Money or value transfer services

In its 2018 MER, Latvia was rated largely compliant with R.14, based on the following deficiencies: fines for unregistered/ unlicensed Money or Value Transfer Services (MVTS) activities were not dissuasive and MVTS providers were not required to monitor their agents for compliance with AML/CFT programmes. Latvian authorities inform that some non-material changes have been introduced, such as: sanctions framework has been revised, the Latvian post acquired a PI licence and is now regulated under Law on Payment Services and Electronic Money (LPSEM) and supervised by the Latvijas Banka from June 2019 therefore previous references in the MER 2018 to Latvian Post have been removed.

Criterion 14.1 – MVTS in Latvia can be provided by credit institutions, PIs, EMIs; these institutions should be licensed or registered by the Latvijas Banka (Sec. 4 LPSEM).

Criterion 14.2 – For conducting unlicensed/unregistered activities, a fine can be imposed on natural persons or on a legal person's member of the board fines ranging between EUR 285 to 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 (Art.1662 of the Administrative Violations Code). This lacks proportionality and dissuasiveness.

Criterion 14.3 – The Latvijas Banka supervises credit institutions, EMIs, PIs with AML/CFT/CPF requirements (Sec. 45(1) AML/CFT/CPF Law).

Criterion 14.4 – MVTS provider may offer services directly or through an agent, upon due notification of and non-objection by the Latvijas Banka (Sec. 27-28, LPSEM). The same Law establish rules for institutions registered in another EU Member State to open branches and operate through agents in Latvia, and for institutions registered in Latvia to conduct payment activities in another EU Member State, provided that the Latvijas Banka has agreed to such activity and has informed the supervisory institution of that EU Member

State (Sec. 31 and 32). Information on agents is published on the Latvijas Banka website (separately for PIs and EMIs).

Criterion 14.5 – An FI intending to operate through an agent shall submit a written application to the Latvijas Banka 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/TF (Sec. 27(4) LPSEM). It is not explicit that FIs have to monitor agents for compliance with AML/CFT programmes.

Weighting and Conclusion

R.14 is rated largely compliant. Latvia demonstrates a good level of compliance with MVTS' regulatory regime; however, the following deficiencies remain: (i) fines for unlicensed MVTS are not proportionate and dissuasive; (ii) it is not explicit that FIs have to monitor agents for compliance with AML/CFT programmes.

Recommendation 15 – New technologies

In the 2018 MER, Latvia was rated as largely compliant with R.15. National ML/FT risk assessments overlook identifying and assessing risks related to the development of new products and business practices, delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. Since then, R.15 has been amended significantly to include new requirements relating to virtual assets and VASPs.

Criterion 15.1 – Latvia has identified and assessed the ML/TF risks related to new technologies, products, and services (NRA2; FIU's 2022 "Virtual Assets: ML/TF/PF Risk Assessment"). REs are required to identify and assess the ML/TF risks associated with the business activities in which they engage, before introducing changes in its services and products provided and delivery channels, as well as before introducing new technologies or services (AML/CFT/CPF Law, Sec.8(3)). The notion "new technologies and services" in the mentioned provision does not cover the terms "new products" and "new delivery mechanisms".

Criterion 15.2 – (a) According to Sec.8(3), the assessment of ML/TF risk as set out in c.15.1 has to be undertaken before introducing changes in the products, practices and prior to introduction of new technologies or services.

(b) The REs have to take measures for improving their internal control systems when they plan to introduce changes in its operational processes, governance structure, services and products provided and their delivery channels, customer base or geographical regions of operation, as well as before introducing new technologies or services (AML/CFT/CPF Law, Sec.8(3), Clause 2).

Criterion 15.3 – Following the amendments of AML/CFT/CPF Law in July and October 2024, the new definition of crypto assets and crypto asset service providers is aligned with the FATF definition of virtual assets and VASPs, covering both legal and natural persons (AML/CFT/CPF Law, Sec.1(1), Clauses 2^2 & 2^3).

(a) At EU level, the European Commission conducts and publishes an assessment of the risks of ML and TF affecting the internal market and relating to cross-border activities in line with the requirements of the Directive (EU) 2015/849 as amended by Directive (EU) 2018/843 (Art. 6) that also identifies and assesses the risks emerging from virtual assets and the activities and operations from VASPs. The EU level risk assessment shall be updated by a report at least every two years.

Since 2019, the FIU Latvia has conducted an annual risk assessment of the ML/TF/PF risks of virtual assets and VASPs, as part of the assessment of threats of new and emerging technologies. This obligation to produce an annual assessment is codified in the AML/CFT/CPF Action Plan for 2023-2025 (CoM Order No 940 "On the Action Plan to Prevent ML/TF/PF 2023-2025", adopted December 2022). NRA2 also assessed the risks associated with VAs and VASPs. NRA2 concluded that foreign VASPs pose a significantly higher risk than domestic VASPs (10.2.4 of NRA2).

(b) In response to the identified risks Latvia has implemented, or is in the process of implementing, a number of risk mitigation measures, including the following:

- VASPs are subject to registration requirements, AML/CFT/CPF Law obligations and supervision (Sec. 46 (1), Clause 16) implementing the AML/CFT/CPF Action Plan 2020-2022 Measures.

- as of 1 July 2024, crypto-asset service providers are required to conduct CDD before conducting an occasional virtual currency transaction in the amount of EUR 1 000 or above (AML/CFT/CPF Law, Sec. 11 (1), Clause 7).

Moreover, the AML/CFT/CPF Action Plans for both, 2020-2022 and 2023-2025 include specific action points focusing on mitigating risk related to virtual assets and VASPs, including:

- Increasing effectiveness of the supervisory system for VASPs by implementing the Crypto-asset Services Law and introducing a licensing regime.

- Developing regulatory framework for virtual assets.

- Obtaining a virtual asset investigation software for the FIU to enable effective tracing of criminal flows in the virtual assets, which is currently being introduced.

(c) VASPs are required to take the necessary steps to identify, assess, manage and mitigate their ML/TF/PF risks as required by criterion 1.10, 1.11 and 1.13 (AML/CFT/CPF Law, Sec. 6 (1), Section 8(2), see also Sec. 11.1 (4) and (5) of AML/CFT/CPF Law specifying the risk mitigation measures that VASPs must, take into account).

Criterion 15.4 – (a) The definition of crypto-asset service providers (VASPs) amended in July 2024 covers all five activities as defined by FATF (AML/CFT/CPF Law, Sec. 1(2.^{3})). VASPs are required to register with the SRS (AML/CFT/CPF Law, Sec.45(3)). In accordance with Sec.45(3) of AML/CFT/CPF Law, subjects to the supervision of the SRS shall, within 10 working days after being registered in the ER or the Register of Taxpayers of the SRS, submit a report to the SRS on the nature of their activities. When providing crypto asset services, both legal and natural persons have the obligation to register at the SRS this type of activity to fall under its supervision. It is preceded and follows the obligation to register as taxpayer, either through registration with ER for defined types of legal persons, or directly with SRS for other categories of legal persons and all natural persons (Law on Taxes and Fees, Sec.1(4) and Sec. 15^{1}).

(b) Amended Sec.10^{1}(1) & (1^{1}) of the AML/CFT/CPF Law prevents criminals from holding (or being the BO of) a significant or controlling interest and from being members of the senior management or the compliance officer of the RE. There is no formal definition of the term "impeccable reputation". However, authorities consider a person to have an "impeccable reputation" if no negative information is detected and the person has no criminal record when applying for a senior management position or a position of responsible for compliance. However, (i) these requirements do not cover associates of persons with criminal record; (ii) the provisions do not apply to all individuals holding the management functions.

Criterion 15.5 – Failure by covered VASPs to register with SRS when carrying out the activities in c.15.4(a) can result in proportionate and dissuasive sanctions (see R.35 for violations of AML/CFT/CPF Law). The SRS has a system in place to monitor and identify natural or legal persons conducting VASP activities without the required registration. It is empowered to impose administrative fines or order the cessation of unauthorised activities. Authorities explained that during its bi-monthly risk analysis of supervised entities, the SRS considers various criteria and sources of information, including inputs from other SRS departments, public authorities, and individuals. It also monitors publicly available information, such as social media and advertisement portals, to detect unregistered activities.

Criterion 15.6 – (a) SRS is the competent authority for the registration and supervision of VASPs (AML/CFT/CPF Law, Sec.46(1)). SRS has obligation to implement supervisory measures on the basis of ML/TF/PF risk assessment (AML/CFT/CPF Law, Sec.46(1), Clause 11). This entails ensuring that frequency of on-site and off-site inspections corresponds to the risk assessment. SRS has an automatic risk categorisation matrix for the classification of its subjects, including VASPs, according to risk criteria that are reviewed at least annually (SRS Internal Regulation on Procedure for risk analysis No.6, Sec. 2 and 11). The SRS is in terms of Sec.46(1) Clause 12, required to regularly revise the RE's risk assessment including when there are significant events and changes in the operational processes or governance structure of the VASPs. Regarding the risk-based supervision capacities of the SRS, considerations under R.26 apply.

(b) SRS has powers to supervise and ensure that VASPs comply with the AML/CFT requirements, including authority to conduct onsite inspections and compel the production of information required for AML/CFT supervision (AML/CFT/CPF Law, Sec.47). Failure to provide information to the SRS for supervisory purposes is subject to enforcement measures as set out under Sec.78(1)- see R.35. SRS is empowered to

impose disciplinary and financial sanctions on VASPs for the violations of AML/CFT requirements, including suspension of activity or cancellation of VASP registration (AML/CFT/CPF Law, Sec.78(1))- see R.35. These powers are further explained under the analysis of R.27.

Criterion 15.7 – SRS has developed guidelines for all REs under its supervision. This includes sector specific guidance for VASPs to assist them in undertaking risk assessments and comply with AML/CFT obligations (Sec.2.8 and 3.12 of SRS Guidelines), as well as sector specific red flags and typologies to help VASPs in identifying suspicious transactions in virtual assets (Sec.7.6. of SRS Guidelines). The SRS communicates with its supervised entities primarily through video seminars and e-learning platforms. Authorities advised that the SRS annually publishes training materials and e-learning courses in the EDS on various aspects of the AML/CFT/CPF Law and Law on Sanctions, including theoretical information and Q&A sections; examples include courses on AML/CFT/CPF Law application, sanctions implementation and reporting infringements that are available to all REs, including VASPs. There were no specific seminars or e-learnings prepared and conducted specifically for VASPs. Authorities advised that the SRS communicates with VASPs primarily through annual inspections, providing consultations, clarifications, and feedback on AML/CFT/CPF compliance (AML/CFT/CPF Law, Sec.46(2)). However, the legislation does not specify whether SRS is required to provide feedback to VASPs to help them implement national measures against ML/TF.

Criterion 15.8 – (a) See analysis for c.35.1; (b) See analysis for c.35.2.

Criterion 15.9 – VASPs are subjects of the AML/CFT/CPF Law and bound by the AML obligations mirroring the requirements set out in R.10-R.21 and the analysis and shortcomings identified for these recommendations likewise apply.

(a) as of 1 July 2024, VASPs must conduct the CDD before the occasional transactions where the crypto asset service is provided and it equals or exceeds EUR 1 000 (AML/CFT/CPF Law, Sec.11(1), Cl. 7).

(b) VASPs are subject to wire transfer rules as follows:

(i) & (ii) Originating and beneficiary VASPs must obtain the relevant identifying information for the originator and the beneficiary of any crypto-asset transfer (Sec.11^2(1)&(2)). The amount and type of information to be collected depends on the value of the transfer (whether less or more than EUR 1 000). The following information must be collected and transmitted by the covered originating VASP in case of transfers that equal or exceed EUR 1 000: (i) the initiator's name, account number, address, national or customer identification number, or date and place of birth; (ii) the recipient's name and account number (AML/CFT/CPF Law, Sec.11^2(1)). The mentioned information must be transmitted promptly to the beneficiary VASP or FI (Sec.11^2(6)). In case of transfer below EUR 1 000 such required information consists of name of the initiator and the beneficiary, and the unique identifier of the transaction (Sec.11^2(2)) and is to be transmitted upon the request of the beneficiary VASP or other FI (Sec. 11^2(7)). The originator and beneficiary VASP is subject to CDD obligations which entail the verification of identification information for clients and BOs where a business relationship is established or where an occasional VC transfer of EUR 1 000 or more is carried out, or regardless the amount of transfer when there is suspicion that the customer is involved in ML/TF/PF (Sec. 11^2(5)). The collected information on the originator and beneficiary has to be made available to the competent authorities (SRS, FIU and LEAs) immediately upon request and regardless of the amount of the transfer (Sec. 11^2(8)). There is no specific provision setting out that the information that is transmitted must be held by the covered originating and beneficiary VASP.

(iii) The beneficiary VASP is required to perform post-event or real time monitoring in case of transfers which lack required originator or beneficiary information (Sec.11^2(10)). Likewise, the beneficiary VASPs are required to have risk-based policies and procedures in order to determine whether to reject or suspend a VC transfer and take appropriate follow-up up actions (Sec.11^2(11)). Where information is missing, the originating VASP has three days in which to submit the required and accurate information (Sec.11^2(9)), however there is no provision prohibiting conclusion of the transfer without this information.

TFS obligations, including freezing requirement apply to VASPs in the same manner as they apply to other REs. See analysis for R.6 and R.7.

(iv) The obligations explained under (i)-(iii) apply to all institutions that carry out VA transactions, hence including FIs when sending or receiving VA transfers on behalf of a customer (AML/CFT/CPF Law, Sec.1(2)[3]defining VASPs).

Criterion 15.10 – TF/PF TFS obligations apply to VASPs in the same manner as they apply to other REs. Please refer to analysis of criteria 6.5(d), 6.5(e), 6.6(g), 7.2(d), 7.2(e), 7.3 and 7.4(d) as they apply to VASPs.

Criterion 15.11 – The international co-operation measures and exchange of information described in R.37 to R.40 apply to activities related to VAs or concerning VASPs.

Weighting and Conclusion

Latvia has identified and assessed ML/TF risks related to new technologies, products, and services. VASPs are required to be registered and, as of July 2024, all five activities described by the FATF standard are encompassed by the definition of VASPs. However, implementation of AML/CFT obligations has minor shortcomings due to the applicable deficiencies identified under R.10-21 and those regarding the VA transfers. Feedback mechanisms for VASPs are not specified in the legislation. **R.15 is rated largely compliant.**

Recommendation 16 – Wire transfers

In the 2018 MER, Latvia was rated largely compliant with R.16 due to the following deficiencies: (i) MVTS providers are not required to take into account all information from both the ordering and beneficiary sides (only missing or incomplete information on the originator or the beneficiary); (ii) MTVS providers are not required to submit an STR in all countries affected by a suspicious wire transfer and make the relevant transaction information available to the FIU.

Criterion 16.1 – Art.4 of Regulation (EU) 2015/847 implements partially the FATF requirement regarding all cross-border wire transfers exceeding EUR 1 000 to be always accompanied by required and accurate originator information, as well as by required beneficiary information. Transfer of funds that equal EUR 1 000 are not covered by Regulation (EU) 2015/847, however, this is considered as minor shortcoming.

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.

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.

Criterion 16.4 – According to Art.6 of Regulation (EU) 2015/847, FIs need not verify the information on the originator unless, inter alia, they have reasonable grounds for suspecting ML/TF.

Criterion 16.5 & 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.

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 EU 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/TF purposes. That further retention period shall not exceed five years.

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.

Criterion 16.9 –Intermediary FI is required to ensure that all the information received on the originator and the beneficiary, that accompanies a transfer of funds, is retained with the transfer (Regulation (EU) 2015/847, Art.10; FCMC Regulation No. 144, Par.13).

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.

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.

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.

Criterion 16.13 – 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.

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.

Criterion 16.15 – 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.

Criterion 16.16 – Regulation EU 2015/847 applies to MVTS providers established in the EU or EEA that execute fund transfers, whether they operate directly or through their agents (Regulation (EU) 2015/847, Art. 2(1)). MVTS providers ensure that their branches, agents, and subsidiaries providing financial services in Member States and third countries comply with Latvian ML/TF prevention requirements (AML/CFT/CPF Law, Section 3 (2)).

Criterion 16.17 – (a) MVTS provider controlling both the ordering and beneficiary institutions, is required to take into account missing or incomplete information on both the ordering and beneficiary sides in order to determine whether an STR has to be filed (Regulation EU 2015/847, Art. 9 & 13).

(b) There is no requirement for MVTS to file a STR in each country affected by the suspicious wire transfer and to make relevant transaction information available to the FIU.

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

The following shortcomings apply: (i) transfers of funds that equal EUR 1 000 do not fall under the scope of wire transfer regulation (c.16.1); (ii) MVTS providers are not required to submit a SAR in all countries affected by a suspicious wire transfer and make the relevant transaction information available to the FIU (c.16.17(b)). **R.16 is rated largely compliant.**

Recommendation 17 – Reliance on third parties

In the 2018 MER, Latvia was rated largely compliant with R.17 due to the following deficiencies: (i) relying parties are required to immediately receive, but not immediately obtain, necessary information concerning CDD measures; (ii) compliance with the AML/CFT/CPF 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.

Criterion 17.1 – According to Sec.29(1) AML/CFT/CPF Law, a credit or financial institution is entitled to recognise and accept outcomes of certain CDD measures[126] carried out by acceptable third parties,[127] if it: 1) is able to immediately obtain, if necessary, 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/CPF Law, and that it is supervised and controlled at least to the same extent as laid down in the AML/CFT/CPF Law. The amended Sec.29 stipulates that relying parties are required to obtain immediately, though only, if necessary, the obligatory information concerning the mentioned CDD measures. In addition, compliance with the Latvian AML/CFT/CPF Law does not necessarily amount to compliance with the requirements set out in the R.10 and R.11.

Criterion 17.2 –Sec.29(1) AML/CFT/CPF Law defines that credit or financial institutions are entitled to recognise and accept outcomes of certain CDD measures carried out by acceptable third parties, if they assess and mitigate risks related to the third party or its country of operation, considering high-risk countries as defined by Sec.1(12[1]) AML/CFT/CPF Law.

Criterion 17.3 – According to Art.29(4) AML/CFT/CPF 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/TF prevention requirements applied within the group comply with the requirements of the Latvian AML/CFT/CPF Law; 3) effective implementation of these requirements is supervised at group level by a competent authority of the home EU Member State or of the third country. It should be noted that compliance with the Latvian AML/CFT/CPF Law does not necessarily amount to compliance with the requirements set out in R.10 to R.12 and R.18 (see analysis R.10-R.12 and R.18).

Weighting and Conclusion

The relying parties are not always required to obtain immediately, but only, if necessary, the obligatory information concerning CDD measures. Compliance with the AML/CFT/CPF 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 largely compliant.**

Recommendation 18 – Internal controls and foreign branches and subsidiaries

In the 2018 MER, Latvia was rated largely compliant with R.18 due to the deficiencies: (i) the position of the Board member lacks relevant powers and responsibilities to qualify for that of the compliance officer appointed at the management level as required by the FATF standard; (ii) employee screening requirement applies only to banks and PI/EMIs; (iii) independent audit function availability is made contingent on an undefined number of employees of the RE.

Criterion 18.1 – Sec.6(1) AML/CFT/CPF Law defines that the REs, in conformity with the type and extent of their activity, shall perform and document the assessment of the ML/TF risks and, on the basis of such assessment, shall establish an internal control system for AML/CFT, including by developing and documenting the relevant policies and procedures.

a) Compliance management arrangements – REs are required to appoint one or several employees, including from senior management, who are responsible and directly liable for compliance with the requirements of the Law (AML/CFT/CPF Law, Sec.10(1)). Credit institutions, licensed PIs, licensed EMIs and investment firms are required, in addition to appointing compliance officer, also appoint a member of the Board responsible for supervision and practical fulfilment of AML/CFT requirements by the respective legal person (AML/CFT/CPF Law, Sec.10(2). Nonetheless, it does not appear that the position of the Board member, in terms of relevant powers and responsibilities, qualifies as that of a compliance officer appointed at the management level as required by the FATF Standard.

b) Employee screening –The obligation to develop a policy for suitability of compliance officers and the

126. 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.
127. Which are defined as credit and financial institutions in Member States or in third countries.

responsible Board member does not apply to FIs other than banks, PI and EMIs.

c) On-going training – Sec.9 AML/CFT/CPF Law requires the REs to ensure that employees are aware of the ML/TF risks and the regulatory enactments governing the prevention of ML/TF, and to conduct regular training of employees on these matters.

d) Independent audit function – The availability of independent audit function is made contingent on an undefined number of employees of the RE.

Criterion 18.2 – Financial groups are required to implement group-wide AML/CFT programmes, which must be applicable and appropriate to all branches and majority-owned subsidiaries of the financial group. (AML/CFT/CPF Law, Sec.1(2[1]); Sec.3(2)).

(a) Sec.3(2) of the AML/CFT/CPF 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/TF risk management, as well. Such group-wide policy and procedures shall be effectively implemented in the EU Member States and third countries also at the level of branches and majority-owned subsidiary undertakings.

(b) Sec.3(2 [1]) AML/CFT/CPF 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.

(c) Sec.3(2) AML/CFT/CPF Law defines that the REs belonging to a certain group shall implement, inter alia, the group-wide personal data processing policy, as well as the information exchange policy and procedures established within the group for AML/CFT purposes.

Criterion 18.3 – According to Sec.3(3) AML/CFT/CPF Law, the REs, whose branches or legal representatives operate (offer services) in another EU Member State, shall ensure that those branches and legal representatives comply with the requirements of the legal framework of the relevant EU Member State in the field of AML/CFT.

Sec.3(3[1]) of the AML/CFT/CPF Law defines that where the REs have branches or majority-owned subsidiary undertakings in EU 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 AML/CFT/CPF 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 EU Member States or third countries take additional measures to effectively restrict the ML/TF risk and inform their SCA in Latvia.

Weighting and Conclusion

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 RE. **R.18 is rated largely compliant.**

Recommendation 19 – Higher-risk countries

In the 2018 MER, Latvia was rated largely compliant with R.19. The assessment identified a deficiency in proactively advising REs about weaknesses in the AML/CFT systems of other countries.

Criterion 19.1 –REs are required to apply EDD in case of establishing business relationships or conducting occasional transactions whenever, inter alia, higher ML/TF/PF risk is present (AML/CFT/CPF Law, Sec.22(2)). Specifically, Sec.11(3) ensures that REs account for risks associated with customers or BOs linked to high-risk jurisdictions, including those no-cooperative in international AML/CFT efforts for which certain actions are called for by the FATF.

Criterion 19.2 –The legal framework equips SCAs with the necessary empowerments and instruments enabling the application of countermeasures proportionate to the risks when called upon to do so by the FATF or when decided so by the state authorities (AML/CFT/CPF Law, Sec.46(11) & (12), Sec.47(1), Sec.78(1)).

Criterion 19.3 – The Latvijas Banka website provides links to the FATF website. Latvijas Banka provides monthly updates to the market participants on recent news (including the ones from websites of FATF, MONEYVAL, Basel Committee, EBA, etc.). The AT 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 FIs are advised of concerns about weaknesses in the AML/CFT systems of other countries.

Weighting and Conclusion

Minor deficiency remains in the proactive communication of concerns to FIs about weaknesses in the AML/CFT systems of other countries. **R.19 is rated largely compliant.**

Recommendation 20 – Reporting of suspicious transaction

In the 2018 MER, Latvia was rated largely compliant with R.20, as the AML/CFT/CPF Law did not appear to cover the element of carelessness or negligence in relation to the obligation to report in the presence of suspicion.

Criterion 20.1 **–** Latvian AML/CFT/CPF Law defines the obligation of the REs to notify the FIU without delay (i.e. within 24 hours) regarding each unusual or suspicious transaction (Sec.30, AML/CFT/CPF Law). 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 TF or an attempt to carry out such actions, but not yet involved in a committed or attempted transaction.

The AML/CFT/CPF 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 (Sec.4(1) AML/CFT/CPF Law). Moreover, the AML/CFT/CPF Law stipulates, that funds owned by or being under direct or indirect control of the persons included in the lists of persons related to terrorism or proliferation are considered to be proceeds of crime regardless of their legitimate origin (Sec.4(3), AML/CFT/CPF Law). Finally, the AML/CFT/CPF Law prescribes to recognise a crime as ML even in cases when the predicate offense has been committed outside Latvia recognises ML as such irrespective of whether or not the exact criminal offence, from which the proceeds have originated, has been identified (Sec.5(2) and Sec.5(2.1), AML/CFT/CPF Law).

While addressing the element of reporting in the presence of suspicions ("a suspicious transaction" or "funds creating suspicions"), this does not appear to cover the element of carelessness or negligence this included the situations where there are reasonable grounds for suspicions, which are nevertheless neglected.

Latvian regulations establish the indicators for unusual transactions, as well as the procedure and the form 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. Latvian regulations also define "red flags" for credit institutions to identify suspicious transactions.

Criterion 20.2 – The obligation to report covers all suspicious transactions, included the attempted ones, regardless of the amount of the transaction. Moreover, Latvian regulations require 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

While addressing the element of reporting in the presence of suspicions, the AML/CFT/CPF 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 largely compliant.**

Recommendation 21 – Tipping-off and confidentiality

In the 2018 MER, Latvia was rated compliant with R.21.

Criterion 21.1 – According to Sec.40 AML/CFT/CPF Law, if the RE has reported in good faith to the FIU in compliance with the requirements of the AML/CFT/CPF Law, irrespective of whether or not the committed or attempted ML/TF 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 RE, such reporting shall not be deemed as disclosure of confidential information and, therefore, the RE – 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).

Moreover, actions of the REs in compliance with the requirements of the AML/CFT/CPF Law may not be qualified as a violation of the norms regulating the professional activity or the requirements of the SCAs.

Criterion 21.2 – Sec.38 AML/CFT/CPF Law prohibits the REs – including its management and employees – to notify the customer, BO, as well as other persons (except for SCAs) 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/TF.

Sec.32(1) of the AML/CFT/CPF 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/TF, or that the funds are directly or indirectly obtained in the result of a committed or attempted criminal offence, including TF. 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

Latvia is compliant with R.21.

Recommendation 22 – DNFBPs: Customer due diligence

In its 2018 MER, Latvia was rated partially compliant with R.22, based on deficiencies identified in R.10, 11, 12, 15 and 17 which are equally relevant to DNFBPs. In FUR 2019, most of the deficiencies have been addressed and rating upgraded to largely compliant.

Criterion 22.1 – Reference is made to the analysis for R.10 on the general coverage of CDD requirements within Latvian legislation.

a) Casinos – The organisers of lotteries and gambling as REs, are required to comply with the CDD requirements, particularly when they engage in transactions[128] 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 (AML/CFT/CPF Law, Sec.11(4)).

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. Real estate agents comply with the requirements set out in R.10 with respect to both the purchasers and the vendors of the property (AML/CFT/CPF Law, Sec. 11(9)).

c) DPMS –Other legal or natural persons trading in precious metals, precious stones and other goods are required 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 carried out in a single operation or in several mutually related operations (AML/CFT/CPF Law, Sec.11(5)).

128. Including the cases when the customer wins, buys the means for participation in the game or lottery tickets, or exchanges currency for such purpose.

d) Sworn lawyers, notaries, other independent legal professionals and accountants (tax advisors) are required to apply CDD measures when they act 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 FIs; d) creating, managing or providing operation of legal arrangements, as well as organising contributions necessary for the creation, operation or management of legal persons or legal arrangement. Nonetheless, according to Sec.11(8) AML/CFT/CPF Law these categories of DNFBPs 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. This exemption diverges from the FATF-defined legal professional privilege stipulated for STR reporting only.

e) Trust and company service providers – 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 which are subject to CDD requirements, without specifying the situations in which they obtain the said status. Latvian law does not recognise trusts as a distinct type of legal arrangement.

Criterion 22.2 – Reference is made to the analysis for R.11 on the general coverage of record-keeping requirements within Latvian legislation applying to all subjects of the AML/CFT/CPF Law, including DNFBPs.

Criterion 22.3 – Reference is made to the analysis for R.12 on the general coverage of PEP requirements within Latvian legislation applying to all subjects of the AML/CFT/CPF Law, including DNFBPs (AML/CFT/CPF Law, Sec.25).

Criterion 22.4 – Reference is made to the analysis for R.15 on the general coverage of new technologies requirements within Latvian legislation applying to all subjects of the AML/CFT/CPF Law, including DNFBPs.

Criterion 22.5 – Reference is made to the analysis for R.17 on the general coverage of third-party reliance requirements within Latvian legislation. According to Sec.29 AML/CFT/CPF Law, only credit and FIs among the REs are permitted to recognise 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.[129] Thus, this permission does not extend to DNFBPs; they are not allowed to recognise or accept outcomes of CDD carried out by the acceptable third parties.

Weighting and Conclusion

Reference is made to the deficiencies identified with regard to R.10, 11, 12, 15 and 17. 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 largely compliant.**

Recommendation 23 – DNFBPs: Other measures

In the 2018 MER, Latvia was rated largely compliant with R.23 due to deficiencies identified with regard to R.18-21. In addition, the requirement to have employee screening procedures did not apply to any DNFBPs.

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.

129. The acceptable third parties are defined as credit and financial institutions.

Criterion 23.1 – Reference is made to the analysis for R.20 on the general coverage of STR reporting requirements within Latvian legislation.

Sec.31^4(1) AML/CFT/CPF Law requires all DNFBPs subject to qualification as REs as set out in c.22.1 (see above), to immediately report on every suspicious transaction to the FIU. Sec.31^4(5) of the AML/CFT/CPF Law contains a legal privilege-based exemption to the reporting obligation for sworn lawyers, notaries, other independent legal professionals and accountants (tax advisors) where 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/CPF. 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.

Criterion 23.2 – Requirements and shortcoming described in the AML/CFT/CPF Law for covered FIs under R.18 are equally applicable to covered DNFBPs. The requirement to have employee screening procedures, as set out in Sec.10(21) of the AML/CFT/CPF Law does not apply to any DNFBPs.

Criterion 23.3 – The requirements concerning high risk countries are equally applicable to both covered DNFBPs and FIs (see R.19).

Criterion 23.4 – Requirements described in the AML/CFT/CPF Law for covered FIs under R.21 are equally applicable to covered DNFBPs.

Sec.40(4) of the AML/CFT/CPF 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

Reference is made to the deficiencies identified with regard to R.18 and R.20. In addition, the requirement to have employee screening procedures does not apply to any DNFBPs. **Latvia is rated largely compliant.**

Recommendation 24 – Transparency and beneficial ownership of legal persons

In its 2018 MER Latvia was rated largely compliant due to: lack of explicit requirement placed on companies to keep basic information and information on shareholders and members in Latvia; not all types legal persons were required to keep BO information accurate and up-to-date; there was no specific legal provision requiring 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; lack of clarity whether records' retention requirement captures BO information (for dissolved companies); there was no explicit prohibition against a person acting as a nominee director; no specific provisions concerning international exchange of information on shareholders; no processes in place to assess the quality of international assistance regarding basic and beneficial information received.

Criterion 24.1 – The following legal persons exist in Latvia: (a) Companies: LLC, stock company, European company; (b) Foundation, limited partnership; (c) Other types of legal persons: Association, Trade Union, co-operative society, general partnership, religious organisations, political party, and European Economic Interest Grouping. The requirements of Recommendation 24 apply to all legal domestic persons in Latvia. All legal persons are required to register with the relevant register, and these registers are brought together in the ER, Section 1 and $2^{1\text{-}20}$ of the ER Law. Legal persons only have legal status once they are registered: Section 135(2) Commercial Law for LLCs and JSCs, Section 3 Associations and Foundations Law for foundations, associations and trade unions, Section 78(1) Commercial Law for Limited Partnerships and general partnerships, Section 3(2) Co-operative societies Law for co-operative societies, Section 13(1) Law on Religious Organisations for religious organisations, Section 3 Law on Political Parties for political parties. The laws governing general partnerships extend to EEA Interest groups, in so far as they are not otherwise provided for by the laws covering European Economic Interest Groups, namely Council Regulation No 2137/85 and European Economic Interest Grouping Law. (d) Foreign legal persons assessed to present a ML/TF risk and have sufficient nexus to Latvia are those with a branch or representative office in Latvia,

foreign legal persons with a domestic tax liability and those with account with Latvian REs. These foreign legal persons are subject to the requirements of c.24.3(b) and c.24.10.

Criterion 24.2 – Information covering all types of domestic legal persons, including the forms, basic features and the creation process is publicly available[130] as well as information on how to obtain and record basic and BO information.

Criterion 24.3 – Article 51(1) AML/CFT/CPF Law requires the FIU to conduct risk assessments. The risks associated with domestic legal persons were considered in the NRA2 (covering 2020-2022) and previously the NRA1 (covering 2017-2019). Some types of legal persons, such as foundations and political parties, are considered as part of the assessment of NPOs (Section 9 NRA2). The NRA2 examines the financial flows of foreign legal persons as well as analysis of foreign legal person BOs, see section 9.2.14-26 of NRA2. Mitigations are in place in relation to identified risks, including BO disclosure requirements for foreign legal persons who register a branch or representative office in Latvia (S. 18^1(1),18^2(7) AML/CFT/CPF Law), and requiring foreign legal persons with tax liability who are not required to register with the ER to register with the SRS (Section 15.1 Law on Income Taxes and Fees). The Accounts Register Law (section 5(2)(5)) requires information on foreign legal persons who have accounts with Latvian FIs to be available on the Accounts Register. If beneficial ownership information is collected on a foreign legal person customer, the following information is required to be recorded: the given name, surname, date of birth of a natural person, the number of personal identification document, the name of the issuing country. Failure to comply with these requirements can result in a warning, financial penalty, restriction in permission to provide services or cancellation of a licence (Section 196 (1) of the Credit Institution Law and Section 56 (1) of the Law on Payment Services and Electronic Money). These mitigations are largely appropriate in the context of Latvia, however, the risk assessment for foreign legal persons, whilst sufficient, is still nascent, especially regarding in depth consideration of geographical risks. See more at IO.5

Criterion 24.4 – All companies created in Latvia are required to be registered in a company registry (ER) (see also Criterion 24.1). The information collected and recorded for commercial companies covers broadly basic information requirements listed at c.24.5(a) (Sec. 8(3)(4), 149, 187 Commercial Law). All information in the ER 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 societies covers the requirements under this criterion (Co-operative 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 the requirements under this criterion (Sec.13, 15, 26 and 92 Associations and Foundations Law).

Criterion 24.5 – (a) There is no explicit legal obligation on companies to record and hold the information listed in criterion 24.5(a), however, this information must be submitted to the ER within 14 days from a change (Section 16 Commercial Law, Section 8(3) Enterprise Register Law). (b) All legal persons with shareholders are required to maintain a register of their registered shareholders (Section 187 Commercial Law for LLCs, Section 234-235 Commercial Law for JSCs, Section 16 Co-operative Society Law for co-operative societies. Legal persons with members (as opposed to shareholders) are required to maintain membership registers (see Section 27(1) of Law on Political Parties and section 28(2) of the Associations and Foundations Law). These include names of shareholders, number of shares, categories of shares and voting rights. ***(c)*** There is no explicit legal obligation for companies to hold basic information within the country (either at its registered office or at another location notified to the ER). However, all companies are required to submit information about their shareholders to the ER. This requirement in relation to JSCs came into effect in July 2023, with a deadline of 30 September 2024 for filing.

Criterion 24.6 – BOs are defined by Section 1(1)(5) of the AML/CFT/CPF Law as a natural person who owns, in the form of direct or indirect participation, more than 25 per cent of the capital shares or voting stock of the legal person or who directly or indirectly controls it. Indirect control is not defined in the AML/CFT/CPF Law, but guidance is available from the ER on its website and in the Latvijas Banka *Guidelines for the Establishment of the Internal Control System for Anti-Money Laundering*.

(a) Legal persons, partnerships and foreign subjects are required to store information on BOs. Adequacy, accuracy and up-to-date of BO information is ensured by the AML/CFT/CPF Law stipulating details of BO

130. Available at https://www.ur.gov.lv/en/register/.

information that has to be kept, requiring continuous update of such information and documentary justification of the control exercised (Sec.18^1(4) AML/CFT/CPF Law). In addition, natural persons are required to report their BO status to the legal person, partnership or foreign subject (Section 18^1 (1), AML/CFT/CPF Law).

As for the co-operation with the competent authorities, LEAs have power to request information from any person when carrying out their duties and conduct removal and search in case of non-co-operation (CPL, Section 190(1-2)).

There is no specific legal obligation placed on legal persons to co-operate with FIs/DNFBPs to provide accurate, adequate and up-to-date information.

(b) Latvia has in place a company register: the ER, see more at c.24.1. Latvia has had a registry since 1990 and has progressively included more types of legal person within the registry as well as extending information reporting requirements. No documented decision was made available to the AT regarding chosen mechanisms to source BO information that are most appropriate in Latvia given its risk, context and materiality.

(i-ii) Information on the registers is publicly available free of charge and may be efficiently accessed online. LEAs, FIU Latvia, the PO and SCAs all have direct access and administrative rights over information in the ER. Beneficial ownership information must be filed with the ER within 14 days of a change (Section 18^2(1) of the AML/CFT/CPF Law) and upon incorporation of a legal person (Section 18^2(2) of the AML/CFT/CPF Law). In addition to a public beneficial ownership register, REs are required to conduct CDD, including identifying the BOs (see Recommendation 10 and 22). FIs and DNFBPs are required to use information from the ER to determine the BO and, on the basis of risk assessment, to cross check this data by employing one or several additional means: statement from the customer on BO, information from IT systems, by determining BO on its own (Section 18(3) AML/CFT/CPF Law, see also Chapter 3 of Latvijas Banka's AML Guidelines on clarifying and verifying the BO). Where a relevant person establishes that BO information does not conform to information on the ER they must report the non-conformity within three days (Section 18(3^1) AML/CFT/CPF Law). The ER must then place a warning on the register (which is visible to all relevant persons, competent authorities and supervisors) within one day, which remains in place until the original notification is revoked, or law enforcement informs the ER that there are no grounds to believe that the BO information is false (Section 18(3^2 -3^3) AML/CFT/CPF Law).

(iii) REs are required, throughout the course of conducting CDD, identify and verify BO (Section 11, 18 of the AML/CFT/CPF Law). This enables BO information to be sourced from the FIs and DNFBPs. The discrepancy reporting mechanism, as described above, helps to ensure a level of accuracy and adequacy of BO information.

Criterion 24.7 – Legal persons. Legal persons and partnerships are required to store the information on BO (Section $18^1$4 AML/CFT/CPF Law), however, no period for retention is prescribed. No explicit requirement exists for the company (or its administrators, liquidators and other persons involved in the dissolution of the company) to maintain the BO information and records at least for five years the company ceases to exist or is dissolved.

ER. BO information on the ER must be held for exactly 10 years after the company has ceased to exist (Section 18^3(4) AML/CFT/CPF Law).

REs. REs must retain and store all information gathered during the course of CDD for a period of five years after the termination of a business relationship, or the execution of an occasional transaction (Section 37(2) AML/CFT/CPF Law).

Criterion 24.8 – Latvia has in place mechanisms to ensure that BO information is adequate, accurate and up to date. This includes risk-based verification of data submitted to the ER (including formalised rules) and a complimentary discrepancy reporting requirement on entities subject to the AML/CFT/CPF Law.

Adequate

(i) Registry. The following basic information, as a minimum, is required to be collected and transmitted to the registry: the name of legal person, proof of incorporation, legal form and status, the address of the registered office, basic regulating powers (articles of association), and a list of directors (Section 8, paragraph 3, paragraph 5 (1., 2., 4., 4.1 and 5), paragraph 7, Section 9, paragraph 1, Section 143, Section 144, Section

149, Section 187. and 187.1, Section 235 and 235.1 of the Commercial Law). The following information on BOs is required to be collected by legal persons and transmitted to the ER: name, personal identification number (if available), date and place of birth, number and date of issue of identity document, country and issuing institution of identity document, a nationality (in case of multiple nationalities, only the nationality declared in application is recorded) and country of permanent residence (Section 18^1(4) and 18^2(1) AML/CFT/CPF Law). Legal persons are also required to identify the means by which the natural persons exercise control and provide documentary evidence (Section 18^2(1) AML/CFT/CPF Law). Latvia also has in place a legal requirement for REs under the AML/CFT/CPF law to report discrepancies to the ER(see c.24.6(b)).

(ii) REs. REs are required to identify and verify the client legal person and BO by obtaining identification details on basic and BO information listed in the AML/CFT/CPF Law (see 10.8-10.10).

(iii) Companies holding BO information. Companies are not required to hold basic information (see c.24.5) but are required to hold adequate BO information (see c.24.6 (a) for more information).

Accurate

(i) Registry. Latvia takes a risk-based approach to the verification of information. All information submitted to the ER is subject to checks to ensure that the natural person's identity is real and that the documents provided are valid. Where the ER identifies an increased risk, for example, about the legal address, where individuals hold multiple roles across different legal persons, or potential tax compliance risks, the ER can ask the SRS to verify submitted information by cross referencing it with information held by the SRS. The verification mechanisms used by the ER are codified in the ER's internal procedures. The ER has the power to request further information from legal persons, (Section 18.2 AML/CFT/CPF Law) such as documents to justify the nature of ownership or control and documents to verify the validity of ID documents (for example, notarised documents).

(ii) REs. If BO information obtained by REs does not conform to the information in the ER, discrepancy report should be submitted (AML/CFT/CPF Law, Section 18(3^1)). This obligation does not extend to basic information. The legal duty to report discrepancies in BO information is placed on REs and supervisory authorities. This ensures additional level of accuracy of the information held in the ER and by the REs. It is not clear whether the information held in the ER database is checked against that held on the account register.

(iii) Companies holding BO information. No information was made available on the compliance monitoring mechanisms with the accuracy of basic and beneficial information held and reported by the legal persons. However, if the basic and BO information submitted to the ER is incomplete or lacks accuracy, the ER has the right to request further clarifications and postpone registration of the submitted documents (Sec. 8, the ER Law). Failure to provide information and/or provision of false information is subject to a criminal liability and is dealt with by LEAs (CL, 195^1), as well as by limiting voting rights, dividend payout and in severe cases – shareholder rights may be revoked (Sec. 136^1 Commercial Law).

Up to date

(i) Registry. Legal persons are required by law to notify the ER of changes within 14 days of the change (Section 18^2(1) AML/CFT/CPF Law).

(ii) REs. The above is complimented by a legal duty of REs under the AML/CFT/CPF Law to report discrepancies to the ER within three working days (Section 18(3^1) AML/CFT/CPF Law). REs are required to identify legal persons and their BOs and continuously update, store, and regularly evaluate documents, personal data, and information acquired through CDD in line with identified risks, and at a minimum, at least every five years (Section 13, 18(1-2) and 11(1)(5) AML/CFT/CPF Law).

(iii) Companies holding BO information. Legal persons are legally required to maintain a register of their registered shareholders (Commercial Law) and keep and update information on BOs (AML/CFT/CPF Law, 18.1(4)).

Criterion 24.9 – Information held in the registers. Information on the ER and SRS is publicly available, free of charge (see c.24.6(b)). Law enforcement, the FIU and AML/CFT supervisory authorities can obtain all documents held by the ER directly (Section 4(15)(4) the ER Law). Non-public information is available via direct access or upon request by competent authorities. Entities responsible for public procurement are able

to freely access the public facing information on the ER and SRS databases and request access to non-public (e.g., historic data) on the databases.

Information held by FIs, DNFBPs and companies. SCAs are able to request information from REs for the purposes of AML, CFT and CPF (Section 47(1)(2) AML/CFT/CPF Law). LEAs and the FIU have a general right to request information from any natural or legal person when carrying out their duties, which is applicable also to FIs, VASPs and DNFBPs and any legal person (Section 190(1) CPL). LEAs have a right to conduct a removal or search if a person is not co-operative (Section 190(2) CPL).

Criterion 24.10 – Latvia uses two mechanisms that enable it to access basic and BO information of foreign legal persons that may present a ML/TF risk in Latvia and which have a sufficient link to Latvia. Basic and BO information of non-resident companies with permanent establishments or resident offices in Latvia can be obtained through the SRS portal (direct and full access to the authorities). Legal persons who are customers of Latvian FIs (credit institutions, providers of payment services, savings and loan associations) can be identified using Latvia's Account Register (Section 5(2) of the Account Register Law requires the collection of this information). The information submitted to the account register does not cover all the elements constituting basic and BO information, however, is largely sufficient to identify a legal person or BO: i.e., for a legal person - name, registration number, country of registration; for a BO and authorised representative – name, date of birth. This information is accessed free of charge by Latvian competent authorities and the FIU upon a "justified request"[131] (Section 6 and 8(1), the Account Register Law). This allows Latvian authorities to identify FIs who hold CDD information on the foreign legal persons of interest. These measures are largely in line with the risks identified by Latvia.

Criterion 24.11 – Basic and BO information held on the ER is publicly available (Section 18^3(1) AML/CFT/CPF Law). Additional information, such as copies of documents, are available upon a justified request for a fee.

Criterion 24.12 – The issuance of new bearer shares in paper form is not possible under Latvian Law since 2008, and new issuance of any kind of bearer shares is not possible since 2022. The Commercial Law recognises two types of shares: registered shares and dematerialised shares. A registered stock is accounted in the register of stockholders, and a dematerialised stock is recorded in the central securities depository (Sec. 228 Commercial Law). Pre-existing bearer shares were converted into dematerialised shares as of 1 July 2023 and recorded in the central depository (Sections 2361-2363 Commercial Law). If shares were not registered, they no longer have legal effect. JSCs were required to submit all stocks, including bearer stocks not later than by 30 September 2024.

Criterion 24.13 – Only natural persons may be members of the executive or supervisory board (Sections 221(3), 295(1) and 304(2) of the Commercial Law) and are elected by a shareholder meeting, or by a Council meeting There is no explicit legal prohibition on nominee shareholders or directors. There is no explicit legal provision which requires a nominator to declare themselves as a nominator and for this to be registered on the ER. However, a natural person with the power to appoint a board member must declare themselves to the ER as a BO by virtue of exercising sufficient control (through means other than share ownership) and this information is publicly available. Provision of false information regarding a transaction and the true owner and true beneficiary of the financial resources or other property is a criminal offence (Sec. 195^1(1) CL).

Board members can formally delegate some elements of their duties/powers to a procurator. In these circumstances both the board member and the procurator are recorded publicly on the register as is the nature of this appointment. This arrangement is not considered to meet the FATF glossary definition of a nominee arrangement (see paragraph 135 of the FATF beneficial ownership guidance). If a situation arose where this arrangement met the threshold to be considered a nominee arrangement the disclosure requirements are in compliance with c.24.13(a).

There are no requirements for nominee directors and shareholders to disclose their status, to register or licence except for registration requirements applicable to TCSPs that might indirectly capture some providers of nominee services, however, this service is not explicitly disclosed when registering.

131. In accordance with the purpose of such requests.

Criterion 24.14 – *(i) Sanctions for* natural persons. For the failure to provide information, inadequate provision of information, or provision of false information to the ER, a warning or a fine of up to EUR 700 can be imposed on a natural person or a board member with or without deprivation of the board member's right to hold specific offices in commercial companies for a period up to three years (Section 3(2), Law on Administrative Penalties for Offences in the Field of Administration, Public Order, and Use of the Official Language). Failure of BOs natural persons to disclose their status to the legal person can result in a loss of a shareholder status, dividends or voting rights (CL, Sec. 195^1 and Commercial Law, Sec. 136^1).

*(ii) Sanctions for l*egal persons (companies). Legal persons have an obligation to determine BOs (Article 18^1(3) AML/CFT/CPF Law) and to file basic and BO information with the relevant registry (Article 18^2(1) AML/CFT/CPF Law). Failure by the legal persons to file this information leads to postponement or refusal of registration and simplified (expedited) liquidation process (AML/CFT/CPF Law transition rule 49). The ER possesses the authority to dissolve a legal entity through a simplified (expedited) liquidation process. The inability to register BO information, or the presence of other conditions indicative of economic inactivity (such as the absence of a board for more than three months, lack of a registered BO, inaccessibility at its legal address, or being marked for removal following a decision by the tax authorities), initiates the activation of the simplified (expedited) liquidation process by the ER (Section 314^1, Commercial Law). It is not clear whether sanctions are in place applicable to legal persons for failure to store and update BO information.

If capital companies (registered prior to December 1, 2017) fail to submit BO information to the ER, they are liquidated by the ER (transitional rule 49, AML/CFT/CPF Law).

Failure to register bearer shares can result into a dissolution of the company (transitional rule 70, the Commercial Law). These measures are yet to be applied starting from October 2024.

(iii) Sanctions for REs. REs are required to obtain accurate information on beneficial ownership as part of their CDD (see R.10). Sanctions for breaches of AML/CFT/CPF requirements, CDD (thus also identification and verification of a client and BO) being an integral part, are stipulated in AML/CFT/CPF Law (Art. 78(1)): publication of a sanction, warning, a fine for legal and natural person (double the profit or max EUR 1 million), restriction of business activity or dismissal from the position held; as well a fine on a legal person in the amount of up to 10 per cent of the total annual turnover (Art. 78(3)(1) of the same Law), see more at R.35.

Criterion 24.15 – (a) There is nothing in legislation that would unduly restrict the exchange of assistance of basic and BO information especially given the public availability of such information (see below).

(b) Latvia makes current basic and beneficial ownership publicly available, meaning there are no restrictions placed on the sharing of this information with international counterparts and information is kept in a manner that is readily accessible in both the ER and the SRS. The right to access all current information is conferred on any person in order to effectively limit ML/TF/PF risks (Section 18^3(1) AML/CFT/CPF Law). Information from SRS registers, for which the SRS is the primary source, are not available for public use. In such scenarios other institutions can enter into an agreement with SRS on receiving specific data that is necessary for the performance of the institution's functions. Historic data is available upon request.

(c) See c.24.15(b) above.

(d) Latvian authorities can use domestic powers in the execution of a foreign request on behalf of the foreign counterparts (Section 847 of the CPL).

(e) No information was provided by the competent authorities (except for Latvijas Banka) on monitoring the quality of assistance received.

(f) Authorities store basic and BO information obtained from foreign countries on internal systems which are subject to Internal Regulations on record keeping and information security.

(g) The competent authorities for MLA are stated in Section 846 of the CPL.

Weighting and Conclusion

Latvia has a generally robust framework in place to ensure transparency of and access to basic and beneficial ownership information. The remaining shortcomings are minor except for one relating to the absence of specific FATF prescribed measures concerning nominee arrangements which is considered moderate. The

latter does not have a fundamental weight given that nominee services are not widespread in Latvia and there are some other mitigants in place. **R.24 is rated largely compliant.**

Recommendation 25 – Transparency and beneficial ownership of legal arrangements

In the 2018 MER, Latvia was rated largely compliant with R.25, since there was 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.

Criterion 25.1 – Latvia law does not permit the creation of express trusts or other similar legal arrangements. Latvian residents natural persons and legal persons registered in Latvia acting as trustees or holding equivalent positions in a foreign legal arrangement are required to determine the BO and submit this information to the ER for registration within 14 days following the change of beneficial ownership, except in the case when BOs of the legal arrangement are registered on the register of a EU Member State (Section 18^4-18^5 AML/CFT/CPF Law). Authorities inform that this exemption derives from the EU AML Directive 2018/843. The registration requirements came into force in January 2024.

Criterion 25.2 – Latvian law does not permit express trusts or other similar legal arrangements.

Criterion 25.3 – *(a)* there are no trusts governed under Latvian Law thus c.25.2(a) is not applicable; (b/c) risk assessment of foreign law trusts for which the trustee or equivalent resides in the country (c.25.3(b)) and foreign legal arrangements that have sufficient links with Latvia (c.25.3(c)) has been completed. See IO.5 for more information.

Criterion 25.4 – *(a)* Trustees of foreign trusts, and those in equivalent positions, are required to store and continuously update information on all of the fields listed in Criterion 25.4(a), except class of beneficiaries and objects of a power and is silent on equivalent positions in similar legal arrangements other than trusts (AML/CFT/CPF Law, Art.18^4(1)). In addition, the AML/CFT/CPF Law uses singular terms for settlor, trustee, and protector. This creates ambiguity about whether information on all settlors, trustees, and protectors needs to be captured. The above information is not required to be held where the BOs are registered on the register of an EU Member State which is considered to be a minor limitation. (*b)* Trustees of foreign trusts are not required to obtain and hold basic and BO information of the parties to the trusts *(c)* Trustees of foreign trusts are not required to hold basic information on other regulated agents of, and service providers to, the trust or similar legal arrangement.

Criterion 25.5 – There is no specific requirement on trustees to hold information listed at c.25.4 for a period of five years after their involvement with the trust ceases. Trustees are required to submit the information referred to in c.25.4(a) to the ER (AML/CFT/CPF Law, Section 18^6) as of 2 January 2024. There is no requirement to hold or submit to the ER the information captured by c.25.4(b) and (c).

Criterion 25.6 – Trustees have a legal obligation to store and continuously update information on the ER (by submitting application) no later than 14 days of a change affecting beneficial ownership taking place (Section 18^5 ((1) and 3) AML/CFT/CPF Law). However, there is no requirement to hold or submit to the ER the information captured by c.25.4(b) and (c).

Criterion 25.7 – *(a)* There is no explicit legal obligation placed on trustees to disclose their status to FIs and DNFBPs. *(b-c)* There is no prohibition set out in the laws or enforceable means for the trustees to provide information regarding beneficial ownership, any assets held by the trust or similar legal arrangement. Trustees are required to declare BO information to the ER, which is publicly available.

Criterion 25.8 – (i) adequacy: Trustees are required to collect and transmit to the ER information listed in criterion c. 25.4(a) including the means through which control is exercised, certain minor limitations apply (see c.25.4(a)). (ii) accuracy: Trustees of a foreign law trust, and those in equivalent positions, are required to store and continuously update information BO information (Section 18^4 (1) AML/CFT/CPF Law). Latvian authorities inform that the same verification checks aimed at ensuring accuracy would apply to legal arrangements as for legal persons (see R.24). (iii) up-to-date information: trustees have a legal obligation to update information on the ER no later than 14 days of a change taking place (Section 18^5 (3) AML/CFT/CPF Law) (new requirements for registration came in force in January 2024). Where BOs of the legal arrangement are registered in other EU member state, Latvian authorities are reliant on EU countries to keep this information adequate, accurate and up-to-date. Shortcomings identified at c.25.7(a) (no requirement placed

on trustees to disclose their status to FI/DNFBP) and c.25.4(b-c) (no requirement to hold information on the parties to and other regulated agents to the trust/legal arrangement) have an impact here.

Criterion 25.9 – Basic and BO information is collected on the ER for foreign trusts with a Latvian resident trustee(s), except for EU-registered trusts and is accessible to LEAs, FIU, SCAs. No explicit legal requirements exist to identify trust assets. However, where the trust is a customer of a Latvian FI or DNFBP competent authorities can compel the disclosure of similar information if it exists amongst the RE's records.

Criterion 25.10 – Latvia competent authorities and FIUs have the power to access information held by the ER directly, including basic, BO information and permanent place of residence of the trustee (18^{6}(3)(6)(c) AML/CFT/CPF Law) on non-EU foreign trusts with Latvia resident trustees. The competent authorities also have the power(s) to compel the disclosure of CDD information from Latvia FIs and DNFBPs on their clients, including in relation to legal arrangements. Competent authorities have the power to compel information from natural and legal persons (Section190(1) of the CPL).

Criterion 25.11 – *(a-b)* Latvian resident trustees of a foreign law trusts are under an obligation to collect basic and BO information on all non-EU legal arrangements that they act as a trustee for. The exemptions relating to the EU-registered trusts have an impact on this criterion. For the failure to provide information, inadequate provision of information, or provision of false information to the ER, a warning or a fine of up to EUR 700 of fine can be imposed on a natural person or a board member with or without deprivation of the board member's right to hold specific offices in commercial companies for a period up to three years (Section 3(2), Law on Administrative Penalties for Offences in the Field of Administration, Public Order, and Use of the Official Language). Deliberately supplying false information in punishable with a custodian sentence of up to one year (rising to two years if substantial harm has been caused), or a financial penalty (Section 195^{1}CL). No information was made available to the AT on sanctions for unco-operative trustees (see c.25.(b)). *(c)* No information available on sanctions for failing to grant timely access to the competent authorities to information discussed at c.25.4 and 25.5 held by trustees.

Shortcomings identified at 25.4(b-c), c.25.5, c.25.7(a) have an impact on this criterion due to the absence of requirements a failure to comply with would result into a sanction.

Criterion 25.12 – Technically, current basic and beneficial ownership information on non-EU trusts with a Latvia resident trustee should be publicly and freely available as of January 2024 on the ER. In practice, no entries in the ER have been made to date. There are therefore no restrictions placed on the sharing of this information with international counterparts and information is kept in a manner that is readily accessible. The right to access all current information is conferred on any person in order to effectively limit ML/TF/PF risks (Section 18.3(1) AML/CFT/CPF Law). Latvian authorities are able to use domestic powers in the execution of a foreign request (Section 847 of the CPL). No information provided by the Latvian authorities on the procedures in place for law enforcement, the registry or other competent authorities for monitoring requests for basic and BO information. There is no publicly known agency responsible for execution of requests for BO information. Also see R. 37-40.

Weighting and Conclusion

The framework to ensure transparency and beneficial ownership of legal arrangements has several shortcomings that are minor and moderate nature. However, Latvian law does not permit the creation of express trusts or other similar legal arrangements and the country's exposure to foreign trusts is limited. **R.25 is partially compliant.**

Recommendation 26 – Regulation and supervision of financial institutions

In its 2018 MER, Latvia was rated partially compliant with R.26 based on the following deficiencies: market entry gaps for AIFs; limited coverage of criminal associations; gaps in risk-based supervision of some sectors. In 2019 FUR R.26 was re-rated as largely compliant due to the progress made, however, some deficiencies still remained: licensing related issues of AIFs and general coverage of criminal associations; limited supervision by the SRS, CRPC and currency exchange offices.

In 2021 a new Law on Latvijas Banka was adopted. The new law provides a framework for the Central Bank and the FCMC to function as a single entity as of 1 January 2023 – the Latvijas Banka. Therefore, the references to *the FCMC* as found in MER 2018 and FUR 2019 are replaced with references to the *Latvijas*

Banka in this MER; references to the *Latvian Post* have been also removed, the reasons explained at R.14.

Criterion 26.1 – Supervisory responsibilities in relation to FIs are defined in AML/CFT/CPF Law Section 45. The Latvijas Banka supervises credit institutions, EMIs, insurance companies and insurance intermediaries, private pension funds, investment firms, managers of AIFs, investment management companies, savings and loans associations, providers of re-insurance services, PIs, foreign currency exchangers. The SRS supervises FIs which are not supervised by Latvijas Banka and which provide credit services including financial leasing, if provision of services is not subject to licensing; issuance of guarantees; cash collection and virtual asset services. The CRPC supervises persons engaged in the provision of consumer credit services (this includes loans to legal persons) by way of business and are not holding other licenses, e.g., credit institution (Sec. 8 Consumer Rights Protection Law).

Criterion 26.2 – Core principle FIs are licensed with AIFs being an exemption (simplified registration requirements apply). Licensing of credit institutions are regulated by the Credit Institution Law (Chapter II, including Section 11). Electronic money, PIs and currency exchange companies shall be registered or licensed according to LPSEM (Chapter II, including Section 4, Chapter II2 for currency trading companies). Insurance and reinsurance companies are regulated by Insurance and Reinsurance law (Chapter II and Chapter III, including Section 4). Insurance intermediaries have to be registered in accordance with Chapter II of Insurance and Reinsurance Distribution Law, AIFMs are regulated by Law on Alternative Investment Funds and Managers Thereof (Chapter II Activities, Registration, and Licensing of the Manager, including Section 7 and 10), Savings and loan associations are regulated by Law on Savings and Loans Associations Chapter II, Investment firms – by Law on Investment Firms, Chapter II. Investment management companies by – Law on Investment Management Companies, Chapter II. Private Pension funds by – Private Pension Fund Law, Section 8. Other FIs are being registered. Establishment and operation of shell banks is prohibited in Latvia (Section 21(2) AML/CFT/CPF Law).

Criterion 26.3 – Criminality checks on BOs and managers for Latvijas Banka licensed/registered entities are conducted at the initial licensing stage and subsequent changes (such as increase of shareholding, acquisition of qualifying holding, change of management). General requirements are set out in various sectorial laws. Whilst the notion of "criminal associates" is not defined in the legislation, the Latvijas Banka considers criminal associations when assessing reputation of BOs and managers. The effectiveness of controls by all licensing/registration authorities aimed at preventing criminals from entering the regulated financial market through beneficial ownership or managerial role are discussed in detail under IO.3.

Criterion 26.4 – a) Core Principles FIs: Latvia has not been subject to official assessments of the Basel Committee Principles, the International Association of Insurance Supervisors (IAIS) Principles or the International Organisation of Securities Commissions (IOSCO) Principles.

Latvijas Banka is required to carry out consolidated group supervision of the credit institutions (Section 112^2 of the Credit Institution Law), investment brokerage companies (investment firm) (Section 142 of the Financial Instrument Market Law); investment management companies (according to Section 8 of the Law on Investment Management Companies); insurance/reinsurance groups (Section 221 of the Insurance and Reinsurance Law); managers of an AIF (Section 16 of the Law on Alternative Investment Funds And Managers).

b) Supervision of non-core FIs is performed by taking into account ML/TF risks (with the exception of the CRPC), however, the extent to which risks are being considered for supervisory purposes varies (also see c.26.5). Some internal rules are in place for monitoring compliance with AML/CFT measures.

Criterion 26.5 – Generally, the financial supervisors are required to determine the frequency of supervision on the basis of ML/TF risk (Sec. 46(1) AML/CFT/CPF Law). Internal methodologies detailing supervisory processes are in place. However, risk-based approach to supervision covering currency exchange offices and other FIs supervised by the CRPC and SRS has shortcomings.

Criterion 26.6 – The SCAs are required to review risk assessments of the FIs regularly on the basis ML/TF risks in accordance with the conditions specified in the Sec. 46(1)(11-12) AML/CFT/CPF Law. This is further detailed in the internal procedures of the Latvijas Banka. Other than the requirements of the AML/CFT/CPF Law there are no formal additional procedures covering all non-banking FIs to review the risk profiles on the basis of major events or developments in the management and operations of the FI or group.

Weighting and Conclusion

R.26 is rated largely compliant. Minor shortcomings remain elating to market entry measures, risk-based supervision of some non-banking FIs and moderate shortcomings relating to the absence of official assessments with the core principles.

Recommendation 27 – Powers of supervisors

In the 2018 MER, Latvia was rated compliant with R.27. Changes pertaining to this recommendation commenced in the period of 2021-2023 following the merger of Latvijas Banka and the former financial market supervisor – the FCMC. The following changes have been introduced since the last MER: the SCAs have extended supervisory powers over REs on insolvency or liquidation; more powers were given to the Latvijas Banka to revoke licenses.

Criterion 27.1 – The supervisory authorities are required to supervise and ensure compliance of FIs with AML/CFT/CPF requirements (Sec. 45 AML/CFT/CPF Law).

Criterion 27.2 – The SCAs are required to conduct inspections (Sec.46(1)(3) AML/CFT/CPF Law) and have the right to visit premises of the supervised REs.

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/CPF Law).

Criterion 27.4 – The SCAs can issue sanctions for failure to comply with the AML/CFT/CPF Law (Sec. 77(1), 78(1)). These include fines, temporary suspension of any RE's official that is held liable for the breaches, revocation of a licence and other measures provided for in the AML/CFT/CPF Law.

Weighting and Conclusion

R.27 is rated compliant.

Recommendation 28 – Regulation and supervision of DNFBPs

In its 2018 MER, Latvia was rated partially compliant with R.28 due to the following deficiencies: (i) it was not clear if there were measures in place to prevent criminals from controlling DNFBPs (except for Notaries); and (ii) there were deficiencies in the ML/TF risk-based supervision conducted by the supervisory authorities. In the FUR 2019, the majority of identified deficiencies have been addressed and R.28 was re-rated as largely compliant.

Criterion 28.1 – (a) Gambling operators (land-based and online casinos) and lotteries are required to be licensed in Latvia (Law on Gambling and Lotteries, Sec. 3 and 46). Licences are issued by the LGSI.

(b) Members of the Board and the auditor of the gambling operator must have impeccable reputation and not be prohibited from the right to engage in business activities. This explicitly excludes those with criminal records from acting (Sec.9(2) and (3) of the Law on Gambling and Lotteries)). In addition, amended Sec.10^{1}(1) of the AML/CFT/CPF Law prevents criminals from being members of the senior management or the compliance officer of the RE. However, this requirement does not extend to associates of persons with criminal record, nor does it cover persons holding (or being BO of) a significant or controlling interest, or their associates.

(c) The LGSI is the designated casino supervisor responsible for AML/CFT/CPF supervision (Sec.45(7) AML/CFT/CPF Law). The LGSI conducts onsite inspections of casinos.

Criterion 28.2 – Latvia lists the following DNFBPs all of which are subject to the AML/CFT/CPF Law: 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.

The AML/CFT supervisors are listed in the AML/CFT/CPF Law and are as follows: Real estate agents are supervised by the SRS (Sec.45(2)(4)); DPMS are supervised by the SRS (Sec.45(2)(5)); Lawyers are supervised by the LCSA (Sec.45(1)(2)); Notaries are supervised by the LCSN (Sec.45(1)(3)); Auditors are supervised by the Latvian Association of Sworn Auditors and SRS (Sec.45(1)(4)); Accountants are

supervised by the SRS (Sec.45(2)(1)); Company Service Providers (including trustees) and independent legal professional are supervised by the SRS (Sec.45(2) (2) &(3).

Criterion 28.3 – See 28.2

Criterion 28.4 – (a) Sec.45-47 AML/CFT/CPF Law appear to give the supervisors/self-regulatory organisations 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/CPF 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/CPF Law Sec.47(1)(2)). This includes the authority to request explanations from the REs.

(b) Amended Sec.10[1] of the AML/CFT/CPF Law prevents criminals from being members of the senior management or the compliance officer of the RE (Sec.10[1](1)). However, this requirement does not cover associates of persons with criminal record. Reference is made to c.28.1(b) with regard to shortcoming relating to persons holding (or being BO of) a significant or controlling interest.

(c) A SCA shall impose the sanctions laid down in Sec.78 AML/CFT/CPF Law, if the offences of the legal framework in the field of AML/CFT are detected. The provisions of Sec.78 AML/CFT/CPF Law described under c.27.4 and the framework described in R.35 apply to DNFBPs, including shortcomings related to the supervisory authorities and lack of clear legal basis for imposing sanctions for non-compliance with R.6 (see c.35.1).

Sanctions laid down in Sec.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 SCA- Latvian Association of Certified Auditors (LACA).

Criterion 28.5 – (a) Amended Section 46(1)(11) of the AML/CFT/CPF Law provides that SCAs should implement supervisory measures based on the ML/TF/PF risk assessment and conduct the risk assessment and regular revision thereof according to the risk level.

The SRS is conducting ML/TF risk-based supervision. However, it should be noted that the risk-based approach applied by the SRS does not cover all the requirements under 28.5; i.e. internal controls and procedures are not considered for the risk assessment of institutions. It is also not clear what will be the impact of risk criteria considered on the intensity and frequency of inspections.

The LCSN considers seven risk factors for risk assessment: results of previous assessments, employees' qualifications, experience, concerns of the LCSN, reputation (complaints, disciplinary action), total debts, financial results and notary's professional activities outside the office.

According to its internal rules, the LGSI appears to follow risk-based approach for supervising casinos.

The LCSA uses risk classification system to classify risk categories of sworn advocates.

The LACA introduced some elements of risk-based supervision for conducting targeted inspections of certified auditors.

(b) Supervisory risk profiles: The LSCN 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 prioritise 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

Whilst a framework for market entry and supervision of DNFBPs is in place, there are still shortcomings, including (i) there are no measures to prevent the associates of criminals from involvement in the ownership or activities of these types of REs, and (ii) there are deficiencies in the ML/TF risk-based supervision conducted by the supervisory authorities. **R.28 is rated largely compliant**.

Recommendation 29 - Financial intelligence units

Latvia was rated largely compliant in the 2018 MER. The deficiencies identified related to limitations to the FIUs access to a broad range of information and limitations in dissemination capacities. The 2018 MER also noted issues regarding operational independence. Several aspects of the AML/CFT/CPF Law and regulations governing the FIU were overhauled in 2019, which resulted in improvements to: the FIU's access to information (29.3); ability to provide information with clear grounds for refusal (29.5) and; operational independence (29.7).

Criterion 29.1 – Latvia established a national FIU in 1998. In 2019 revisions to the AML/CFT/CPF Law represented an overhaul which resulted in a significant increase in the FIU's responsibilities in the country's AML/CFT regime. These legal reforms moved the FIU from under the auspices of the PO into its own independent agency. The AML/CFT/CPF Law establishes the legal status; rights and obligations; and responsibilities of the FIU. The AML/CFT/CPF Law provides that the FIU is the national centre for receipt of STRs, and other information relevant to ML, associated predicate offences and TF, and for the dissemination of this analysis to relevant authorities (Ch. IX, Sec.50(1), AML/CFT/CPF Law,).

Criterion 29.2 – The FIU serves as the central agency for the receipt of disclosures filed by the REs, including:

a) STRs filed by REs related to ML, associated predicate offences and TF (Sec.50, AML/CFT/CPF Law,). The AML/CFT/CPF 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. REs have an obligation to report suspicious transactions immediately, applied to a variety of suspicions related to ML, TF and associated predicate offences (Ch. IV, Sec 31 (4) AML/CFT/CPF Law).

b) Threshold-based declarations for certain REs that are defined in the CoM Regulations (CoM Reg. No. 550).

REs are required by law to register on the goAML system through which reports are submitted to the FIU.

Criterion 29.3 – In relation to obtaining and accessing information:

(a) REs must provide the additional information requested by the FIU immediately, but not later than within three working days after receipt of the relevant request, if it is related to the order of the FIU Latvia on temporary freezing of the funds for five working days or according to the urgency indicated therein, or within seven working days in other cases (Section 31.4 (2) of the AML/CFT/CPF Law).

(b) the FIU has direct access to a wide range of information and databases and is able to require public authorities to provide any information necessary for the FIU to fulfil its functions (Section 51 (1), AML/CFT/CPF Law). These include direct access to the account register (and information on BO); database of the ER (including BO section); criminal procedure information and criminal records database; customs declarations and ship registers; Border Crossing Information System; vehicle and land registries; tax information; etc.

Criterion 29.4 – In relation to analysis carried out by the FIU:

(a) and (b) Latvia's FIU carries-out operational and strategic in practise. The FIU must undertake this 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, and there are various mechanisms for evaluating the quality of the FIU's strategic analysis, the usability and relevance (Sec. 51, AML/CFT/CPF Law).

Criterion 29.5 – The FIU has the capacity and the channels to disseminate the results of is analysis spontaneously and upon request to relevant competent authorities in a secure manner. The dissemination of these information requests are subject to the discretion and approval of the FIU. The FIU considers each request based on requirements set out in the AML/CFT/CPF Law (Sec. 56, AML/CFT/CPF Law). In practice the FIU sends and receives information to other competent authorities through the goAML application, which provides encryption capability and a secure data transfer protocol.

Criterion 29.6 – Latvia's AML/CFT/CPF Law stipulates that the FIU must secure and enforce the confidentiality, establish clearance protocols and limit access to its information (see (a) to (c) below) (Section

53, AML/CFT/CPF Law). To achieve this, FIU Latvia also has a series of internal rules and guidelines in place that govern their practical implementation and enforcement:

(a) FIU Latvia has rules in place governing the security and confidentiality of information including the handling and storage procedures for this information. It maintains an up-to-date (yearly) list of the types of information and access levels required. There are a series of administrative, technical and organisational measures in place according to several CoM Regulations and there is criminal liability for disclosure of restricted access information (Section 200, CL). Latvia also relies on the Constitution Protection Bureau to establish and enforce its security accreditation. FIU Latvia has been assessed by the bureau and it received the required security accreditation in April 2024.

(b) The FIU sets internal regulations for the relevant security clearance required for classified posts in accordance with Latvia's Law on Official Secrets. It ensures that personnel are security cleared before undertaking their duties and requires that employees are familiar with protocols and rules to access information and liability of breaching their obligations (CoM Reg. No. 822).

(c) The FIU also ensures that there is limited physical access to its facilities and data. Its facilities are secured, protected and restricted with security guards, and access gates and locks. Its data is protected using a variety of electronic measures (CoM Reg. No. 442). FIU Latvia recently created the post of Information Systems Security Manager (July 2022) to bolster their IT and data security.

Criterion 29.7 – In relation to the operational independence and autonomy of the FIU Latvia:

(a) The FIU has the authority and capacity to carry out its functions freely thanks to legal amendments of the AML/CFT/CPF Law in 2019, which sets out the FIU as a fully autonomous and independent administration (Sec 50, AML/CFT/CPF Law). The FIU remains under the supervision of the CoM, which the MoI implements. This supervision does not apply to the implementation of the tasks and rights assigned to the FIU, or internal regulations, statements, or decisions regarding employees.

(b) The FIU Latvia is able to make arrangements or engage independently with domestic competent authorities or foreign counterparts on the exchange of information. In addition, FIU Latvia has the power to independently and exclusively negotiate on and conclude MoUs and agreements with domestic competent authorities and foreign FIUs or other relevant partners (AML/CFT/CPF Law Section 50).

(c) (Not applicable)

(d) The FIU is able to obtain and deploy resources necessary for its functions. The FIU Latvia is financed from the State budget (Sec. 50, AML/CFT/CPF Law). Additionally, the FIU has a clear procedure for appointment, suspension, and dismissal of the Head of the FIU (Section 50.1 and 50.2, AML/CFT/CPF Law). In addition to an annual budget allocation from the government (which has increased year on year since 2018) the FIU has been able to obtain supplemental funds from a variety of sources, including the national confiscation fund.

Criterion 29.8 – FIU Latvia has been a member of the Egmont Group since 1999.

Weighting and Conclusion

Recommendation 29 is rated as compliant.

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

In the 2018 MER of 2018, Latvia was rated largely compliant to responsibilities of law enforcement and investigative authorities. The major deficiency was that LEAs were not required to routinely conduct parallel financial investigations (c.30.2). Latvia has since updated its internal guidance to LEAs, which now requires the conduct of routine financial investigations.

Criterion 30.1 – Latvia has a broad range of LEAs that have responsibility to investigate ML, associated predicate offences and TF. The Prosecutor General has rights to determine the institutional jurisdiction of specific criminal offences (Section 387 (11) of the CPL). On 2021 Section 26.1 was introduced to CPL which contains powers of the EPPO to conduct criminal proceedings.

ML and associated predicate offences

Unless otherwise provided by Sec.387 CPL, the State Police shall investigate any criminal offence. Also, if the predicate offence cannot be identified and is not suspected, including abroad, then the investigation is carried out by the State Police. The State Police Main Criminal Police Department (MCPD) includes the ECED, whose individual units specialise in investigating complex economic crimes. In addition, Latvia created in 2022 the Cybercrime Enforcement Department in order to prevent and combat high-tech crime, including ML involving crypto-assets. At the same time, each investigator is authorised to investigate ML.

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: SRS TCPD (regarding criminal offences in the field of State revenue and customs matters); CPCB (regarding criminal offences related to violations of the provisions of the financing of political organisations); the Internal Security Department of the SRS (regarding corruption related criminal offences committed by their officials and employees which are related to the fulfilment of their official duties) and the SBG (regarding criminal offences related to the illegal crossing of the State border).

TF offences

TF offences are investigated by the SeP, which is one of the three State security institutions in Latvia and which is subordinated to the MoI. In the field of national security, the State Security Service *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).

Criterion 30.2 – The CPL establishes a clear institutional jurisdiction of every investigative institution (LEA) in Latvia to investigate any related ML/TF offences during an investigation of a predicate offence (or in a course of parallel financial investigation), regardless of where the predicate offences occurred. In 2022, the PO issued guidelines on parallel financial investigations to investigators, prosecutors, and training units. Additionally, LEAs have issued internal documents required to perform routine parallel financial investigations.

Criterion 30.3 – Law enforcement investigators can identify, trace, and initiate the freezing and seizing of property (Ch 28, Sec.361 CPL). The property shall be seized with a decision approved by an investigating judge. In emergency cases, the property may be seized with the consent of a prosecutor. A designated competent authority is established as an ARO within the State Police, with the basic function of search, identification and recovery of illegally acquired property. All LEAs may engage the ARO when in need of assistance in asset-tracing and confiscation. All LEAs have adopted internal guidelines on parallel financial investigations, which involve guidelines on tracing, identifying, freezing and seizing.

Criterion 30.4 – Latvia does not have competent authorities which are not LEAs but pursue nonetheless financial investigations of predicate offences.

Criterion 30.5 – In accordance with Section 387 (6) of the CPL the CPCB is authorised to investigate criminal offences related to corruption committed in the State Authority Service. Additionally, the Internal Security Department of the SRS has rights to investigate corruption related criminal offences committed by their officials and employees which are related to the fulfilment of their official duties. The Internal Security Bureau has rights to investigate corruption related crimes committed by the officials and employees of institutions subordinate to the MoI. All LEAs have the authority to identify, trace, and initiate the freezing and seizing of property (Sec.361 CPL).

Weighting and Conclusion

Latvia is compliant with R.30.

Recommendation 31 - Powers of law enforcement and investigative authorities

In the 2018 MER, Latvia was rated largely compliant with Recommendation 31. Although competent authorities had powers to use a wide range of compulsory measures and investigative techniques, the provision of information to them from the FIU was not conducted unconditionally, as the FIU disseminations were subject to GPO approval. The AML/CFT/CPF law has since been amended (see R.29).

Criterion 31.1 – LEAs responsible for investigating ML, associated predicate offences and TF are able to obtain access to all necessary documents and information for use in those investigations. The range of compulsory measures available to ensure this includes the following:

a) The production of records held by FIs, DNFBPs and other natural or legal persons

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). 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). 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). Professional secrets may be requested only by a judicial order.

b) Search of persons and premises

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

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

In addition to the provisions of the Sec. 190 (1) CPL obligating 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 TF, the authorities can seize them in accordance with the procedure under Sec.186 et seq. CPL. Removal is an investigative action whose content is the removal of objects or documents significant to a case. The decision on removal is taken by the person directing the proceedings (investigator or prosecutor) and it is not subject to appeal. The compulsory order for the disclosure of data stored in an electronic information system is possible with the consent of the PO or the investigating judge (Sec.192 CPL).

Criterion 31.2 – In Latvia investigative techniques are regulated by the Operational Activities Law, which applies prior to the initiation of criminal proceedings 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 accordance with the procedures laid down in the CPL. Chapter 11 (Sec.210 et seq.) of the CPL deals with "special investigative techniques".

Competent authorities conducting investigations of ML offences and TF offences have access to a wide range of investigative techniques under Sec.6 OAL, including : 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.

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.

Special investigative actions shall be performed on the basis of a decision or approval by the judicial authority. In emergency cases, a prosecutor may give consent, but the investigating judge needs to approve within the next working day. The duration of a special investigative action shall not exceed 3 months, but the period can be extended. The performance of special investigative action shall be permitted only in investigating "less serious crimes" (i.e. 3 months – 3 years' imprisonment, Sec.7(3) CL), "serious crimes" (i.e. 3 – 8 years' imprisonment, Sec.7(4) CL), or "particularly serious crimes" (i.e. 8 years to life imprisonment, Sec.7(5) CL).

Criterion 31.3 – Latvia possesses the legal framework 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. According to Sec.5(1) of the Law on Account Register, credit institutions, credit unions and payment service providers shall provide information to the investigation authorities and the PO about account holders and their BOs, as well as recipients of the individual safe-deposit box services. Sec.63 (1) 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 PO. It should be noted that Sec.121.5 CPL requires, in order for the authorities to obtain non-disclosable information by FIs (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.

Criterion 31.4 – Competent authorities conducting investigations of ML, associated predicate offences or TF are able to request relevant information held by the FIU, as provided by Sec.56 AML/CFT/CPF Law. This section states that, at the request of the bodies performing operational activities, investigating institutions, the PO, as well as a court, the FIU shall provide information in accordance with the requirements of the AML/CFT/CPF Law within the operational activities procedure or criminal proceedings. The same 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 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 FIU shall be under no obligation to comply with the request for information.

Weighting and Conclusion

Latvia is compliant with R.31.

Recommendation 32 – Cash Couriers

Latvia is a member of the EU, and its national borders are also borders of the EU. In its 2018 MER, Latvia was rated partially compliant with R.32, based on the following deficiencies: it did not have an EU-internal border declaration system for cash and BNIs and for EU-external borders, sanctions for non-declaration or false declarations were not dissuasive enough. However, in a short period of time, the country managed to address the majority of deficiencies. Nevertheless, the failure to achieve complete control and sanctioning of EU-internal border transportation of currency and BNIs led to a rating of largely compliant during the 2019 FUR.

Criteria 32.1 –The country has implemented a declaration system for incoming and outgoing cross-border transportation of currency and BNI, including intra-EU cash movements. The general framework is set forth in the EU Regulation (EC) No 2018/1672[1]: Article 3 of EU Regulation 2018/1672 requires natural persons

entering or leaving the EU to declare accompanied cash (defined, inter alia, to include any currency and BNIs, to the value of EUR 10 000 or more. This applies if the cash is on the traveller's person, in their luggage or in their means of transport. Art. 4 of the Regulation provides that where unaccompanied cash (including by post, courier, unaccompanied luggage or containerised cargo) of EUR 10 000 or more is entering or leaving the EU, the competent authorities (defined as customs and any other authorised authorities) may require the sender or recipient (or an authorised representative) to make a disclosure declaration within a deadline of 30 days.

The EC regulation is implemented and completed by the Law on Declaration of Cash at the State Border (Section 5, Law on Declaration of Cash at the State Border). The declaration system is also complemented by a declaration disclosure system in place when crossing the internal EU borders with the same amount of cash or BNIs. Natural persons may also be requested by the competent authority to complete a cash declaration form.

For controls on unaccompanied cash above EUR 10 000, including through postal consignments and containerised cargo, the competent authority may request that the sender or recipient, or their representative, completes a cash declaration disclosure within 30 days of the request.

Criteria 32.2 – b) Latvia has implemented a written declaration system for all travellers carrying amounts above a threshold of EUR 10 000. The declaration is always mandatory when crossing the EU external borders Article 3 of the Regulation requires a written declaration for all travellers carrying cash to the value of EUR 10 000 or more, using a template declaration form as laid out in Commission Implementing Regulation (EU) 2021/776. Art 3 also states that "The obligation to declare cash shall not be deemed to be fulfilled if the information provided is incorrect or incomplete or if the cash is not made available for control" i.e. an obligation that the declaration is truthful.

Criterion 32.3 – For intra-EU border crossings, the person making the physical cross-border transportation of cash or BNIs above the threshold, or a person sending or receiving unaccompanied cash above the threshold (via postal or courier) may be requested by relevant competent authorities to make a disclosure.

For unaccompanied cash, Art. 4 of the EU Regulation 2018/1672 provides that "The obligation to disclose unaccompanied cash shall not be deemed to be fulfilled where the declaration is not made before the deadline expires, the information provided is incorrect or incomplete, or the cash is not made available for control" i.e. to provide authorities with appropriate and truthful information upon request.

Criterion 32.4 – See c.32.2 and 32.3 above. The Tax and Customs Police of the SRS may investigate criminal offences related to the false or non-declaration of cash and BNI (Sec 387 (7), CPL). This is in line with EU Regulation 2018/1672, which allows competent authorities to temporarily detain the cash in such cases (see c.32.8). However, it does not provide any power to request or obtain additional information from a traveller (in the case of a false declaration) or a sender/recipient (in cases of a false disclosure declaration). Nevertheless, competent authorities have the power to request and obtain further information on the origin of the currency or BNIs and their intended use, which is granted on the basis of domestic provisions (point 5 of the CoM Reg. No. 303 adopted on 2 July 2019). An official of the competent authority can request more information, inspect the verify the information provided in the declaration. The carrier has an obligation to present the declared cash and to participate in the control of the declared cash. (Sec 5^2 (1) of the Law on Declaration of Cash at the State Border).

Criterion 32.5 – Failure to comply with EU external and internal cross-border obligations (false and non-declaration of cash or BNI) is an administrative offence punishable by a fine of 20% of the undeclared or falsely declared amount (Section 7 of the Law on Declaration of Cash at the State Border). This aligns with Article 14 of the Regulation, which requires member states to introduce effective, proportionate and dissuasive penalties for cases where there has been a failure to comply with the declaration or disclosure requirements. Thus, each member state determines the amount and nature of any sanctions and should do so in line with Art.14.

False and non-declaration of cash or BNI in a large scale (above the amount of EUR 35 000), shall initiate criminal proceedings (Section 195^2 (2) of the CL). In cases where the competent authority identifies indications of ML, no matter the amount of suspicious cash, criminal proceedings on alleged ML shall be initiated. For a person who fails to declare or commits false declaration of cash on a large scale (above the amount of EUR 35 000) when crossing the State internal border, the applicable punishment is the deprivation

of liberty for a period of up to two years or temporary deprivation of liberty, or community service, or fine, while when crossing the State external border the applicable punishment is the deprivation of liberty for a period of up to three years. If the non-declaration or false declaration of cash is conducted on a large scale (above the amount of EUR 35 000) and involves criminally acquired cash or is committed by an organised group, then the applicable punishment is a sentence of up to four years.

Within the respective administrative or criminal proceedings, Latvian authorities have the power to seize and confiscate false or non-declared cash on internal or external border of Latvia.

Criterion 32.6 – Information obtained from cash declarations and cash disclosure declarations is stored in the Electronic Customs Information System, to which the FIU has direct access. This is aligned with Article 9 of EU Regulation 1672, which requires that the relevant competent authorities shall record the declaration and disclosure information and make it available to the national FIU as soon as possible, and in any event within 15 days. The information is also required to be shared by the FIU with relevant FIUs from other EU Member States.

Criterion 32.7 – According to EU regulation 1672, Information is required to be shared by Tax and Customs Police with the FIU (see above), but there are no requirements in Regulation 1672 concerning co-ordination between relevant authorities at a national level on declarations/disclosures. The co-ordination in matters of state border security among authorities - including the SBG, the State Police and the SRS - is regulated by CoM Instruction No. 5 adopted in 2010. The Agreement No. 86 "for the Organization of Activities and Cooperation of Institutions at Border Crossing Points" (22.04.2020) determines forms of co-operation between the SBG and the Customs Administration, as well as SRS and the SBG have concluded to an agreement determining the timely exchange of information. The State Police has the rights and tools to check information in SBG and SRS registers and all three authorities have signed co-operation agreement on combating the illegal movement of excise goods, providing designated officials who act as contact points and carry out operational exchange of information.

Criterion 32.8 – a), b) When there is a suspicion of ML/TF or predicate offences; or in the case of a false declaration, the internal regulations of the SRS provide the possibility for the customs officer to stop or restrain currency or BNIs for a reasonable time in order to contact the Tax and Customs Police board to ascertain whether evidence of illegal activities may be found.

Seizure is applicable if a criminal investigation is launched (Section 186, CPL). Customs may open a criminal proceeding in consultation with other competent authorities (SRS TCPD Investigators (SRS internal regulation No 29). This aligns with EU Article 7 of Reg. 1672, which has to be implemented under national law, and allows competent authorities to temporarily detain cash and/or BNIs when the obligation to declare or disclose cash has not been fulfilled or when there are indications that the cash (irrespective of the amount) is related to criminal activity. The initial detention period is limited to 30 days, but this can be extended by competent authorities to 90 days in appropriate cases, where this is necessary and proportionate.

Criterion 32.9 – False and suspicious declarations and disclosures are mainly regulated by European Regulations (Regulation (EU) 2018/1672). Article 10 requires exchange of declaration/disclosure information with competent authorities in other EU Member States, and Art.11 allows such exchange of such information through MLA with authorities in third countries (subject to conditions). Art.9 also requires exchange of such information between EU member state FIUs. Under Art.13 all declaration/disclosure information (which includes information on the currency/BNI, and the identification data of the traveller/carrier) is to be retained for five years and may be further retained for an additional period of up to three years in specific circumstances. Every cash declaration, including information on false and suspicious declarations, is stored in the Electronic Customs Data Processing System, without any time-limit for their storage. Hence, the information from this database can be provided to a foreign country upon request.

Criterion 32.10 – The confidentiality of information is safeguarded by Section 2 of Personal Data Proceeding Law, implementing the provisions set out in the Article 13 of the EU Regulation No 2018/1672. Within the EU, freedom of capital movements and the free and safe movement of goods and services are guaranteed basic principles. There is nothing in the Regulation which restricts such movements.

Criterion 32.11 – Persons who are carrying out physical cross-border transportation of currency or BNIs that are related to ML/TF or predicate offences can be subject to a) criminal sanctions under either the ML/TF offences or for "avoidance of declaring of cash" under Sec.195^2 of the CL (as mentioned under Criterion

32.5), i.e. up to four years or more in cases of organised ML (these are proportionate and dissuasive sanctions for ML/TF). Persons who are carrying out these acts are also subject to b) measures consistent with recommendation 4, that enable the seizure of criminally acquired property, including cash and BNIs, that shall be seized and later confiscated (Sec.355/1 and 358/1 CPL). Sanctions for ML, TF and predicate offences and confiscation measures are not dealt with in the EU Regulation. These are issues for national law.

Weighting and Conclusion

Latvia is compliant with R.32.

Recommendation 33 – Statistics

In its 2018 MER, Latvia was rated largely compliant with regards to R.33 as there were some inconsistencies on the keeping of statistics on STRs. There were no statistics on confiscation from cross-border movements of cash and no information was collected. Latvian authorities have since addressed these shortfalls by introducing the amendments to the AML/CFT/CPF Law, designating the FIU as the central repository for all statistics relating to ML/TF/PF, including (but not limited to) all the categories of data set out in R.33.

Criterion 33.1 – Latvia keeps statistics on:

a) STR statistics (including receipt and dissemination). The data on STRs is held by the FIU and are compiled annually into a national report.

b) ML/TF investigations, prosecutions and convictions. These statistics are also held centrally by the FIU.

c) Property frozen; seized and confiscated. This information is also held centrally by the FIU.

d) MLA and other international requests. This information is also held centrally by the FIU.

Weighting and Conclusion

Latvia is compliant with R.33.

Recommendation 34 – Guidance and feedback

In its 2018 MER, Latvia was rated compliant with the R.34. Since then, additional FIU duties were introduced relating to the feedback to the SCAs and additional guidance.

Criterion 34.1 – Supervisory authorities are required to provide training to the REs and issue AML/CFT/CPF guidelines (AML/CFT/CPF Law, Sec. 46(1)(2)). The FIU is required to analyse quality of STRs, its further use and to inform the REs (AML/CFT/CPF Law Sec.51(1)(3)). More information on the extent to which these obligations are implemented by the supervisory authorities and the FIU can be found in the effectiveness analysis.

Weighting and Conclusion

R.34 is rated compliant.

Recommendation 35 – Sanctions

In its 2018 MER Latvia was rated largely compliant with R.35, as there were no clear legal bases for all the supervisory authorities to apply sanctions for failure to comply with requirements of R.6.

Criterion 35.1 – The AML/CFT/CPF Law gives authority as noted below to impose penalties for violations of the laws and regulations in the field of the prevention of ML/TF/PF.

Sec.78 AML/CFT/CPF Law stipulates the range of proportionate and dissuasive administrative sanctions for failure of the AML/CFT/CPF legislation, including public announcements specifying the person liable for the offence and the nature of the offence, warning, fine up to EUR 1 million, revocation of a licence or cancellation of the record in the relevant register, temporary prohibition from duties; duty to perform certain action or refrain therefrom; and mandatory dismissal of responsible individuals. For credit and financial institutions, fines can reach 10% of the annual turnover or up to EUR 5 million if 10% is less than this amount. Additionally, fines up to EUR 5 million can be imposed on individuals who have been liable for the

performance of a particular action on assignment or in the interests of a credit institution or FI at the time of committal of the offence (AML/CFT/CPF Law, Sec.78(3)).

Sanctions decisions are published on respective SCA's website. Following assessment of the potential impact on financial market stability, ongoing criminal proceedings, or harm to the involved persons, the authority has discretion to publish the sanctions information without identifying the individual (AML/CFT/CPF Law, Sec. 78 (8) & (9)).

There are no clear legal bases for all the supervisory authorities to apply sanctions for failure to comply with requirements of R.6.

Criterion 35.2 – The following sanctions available under Sec.78(3) Clause 2 of the AML/CFT/CPF Law apply to individuals: temporary prohibition for a person liable for the offence to fulfil the duties prescribed for them by the RE and duty on the RE to dismiss the person liable for the offence from the position held; and fine of up to EUR 5 million 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

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[132]

In the 2018 MER, Latvia was rated largely compliant with R.36. There have been no material changes in implementation of criterion 36.1. since it was rated in Latvia's MER in July 2018. 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.

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.

Criterion 36.2 – Latvia implements the provisions of the Vienna, Palermo, Merida and TF Conventions through domestic legislation.

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).

Concerning the Merida Convention, embezzlement in the public sector is criminalised 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 AT shares the concerns of the UN[133] 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

132. The UNCAC Implementation Review Mechanism (IRM), for which the UNODC serves as secretariat, is responsible for assessing the implementation of the UNCAC. The FATF assesses compliance with FATF Recommendation 36 which, in relation to the UNCAC, has a narrower scope and focus. In some cases, the findings may differ due to differences in the FATF and the IRM's respective methodologies, objectives and scope of the standards.

133. Available at http://www.unodc.org/documents/treaties/UNCAC/CountryVisitFinalReports/2014_10_24_Latvia_Final_Country_Report.pdf.

procedural immunity could apply to criminal prosecution only (and not to pre-trial investigation), as the UN suggests.

Regarding the Palermo Convention, Art.5 has not been fully implemented, since conspiracy or participation in OCGs are not offences under the CL, but instrumental elements of other offences. Art.12(4) is not explicitly reflected in Latvian legislation.

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

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 largely compliant.**

Recommendation 37 - Mutual legal assistance

Latvia was rated largely compliant in the 2018 MER. The deficiencies identified included the absence of a clear process for the timely prioritisation and execution of MLA requests, and of a clear case management system.

Criterion 37.1 – Latvia is a party to international agreements such as the 1959 European Convention on MLA 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.

MLA is regulated in "Part C" of the CPL, which establishes that Latvia provides international co-operation 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 co-operation is also allowed (Sec.675 CPL).

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.

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).

As per Sec.848 CPL, the admissibility of MLA requests should be assessed within 10 days. Deadlines for the response to the request are set by the directives of the European Parliament and of the Council (Directive 2014/41/EU of April 3, 2014) on the EIO in criminal cases. This directive also applies to other third-party-country case (Sec 848, paragraph 2, CPL).

Criterion 37.2 – Three competent institutions are appointed as central authorities, depending on the stage of the criminal proceedings: the State Police 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.

Direct co-operation is also possible if a previous agreement between competent authorities has been reached (Sec.675(2) and 846(3) CPL).

In 2014, an Information System on Judicial Co-operation in criminal matters was established for use by the central authorities. There are 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 (CoM Reg. No. 1045, issued under Sec.673 CPL) The system should register the receipt, attribution and status of execution of assistance requests.

In 2022, the Latvian authorities also introduced the 'eEvidence' platform which handles MLA requests and EIOs for EU Member States. This system is still under development and there are plans to integrate the two aforementioned platforms. However, Latvia has not provided information on the actual time of execution of MLA requests, which suggests that the Information System does not systematically gather such data and cannot adequately manage and prioritise 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.

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 co-operation domain (prejudice to sovereignty, security, social order, dual criminality, political exceptions).

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) Legal professional secrecy might reasonably be grounds for refusing an MLA request, however there is a provision in Latvian law analogous to a "crime/fraud exception" in which otherwise legally privileged material might be excluded from privilege on the basis that the legal advice involved the of promotion of unlawful activity (Section 122 (1)(4) of the CPL).

Criterion 37.5 – 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.847 (1) and 396, CPL). The information obtained in pre-trial criminal proceedings can be disclosed upon authorisation of the investigator or a public prosecutor.

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 for 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).

Criterion 37.7 – Dual criminality is not a ground for refusal of the execution of a request of a foreign state (Section 850 of the 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 (Sec.852 CPL). 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).

Criterion 37.8 – The provisions of CPL state that all procedural actions provided by the CPL in Latvia can also be applied in the execution of MLA requests (Section 847, CPL). These actions include "investigative actions" (e.g., searches and seizures) and "special investigative actions".[134] 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.

Weighting and Conclusion

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.**

134. 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.

Recommendation 38 – Mutual legal assistance: freezing and confiscation

In the 2018 MER, Latvia was rated largely compliant with the Recommendation on MLA in relation to freezing and confiscation. This was mainly due to the lack of clear provisions on co-ordination arrangements in relation to seizure and confiscation and mechanisms for managing frozen, seized or confiscated property. Additionally, Latvia did not demonstrate that it had authorities to expeditiously action responses to requests, nor the authority to oblige requests without dual criminalisation of the underlying offence and a criminal conviction. Since then, the Regulation (EU) 2018/1805 on the mutual recognition of freezing orders and confiscation orders has come into force and the GPO has adopted prioritisation criteria for responses, and address some of these deficiencies. Latvia has also modified provisions to include confiscation regardless of the foreign proceedings.

Criterion 38.1 – As noted under Criteria 4.1 and 4.2, Latvian authorities have a broad set of legal powers to expeditiously identify, freeze, seize, or confiscate directly and indirectly criminally acquired property, laundered property and instrumentalities of crime (including for use or intent for use in ML, predicate or TF offences), and property of corresponding value. Latvia's Law stipulates that the same powers and actions are used to execute MLA as if the activity would be performed in national case (Section 847, CPL). The competent authority (the State Police, the GPO or the MoJ) has the authority to execute the requests immediately, but not later than within a term of 10 days after the receipt thereof.

Requests for confiscation by a foreign country are executed if it has been imposed in a foreign country. A court shall indicate in a ruling the type of confiscation of property and the property to be confiscated. Confiscation of property shall be executed regardless of in which proceedings it was applied in the foreign country, ensuring the execution of NCBC (Section 791 of the CPL).

Requests for the execution of a judgment from EU Member States that is bound by EC Regulation No 2018/1805 and are executed in accordance with the Regulation (i.e. without decision of the courts). For requests for the execution of a judgment of EU Member State that is not bound by Regulation No 2018/1805, these requests are regulated by domestic law (Section 793 (2) of the CPL), where a decision of a court of Latvia is needed. Latvia's law also enumerates the reasons why a court may defer the execution in such cases (Section 795 CPL).

Criterion 38.2 – NCBC is provided for under Latvian law and is available when the perpetrator is unavailable by reason of death, flight, absence or is unknown (Ch.59, CPL). Concerning confiscation, Latvia ensures the execution of foreign confiscation orders, establishing that the referred execution would be applied regardless of the proceeding applied in the foreign state (Sec.791, CPL). A court shall indicate in a ruling the type of confiscation of property and the property to be confiscated.

Criterion 38.3 – (a) Latvia has established since 2009 an ARO and is also a member of the CARIN network, which is used on a case-by-case basis to co-ordinate seizure and confiscation. In the case of European seizure and confiscation actions, the authorities may also co-ordinate through Eurojust. In addition, Latvia law allows for a representative of a foreign country to participate in the performance of procedural action, or to personally perform such operation in the presence of a representative of the institution fulfilling the request (Section 847 of the CPL). In case of an urgent request for tracing assets, the FIU may also be called upon to perform freezing, upon request from the ARO.

(b) As outlined in Recommendation 4, Latvia has implemented mechanisms for managing frozen or seized property (Sec 365, CPL and CoM Reg. No. 1025). 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.

Criterion 38.4 – Latvia may share confiscated property and property of corresponding value with other countries on a case-by-case basis (Sec.792 and 800 CPL). In any case, the approval of the MoJ is required. Latvia has also adopted new procedures for the distribution and for the transfer of funds, as well as the criteria for the distribution of funds, has been issued (CoM Reg. No. 265).

Weighting and Conclusion

R.38 is rated as compliant.

Recommendation 39 – Extradition

In the 2018 MER, Latvia was rated partially compliant with R.39 as it was only compliant with three of four criteria. However, in its 2019 FUR, Latvia was rated largely compliant as it implemented a clear process for timely prioritisation and execution of extradition requests; guidelines for the treatment of cases with regard to nationals, EU and non-EU nationals. It began to implement a case management system, but this was not yet in place. Latvia has since not made any material updates to R.39.

Criterion 39.1 – a) Latvia ensures that ML and TF are extraditable offences. It may execute extradition requests for the purpose of criminal prosecution, trial or the execution of a judgement regarding offences that are criminal according to both the Latvian and the requesting State's Law (dual criminality principle). Latvia is a party to the European Convention on Extradition (1957) and, as an EU Member State, has implemented EAWs. 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 TF are both associated with maximum penalties of deprivation of liberty exceeding one year.

(b) the GPO (as the central authority for the execution of extradition requests) adopted on 3 April 2019 an order which sets out rules for prioritisation and timely execution of extradition requests. The order stipulates that, upon receipt of requests for extradition, the priority order for their examination and enforcement is determined according to the category of a criminal offence. Requests for extradition of persons in relation to ML and TF are considered as priority requests. The introduction of a case management system is planned but is not yet finalised, as it appears to form part of a wider reform for electronic case management in the Latvian judiciary.

(c) Latvia does not place unreasonable or unduly restrictive conditions on the execution of requests

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.

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[135] criminal proceedings shall be executed (Sec.725(3) CPL). In practise this is typically achieved by agreement by both States that the criminal proceedings should be taken over by Latvia.

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. Latvian law stipulates that extradition requests may be obliged if they are for the purpose of criminal prosecution, trial or the execution of a judgement for offences that are criminal, and a punishment stipulated for the offence is deprivation of liberty the maximum limit of which is not less than one year, or a more serious punishment, if the international agreement does not provide otherwise. For execution of a judgment a person may be extradited if the person is convicted with a punishment that is related to deprivation of liberty for a term of not less than four months, if the international agreement does not provide otherwise. According to Section 195 and Section 79.2. of the CPL, ML and TF are criminal offences and both are both associated with maximum penalties of deprivation of liberty exceeding one year (Sec. 696, CPL).

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.

135. 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.

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

Latvia has addressed most of the deficiencies identified for R.39 in the 5th round MER. Minor deficiencies remain, since the introduction of a case management system is underway but not yet fully completed. **R.39 is rated largely compliant.**

Recommendation 40 – Other forms of international co-operation

In its 2018 MER, Latvia was rated partially compliant with R.40 on account of the following deficiencies: there was no explicit legal provision to provide assistance rapidly; there was no prioritisation of a case management system to process foreign requests; competent authorities, except for the FIU, did not have an obligation to provide feedback to foreign partners; the ability of the FIU to provide assistance was limited by some legal restrictions; there were limited provisions ensuring the confidentiality of foreign requests and information contained therein; and there was no explicit requirement or authorisation for supervisors to conduct inquiries on behalf of foreign partners. Latvia has addressed most deficiencies identified in the MER.

Criterion 40.1 – Latvian competent authorities can generally ensure that they can provide a wide range of international co-operation in relation to ML, TF and associated predicate offences both spontaneously and upon request. Latvia has adopted internal guidelines on International Co-operation and these stipulate that competent authorities (including supervisory authorities) must execute foreign requests without delay (and not later than within 10 days.). However, it is not clear if the FIU must meet this same requirement "without delay".

Criterion 40.2 – (a) Generally, Latvian competent authorities have a legal basis for providing international co-operation: Sec.62 and 63 AML/CFT/CPF Law for the FIU, Sec.46 AML/CFT/CPF 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 co-operation, 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. Latvijas Banka 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 supervisory authorities and control agencies have established secure exchange requirements.

(d) Latvia's Guidelines on International Co-operation require authorities (including supervisory authorities) to establish a priority order of requests received from foreign partners, and protection of information requests.

(e) Authorities have clear processes for safeguarding the information received. 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/CPF Law). LEAs information is also safeguarded on the basis of the State Police legal framework (Sec.375 CPL and Art.6(2) of the Police Act). Supervisors are directed by the Guidelines on International Co-operation to safeguard information.

Criterion 40.3 – In general, competent authorities do not need agreements to co-operate. However, Latvia is part of a large number of bilateral and multilateral agreements in order to facilitate co-operation. In particular, the FIU, has signed 46 MoUs. The FCMC has signed a number of MoUs with non-EU Member States authorities. The LGSI has signed a number of "Co-operation 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 co-operation agreements with Estonia, Lithuania and Georgia.

Latvia is part of a large number of bilateral and multilateral agreements in order to facilitate co-operation. The FIU does not need agreements or arrangements to co-operate; however, to facilitate co-operation, the FIU has signed 46 MoUs. The FCMC does not need agreements or arrangements to co-operate with EU Member States and has signed a number of MoUs with non-EU Member States authorities. The LGSI has

signed a number of "Co-operation arrangements between gambling supervisory institutions of EEA member states in the field of online gambling", on information exchange, initiated by the European Commission. Latvijas Banka does not need agreements or arrangements to co-operate in the area of AML/CFT/CPF and has not signed any co-operation agreements. The SRS FPD has concluded several bilateral co-operation agreements with Estonia, Lithuania and Georgia.

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". However, it is not clear whether there is such an obligation for the FIU and the LEAs in practice.

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 co-operation: the dual criminality condition may be an obstacle to exchanging information with LEAs or courts in relation to offences such as participation in an OCG; 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/CPF.

Criterion 40.6 – Sec.62 AML/CFT/CPF 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.

Additionally, Sec.46 AML/CFT/CPF Law does not mention any control or safeguards beyond requiring mutual agreement on use of information exchanged.

In line with the Manual on Law Enforcement Information Exchange, the State Police'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.

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.

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/CPF Law regardless of how the information has been acquired, including from a foreign partner.

Sec.46(9) and 48 AML/CFT/CPF 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.

Criterion 40.8 – FIU and the FCMC are authorised to conduct inquiries on behalf of foreign partners and such inquiries are conducted in practice (Sec. 46 (1) AML/CFT/CPF Law). To implement this Law, the MoJ circulated guidelines and issued a decision to introduce and amend internal regulations to authorise and conduct of enquiries on behalf of foreign authorities.

Criterion 40.9 – Chapter XIII of the AML/CFT/CPF Law establishes a wide range of international co-operation possibilities for the FIU, including for ML, associated predicate offences and TF. Latvia's law establishes the grounds for co-operation regardless of whether foreign FIUs are administrative, LEAs or judicial FIUs. This co-operation is subject to the dual criminality principle, and concerns exist in relation to the ability to co-operate when the request is only related to a crime of participation in a criminal group.

Criterion 40.10 – As per new Sec.62(2) AML/CFT/CPF 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).

Criterion 40.11 – FIUs have the power to exchange a) all information required to be accessible or obtainable directly or indirectly by the FIU and b) any other information which they have the power to obtain or access directly or indirectly at the domestic level (Sec.62 AML/CFT/CPF Law). Restrictions of exchanges

are defined on the basis of the potential use of information (see c.40.5) and reciprocity, not their nature (Sec. 675, CPL).

Criterion 40.12 – Under Sec.46(7) and 46(10), financial supervisors must, spontaneously or upon request, exchange information, including information related to or relevant for AML/CFT/CPF purposes. They may conduct this exchange with 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 Latvijas Banka Reg. 36 on the Purchasing and Selling of Cash Foreign Currencies complement that legal basis for the FCMC and Latvijas Banka respectively).

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).

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.

Criterion 40.15 – The FCMC may conduct inquiries on behalf foreign counterparts. but this power does not fully cover c.40.15. 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 EU 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 EU Member State for the performance of consolidated supervision (Sec.107.[1] and 107.[2] of the Credit Institutions Law).

Criterion 40.16 – As per Sec.46 AML/CFT/CPF, 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.

Criterion 40.17 – Latvia's LEAs can exchange domestically available information with foreign counterparts for intelligence or investigative purposes, including for ML, associated predicate offences or TF. The CPL, which is the legal basis for the co-operation of the State Police, establishes a wide range of LEAs co-operation (Ch.6, CPL). The State Police Law establish a broad range of co-operation of the State Police department (Art. 7, 14, Police Law).

Criterion 40.18 – LEAs are able to use their powers, including investigative techniques in-line with their domestic law to conduct inquiries and obtain information on behalf of foreign counterparts (Ch. 81, CPL). This includes the possibility to obtain the necessary information from natural and legal persons. The State 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).

Criterion 40.19 – LEAs in Latvia are able to form and participate in 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.

Criterion 40.20 – Sec.62(4) AML/CFT/CPF Law allows the FIU to make requests 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/CPF Law), information that could be used by the FIU for the purpose of international co-operation.

Weighting and Conclusion

While some deficiencies remain, this does not preclude the overall conclusion that the level of compliance with R.40 is brought to a level of largely compliant.

R.40 is rated largely compliant.

Annex B. Technical compliance shortcomings

Annex Table 1. Compliance with FATF Recommendations

Recommendations	Rating	Factor(s) underlying the rating
1. Assessing risks & applying a risk-based approach	C	
2. National co-operation and co-ordination	C	
3. Money laundering offences	LC	• Definition of the "commission of an offence within an organised crime group" 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
4. Confiscation and provisional measures	C	
5. Terrorist financing offence	LC	• Liability of legal persons can be established only in cases where a crime is committed in the interest or for the benefit of legal persons which narrows its application for TF; committing an offence within an "organised group" requires a previous agreement with divided responsibilities, which appears more restrictive than the mere acting with a common purpose
6. Targeted financial sanctions related to terrorism & TF	LC	• No definition of "funds and financial instruments," leaving the scope of assets subject to freezing unclear • No explicit reference to "other services", leaving their prohibition unclear • The procedures do not explicitly highlight an obligation to respect de-listing • It is not defined which circumstances must apply before authorising access to frozen funds or assets
7. Targeted financial sanctions related to proliferation	LC	• Deficiencies noted under R.6 apply
8. Non-profit organisations	LC	• Identification of NPOs meeting the FATF definition is not complete
9. Financial institution secrecy laws	C	
10. Customer due diligence	LC	• There is no explicit requirement to obtain names of the persons holding senior manager positions of legal arrangements.
11. Record keeping	LC	• Results of analyses are not explicitly mentioned among the documentation that is required to be kept.
12. Politically exposed persons	LC	• Timeframe of 12 months for derecognising PEP status after cassation of its functions (provided there is no high risk) is considered a limitation.
13. Correspondent banking	LC	• Definition of a shell bank has minor shortcomings.
14. Money or value transfer services	LC	• Fines for unlicensed MVTS are not proportionate and dissuasive; • It is not explicit that FIs have to monitor agents for compliance with AML/CFT programmes.
15. New technologies	LC	• Risk assessment requirements does not explicitly cover "new products" and "new delivery mechanisms" • Fit-and-proper requirements do not extend to associates of criminals and fail to cover all managerial roles in VASPs • Reference is made to shortcomings identified under Recommendations 10-21 • Feedback mechanisms for VASPs are not specified in the legislation • Shortcomings with sanctions envisaged under R.35 apply also to VASPs • There is no provision setting out that the information that is transmitted must be held by the covered originating and beneficiary VASP • There is no provision prohibiting conclusion of the transfer without required originator or beneficiary information • The deficiencies set out under c.6.5(d), 6.6(g), 7.2(d) and 7.4(d) apply to covered VASPs • Reference is made to deficiencies identified under Recommendations 37, 39 and 40
16. Wire transfers	LC	• Transfers of funds that equal EUR 1 000 do not fall under the scope of wire transfer regulation

Recommendations	Rating	Factor(s) underlying the rating
		• MVTS providers are not required to submit a SAR in all countries affected by a suspicious wire transfer and make the relevant transaction information available to the FIU
17. Reliance on third parties	LC	• The relying parties are not always required to obtain immediately, but only, if necessary, the obligatory information concerning CDD measures • Compliance with the Latvian AML/CFT/CPF Law does not necessarily amount to compliance with the requirements set out in R.10 to R.12 and R.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 RE
19. Higher-risk countries	LC	• More proactive communication of concerns to FIs 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 ("a suspicious transaction" or "funds creating suspicions"), this does not appear to cover the element of carelessness or negligence this included the situations where there are reasonable grounds for suspicions, which are nevertheless neglected.
21. Tipping-off and confidentiality	C	
22. DNFBPs: Customer due diligence	LC	• Reference is made to the deficiencies identified with regard to Recommendations 10, 11, 12, 15 and 17 • 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	• Risk assessment of foreign legal persons require some improvements (c.24.1); • There is no legal obligation placed on companies to record and hold basic listed in criterion 24.5(a); • Indirect control is not defined in the AML/CFT/CPF Law and there is no specific legal obligation placed on legal persons to co-operate with FIs/DNFBPs to provide accurate, adequate and up-to-date information (c.24.6(a)); • No documented decision was made available to the AT regarding chosen mechanisms to source BO information that are most appropriate in Latvia given its risk, context and materiality (c.24.6(b)); • No BO information retention period is prescribed for legal persons (c.24.7); • No information was made available on the compliance monitoring mechanisms with the accuracy of basic and beneficial information held by the legal persons (c.24.8); • Nominees are not explicitly prohibited, required to disclose their status or to be licenced (c.24.13); • It is not clear whether sanctions are in place applicable to legal persons for failure to store and update BO information (c.24.14); • No information was provided by the competent authorities (except for Latvijas Banka) on monitoring of the quality of assistance received (c.24.15).
25. Transparency and beneficial ownership of legal arrangements	PC	• No deadline set for registration of trustees of a foreign law trust; trustees of a EU law trust are exempted from registration in Latvia (c.25.1); • Trustees are not required to store the following information: class of beneficiaries, objects of a power and equivalent positions in similar legal arrangements other than a trust, basic and BO information of the parties to the trusts as well as basic information on other regulated agents of, and service providers to, the trust or similar legal arrangement (c.25.4); • There is no specific requirement placed on trustees to hold information listed at

Recommendations	Rating	Factor(s) underlying the rating
		c.25.4 for a period of five years after their involvement with the trust ceases and no requirement to hold or submit to the ER the information captured by c.25.4(b) and (c) (c.25.5); • There is no legal obligation placed on trustees to disclose their status to FIs and DNFBPs (c.25.7(a)); • Where BOs of the legal arrangement are registered in other EU member state, Latvian authorities are reliant on EU countries to keep this information adequate, accurate and up-to-date (c.25.8); • No explicit legal requirements exist to identify assets or income relating to the legal arrangements (c.25.9); (vii) no information was made available to the AT on sanctions for unco-operative trustees and for failing to grant timely access to the competent authorities to information discussed at c.25.4 and 25.5 held by trustees (c.25.11(b-c)); • No information provided by the law enforcement, the registry or other relevant competent authorities for monitoring requests for basic and BO information (c.25.12).
26. Regulation and supervision of financial institutions	LC	• AIFs are not subject to licensing, certain exemptions to registration apply (c.26.2); • Criminal associations are not explicitly covered by the legislation; however, certain internal processes are in place covering identification of criminal associates (c.26.3); • Latvia has not been subject to official assessments of the Basel Committee Principles, the IAIS Principles or the IOSCO Principles; for non-banking FIs, the extent to which risks are being considered for supervisory purposes varies (c.26.4); • Risk-based approach to supervision covering currency exchange offices and other FIs supervised by the CRPC and SRS has shortcomings, (c.26.5); • No detailed procedures covering all non-banking FIs to review the risk profiles on the basis of major events or developments in the management and operations of the FI or group (c.26.6).
27. Powers of supervisors	C	
28. Regulation and supervision of DNFBPs	LC	• There are no measures to prevent the associates of criminals from involvement in the ownership or activities of DNFBPs • No measures to prevent persons holding (or being BO of) a significant or controlling interest in the DNFBPs • There are deficiencies in the ML/TF risk-based supervision conducted by the supervisory authorities. • The reference is made to deficiency identified under R.35
29. Financial intelligence units	C	
30. Responsibilities of law enforcement and investigative authorities	C	
31. Powers of law enforcement and investigative authorities	C	
32. Cash couriers	C	
33. Statistics	C	
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	• 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.
37. Mutual legal assistance	LC	• Absence of a clear process for the timely prioritisation and execution of MLA requests • Absence of a complete case management system
38. Mutual legal assistance: freezing and confiscation	C	
39. Extradition	LC	• The introduction of a case management system for extradition requests is underway but not yet fully completed
40. Other forms of	LC	• CEs must execute foreign requests without delay, but not clear if FIU must meet

Recommendations	Rating	Factor(s) underlying the rating
international co-operation		same requirement. • Not clear if FIU and LEAs must provide feedback, as they are required "if possible", which is unclear • For FIU, there are concerns that the criminality condition may be an obstacle to exchanging information with LEAs or courts in relation to offences such as participation in an OCG (see R.3); 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 • 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. • There are some limits on the ability of the FCMC to conduct inquiries on behalf of foreign counterparts

Glossary of Acronyms[136]

	DEFINITION
Accountant (outsourced accountant)	A person regulated under the Accounting Law that is a qualified and experienced person who, on the basis of a written contract with an undertaking (except for a work-performance contract), pledges to provide or provides accounting services to the client.
Advocate (sworn advocate)	A person regulated under the Advocacy Law
AIF	Alternative Investment Fund
AIFP	Alternative Investment Fund Manager
AKUS	Unified Gaming Machine Control and Monitoring System
AML/CFT/CPF	Anti-Money Laundering, Combating the Financing of Terrorism and Combatting the Financing of Proliferation of Weapons of Mass Destruction
AML/CFT/CPF Action Plan	Cabinet Order ''Action plan for the Prevention of Money Laundering and Terrorism and Proliferation Financing''
AMLA	Anti-Money Laundering and Countering the Financing of Terrorism
AML/CFT/CPF Law	Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing
AMLCU	Anti-Money Laundering Coordination Unit
ARIN	Asset Recovery Inter-Agency Network
ARO	Asset Recovery Office
AT	Assessment Team
BNI	Bearer Negotiable Instruments
BO	Beneficial Owner
CARIN	Camden Asset Recovery Network
CCG	Cooperation Coordination Group
CIFG	Counter ISIS Finance Group
CIS	Commonwealth of Independent States
CFSP/Council Decision	The Common Foreign and Security Policy
CL	Criminal Law
CoM	Cabinet of Ministers
CoM Reg. No.	Cabinet of Ministers Regulation Number
CPC	Crime Prevention Council
CPCB	Corruption Prevention and Combating Bureau
CPL	Criminal Procedure Law
CRPC	Consumer Rights Protection Centre
CTFTI	Counter Terrorist Financing Taskforce- Israel
CTR	Threshold Report
EAW	European Arrest Warrant
EBA	European Banking Authority
ECB	European Central Bank
ECED	Economic Crime Enforcement Department
ECOFEL	Egmont Centre of FIU Excellence and Leadership
EDD	Enhanced Due Diligence
EDS	Electronic Declaration System
EEA	European Economic Area
EIO	European Investigation Order
EMI	Electronic Money Institution
EPPO	European Public Prosecutor's Office
ER	Enterprise Register
EU	European Union
EUR	Euro
FCMC	Financial and Capital Market Commission
FI	Financial Institution

136. Acronyms already defined in the *FATF 40 Recommendations* are not included into this Glossary.

FIU Latvia	Financial Intelligence Unit of Latvia
FSDB	Financial Sector Development Board
GDP	Gross Domestic Product
GDPR	EU General Data Protection Regulation
goAML	Main Software Solution of Financial Intelligence Data Receipt and Analysis System for FIU Latvia
GPO	General Prosecutor's Office
HUMINT	Human Intelligence
IAIS	International Association of Insurance Supervisors
IFIT	International Financial Intelligence Task Force
IMF	International Monetary Fund
IOSCO	International Organisation of Securities Commissions
IT	Information Technology
JIT	Joint Investigation Team
JSC	Joint Stock Company
LACA	Latvian Association of Certified Auditors
Latvijas Banka	The Central Bank of Latvia
Law on Sanctions	Law on International Sanctions and National Sanctions of the Republic of Latvia
LCSA	Latvian Council of Sworn Advocates
LCSN	Latvian Council of Sworn Notaries
LGSI	Lotteries and Gambling Supervisory Inspection
LLC	Limited Liability Company
LPSEM	Law on Payment Services and Electronic Money
MCPD	State Police Main Criminal Police Department
MFA	Ministry of Foreign Affairs
MLA	Mutual Legal Assistance
MoF	Ministry of Finance
MoI	Ministry of the Interior
MoJ	Ministry of Justice
MONEYVAL	The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism
MoU	Memorandum of Understanding
NCBC	Non-Conviction-Based Confiscation
NCIM	National Criminal Intelligence Model
Notary (sworn notary)	A person regulated under the Notariate Law.
NRA	National Risk Assessment
NRA1	Latvia's National Risk Assessment 2017-2019
NRA2	Latvia's National Risk Assessment 2020-2022
OCG	Organised Crime Group
OECD	Organisation for Economic Cooperation and Development
OpCEN	Operational Centre
OSINT	Open-Source Intelligence
PBO	Public Benefit Organization
PF	Proliferation Financing
PI	Payment Institutions
PO	Prosecutor's Office
RE (Reporting Entity)	Person subject to AML/CFT/CPF Law
SAR	Suspicious Activity Report
SBG	State Border Guard
SCA	Supervisory and Control Authority
SCC	Sanctions Coordination Council
SDD	Simplified Due Diligence
SIENA	Europol's Secured Information Exchange Application

SRA	Sectorial Risk Assessment
SRS	State Revenue Service
SRS TCPD	Tax and Customs Police Department of the State Revenue Service
SSM	Single Supervisory Mechanism
TF	Terrorist Financing
TFS	Targeted Financial Sanctions
UN	The United Nations
UNSCR	United Nations Security Council Resolution
UTR	Unusual Transaction Report
VASP	Virtual Asset Service Provider
WG	Working Group
WMD	Weapons of Mass Destruction
XBD	Cross-Border Dissemination
XBR	Cross-Border Report

www.coe.int/MONEYVAL

February 2026

Anti-money laundering and counter-terrorist financing measures - **Latvia**

Sixth Round Mutual Evaluation Report

This report provides a summary of AML/CFT measures in place in Latvia as at the date of the on-site visit (4-15 November 2024). It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Latvia AML/CFT system, and provides recommendations on how the system could be strengthened.