



# Lithuania

## Fifth Round Mutual Evaluation Report

### Executive Summary

1. This report provides a summary of the anti-money laundering (AML) and countering the financing of terrorism (CFT) measures in place in Lithuania as at the date of the on-site visit (7-18 May 2018). It analyses the level of compliance with the Financial Action Task Force (FATF) 40 Recommendations and the level of effectiveness of Lithuania's AML/CFT system, and provides recommendations on how the system could be strengthened.

#### *Key Findings*

- Lithuania's overall understanding of money laundering (ML) and financing of terrorism (FT) risks is limited as it largely depends on a national risk assessment (NRA) completed in 2015, which was found by the assessment team not to be comprehensive enough. Despite the various shortcomings identified in relation to the NRA, the understanding of certain risks at institutional level is more developed, particularly in relation to the use of cash, non-resident business, organised criminality, fictitious companies and FT. Lithuania has taken steps to address some identified threats and vulnerabilities, with concrete results e.g. reduction in tax evasion and the shadow economy. Lithuania has strong national co-ordination mechanisms in place in relation to ML and FT but not proliferation financing (PF).
- In recent years, as a result of greater enforcement of prosecutorial policies, major efforts have been made to target ML as an offence worth pursuing in its own right, in relation to criminal activity posing the highest ML threat. While the number of ML investigations has declined, there has been marked improvement in the ability of law enforcement authorities (LEAs) to investigate complex ML cases. In 2017 and 2018, some major ML convictions were achieved, involving substantial sums and complex laundering schemes. However, most ML convictions are for self-laundering. While a conviction for a predicate offence is not necessary to achieve a ML conviction, there is still some uncertainty as to the level of evidence that would be needed to convince the judiciary that funds derive from criminal activity in the absence of a criminal conviction. It is therefore not surprising that the number of third party/stand-alone ML convictions is limited. Sanctions have the potential to be dissuasive but have not been used effectively. There have only been few ML convictions involving legal persons.
- Depriving criminals of proceeds of crime is a policy objective endorsed at the highest levels. LEAs and prosecutors are aware of and implement the binding recommendations on financial investigations issued by the Prosecutor General (PG). The level of sophistication of financial investigations to trace proceeds of crime has improved and the amount of provisionally seized assets

has increased considerably. The volume of confiscated assets remains somewhat modest. The absence of a sound mechanism at the border to identify suspicious transportation of cash at the borders and confiscate such cash raises significant concern, in view of the risks that Lithuania faces.

- The Financial Intelligence Unit (FIU) has a reasonably thorough analysis procedure. LEAs have used the analytical products of the FIU to pursue ML and associated predicate offences to some extent. However, they do not exploit the full potential of the FIU. There are factors which may limit the effectiveness of the FIU's analysis process, particularly the lack of advanced IT analytical tools, limited human resources and absence of a prioritisation mechanism for suspicious transaction reports (STRs). While the number of STRs has increased, the overall quality is still not up to a satisfactory level. It is positive that LEAs have used financial intelligence generated through financial investigations carried out at the intelligence stage to pursue unlawful enrichment and tax evasion, although to a lesser extent ML.
- Financial institutions (FIs) have a good understanding of ML/FT risks and are aware of their anti-money laundering/countering financing of terrorism (AML/CFT) obligations, although major weaknesses have been observed in some money and value transfer services (MVTs) and currency exchange offices, especially in relation to TFS obligations and FT risks. Understanding of ML/FT risks among designated non-financial businesses and professions (DNFBPs) is insufficient, especially in the real estate sector and traders over EUR 10,000 in cash. The application of CDD measures in the financial sector (especially banks) is good, except for difficulties in verifying BOs of foreign legal persons. CDD by DNFBPs is of a lower quality. Training is deemed insufficient by the private sector, especially non-bank FIs and DNFBPs.
- Licensing controls undertaken by the BoL in relation to FIs are very good. This is less so the case with respect to DNFBP supervisors, also as a result of the absence of registration requirements for company service providers (CSPs), real estate agents and accountants. While the BoL and the FIU have a good understanding of ML risks, DNFBP supervisors have a limited understanding. The BoL has increased the level of supervision significantly during the last two years with some strong elements of risk-based supervision. Risk-based approaches and the levels of supervision undertaken require improvement by most of the DNFBP supervisors. The level of sanctions applied by the BoL has generally been commensurate with its supervisory findings. There are very good elements of effectiveness and dissuasiveness of sanctions although the regime is not yet fully effective and dissuasive. In relation to DNFBPs, the application of the sanctions framework is at a relatively early stage of development.
- ML/FT risks posed by Lithuanian legal entities have not been assessed. However, there is universal agreement among the authorities that fictitious private limited liability companies pose the highest risk. The mechanism which ensures that beneficial ownership (BO) information of legal entities is maintained and made available to competent authorities relies on customer due diligence (CDD) measures applied by the private sector, mainly banks. The mechanism is broadly adequate. Basic information is available on all types of legal persons. Shareholder information is not available on certain types of legal persons. There is no system to ensure that the information kept by the registry is kept accurate and current.
- Authorities have an uneven but broadly adequate understanding of FT risks, consistent with Lithuania's risk profile. There have only been two FT cases in Lithuania. One resulted in a FT conviction. The other is still on-going. While there have been seven terrorism related investigations, no financial investigations were carried out alongside these investigations. There appear to be

mechanisms in place for the identification, investigation and prosecution of FT. However, the skills required to deal with such cases need to be developed further. The Customs Service does not have the specific power to stop and restrain currency at the borders in order to ascertain whether evidence of ML/FT may be found. In addition, MVTs providers may not be submitting relevant FT suspicions. Both of these circumstances may result in the non-detection of FT.

- Although no funds have been frozen and the legal framework for targeted financial sanctions (TFS), both for FT and PF, is not fully in line with the Standards (in particular, EU procedures create delays in transposing designations), Lithuania displays elements of an effective TFS system. FIs are aware of UN and EU designations and have customer and transaction screening systems. However, DNFBPs demonstrated limited understanding of TFS obligations. There is no formal procedure to identify targets for designations and no designation has been made or proposed. The operational framework for the implementation of TFS by the authorities lacks clarity. Although there is no dedicated interagency mechanism, a weekly coordination meeting takes place at the ministerial level on PF-related policy issues. Outreach is provided to the private sector but remains insufficient. Supervisors exhibited limited proactivity in relation to PF-related TFS obligations and evasion challenges.
- Based on a sound legal and procedural framework, Lithuania exchanges information with foreign partners in a comprehensive, proactive and timely manner, both upon request and spontaneously, and in line with its risk profile. The mutual legal assistance (MLA) provided is of good quality as evidenced by the feedback provided by the global network. Lithuania actively seeks international co-operation from other states. This has resulted in convictions and the seizure and confiscation of proceeds of crime, as evidenced by various case studies provided to the assessment team. Informal co-operation is conducted effectively.

### ***Risks and General Situation***

2. The financial sector in Lithuania is bank-centric (79.2 % of the financial system assets), and is largely concentrated around three foreign-owned banks. The banking services are mainly traditional and include loans and deposits. Banks have been reducing their non-resident customer base for de-risking purposes; and the number of higher risk non-resident customers appears to be very low. In recent years, the Bank of Lithuania has aimed to create an attractive regulatory environment to foreign finance institutions and Fintech start-ups in the country. In 2014, a residence-by-investment programme was also established to attract foreign business.

3. While there is no information on the volume of foreign proceeds invested in or flowing through Lithuania, the NRA notes that the main domestic sources of criminal proceeds are corruption, fraud (including tax fraud), drug trafficking and smuggling of goods. Organised crime (involved in smuggling of goods, drug trafficking and fraud) maintains a strong presence in Lithuania. The significant shadow economy in Lithuania, which is exacerbated by tax offences, and combined with the widespread use of cash, constitutes another important vulnerability. In the financial sector, the NRA cites the increase of technologies in money transfers and the use of cash as the main vulnerabilities. Major vulnerabilities are also found in relation to formal and informal remittances, which play an important role in Lithuania's economy. The DNFBP sector as a whole constitutes a vulnerability due to its poor understanding of ML/FT risks and implementation of AML/CFT requirements.

4. The authorities assess the terrorist threat as low in Lithuania. There has only been one FT conviction. While FT is considered to have a low expectancy level, the NRA notes that (foreign) residents may support known terrorist organisations abroad and lists “lone wolf” terrorism (involving self-financing) as a high-risk priority.

### ***Overall Level of Effectiveness and Technical Compliance***

5. Since the last evaluation, Lithuania has taken steps to improve its AML/CFT framework. In 2013, the Criminal Code was amended to explicitly criminalise the financing and support of terrorism and extend the list of activities which are punishable as ML. Amendments to the AML/CFT Law were adopted in 2014 to reorganise the STR regime and address deficiencies concerning CDD and record keeping obligations. Further amendments to the AML/CFT Law were adopted on 13 July 2017 to transpose the Directive of the European Parliament and Council (EU) 2015/849. The amendments extended the scope of obliged entities and reinforced sanctions for breaches of AML/CFT preventive measures. However, some deficiencies remain in Lithuania’s technical compliance framework, in particular in relation to risk assessment, national cooperation and coordination and targeted financial sanctions.

6. Lithuania has demonstrated a substantial level of effectiveness in engaging in international cooperation. A moderate level of effectiveness has been achieved in all the other areas covered by the FATF Standards.

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

7. Lithuania’s understanding of ML/FT risks is limited and high-level in nature. The understanding of risks is largely based on the 2015 NRA, which presents a number of weaknesses. The document is informed by an insufficient range of information sources and the analysis remains high-level in nature. The NRA focuses mainly on threats and vulnerabilities, leaving aside the resulting risks. It does not describe the main ML methods, trends and typologies or give adequate consideration to cross-border threats and the Fintech sector. The understanding of risks at the institutional level is more developed concerning issues such as the use of fictitious companies and the use of cash.

8. Based on an action plan which was completed in 2017, Lithuania has taken steps to address a number of threats and vulnerabilities, with concrete results, in particular, in reducing tax evasion and the shadow economy. However, further efforts are needed to mitigate other significant vulnerabilities, in particular in relation to investigation and prosecution of ML and AML/CFT supervision.

9. Lithuania has strong co-ordination mechanisms in place, including the AML/CFT Coordination Group and many agreements on exchange of information between authorities at the operational level. However, there are no co-ordination mechanisms with respect to PF.

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

10. The FIU has a reasonably sound analysis procedure and the products disseminated by the FIU were effectively used by LEAs to some extent to initiate pre-trial investigations. The FIU has broad and unhindered access to information sources. The FIU regularly makes use of these sources in the

course of its analysis. Analysts appear knowledgeable and have produced complex analysis. There are some factors which have a negative impact on the effectiveness of analysis: insufficient human resources and the lack of advanced IT tools and prioritisation mechanisms for STRs.

11. The number of STRs has increased considerably in the period under review, but their overall quality remains unsatisfactory. MVTs, real estate agents, notaries and CSPs have filed few or no STRs, which is a concern in light of the ML/FT risks they face. No analysis has been initiated on the basis of customs declarations.

12. It is positive that LEAs have used financial intelligence generated through financial investigations carried out at the intelligence stage to pursue unlawful enrichment and tax evasion, although to a lesser extent ML.

13. At the beginning of the period under review, opportunities to identify ML in the course of predicate offence investigations were not explored to the greatest extent possible, the degree to which ML was targeted by each LEA varied and the approach to proactively pursue ML cases was fragmented. Latterly, concrete efforts have been made to target ML as an offence worth pursuing in its own right, separately from the prevention and repression of predicate criminality, as a result of greater enforcement of prosecutorial policies, which classify ML as a high priority offence. This is supported by a number of on-going investigations presented to the assessment team, some of which have already resulted in ML convictions. However, a national ML-specific operational policy is needed to ensure a more uniform and effective approach across all LEAs involved.

14. In 2017 and 2018, some major ML convictions were achieved, involving substantial sums and complex laundering schemes. However, most ML convictions are for self-laundering. While a conviction for a predicate offence is not necessary to achieve a ML conviction, there is some uncertainty as to the level of evidence that would be needed to convince the judiciary that funds derive from criminal activity. The use of circumstantial evidence to prove that the launderer knew that the property derived from criminal activity is not always accepted by the courts, although there are clear precedents. It is therefore not surprising that the number of third party and stand-alone ML convictions is limited.

15. The sanctions under Article 216 have the potential to be dissuasive. However, sanctions have not been used effectively and dissuasively. Many of the sentences involved a fine, often lower than the laundered proceeds. Most imprisonment sentences were suspended. There have not been many ML convictions for legal persons, despite the fact that legal persons feature recurrently in cases presented by the authorities.

16. Depriving criminals of proceeds of crime is a policy issue endorsed at the highest levels within the prosecutorial and law enforcement structures in Lithuania. The complexity and sophistication of financial investigations appears to have improved in the last couple of years. It has now become increasingly common, when investigating complex proceeds-generating crimes, to set up joint investigation teams, involving case investigators, intelligence officers and financial specialists. However, further progress is needed to continue enhancing the quality of financial investigations, especially within the State Investigation Service.

17. Data on the volume of assets seized and confiscated in relation to ML and other predicate offences and on restitution to victims demonstrates a visible improvement in the implementation of seizure and confiscation requirements, especially when compared to the situation at the time of the

4th Round MER adopted in 2012. While the volume of seized assets has increased significantly, the volume of confiscated assets remains somewhat modest.

18. The absence of a sound mechanism at the border to identify suspicious transportation of cash at the borders and confiscate such cash raises significant concern.

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

19. The authorities involved in the prevention and investigation of FT and terrorist-related crimes have a broad understanding of FT risks and threats, which is consistent with the level of risk present in the country. The SSD has the most advanced understanding of FT risks.

20. There have only been two FT cases in Lithuania. One resulted in a FT conviction. The other is still on-going. There have been seven terrorism related investigations. No financial investigations were carried out alongside these investigations. While there appear to be mechanisms in place for the identification, investigation and prosecution of FT, the skills required to deal with such cases need to be developed further.

21. The Customs Service does not have the specific power to stop and restrain currency at the borders in order to ascertain whether evidence of ML/FT may be found. In addition, MVTs providers may not be submitting relevant FT suspicions. Both of these circumstances may result in the non-detection of FT.

22. While the Public Security Programme (2015-2025) contains a specific goal relating to terrorism and FT, it does not appear that an action plan has been developed to implement this goal in practice. Therefore, the assessment team could not determine that the investigation of FT would be integrated, and used to support, national counter-terrorism strategies and investigations.

23. The sanctions provided in the CC for FT offences appear to be proportionate and dissuasive. In the one court decision related to FT the most severe punishment was applied. The instrument of the crime was confiscated.

24. Lithuania has identified potential vulnerabilities within the NPO sector. Although NPOs are only supervised for tax-related issues, the SSD closely monitors those NPOs that could be misused for FT purposes. Outreach to NPOs is insufficient.

25. The legal framework for FT- and PF-related TFS is not fully in line with the Standards. In particular, EU procedures impose delays in transposing designations (except for Iran). Although no funds have been frozen, Lithuania displays elements of an effective system to implement TFS pursuant to UNSCRs 1267 and 1373. FIs, including Fintech operators, are aware of UN and EU designations and have systems in place to monitor customers and transactions against the relevant lists. DNFBSs demonstrated limited understanding of these obligations. Lithuania does not have formal procedures to identify targets for designations and has not proposed or made any designations. The operational framework governing the implementation of TFS by the authorities lacks clarity.

26. While no PF-related funds have been frozen, awareness of PF-related TFS is widespread in the financial sector, in particular among banks. In many cases banks demonstrated a strict compliance approach that has resulted in refusing payments not subject to TFS (e.g. any transaction linked to Iran). As with FT, DNFBSs show a limited awareness of PF lists and follow a seemingly sporadic screening approach. The Ministry of Foreign Affairs is the lead agency for countering PF. Although



there is no dedicated interagency mechanism, a weekly coordination meeting on takes place at the ministerial level on PF-related policy issues. The Ministry of Economy, as the licensing authority for dual-use goods, regularly holds workshops for industry associations, in which updates on TFS lists are provided. Both the FIU and the MFA have adopted a more targeted approach in assisting banks to comply with their PF-related TFS obligations, including to prevent sanctions evasion. Additional outreach and typologies would be beneficial. Supervisors exhibited limited proactivity in relation to PF-related TFS obligations and evasion challenges.

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

27. Banks have a high-level of understanding of ML/TF risks and are aware of their AML/CFT obligations. This is broadly the case for other financial institutions, but major weaknesses have been observed in some MVTs and currency exchange offices, especially in relation to TFS obligations and FT risks. Understanding of ML/FT risks among the DNFBPs sector is not sufficient, especially in the real estate sector and traders over EUR 10,000 in cash. The application of CDD measures in the financial sector (especially banks) is good, except for difficulties in verifying BOs. CDD by DNFBPs is of a lower quality, with very limited understanding of the minimum requirements set by the law in some cases. Overall, REs understand the STR procedure, but reports from MVTs, currency exchange offices, real estate agents, notaries and lawyers are limited in light of their risk profile. Training is deemed insufficient by the private sector, especially non-bank FIs and DNFBPs.

#### *Supervision (Chapter 6 - IO3; R.26-28, R. 34-35)*

28. The BoL applies very good controls in relation to the licensing of FIs to prevent criminals from holding, or being the BO of, a significant or controlling interest or holding a management function in FIs. The BoL has a good understanding of ML risk within banks, and the products and services offered by FIs and a general understanding of ML risks in the sectors it supervises. It broadly understands FT risk. The BoL is a proactive supervisor and has increased the level of supervision significantly during the last two years. It has some strong elements of risk-based supervision and it is moving towards both a comprehensive risk-based approach and a level of supervision in line with risks. The level of sanctions applied by the BoL has generally been commensurate with its supervisory findings. There are very good elements of effectiveness and dissuasiveness of the sanctions regime although it is not yet fully effective and dissuasive.

29. Licensing controls in relation to DNFBPs vary, including an absence of registration requirements for CSPs, real estate agents and accountants. In general, DNFBP supervisory authorities except the FIU (which has a generally good understanding of the ML/FT risks of real estate agents and accountants) have a developing understanding of risk. The extent of AML/CFT supervision and the degree this is risk-based varies, with the GCA, the FIU and the LAO being most proactive authorities; overall, risk-based approaches and the levels of supervision undertaken require improvement. Some sanctions have been applied by DNFBP supervisory authorities and the courts in relation to DNFBPs. Overall, the application of the frameworks and their effectiveness is at a relatively early stage of development.

*Transparency of Legal Persons and Arrangements (Chapter 7 - IO5; R. 24-25)*

30. While Lithuania has not conducted a formal assessment of risks posed by legal persons, it is universally understood by competent authorities that the use of fictitious private limited companies in criminal schemes constitutes a significant ML/FT risk.

31. The Register of Legal Entities (RLE) maintains basic information on all types of legal persons, which is publicly-available. This ensures that access to competent authorities is timely. However, there is no system to ensure that the information is kept accurate and current. Shareholder information on the vast majority of legal persons is available either from the RLE or at the Information System of Members of legal Entities ("JADIS"), which jointly hold information on 83.8% of legal persons registered in Lithuania. Shareholder information in JADIS is available to competent authorities (free of charge) and to reporting entities (against a fee), though this information is not verified to ensure that it is accurate and current.

32. The mechanism to ensure availability of BO information relies on CDD performed by private sector entities, mainly banks, which verify information on the basis of information maintained at the RLE and JADIS. Given that most legal persons registered in Lithuania are owned and controlled by Lithuanian natural (81.1%) and legal persons (6.6%), this mechanism is broadly adequate with respect to legal persons whose information is contained in JADIS. In fact, competent authorities have not encountered any difficulties in obtaining BO information in this manner. However, there remains a small gap with respect to some legal persons in relation to which information is not available at the RLE or JADIS (16.2% of all legal persons). Additionally, there is no system of verification of information entered into JADIS. Furthermore, there is no complete information on the number of Lithuanian corporate shareholders whose shareholders are legal persons registered outside of Lithuania.

33. Lithuania has implemented effective mitigating measures against the use of fictitious private limited liability companies for criminal purposes, which are considered to pose highest risk, compared to other legal persons. The STI actively monitors information on VAT payers to identify fictitious companies. Many cases involving the use of fictitious companies have been prosecuted. The FIU conducts typology exercised to assist in determining the scale of the problem and forward cases to LEAs.

*International Cooperation (Chapter 8 - IO2; R. 36-40)*

34. Lithuania has a sound legal and procedural framework to exchange information and cooperate with its foreign counterparts in relation to ML, associated predicate offences and FT. Information is exchanged comprehensively, proactively and in a timely manner, both upon request and spontaneously. The evaluation team received positive feedback from the AML/CFT global network in relation to the quality and timeliness of assistance provided by Lithuania.

35. Lithuania actively seeks international co-operation from other states. This has resulted in convictions and the seizure and confiscation of proceeds of crime, as evidence by various case studies provided to the assessment team.

36. Effective cooperation between Lithuania and other EU Member States is well-developed, especially with the other Baltic States. Regular cooperation based on UN instruments and bilateral agreements also takes place outside of the EU, especially with neighbouring countries.



37. On average, requests for MLA are processed within 1 to 4 months, depending on the nature of the request, the type of assistance requested and the complexity of the request. Urgent requests are executed within shorter time-frames.

38. The authorities advised that not a single MLA request related to ML/FT was refused in the period under review. This was also confirmed by the AML/CFT global network. In the few instances where MLA was not provided in relation to predicate offences, the authorities explained that this was due to deficiencies in the form and content of a request as laid down in international treaties, statute of limitations and/or requests relating to acts which did not involve criminal liability.

39. While extradition figures show that only a portion of extradition requests is actually executed, the authorities explained that a significant part of these requests involved persons who did not reside in Lithuania. The others were refused on the grounds that Lithuania cannot extradite its own nationals.

40. In terms of informal co-operation, the FIU has a broad legal basis for the exchange of information with its foreign counterparts. Spontaneous information is regularly exchanged. The assistance provided is considered effective in terms of timeliness and quality. LEAs are also active in the sphere of informal cooperation through direct communication via Europol, Interpol, SIENA and CARIN. The creation of joint investigative teams between Lithuanian LEAs and their foreign counterparts on large scale cases has become increasingly common. The BoL makes full use of a large number of bilateral and multilateral agreements to exchange information with its counterparts, especially in relation to AML/CFT on-site inspections.

### ***Priority Actions***

1. Lithuania should, as a matter of priority, conduct the next iteration of the NRA, which should:
  - a) involve supervisory authorities, especially the BoL, more directly – for instance all supervisory authorities should be involved in the discussions of working groups set up to discuss threats and vulnerabilities and not just be required to complete questionnaires;
  - b) be based on a more comprehensive set of qualitative and quantitative information sources – for instance, information from the SSD on FT risks, information from the BoL on the risks posed by cash and non-resident customers, information from the FIU on typologies and more detailed statistics;
  - c) consider to a larger degree the cross-border ML threat (at least include an assessment of: financial flows to and from high risk countries, MLA requests received and sent, international informal requests from and to FIU and LEA, STRs and cash declarations), the use of fictitious companies (by analysing information from LEAs), the use of cash (by analysing information from the FIU, the BoL, the Customs Department and the STI);
  - d) assess the vulnerabilities of the Fintech sector;
  - e) for the purpose of the assessment of FT risks, separately consider the risks of movement, collection, provision and use of funds and include an assessment of the vulnerabilities of financial instruments and risks related to flows to high-risk jurisdictions.
2. Establish mechanisms for the co-ordination of PF actions. The authorities may wish to extend the mandate of the AML/CFT Coordination Group to cover PF issues and the membership of the Group to include other relevant stakeholders, such as the MoE.

3. The use of financial intelligence developed through financial investigations at the intelligence stage should be widened to, inter alia, target ML and FT elements (in addition to unlawful enrichment and tax-related offences<sup>1</sup>), follow the trail of potential proceeds of crime and identify other involved parties, such as beneficiaries of transactions, to establish new or additional links and leads for investigations.
4. The authorities should take measures to improve the quality of STRs, including by: 1) determining whether the suspicious indicators need to be further enhanced; 2) holding discussions with banks to ensure that reporting is further aligned with the risks facing Lithuania; 3) assess whether the quality and reporting level by each bank are adequate; 4) hold awareness-raising activities with reporting entities facing a higher risk of ML/FT on reporting; 5) provide more systematic feedback to reporting entities on reporting; 6) consider why other reporting entities have not submitted any STRs (other than banks and MVTs); 7) consider whether the limited number of FT STRs is entirely in line with the risks that Lithuania faces.
5. The Customs Department should develop sound mechanisms to be able to detect false or non-declarations and suspicions of either ML or FT (which could arise even where declarations are submitted).
6. The FIU should re-calibrate its analysis and dissemination priorities to focus on the highest ML risks and make more effective use of its limited resources.
7. Enhance the technical capacities (IT tools) of the analysis function of the FIU and ensure that it is adequately resourced in terms of staff. Compliance responsibility should not deprive resources from the analysis section. Compliance matters should be dealt completely separately from the analysis section.
8. Lithuania should strengthen existing law enforcement strategies by developing a ML-specific operational policy which should:
  - a) clearly set out how each LEA is to identify and initiate ML cases, including through parallel financial investigations both at criminal intelligence and pre-trial stage, on the basis of FIU disseminations, in the course of the investigation of a predicate offence; and through the sharing of information between LEAs; and
  - b) include measures to (1) pro-actively identify ML elements at the earliest stages of suspicion and consequently initiate ML investigation rather than focussing only on unlawful enrichment; and (2) trace the sources and destination of proceeds of crime.
9. Law enforcement efforts should be in line with the ML risks. In particular, LEAs should continue targeting more complex and sophisticated types of ML with special attention to cases which involve the misuse of fictitious companies, trade-based ML, fraud, organised crime, corruption and ML related to foreign predicate offences). In complex criminal schemes, LEAs should extend their investigation with the aim of identifying the person(s) who ultimately controls and benefits from the scheme.
10. The PG Recommendations should be updated to improve the ability of LEAs and the Prosecution Service developing 'objective circumstantial and indirect evidence' when proving: (1)

---

<sup>1</sup> The authorities indicated that following the on-site visit measures were taken to update the PG's Recommendations accordingly.

that the property is the proceeds of crime, in the absence of a conviction for the underlying crime; and (2) intent and knowledge of the launderer.

11. LEAs and the PGO should continue challenging the judiciary with stand-alone ML cases where it is not possible to establish precisely the underlying offence(s) but where the courts could infer the existence of predicate criminality from adduced facts and circumstances. More cases related to professional third-party ML should also be brought forward.

12. Revise the PG's Recommendations on financial investigations to extend their scope beyond the financial profile of the suspect and include reference to the identification and tracing of movements of the proceeds of crime and identifying the extent of criminal networks and/or the scale of criminality.

13. Strengthen the enforcement of the PG's Recommendations to ensure that all types of property (laundered property, co-mingled, property of equivalent value and instrumentalities) are provisionally restrained and confiscated upon conviction

14. Lithuania should enable targeted financial sanctions relating to FT and PF to be implemented without delay, in line with the FATF Recommendations and introduce a mechanism(s) for the identification of targets for designations in relation to FT UNSCRs.

15. As planned, registration of TCSPs should be introduced and registration and standard setting frameworks should be put in place for real estate agents and accountants. The GCA should develop its existing approach, while other DNFBP supervisors should take additional steps to prevent criminals from holding, or being the beneficial owner of, a significant or controlling interest or holding a management function in DNFBPs.

16. A mechanism should be introduced so that approaches by the supervisory authorities to addressing risk and the development of comprehensive risk-based supervision are coordinated.

17. The BoL and the FIU should use onsite and offsite tools, and the next iteration of the NRA, to enhance their understanding of ML and FT risks relevant to their sectors. Other supervisory authorities should use these tools and the NRA to develop comprehensive understanding.

18. The BoL should enhance its existing risk-based approach and further develop its ML/FT risk assessment in order to ensure that risk-based supervision is comprehensive. DNFBP supervisors should take the significant steps required to achieve comprehensive risk-based approaches to supervision. Systematic AML/CFT training programmes should be developed by the supervisory authorities.

## Effectiveness & Technical Compliance Ratings

### Effectiveness Ratings

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

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

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

All rights reserved. Reproduction is authorised, provided the source is acknowledged, save where otherwise stated. For any use for commercial purposes, no part of this publication may be translated, reproduced or transmitted, in any form or by any means, electronic (CD-Rom, Internet, etc.) or mechanical, including photocopying, recording or any information storage or retrieval system without prior permission in writing from the MONEYVAL Secretariat, Directorate General of Human Rights and Rule of Law, Council of Europe (F-67075 Strasbourg or [moneyval@coe.int](mailto:moneyval@coe.int)).