

FATF



Anti-money laundering and counter-terrorist financing measures

Luxembourg

Mutual Evaluation Report

September 2023





The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CTF) standard.

For more information about the FATF, please visit the website: www.fatf-gafi.org.

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

This assessment was adopted by the FATF at its June 2023 Plenary meeting.

Citing reference:

FATF (2023), *Anti-money laundering and counter-terrorist financing measures – Luxembourg*, Fourth Round Mutual Evaluation Report, FATF, Paris
<https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Mutualevaluations/Mer-luxembourg-2023.html>

©2023 FATF/OECD -. All rights reserved.

No reproduction or translation of this publication may be made without prior written permission.

Applications for such permission, for all or part of this publication, should be made to

the FATF Secretariat, 2 rue André Pascal 75775 Paris Cedex 16, France

(fax: +33 1 44 30 61 37 or e-mail: contact@fatf-gafi.org).

Photo Credit - Cover: © LMIH/Sabino Parente

Table of Contents

| | |
|---|------------|
| Executive Summary | 3 |
| Key Findings..... | 3 |
| Risks and General Situation | 5 |
| Overall Level of Compliance and Effectiveness | 6 |
| Priority Actions..... | 11 |
| Effectiveness & Technical Compliance Ratings..... | 12 |
| MUTUAL EVALUATION REPORT | 13 |
| Preface | 13 |
| Chapter 1. ML/TF RISKS AND CONTEXT..... | 15 |
| ML/TF Risks and Scoping of Higher Risk Issues..... | 16 |
| Materiality..... | 18 |
| Structural Elements | 19 |
| Background and Other Contextual Factors | 19 |
| Chapter 2. NATIONAL AML/CFT POLICIES AND COORDINATION | 33 |
| Key Findings and Recommended Actions..... | 33 |
| Immediate Outcome 1 (Risk, Policy and Co-ordination)..... | 35 |
| Chapter 3. LEGAL SYSTEM AND OPERATIONAL ISSUES | 45 |
| Key Findings and Recommended Actions..... | 45 |
| Immediate Outcome 6 (Financial Intelligence ML/TF) | 49 |
| Immediate Outcome 7 (ML investigation and prosecution)..... | 65 |
| Immediate Outcome 8 (Confiscation)..... | 89 |
| Chapter 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION | 107 |
| Key Findings and Recommended Actions..... | 107 |
| Immediate Outcome 9 (TF investigation and prosecution)..... | 110 |
| Immediate Outcome 10 (TF preventive measures and financial sanctions) | 120 |
| Immediate Outcome 11 (PF financial sanctions) | 127 |
| Chapter 5. PREVENTIVE MEASURES | 133 |
| Key Findings and Recommended Actions..... | 133 |
| Immediate Outcome 4 (Preventive Measures)..... | 135 |
| Chapter 6. SUPERVISION | 155 |
| Key Findings and Recommended Actions..... | 155 |
| Immediate Outcome 3 (Supervision)..... | 157 |
| Chapter 7. LEGAL PERSONS AND ARRANGEMENTS | 191 |
| Key Findings and Recommended Actions..... | 191 |
| Immediate Outcome 5 (Legal Persons and Arrangements)..... | 192 |
| Chapter 8. INTERNATIONAL COOPERATION | 209 |
| Key Findings and Recommended Actions..... | 209 |
| Immediate Outcome 2 (International Cooperation) | 210 |

| | |
|--|------------|
| TECHNICAL COMPLIANCE | 234 |
| Recommendation 1 – Assessing risks and applying a risk-based approach | 234 |
| Recommendation 2 - National Co-operation and Co-ordination..... | 236 |
| Recommendation 3 - Money laundering offence..... | 237 |
| Recommendation 4 - Confiscation and provisional measures | 238 |
| Recommendation 5 - Terrorist financing offence | 239 |
| Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing | 240 |
| Recommendation 7 – Targeted financial sanctions related to proliferation | 245 |
| Recommendation 8 – Non-profit organisations..... | 247 |
| Recommendation 9 – Financial institution secrecy laws..... | 250 |
| Recommendation 10 – Customer due diligence..... | 250 |
| Recommendation 11 – Record-keeping | 254 |
| Recommendation 12 – Politically exposed persons..... | 254 |
| Recommendation 13 – Correspondent banking | 255 |
| Recommendation 14 – Money or value transfer services | 256 |
| Recommendation 15 – New technologies..... | 257 |
| Recommendation 16 – Wire transfers | 259 |
| Recommendation 17 – Reliance on third parties | 261 |
| Recommendation 18 – Internal controls and foreign branches and subsidiaries..... | 262 |
| Recommendation 19 – Higher risk countries | 263 |
| Recommendation 20 – Reporting of suspicious transactions | 264 |
| Recommendation 21 – Tipping-off and confidentiality..... | 264 |
| Recommendation 22 – DNFBPs: Customer due diligence..... | 265 |
| Recommendation 23 – DNFBPs: Other measures..... | 265 |
| Recommendation 24 – Transparency and beneficial ownership of legal persons..... | 266 |
| Recommendation 25 – Transparency and beneficial ownership of legal arrangements | 270 |
| Recommendation 26 – Regulation and supervision of financial institutions..... | 273 |
| Recommendation 27 – Powers of supervisors | 274 |
| Recommendation 28 – Regulation and supervision of DNFBPs..... | 275 |
| Recommendation 29 – Financial intelligence units..... | 277 |
| Recommendation 30 – Responsibilities of law enforcement and investigative authorities..... | 279 |
| Recommendation 31 - Powers of law enforcement and investigative authorities | 280 |
| Recommendation 32 – Cash Couriers..... | 281 |
| Recommendation 33 – Statistics..... | 283 |
| Recommendation 34 – Guidance and feedback | 283 |
| Recommendation 35 – Sanctions | 284 |
| Recommendation 36 – International instruments | 285 |
| Recommendation 37 - Mutual legal assistance | 285 |
| Recommendation 38 – Mutual legal assistance: freezing and confiscation..... | 286 |
| Recommendation 39 – Extradition | 287 |
| Recommendation 40 – Other forms of international co-operation..... | 288 |
| Summary of Technical Compliance – Key Deficiencies | 293 |
| Glossary of Acronyms | 297 |

Executive Summary

1. This report summarises the anti-money laundering and counter-terrorist financing (AML/CFT) measures in place in Luxembourg as at the date of the on-site visit: 2-18 November 2022. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Luxembourg's AML/CFT system and provides recommendations on how the system could be strengthened.

Key Findings

1. Luxembourg's first national risk assessment (NRA), completed in 2018, triggered several changes in its AML/CFT regime, such as improvements to the legal framework, establishment of new agencies, and investment in automated tools to increase efficiencies. These efforts are starting to bear fruit, in some authorities and sectors more than in others. However, Luxembourg needs to maintain a sustainable path to keep course with these efforts and align them with its role as international financial hub with significant cross-border financial flows, international clientele and high-risk products and services.
2. Luxembourg has a strong understanding of its money laundering (ML) risks and a reasonable understanding of its terrorist financing (TF) risks, which is reflected in its national, vertical and sub-sectoral risk assessments. Luxembourg's 2022 TF Vertical Risk Assessment was a positive development, and its methodological approach and general conclusions were sound, though not fully justified or substantiated. Most authorities' overall TF risk understanding is predominantly focused on smaller-scale TF. However, findings related to larger-scale TF stemming from Luxembourg's status as an international financial centre have not been sufficiently communicated to relevant public and private sector stakeholders. Key strengths of the Luxembourg system lie in its robust domestic co-ordination and co-operation on AML/CFT issues at both the policy and operational levels.
3. The CRF-FIU plays a key role in producing and disseminating a wide range of high-quality financial intelligence products, which are widely used by law enforcement authorities (LEAs) and other competent authorities to support their operational needs. However, its level of human resources and

increasingly complex role give rise to concerns about the CRF-FIU ability to continue effectively performing its various functions going forward.

4. Luxembourg has demonstrated a commitment to investigating and prosecuting ML at the policy level. However, resource limitations in investigative and judicial authorities, and the Council Chamber hamper effectiveness to this end. Unlike the overall volume, the types of ML investigations and prosecutions fall within Luxembourg's risk profile to a large extent.
5. Luxembourg makes effective use of tools for freezing and seizing criminal assets and confiscates proceeds of foreign predicate offences and property of equivalent value, as requested by its foreign counterparts. Management of property frozen, seized or confiscated was an issue for Luxembourg throughout the review period, where the competent authorities focused on confiscating cash and balance on accounts. A dedicated asset management office was established just before the on-site visit.
6. Luxembourg proactively identifies and investigates TF activity alongside terrorism related investigations. Luxembourg had no prosecutions or convictions for TF due to the mitigating measures in place. This is somewhat in line with Luxembourg's risk profile.
7. Luxembourg implemented TF targeted financial sanctions (TFS) generally within one working day, and PF TFS with some delay up to late 2020. Measures to remedy gaps in the TFS regime, several of which were only recently put into place, require further development. Luxembourg has not frozen assets related to TF or PF TFS; however, examples were provided where financial institutions (FIs) reacted immediately to designations under other UN sanctions regimes and froze substantial amounts of assets (i.e., cash and securities).
8. Luxembourg has identified the subset of non-governmental organisations (NGOs) that engage in development and humanitarian projects abroad (DNGOs) that are likely to be at risk of TF abuse. However, the Ministry of Foreign Affairs (MoFA) does not apply a risk-based approach in its supervision of the sector. The sector's understanding of TF risk is very low.
9. Understanding of ML risks and AML/CFT obligations is strong for FIs, good for virtual asset service providers (VASPs) and mixed among designated non-financial businesses and professions (DNFBPs). Real estate agents (REAs) and dealers in precious metals and stones (DPMS) have a weak understanding of ML/TF risks and AML/CFT obligations. Generally, for all sectors, there is a need to further strengthen and develop the understanding of TF risk and, for some FIs and DNFBPs, TFS obligations. Most DNFBPs submit low number of suspicious transaction reports (STRs) while many reports are driven by adverse media hits, which can be a valuable indicator for suspicion. The CRF-FIU provided statistics indicating that most of the STRs filed based on adverse media hits included some level of analysis. However, some FIs and a large number of DNFBPs and VASPs met by the assessment team indicated that they provided STRs based on adverse media without further analysis. Furthermore, the quality and relevancy of TF reporting by some obliged entities is extremely low. Overall, this reduces the reporting levels related to ML/TF suspicion and does not reflect Luxembourg's risk profile as an international financial centre.

10. Eight supervisory authorities and self-regulatory bodies (SRBs) supervise all FIs, DNFBPs and VASPs as defined by the FATF Standards. The Luxembourg supervisory regime started becoming increasingly mature in recent years, with supervisors having expanded supervisory and sanctioning powers, automizing tools and processes, increasing human resources, and combining off-site and on-site work. While there is a clear positive trend, particularly with risk-based supervision for FIs significantly enhanced during the review period, the comprehensiveness of a risk-based approach to supervision is in early stages for DNFBPs and VASPs, with inspections of some high risk DNFBP sectors (professional directors-supervised by the AED-TCSPs) not having started, limited resources in a few DNFBP supervisors, diverging application of sanctions, and the need for continued sustainable efforts to maintain the upward trend.
11. Luxembourg's increased efforts and focus on transparency of legal persons and legal arrangements has a positive impact on preventing misuse of corporate vehicles. At the heart of it are the registers on beneficial ownership for legal persons and legal arrangements. Authorities use a multipronged approach to obtain accurate and up-to-date beneficial ownership information in a timely manner. However, sanctions are applied to a varying extent: notably, only criminal penalties are available for violation of legal person information obligations requiring the involvement of the State Prosecutor and hence significantly limiting the proportionality and effective use of sanctions. The understanding of how legal persons can be or are misused for TF is less developed than that for ML.
12. International co-operation is critical and factors in all areas of Luxembourg's AML/CFT framework. Over the review period, Luxembourg consistently provided constructive, and good quality mutual legal assistance (MLA), extradition and international co-operation. Incoming MLA requests not requiring coercive measures are processed within three to four months. However, timeliness is an issue in some cases, as approximately 30% of incoming MLA requests requiring coercive measures are executed by Luxembourg in a timeframe longer than seven months.

Risks and General Situation

2. Luxembourg is an international financial centre with a large and globally interconnected financial system. The financial and insurance sectors are Luxembourg's largest economic sectors, contributing to approximately 23% of the national GDP. Luxembourg has a very high incoming foreign direct investment stock as a percentage of GDP in 2021, with 169% compared to the EU average of 62%. Luxembourg's banking sector is home to more than 120 credit institutions from 24 countries as of December 2022, and the banks located in Luxembourg specialise, amongst other things, in private banking, in providing custodian services for investment funds and fund administration, and in the distribution of shares in investment funds. With about EUR 5 545 billion net assets under management in Luxembourg funds (as of February 2022), Luxembourg is the leading centre in Europe for investment funds. Luxembourg also hosts major Payment and E-money Institutions (PIs/EMIs). Since March 2020, VASP are required to register with the

CSSF. As of November 2022, the VASP sector counts 9 VASPs. The DNFBP sector is large and fragmented consisting of lawyers, REAs, accountants, and trusts and company service providers (TCSPs) offered by a multitude of professionals (FIs and DNFBPs) including banks, investment firms, specialised Professionals of the Financial Sector providing Corporate Services (specialised PFS), business/office centres, professional directors, lawyers, chartered professional accountants (CPAs) and (approved) statutory auditors and audit firms. Luxembourg has only one land-based casino.

3. Given its position as an international financial hub, Luxembourg identified foreign predicate offences as its main ML threat. The foreign predicate offences that contribute significantly to the ML threat include fraud and forgery, tax crimes, corruption and bribery and drug trafficking. Banks (especially private banking), the investment sector, PIs, E-MIs, TCSPs, real estate activities and some legal persons (i.e., commercial companies) and legal arrangements are the most vulnerable to ML and TF. The threat of domestically generated proceeds being laundered through Luxembourg is less significant, given the low crime rate and limited presence of domestic organised crime. The threat level for certain types of offences (i.e., fraud and forgery, drug trafficking and robbery or theft) may increase due to Luxembourg's wealth, economy and geography, including its open borders within the Schengen area. Luxembourg assesses the threats of terrorism and TF as moderate to low. It has not experienced any terrorist attacks and no terrorist groups have been formed on its territory. As an international financial centre, TF is a likely threat, as funds may be moved through Luxembourg's financial system.

Overall Level of Compliance and Effectiveness

4. Luxembourg has strong results on technical compliance with the FATF Standards. On effectiveness, many of these changes have occurred in the three to five years before the on-site visit, or less, and while some initiatives are beginning to show results, other reforms have been too recent or are structural and require an appropriate period of time to become operational and lead to changes in the effectiveness of the overall system. Changes that were implemented earlier (e.g., introduction of goAML by CRF-FIU in 2017) have led to a material increase in effectiveness, whereas more recent changes (e.g., efforts to improve DNFBP supervision, asset management reform, changes to the 2004 AML/CFT law, and the TFS framework) are starting to show results, but are not yet fully effective.

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

5. Luxembourg has taken a range of steps since its last MER to increase its national ML/TF risk understanding. Luxembourg's first NRA (2018), followed by an update in 2020 provide a good basis for risk understanding and triggered additional topic-focused risk assessments on TF, virtual assets (VA)/VASPs and legal persons and legal arrangements. Luxembourg used bottom-up and top-bottom approaches and engaged with a range of authorities and representatives from the private sector. These initiatives have given Luxembourg a strong understanding of its ML risks stemming mainly from foreign predicate offences, the banking and investment sectors, PIs/EMIs, TCSPs, REAs and legal persons and legal arrangements. Luxembourg's May 2022 TF Vertical Risk Assessment (2022 TF VRA) employed a sound methodology and came to reasonable conclusions, but the analysis could be better supported with additional considerations. Most authorities' overall TF risk understanding is more recent and less well-developed as it focusses on smaller-scale TF and findings related to larger-scale TF stemming from Luxembourg's status as an international financial centre have not been adequately disseminated across all authorities and the private sector.
6. The risk assessments informed national AML/CFT policies and activities resulting in multiple national and agency-level action plans over the course of the past four years. This led to, for instance, a further harmonization of supervision, access to the beneficial ownership information registers by LEAs and the CRF-FIU, and the establishment of an asset recovery office. However, the prioritisation of action items has not been well-communicated to some government stakeholders critical to their implementation, and the fast-paced implementation of successive action plans required diverting resources from non-AML/CFT priorities for several years, raising the question of sustainability.
7. The key strength of the Luxembourg system is the very strong domestic co-ordination and co-operation on AML/CFT issues at both policy and operational levels. Results of risk assessments are extensively communicated to FIs, DNFBPs and VASPs in a proactive and consistent manner. However, the more comprehensive and informative findings of the confidential document of the 2022 TF VRA providing information related to larger-scale TF stemming from Luxembourg's status as an international financial centre have not been adequately communicated to the private sector stakeholders. As a result, private sector stakeholders have not been provided with a detailed assessment of TF risks associated with Luxembourg's status as an international financial centre, and the associated vulnerabilities.

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

8. Competent authorities regularly access and use financial intelligence to support investigation of ML/TF and related predicate offences and trace assets for confiscation. The CRF-FIU plays a key role in producing and disseminating a wide range of good-quality financial intelligence products; however, its limited human resources give rise to concerns about the CRF-FIU's ability to continue effectively performing its various functions.

9. Luxembourg proactively identifies and investigates ML through a wide variety of sources. However, limitations in human resources impacted both on the ability of investigative and judicial authorities in conducting ML investigations, and the capacity of the Council Chamber to prioritise the review of ML cases before prosecution. ML investigations and prosecutions fall within Luxembourg's risk profile to a large extent; however, given the identified limitation in qualitative and quantitative data, the assessment has concerns over the extent to which Luxembourg prosecutes different types of ML more broadly.
10. Luxembourg prioritises confiscation as a prominent feature of its 2019 AML/CFT Strategy. Since 2020, Luxembourg actively confiscates the proceeds of foreign predicate offences, in line with its risk and context. However, statistics on domestic ML cases are not broken down between foreign and domestic predicate offences or stand-alone ML. Therefore, Luxembourg cannot demonstrate what portion of the confiscated sums relates to domestic and foreign predicate offences, other than the proceeds confiscated based on incoming MLA requests. Luxembourg has limited capacity to preserve and manage the value of assets other than cash and balance on accounts that are seized or confiscated, forcing authorities to focus primarily on liquid assets.

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

11. Investigative authorities and LEAs have adequate experience and tools to identify and investigate possible TF activity. Competent authorities engage proactively with foreign counterparts to identify potential TF activity. Over the review period, Luxembourg conducted 30 investigations (preliminary and judicial) solely on TF. However, none of these investigations led to prosecution or conviction due to the mitigating measures in place. This is somewhat in line with Luxembourg's risk profile.
12. Luxembourg implemented TFS for TF generally within one working day and for PF with delay until late 2020. Since then, Luxembourg has put measures in place, some quite recently, to bridge the delay inherent in the EU framework and require all natural and legal persons to freeze the assets of these designated persons without delay and prior notification. Some elements of the TFS regime could be improved.
13. NGOs that engage in development and humanitarian projects abroad (DNGOs) are likely to be at risk of TF abuse. However, the MoFA does not apply a risk-based approach in its supervision of the sector. Since 2019, MoFA has enhanced its contacts with the sector. However, more outreach is necessary to improve the sector's understanding of TF risk, which is very low.
14. Awareness of PF-related TFS in the private sector varies. The financial sector generally has a strong understanding of its TFS obligations; however, this is not the case in some non-bank financial sectors. VASPs understand their TFS obligations and their vulnerability to potential violations of DPRK sanctions in light of the prevalent use of virtual assets in ransomware attacks. DNFBBPs' understanding varies.

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

15. Luxembourg has large and diverse financial and DNFBBP sectors. All FIs, DNFBBPs (as defined by the FATF) and VASPs are required to apply AML/CFT preventive

measures. In general, FIs, including VASPs, have demonstrated a stronger application of the range of preventive measures than DNFBBPs. Understanding of ML risks and AML/CFT obligations is strong for FIs, good for VASPs and mixed among DNFBBPs. Generally, for all sectors, there is a need to further develop the understanding of TF risks and, for some FIs and DNFBBPs, of TFS obligations. Overall, REAs, identified as a high-risk sector, and DPMS have a weak understanding of risks and application of AML/CFT obligations resulting in weaker risk-based mitigating measures. Entities broadly understand and implement their reporting obligations. However, this is not the case across all sectors and firms as evidenced by the low number of suspicious transactions reports (STRs) filed by most DNFBBPs. A large number of reports were based on adverse media hits, which can be a valuable indicator for suspicion particularly when analysed by the obliged entity to establish an actual suspicion of ML/TF. The CRF-FIU provided statistics indicating that most of the STRs filed based on adverse media hits included some level of analysis. However, some FIs and a large number of DNFBBPs and VASPs met by the assessment team indicated that they provided STRs based on adverse media without further analysis. Furthermore, the quality and relevancy of TF-related reports submitted by some obliged entities remains a concern as the level of reporting is low and it is not clear whether there are reports that include the aspect of financing or if they are all related to terrorism itself. This reduces the reporting levels related to ML/TF suspicion and does not reflect Luxembourg's risk profile as an international financial centre.

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

16. All FIs and DNFBBP sectors (as defined by the FATF) are supervised for AML/CFT compliance. In recent years, Luxembourg undertook steps to harmonize DNFBBP supervision and the Commission de Surveillance du Secteur Financier (CSSF) became responsible for registering and supervising VASPs. Consequently, the quality of supervision varies among the eight AML/CFT supervisors. The CSSF, the main supervisor of FIs and VASPs, implemented regular reforms in response to changing risks, such as increasing human resources and establishing a dedicated team for on-site inspections of the investment sector. It uses a multipronged approach by combining off-site supervision and monitoring with on-site inspections. The CSSF assisted other supervisors to bolster up their risk-based approach. DNFBBP supervisors are in the early stages of developing their methodology for risk-based supervision. Limited resources and organisational set-up impede some supervisors' ability to carry out their supervisory tasks. In particular, the Tax Authority on Registration Duties, Estates and VAT (AED) has a low number of staff to conduct on-site inspections, has not yet started the inspections of professionals providing directorship services under its supervision and does not fully execute supervision in line with risks, thus diverting resources that should be dedicated to higher risk professionals.
17. Measures to prevent criminals and associates from entering the market are robust. FI supervisors have a good ML/TF risk understanding, including through sub-sectoral risk assessments and regular interaction with the private sector and other authorities. DNFBBP supervisors have varying levels of ML/TF risk understanding, as they have recently begun to develop and implement their risk-based approach to supervision.

18. Luxembourg uses a range of enforcement measures to address non-compliance to a varying extent. For the CSSF, these have been dissuasive but public statements on enforcement cases convey very limited information on the nature of breaches to assist FIs in understanding what would constitute significant deficiencies, thus impacting the effectiveness. The *Commissariat aux Assurances* (CAA) made limited use of its sanctioning power. As for the DNFBP sectors, sanctions are not considered to be sufficiently dissuasive or effective for the REAs and notaries, which are higher risk.

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

19. All legal persons incorporated in Luxembourg need to register basic information in the Trade and Company Register (RCS) and, since 2019, must also register beneficial ownership (BO) information in the RBE. Since 2020, BO information of legal arrangements must be registered in the Register of *Fiducies* and Trusts (RFT). Overall, Luxembourg has a good understanding of how legal persons could be misused for ML; however, there is a need to improve the understanding of where the TF threats emanate as risk analysis focusses on higher risk categories of legal persons used by NPOs and not on other forms of legal persons.
20. Competent authorities demonstrated an effective use of a multi-pronged approach to satisfy themselves of the accuracy and availability of BO information since the establishment of the RBE (2019) and RFT (2020). Competent authorities and obliged entities clearly understand their obligation to file discrepancy reports to the registrars should they discover inaccurate, missing or out of date information, which helps ensure accuracy.
21. Only criminal penalties are available for violation of legal person BO disclosure requirements and requires the involvement of the State Prosecutor, which detracts resources from higher AML/CFT priorities and limits the timely application of sanctions. Also, limited criminal fines have been imposed for not maintaining or updating lists of members or a register of shares.

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

22. International co-operation is vital for Luxembourg given its status as an international financial centre. Over the review period, Luxembourg consistently provided constructive and good quality mutual legal assistance, extradition and asset recovery (including asset repatriation). Incoming MLA requests not requiring coercive measures are processed within three to four months. However, timeliness is an issue in some cases, as approximately 30% of incoming MLA requests requiring coercive measures are executed by Luxembourg in a timeframe longer than seven months.
23. Most Luxembourgish competent authorities proactively seek and provide (including spontaneously) international co-operation to exchange financial intelligence, supervisory, law enforcement, and basic and BO information, in an appropriate and timely manner with their foreign counterparts for AML/CFT purposes.

Priority Actions

Luxembourg should:

1. Substantially strengthen the detection, investigation, and prosecution of parallel ML investigations related to all higher risk predicate offences to ensure better alignment of investigations and prosecutions with Luxembourg's risk profile.
2. Enhance the capacity of the Asset Recovery Office (ARO), the Asset Management Office (AMO) and the Office of the Investigative Judge to better carry out their mandates on asset investigations, post-conviction asset investigations, asset management and international co-operation.
3. Further develop and disseminate its understanding of TF risks and vulnerabilities, including misuse of legal persons for TF purposes, stemming from its exposure as international financial centre. Luxembourg should also ensure that all public and private stakeholders have a better understanding of TF risk, methods and exposure to larger-scale TF through guidance or other forms of outreach.
4. Ensure that the MoFA develops and implements procedures to apply RBA to its oversight of the NPO sector and undertakes systematic outreach to enhance the sector's poor understanding of TF risk.
5. For DNFBPs, strengthen risk-based AML/CFT supervision, by enhancing comprehensiveness of off-site monitoring and on-site inspections, and applying an appropriate level of resources, including increasing supervisory resources of the AED and Order of Chartered Professional Accountants (OEC).
6. Ensure that penalties and remedial measures are proportionate and dissuasive and applied in a timely and effective manner to ensure a positive effect on compliance by FIs, DNFBPs and VASPs.
7. Luxembourg should take effective steps to reduce the identified delays in the execution of incoming MLA requests on coercive measures.

Effectiveness & Technical Compliance Ratings

Table 1. Effectiveness Ratings

| | | | | | |
|--|--|--|---|--|--------------------------------------|
| IO.1 - Risk, policy and co-ordination | IO.2 International co-operation | IO.3 - Supervision | IO.4 - Preventive measures | IO.5 - Legal persons and arrangements | IO.6 - Financial intelligence |
| Substantial | Substantial | Moderate | Moderate | Substantial | Substantial |
| IO.7 - ML investigation & prosecution | IO.8 - Confiscation | IO.9 - TF investigation & prosecution | IO.10 - TF preventive measures & financial sanctions | IO.11 - PF financial sanctions | |
| Moderate | Moderate | Substantial | Moderate | Moderate | |

Note: Effectiveness ratings can be either a High- HE, Substantial- SE, Moderate- ME, or Low - LE, level of effectiveness.

Table 2. Technical Compliance Ratings

| | | | | | |
|---|--|---|---|--|---|
| R.1 - assessing risk & applying risk-based approach | R.2 - national co-operation and co-ordination | R.3 - money laundering offence | R.4 - confiscation & provisional measures | R.5 - terrorist financing offence | R.6 - targeted financial sanctions - terrorism & terrorist financing |
| C | C | C | LC | C | LC |
| 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 |
| LC | PC | C | C | C | C |
| 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 |
| C | C | LC | C | C | C |
| 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 |
| C | C | C | C | C | LC |
| R.25 - Transparency & BO of legal arrangements | R.26 - Regulation and supervision of financial institutions | R.27 - Powers of supervision | R.28 - Regulation and supervision of DNFBPs | R.29 - Financial intelligence units | R.30 - Responsibilities of law enforcement and investigative authorities |
| C | C | C | C | C | LC |
| R.31 - Powers of law enforcement and investigative authorities | R.32 - Cash couriers | R.33 - Statistics | R.34 - Guidance and feedback | R.35 - Sanctions | R.36 - International instruments |
| C | LC | LC | C | LC | LC |
| R.37 - Mutual legal assistance | R.38 - Mutual legal assistance: freezing and confiscation | R.39 - Extradition | R.40 - Other forms of international co-operation | | |
| C | C | C | LC | | |

Note: Technical compliance ratings can be either a C - compliant, LC - largely compliant, PC - partially compliant or NC - non compliant.

MUTUAL EVALUATION REPORT

Preface

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

This evaluation was based on the 2012 FATF Recommendations and was prepared using the 2013 Methodology. The evaluation was based on information provided by Luxembourg, and information obtained by the evaluation team during its on-site visit to the country from 2 to 18 November 2022.

The evaluation was conducted by an Assessment Team consisting of:

1. Ms Fiona CROCKER, Financial Services Commission, Guernsey (financial expert)
2. Ms Chantal GOUPIL, FINTRAC, Canada (financial expert)
3. Mr Birgir JÓNASSON, Northwest Police District of Iceland, Iceland (law enforcement expert)
4. Mr Young LEE, Office of Terrorist Financing and Financial Crimes, U.S. Department of the Treasury, United States of America (legal expert)
5. Ms Christina LYMPERI, Unit A of the Hellenic AML Authority Hellenic FIU), Greece (legal/FIU/international co-operation expert)

with the support of Ms Kellie BAILEY, Ms Nusrut BAHADUR and Mr Panagiotis (Panos) PSYLLOS, Policy Analysts, FATF Secretariat. The report was reviewed by Colonel Pierfrancesco SANZI (Italy); Ms Nina VISSER (The Netherlands); Mr Richard BERKHOUT (IMF) and Mr Luc FERRAND (France). Ms Giulia MARIANI, Senior Specialist Supervision, Swiss Financial Market Supervisory Authority, served as an assessor from July 2020 to October 2022.

Luxembourg previously underwent a FATF Mutual Evaluation in 2010, conducted according to the 2004 FATF Methodology. The 2010 evaluation is published and available at:

<https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Mutualevaluations/Mutualevaluationofluxembourg.html>

That Mutual Evaluation concluded that the country was compliant with two Recommendations; largely compliant with eight; partially compliant with 30; and non-compliant with 9. Luxembourg was rated compliant or largely compliant with 4 of the 16 Core and Key Recommendations.

In February 2014, the FATF recognised that Luxembourg made significant progress in addressing the deficiencies identified in the 2010 Mutual Evaluation Report and should be removed from the regular follow-up process. At that time, Luxembourg

received re-ratings on all Core and Key Recommendations rated partially compliant or non-compliant in its 2010 Mutual Evaluation.

Chapter 1. ML/TF RISKS AND CONTEXT

24. The Grand-Duchy of Luxembourg (“Luxembourg”) is a landlocked country situated between Belgium, France and Germany. It is one of the smallest sovereign States in Europe. Luxembourg has a population of approximately 645 000 (2021) and about 47% of Luxembourg’s workforce resides in Luxembourg’s neighbouring countries (i.e., France, Belgium and Germany). Luxembourg is a founding member of the European Union (EU) and is a part of the Schengen area. Luxembourg uses the Euro as its currency, and its monetary policy is set by the European Central Bank. Luxembourg is also a capital of the EU, notably home to some of the EU’s financial and judicial institutions, including the European Court of Justice and the General Court, the European Court of Auditors, the European Public Prosecutor’s Office, the European Investment Bank, the European Investment Fund, as well as the European Financial Stability Facility and the European Stability Mechanism.
25. Luxembourg hosts a large international financial centre which has the third largest foreign direct investment (FDI) flows in the world, despite decreases of FDI equity flows from peak levels in 2020. It is the primary centre for European non-bank financial institutions, with total assets valued at EUR 14 trillion in 2020. The financial centre is diversified with a core focus on banking (mainly corporate banking, depositary and custody services for funds as well as private banking), investment funds (primarily asset servicing), insurance (life, non-life and reinsurance) as well as the Payment and E-Money Institutions sector, VASP and capital markets (notably listing and post-trade services). Luxembourg acts as an EU hub and competence centre for international financial institutions in these areas. In 2021, Luxembourg’s gross domestic product (GDP) at market prices amounted to EUR 73.3 billion. The financial and insurance sector are the sectors that contributed the largest share of gross added value in Q4, 2021. Other significant economic sectors include business activities and renting, wholesale, repair, transportation and storage, real estate activities and manufacturing.
26. Luxembourg is a parliamentary democracy in the form of a constitutional monarchy. In accordance with the Constitution, the Government forms the executive power. The Grand Duke is the Head of State and appoints a person to the Government that is supported by parliamentary majority. The Government has overall power to manage public affairs, the right to propose legislation, and manages the State’s revenue and expenditure budget.
27. The legislative power lies in the hands of the Parliament and the Council of State. The Constitution grants the Parliament certain powers with respect to financial matters and bestows upon it the right to examine the Government’s actions. The Parliament’s consent is also mandatory for international treaties to take effect in the country. In accordance with the Constitution, the Council of State serves as a consultative body within the legislative procedure and as such, acts as a moderating second legislative assembly in Luxembourg’s unicameral system. The Council of State also ensures that the bills and amendments thereto are in conformity with the

Constitution, international conventions, legal acts of the EU and general principles of law. All bills submitted either by the Government or Parliament require prior opinion of the Council of State.

28. According to the Constitution, judicial power lies with courts and tribunals, which are independent from the legislative and executive powers. Luxembourg's legal system is based on the Civil Law (continental Europe) family. Luxembourg has a Constitutional Court (preliminary ruling on the constitutionality of laws, excluding those that approve treaties) and three jurisdictions: administrative jurisdictions, social security jurisdictions and ordinary Courts of Law.

ML/TF Risks and Scoping of Higher Risk Issues

Overview of ML/TF Risks

29. Luxembourg identified foreign predicate offences as its main money laundering (ML) threat, given its position as an international financial centre. The magnitude, diversity and openness of financial flows through and into Luxembourg's financial market contribute to this exposure. The foreign predicate offences that contribute significantly to the ML threat include fraud and forgery, tax crimes, corruption and bribery and drug trafficking.¹ Banks (especially private banking), the investment sector, money value transfer services (MVTs), professionals providing trust and company services (TCSPs), real estate activities and some legal persons (i.e., commercial companies) and legal arrangements are the most vulnerable sectors to ML and terrorist financing (TF).
30. The threat of domestically generated proceeds being laundered through Luxembourg is less significant, given Luxembourg's low crime rate and the limited presence of organised crime in its territory. The threat level for the most relevant types of offences (i.e., fraud and forgery, drug trafficking and robbery or theft) may increase due to Luxembourg's wealth, economy and geography, including its open borders within the Schengen area.
31. Luxembourg assesses the threats of terrorism and TF as moderate to low overall. It has not experienced any terrorist attacks and no terrorist groups have been formed in its territory. Because of Luxembourg's status as an international financial centre, TF is a more likely threat, as funds may be moved through Luxembourg's financial system.

Country's Risk Assessment & Scoping of Higher Risk Issues

32. In 2020, Luxembourg published its national ML/TF risk assessment (2020 NRA update), which builds on its 2018 NRA. Both assessments combined qualitative and quantitative information and professional expertise. Both NRAs involved the participation of all competent authorities with AML/CFT responsibilities and key stakeholders, including different ministries, Luxembourg's Financial Intelligence Unit (CRF-FIU), law enforcement agencies (LEAs), supervisory authorities, self-regulatory bodies (SRBs) and representatives from the private sector. Both NRA exercises, identified and assessed ML/TF inherent risks, including threats (i.e., domestic and external exposure to predicate offences) and vulnerabilities (i.e.,

¹ This is in line with data and information on incoming and outgoing mutual legal assistance (MLA) requests, asset seizures executed in Luxembourg and STRs filed by obliged entities.

relative vulnerability of sectors to ML/TF threats). Mitigating factors and their effects on inherent risks were also assessed to measure residual risk level.

33. In addition to the 2018 NRA and 2020 NRA (update), Luxembourg conducted several ML/TF topical (vertical) risk assessments (VRA) on VA/VASPs (2021), legal persons and legal arrangements (2022), and TF (2022). The FI supervisors (CSSF, CAA) also carried out sub-sectorial risk assessments (SSRA) focussing on some areas considered higher risk in the national risk assessments (e.g., private banking, collective investments, TCSP services provided by specialised PFS, life insurance undertakings, brokers/brokerage firms and TCSP services provided by PSAs; see IO.3).
34. In deciding what issues to prioritise for increased focus, the assessors reviewed material provided by Luxembourg on their national ML/TF risks (as outlined above) and information from reliable open sources (e.g., reports of other international organisations and NGOs). The assessors focused on the following priority issues:
 - a. **Cross-border ML/TF risks:** The assessors focused on how the country is using its AML/CFT framework to mitigate these international risks and explored the extent to which international co-operation is provided and sought in an effective manner.
 - b. **The misuse of legal persons and legal arrangements:** Given Luxembourg's actions to further mitigate threats associated with legal persons and legal arrangements, the assessors examined: i) the extent to which AML/CFT measures (as applied to both legal persons and legal arrangements, as well as to their gatekeepers) prevent the misuse of corporate vehicles for criminal purposes; ii) the effectiveness of competent authorities' and SRBs' supervisory co-ordination and use of sanctions; and iii) the ability of competent authorities to access adequate, accurate and up-to-date beneficial ownership (BO) information.
 - c. **Vulnerabilities and threats in the FI and DNFBP sectors:** Given the size and scale of financial and designated non-financial services provided in Luxembourg and Luxembourg's role as a financial hub, assessors considered the risk appetite of FIs and DNFBPs, including their risk assessment and risk mitigation and customer due diligence (CDD) processes in place. The extent to which Luxembourg firms in these sub-sectors are effectively complying with existing AML/CFT and TFS obligations was also an area of greater focus. As many FIs and DNFBPs maintain cross-border operations, assessors considered how international FI or DNFBP groups are supervised for group-wide compliance programmes, internal controls and AML/CFT programmes. Other points of interest were how the risk of financial flows is assessed and monitored by supervisors, whether supervisors and SRBs are adequately resourced to mitigate the higher ML/TF risks identified and how well risk-based supervision is applied in response to the threats posed by the COVID-19 pandemic.
 - d. **Vulnerabilities and threats for MVTs and VASPs:** Considering the evolving risks in these sectors, assessors focused on the country's understanding and response to the risks.
 - e. **Trade-based money laundering and Freeport operators:** Assessors reviewed how Luxembourg implements elements of the AML/CFT framework for Freeport operators.

35. Through the scoping note exercise, the following areas were identified for lesser focus:
- **Domestic proceeds-generating offences:** Luxembourg is a generally safe country with a low domestic crime rate.² Given the profile of the economy, as well as the relatively small geographic size of the country, domestic predicate offences such as murder, environmental offences and piracy are not common, and do not appear to be at risk of exploitation in the country for ML/TF purposes.
 - **Market operators:** Lower focus was given to market operators as these were identified as low risk in the NRA and as there is only one market operator in Luxembourg.

Materiality

36. Luxembourg has an open and fast-growing economy. While the national economy has significantly grown over those past years, the composition of many sectors has remained relatively stable.
37. The financial and insurance sector is Luxembourg's largest economic sector, contributing to approximately 23% of the national GDP.³ Luxembourg has a very high incoming foreign direct investment stock as a percentage of GDP in 2021, with 116.9% compared to the EU average of 62%.⁴ Luxembourg has a very large banking sector and is home to more than 120 credit institutions from 24 countries⁵. The banks located in the country specialise, among other things, in private banking, in providing custodian services for investment funds and fund administration, and in the distribution of shares in investment funds. With about EUR 5 545 billion net assets under management in Luxembourg funds (as of February 2022), Luxembourg is the leading centre in Europe for investment funds. The country is also one of the largest captive reinsurance markets in Europe. In December 2021, Luxembourg counted around 200 reinsurance undertakings.
38. Luxembourg's DNFBP sector is large and fragmented consisting of notaries, lawyers, real estate agents, dealers in precious metals and stones (DPMS), chartered professional accountants and TCSPs offered by different types of professionals (FIs and DNFBPs). Luxembourg has only one land-based casino.

² Statistics Portal of Luxembourg, General crime recorded by the police 2015-2021 ([https://lustat.statec.lu/vis?fs\[0\]=Topics%2C1%7CSocial%20conditions%23C%23%7CCrime%20and%20justice%23C5%23&pg=0&fc=Topics&lc=en&df\[ds\]=ds-release&df\[id\]=DF_C5201&df\[ag\]=LU1&df\[vs\]=1.0&pd=2015%2C2021&dq=A.&vw=tb](https://lustat.statec.lu/vis?fs[0]=Topics%2C1%7CSocial%20conditions%23C%23%7CCrime%20and%20justice%23C5%23&pg=0&fc=Topics&lc=en&df[ds]=ds-release&df[id]=DF_C5201&df[ag]=LU1&df[vs]=1.0&pd=2015%2C2021&dq=A.&vw=tb))

³ STATEC, Gross value added by activity (NaceR2) (at current prices) (in millions EUR) 1995 – 2022-Q4 (https://lustat.statec.lu/vis?pg=0&df%5bds%5d=release&df%5bid%5d=DF_E2600&df%5bag%5d=LU1&df%5bvs%5d=1.0&pd=2015-Q1%2C&dq=.Q&lc=en)

⁴ OECD (2022), FDI stocks (indicator). doi: 10.1787/80eca1f9-en (Accessed on 16 June 2022) (<https://data.oecd.org/fdi/fdi-stocks.htm#indicator-chart>)

⁵ Banque Centrale du Luxembourg, *Statistiques : Etablissements de crédit ; "tableau 11.01" and "tableau 11.05" as of December 2022* (www.bcl.lu/fr/statistiques/series_statistiques_luxembourg/11_etablissements_credit/index.html)

Structural Elements

39. Luxembourg has all the key structural elements required for an effective AML/CFT system including political and institutional stability, a high-level commitment to address AML/CFT issues across various authorities, governmental accountability, the rule of law and a professional and independent judiciary.

Background and Other Contextual Factors

40. Luxembourg's AML/CFT regime is based on a legal framework consistent with the FATF recommendations and the Fourth and Fifth EU AML/CFT Directives ((EU) 2015/849, (EU) 2018/843). Significant enhancements have been made since 2014, supported by a comprehensive institutional set-up involving a wide range of competent authorities to prevent, supervise, detect, investigate prosecute ML/TF and to recover related assets.
41. In 2017, the World Bank reported that 99% of Luxembourg's adult population held a bank account.⁶ The Payment Accounts Law of 13 June 2017 grants anyone residing in the EU, regardless of their place of residence, the right to open a private basic payment account under applicable AML/CFT rules. This includes asylum seekers and homeless people, as well as people without a residence permit but whose expulsion is impossible for legal or factual reasons.
42. Luxembourg has worked to implement the international standard for transparency and exchange of information on request and has been rated by the Global Forum "largely compliant" in this regard. The main achievements were regarding the immobilization of bearer shares, the access to banking information and the prohibition of numbered accounts.
43. Luxembourg figures among the world's least corrupt countries.⁷ It has ratified the UN Convention against Corruption and the OECD Convention on Combatting Bribery of Foreign Public Officials in International Business Transactions.

AML/CFT strategy

44. Luxembourg's AML/CFT strategy is informed by the NRAs and the EU supranational risk assessment (EU SNRA). The first NRA was adopted in 2018 and updated in 2020, whereas the first EU SNRA on the risks of ML/TF affecting the internal market was conducted by the European Commission in 2017 and updated in 2019 and 2022. Since 2019, Luxembourg presented three national AML/CFT Strategies: the national AML/CFT Strategy 2019-2020, the national AML/CFT Strategy 2020-2022 and the national AML/CFT Strategy 2023-2024. These strategies are supported by agency-level action plans and focus on the main vulnerabilities, threats and risks identified in the NRAs.

⁶ World Bank, Global Findex Database, 2017.

⁷ Transparency International, Corruption Perceptions Index 2021 (https://images.transparencycdn.org/images/CPI2021_Report_EN-web.pdf)

45. The **Inter-ministerial Steering Committee** (ISC), formed in 2021, sets the high-level national policy and draws up a multiyear AML/CFT strategic plan, which is presented to the Government Council for validation. The national AML/CFT strategy sets out the main guidelines for combating ML/TF and defines high-level strategic objectives. The ISC reports to the Government on the progress made in implementing the national AML/CFT strategy. The Chair of the Monitoring Committee for Financial Sanctions is represented within the ISC.
46. The **National Prevention Committee** (NPC) is the main co-ordination mechanism for AML/CFT in Luxembourg. It promotes discussions on ML/TF matters and co-ordinates national-level actions and decisions. The NPC co-ordinates the implementation of the national AML/CFT strategy through its operational members. The high-level strategic objectives of the AML/CFT strategy are refined by operational objectives that are reflected in sectoral action plans that are to be implemented by the institutional actors in accordance with their respective competences. The NPC monitors both the progress made in implementing the national AML/CFT strategy and the state of progress of the sectoral action plans. Before 2021, the NPC carried out the functions of the ISC.
47. The **Monitoring Committee for Financial Sanctions** (Monitoring Committee) is chaired by the MoF and acts as the national co-ordination and co-operation mechanism in matters relating to the financial aspects of TFS (including, but not limited to, PF TFS) and their implementation. The Chair of the ISC is represented within the Monitoring Committee.

Legal & institutional framework

48. The 2004 AML/CFT Law is the main pillar of Luxembourg's AML/CFT system. Since Luxembourg's last follow-up report in 2014, the 2004 AML/CFT Law and other legislation was amended to transpose the Fourth and Fifth EU AML/CFT Directives into Luxembourg law. Freeport operators and VASPs, among others, have been included within the scope of the 2004 AML/CFT Law. Other relevant legislation includes:
 - The 2019 RBE Law established the Beneficial Ownership (BO) Register of legal persons in Luxembourg (RBE).
 - The 2020 RFT Law enabled the creation of the Register of *Fiducies* and Trusts (RFT). The RFT became operational during the second half of 2020 and stores information on foreign law trusts with Luxembourg trustees, *fiducies* (a domestic trust) and their respective beneficial owners.
 - The 2018 FIU Law instituted the new operationally independent and autonomous CRF-FIU.
 - The 2020 Sanctions Implementation Law enhanced the established legislative and regulatory framework and introduced the automatic transposition of UN designations across all targeted financial sanctions (TFS) regimes.
49. AML/CFT policies and activities in Luxembourg are co-ordinated between competent authorities, as well as with the private sector. The main AML/CFT authorities include:

Ministries

50. The **Ministry of Justice (MoJ)** plays a central role in the national AML/CFT strategy and co-ordination. It chairs the ISC and the NPC and hosts the Executive Secretariat for both bodies. Among other things, the MoJ is responsible for: (i) authorising gambling, lotteries and sports betting businesses pursuant to the 1977 Gambling Law; and (ii) approving the formation of *fondations* pursuant to the 1928 NPO Law. The MoJ is also in charge of approving the admission of lawyer and notary candidates to the final exam pursuant to the 2009 Regulation on Access to the profession of Lawyer and Notary.
51. The **Ministry of Finance (MoF)** responsible for drafting laws and regulations aiming at enhancing the detection, prevention and suppression of ML/TF in the financial sector. The MoF also deals with all matters regarding implementation of TFS and restrictive measures.
52. The **Ministry of Foreign Affairs (MoFA)** is in charge of the general co-ordination of the implementation of the restrictive measures taken by the UN Security Council and or the EU. The MoFA is also responsible for examining applications received from not-for-profit associations for approval as a non-governmental development organisation (DNGOs) under article 7 of the 1996 Humanitarian Law.
53. The **Ministry of the Economy (MoE)** issues business licences for different types of professionals covered by the 2011 Business Licences Law. As such, the MoE is responsible for verifying the conditions of access to the market of various professions falling under the definition of DNFBP.

Criminal justice and operational agencies

54. Detection activities are primarily driven by Luxembourg's **CRF-FIU**. It is the exclusive recipient of suspicious activity reports (SARs) and suspicious transaction reports (STRs) from obliged entities. The CRF-FIU analyses these reports and disseminates intelligence to competent authorities (including international counterparts). The CRF-FIU is headed by magistrates who operate independently and autonomously.
55. **Prosecution authorities** refers to both the General State Prosecutor's Office with the Superior Court of Justice (PG), and the State Prosecutor's Offices with the District Courts that prosecute those who commit criminal offences, including ML/TF offences. The General State Prosecutor is the central authority for receiving requests for mutual legal assistance in criminal matters.
56. **The Office of the Investigative Judge (investigative judge)** directs the investigation of cases as assigned by State Prosecutors, particularly if coercive measures are required. Their role is to gather evidence to impartially investigate a case. Investigative judges may order measures that restrict individual freedoms (i.e., coercive measures), such as provisional detention, searches or seizures.
57. The **Judicial Police Service (SPJ)** is the department within the Grand-Ducal Police (PGD) in charge of executing most orders from the State Prosecutors and the investigative judges. In addition to a dedicated anti-terrorism unit, the SPJ has an AML unit specialised in investigating ML, TF and in identifying and tracing criminal assets. The SPJ is also responsible for executing measures ordered by an investigative judge in the execution of MLA requests.

58. The **Council Chamber** is an investigating court which, in principle, sits in collegial formation (i.e. with three judges) and in a non-public hearing. It supervises the acts of the investigative judge and decides, on request of the State Prosecutor (or the civil party, e.g. a victim), after completion of a judicial investigation, whether the case shall be referred to a court. In addition, the Council Chamber receives requests from prosecution authorities and any relevant person who can cite a legitimate personal interest to declare invalid a preliminary investigation or any part of this process. As a general rule, the decisions of the 1st instance Council Chamber may be appealed against. Such appeal would be heard by the Council Chamber of the Court of Appeal. On MLA matters, the Council Chamber examines of its own motion the “formal” regularity of the procedure.

Supervisory authorities and SRBs

59. The **Commission de Surveillance du Secteur Financier (CSSF)** ensures the prudential and AML/CFT supervision of Luxembourg’s financial sector, VASPs⁸ and some TCSPs.
60. The **Commissariat aux Assurances (CAA)** ensures the prudential and AML/CFT supervision of Luxembourg’s insurance sector which includes professionals of the insurance sector providing TCSP services (PSA).
61. The **Registration Duties, Estates and VAT Authority (AED)** is Luxembourg’s AML/CFT supervisor for real estate agents, accounting professionals, some TCSPs (business/office centres and professional directors not supervised by another supervisory authority or SRB), the casino, freeport operators, DPMS and some dealers in high value goods. The AED also oversees VAT and taxes, duties and charges relating to the legal circulation of goods.
62. Dedicated **SRBs** supervise for AML/CFT purposes the legal professions (lawyers by the Luxembourg Bar Association (OAL), Diekirch Bar Association (OAD)⁹; notaries by the Chamber of Notaries (CdN)), chartered professional accountants by the Order of Chartered Professional Accountants (OEC) and (approved) statutory auditors and audit firms by the Institute of Statutory Auditors (IRE).

Other relevant authorities

63. Luxembourg’s **Asset Recovery Office (ARO)** identifies, and traces assets linked to domestic and foreign offences and facilitates the exchange of information with authorities abroad.
64. Luxembourg’s **Asset Management Office (AMO)** is responsible for managing and, when necessary, disposing of property frozen, seized or confiscated during domestic or foreign criminal proceedings.

⁸ VASPs that do not hold any other license of financial sector professional (i.e. “pure VASPs”) are only supervised from an AML/CFT perspective by the CSSF. However, VASPs that hold another license such as also banks, PIs or EMIs are actually also supervised from a prudential point of view by the CSSF.

⁹ The OAL is the Bar Association for lawyers and law firms in Luxembourg City, while the OAD is the Bar Association for lawyers and law firms in Diekirch. The OAL supervises around 3 112 lawyers. The OAD represents a small fraction of the profession (around 1,6 %). The OAD practice almost exclusively in the field of litigation, and does not offer TCSP activities.

65. The **Customs and Excise Administration (ADA)** is responsible for border controls, including cross-border currency and bearer-negotiable instrument (BNI) controls. The ADA may temporarily seize undeclared cash or cash suspected as the proceeds or instrumentalities of crime.
66. The **Luxembourg Inland Revenue (ACD)** is responsible for setting and collecting direct taxes. It also reviews relevant tax processes to detect illegal activities and shares findings with Luxembourg's LEAs.

Financial sector, DNFBPs and VASPs

67. Luxembourg has a materially significant financial sector, with the insurance sector, investment sector – consisting of investment firms and investment fund managers – and the sheet assets (see Table 1.1). The supervisory population comprises 5 680 FIs with the CSSF supervising 1 603 FIs (including 122 banks, 96 investment firms and 1 235 investment fund managers) and 9 VASPs as of 30 September 2022, employing more than 41 000 staff, and the CAA supervising 37 life insurance undertakings and over 4 000 intermediaries.¹⁰

Table 1.1. Overview of Luxembourg's financial sector

| Type of FI | Number of obliged entities | Key figures (Q3 2022) |
|--|----------------------------|--|
| Banks | 122 | Balance sheet assets EUR 988.72 billion |
| - Wholesale, corporate and investment banks | 42 | |
| - Private banking | 37 | |
| - Custodians and sub-custodians | 29 | |
| - Retail and business banks | 12 | |
| - Entities operating online | 2 | |
| MVTS | | |
| - Payment / E-money institutions* | 28 | Balance sheet assets EUR 8 billion |
| - Agents and E-money distributors** | 22 | N/A |
| Investment firms | 96 | AUM EUR 56 billion Balance sheet assets EUR 0.97 billion |
| Specialised PFSs (85 provide TCSP activities) | 99 | Balance sheet assets EUR 5.9 billion |
| Investment Fund Managers*** | 1 235 | AUM EUR 5038 billion Balance sheet assets EUR 25 billion |
| Market Operators | 1 | Balance sheet assets EUR 373 million |
| Life insurance undertakings | 37 | Premia**** EUR 19 billion Technical provisions***** EUR 217 billion |
| Insurance Intermediaries**** | 4 040 | Premia from life EUR 2.7 billion***** |

*Note: In addition to "Payment/E-money institutions" licensed by the CSSF, there are also Luxembourg branches of PIs/EMIs established in other EU Member States. As of 30 September 2022, four Luxembourg branches were established in other EU Member States. However, three out of the four branches had no activities yet. The establishment of Luxembourg branches of PIs/EMIs established in other EU Member States is subject to a notification from the Home EU Member State.

¹⁰ These include 109 brokerage firms and brokers, as well as insurance agencies/agents distributing insurance contracts for and on behalf of one or several Luxembourg-based insurance undertakings, and sub-brokers distributing insurance contracts under the responsibility and on behalf of brokerage firms or brokers.

**Note: “Agents/E-money Distributors” means “Agents/E-money Distributors acting on behalf of PIs/EMIs established in another EU Member State”.

***Note: CSSF supervises both IFMs and UCIs active in Luxembourg (through the application of a double layer of supervision) as well as Regulated Securitisation Vehicles and Pension Funds.

****Note: This number also includes the intermediaries who distribute non-life insurance policies.

*****Note: These key figures do not include the branches as data are only available on a yearly basis.

*****Note: This number only refers to brokers and brokerage firms. Data as of 31 December 2021.

68. All DNFBPs, as defined by the FATF Standards, are obliged entities under the Luxembourg AML/CFT framework (see Table 1.2). Apart from some TCSPs falling within the supervision of the CSSF or the CAA, DNFBPs are supervised by the AED or an SRB. Lawyers and real estate agents represent the largest DNFBP sectors in terms of number of professionals, with the real estate sector having a turn-over of EUR 1.1 billion (31 December 2021). There are 131 DPMS, twenty of which cover 86% of the sector’s turnover. The TCSP sector is fragmented as activities are provided by a number of professionals with various supervisors: i.e., banks, investment firms, specialised Professionals of the Financial Sector providing Corporate Services (specialised PFS), Professionals of the Insurance Sector (PSAs), lawyers, CPAs, approved statutory auditors and audit firms, business/office centres and professional directors. In line with the FATF Glossary definition of TCSPs, TCSP activities provided by banks, investment firms, lawyers and CPAs are considered under their respective sectors. Specialised PFS¹¹ and PSAs will be considered under the analysis for FIs as they are supervised by FI supervisors (CSSF, CAA). Unless otherwise stated, reference to TCSPs throughout the report will refer to the following professionals: business/office centres and professional directors supervised by the AED, and (approved) statutory auditors and audit firms supervised by the IRE.

¹¹ Specialised PFS are supervised by CSSF. There are 99 specialised PFS (as of 30 September 2022) of which some provide FI services in addition to TCSP activities, and others provide exclusively TCSP activities (85).

Table 1.2. Overview of Luxembourg's DNFBP sector

| Type of DNFBP | Number of obliged entities (Q3 2022) |
|--|--|
| Casino | 1 |
| Real estate agents (REAs) | 2 832 |
| Dealers in precious metals and stones (DPMS) | 131 |
| Accounting professionals | 610 |
| Chartered Professional Accountants (CPAs) | 1 162 |
| Lawyers | 3 344 out of which 57% fall under FATF standards/the 2004 AML/CFT Law - 3 129 Lawyers - 215 Law firms |
| Notaries | 36 |
| Professionals supervised by the CAA providing TCSP services (PSAs) | 13 |
| (Approved) statutory auditors and audit firms | 663 (25 provide TCSP services) - 404 approved statutory auditors and approved audit firms - 259 statutory auditors and audit firms |
| Professional directors | 204 |
| Business/Office centres | 69 |

Note: Data is as of 30 September 2022, unless stated otherwise.

69. The VASP market is emerging in Luxembourg and consists of nine entities providing VA services (as of 1 November 2022), including five professionals licensed as bank, Payment Institution or E-Money Institution. The VASP registration and supervisory regimes started in March 2020, with the CSSF being the registration and supervisory authority. Out of the nine VASPs, the first was registered in March 2021 and three handle over 99% of the clients and transactions.
70. The assessment team ranked the sectors based on the relative importance, materiality and level of risk to inform their conclusions, by assigning a stronger weighting to positive and negative points in the implementation of the AML/CFT system for sectors of most heavily weighted than for sectors of lesser heavily weighted. This approach has been used throughout the report, but it is more apparent in Chapter 6 on IO.3 and Chapter 5 on IO.4.
71. The banking sector, investment fund managers and TCSPs are weighted *most heavily*:
- **Banking sector:** Luxembourg's banking sector consists of 122 banks from 26 different countries and a GDP of about 1 383% with over EUR 1 013 billion banking assets (as of April 2022). Banks offer a wide range of products and services, such as private and retail banking, and acting as depository, registrar or transfer agent for Luxembourg collective investment schemes. The NRA identified the banking sector at high risk as it is a large, fragmented and complex sector exposed to international, high value and frequent financial flows to a diverse customer base (including international high-net worth individuals, individuals from higher risk jurisdictions and complex legal structures).
 - **Investment fund managers:** they play a predominant role in the Luxembourg and international financial system. The sector consists of more than 1 200 professionals managing assets exceeding EUR 5 000 billion. The

sector is rated in the NRA as high due to it being a large, fragmented and complex sector with significant foreign funds and foreign and diverse client base.

- **Specialised PFS:** they provide TCSP services and FI services to Luxembourg collective investment schemes and are supervised by the CSSF. There are 99 specialised PFS, out of which 85 provide TCSP activities with balance sheet assets totalling EUR 5.9 billion. The NRA considers specialised PFS as high risk.
72. Investment firms, notaries, lawyers, CPAs and real estate agents are weighted *heavily*:
- **Investment firms:** there are 96 firms providing asset and wealth management services to mostly international high-net worth clients. Compared to investment fund managers, these investment firms manage less assets (EUR 56 billion), have fewer clients and lower balance sheet assets (EUR 0.97 billion). The NRA recognises that the ML/TF risk is primarily driven by the high international business share and the nature of clients. In 2019, over half of the investment firms had high-risk clients.
 - **Notaries:** notaries play a key role as gatekeepers to the financial system. While the profession of notary is legally capped to 36 notaries, and requires a comprehensive licensing process, assessors considered a number of factors: the NRA rated the risk level at high, different types of legal persons can only be incorporated by means of a notarial deed and notaries are involved in real estate transactions (i.e., signing the deed to transfer the property rights), notaries are prohibited from performing as TCSPs and notaries are not involved in the set-up of a domestic *fiducie* contract.
 - **Lawyers:** it is a large and fragmented profession, and the NRA identified the sector as high inherent risk. Assessors considered the large clientele, including international customers, lawyers servicing complex legal structures and offering TCSP activities, and the role of lawyers as AML/CFT gatekeeper (e.g., offering domiciliation services).
 - **CPAs:** they provide a key gatekeeper and intermediary role for many transactions that have a high risk for ML/TF risk and the NRA rated the sector as high risk. The profession is large and fragmented with over a thousand chartered professional accountants but one-third is employed by one of the Big 4 firms or assimilated legal entities, and a significant proportion of CPAs' activities relate to TCSP (as at 2021, 47% of CPAs (sole practitioners) offered TCSP services and about 66% of registered legal entities under OEC supervision provided these services).
 - **Real estate agents:** the real estate sector in Luxembourg is large (there are 2 832 agents), fragmented and has a high volume and value of transactions (turnover of EUR 1.1 billion in 2021). The NRA considered the sector as highly vulnerable to ML risk and low exposure to TF risk.
73. PIs, EMIs (and agents/e-money distributors), life insurance undertakings and brokers, PSAs, TCSPs (professional directors, business/office centres, approved statutory auditors and audit firms), DPMS and VASPs are weighted *moderately heavily*.

- **PIs, EMIs and agents and e-money distributors** acting on behalf of PIs and EMIs established in other EU Member States: assessors considered that while the sector has a high turnover (e.g., in 2019 EMIs processed an inflow of 1.3 billion transactions worth EUR 38.4 billion and 50 million outflow transactions worth EUR 27.4 billion), it is highly concentrated (e.g., 99% of revenue is generated by five PIs). There is one bank and one PI licensed in Luxembourg offering money remittance services. The market players are stable and their supervision by the CSSF is robust.
 - **Life insurance undertakings and brokerage firms/brokers¹²**: the NRA considers the sector to be moderately vulnerable with the risk factor being its large size and fragmentation, while the residual risk is low. At the same time, assessors also considered the following factors: the life insurance sector is oriented towards foreign residents, has a large volume of customers and uses intermediary distribution channels.
 - **PSAs**: PSAs are TCSPs as they are service providers of corporate governance and management companies for insurance and reinsurance undertakings, and for pension funds. The NRA considered them as *low* risk due to their mainly advisory role to the respective insurance/reinsurance undertakings or pension funds and thus have limited exposure to ML/TF risk. PSAs are supervised by the CAA.
 - **TCSPs provided by professional directors, business/office centres and (approved) statutory auditors and audit firms**: these professionals provide TCSP activities, but their services have a limited business offering and lower turn-over, as compared to specialised PFS. Assessors also took into account the NRA rating of high and the strong influence of CSSF (and its products) on the understanding of AML/CFT obligations by business office/centres and professional directors supervised by the AED despite the less strong supervisory framework specifically designed for this particular TCSP sector, with on-site inspections for professional directors not having started in 2021 by the AED. As for (approved) statutory auditors and audit firms, they perform a minor share of TCSPs as part of their total activities and have a stronger control by the supervisor (IRE) as compared to the AED supervised TCSPs.
 - **DPMS**: the NRA classified DPMS at medium risk. The assessors considered the concentrated sector and the relatively low turn-over (EUR 109 million in 2021) on the one hand and the limited understanding of ML/TF risks and AML/CFT obligations by DPMS, on the other hand.
 - **VASPs**: there are nine entities providing VA services, including FIs already licensed as a bank or PI/EMI before they were registered as VASP. Assessors considered the relative recency of the market entry control and supervisory regimes for VASPs, introduced in March 2020, paired with the emerging market and risks associated with virtual assets.
74. The only casino in Luxembourg, which is land-based, and accounting professionals are weighted less heavily:

¹² Hereafter defined as “brokers”.

- **Casino:** assessors based this weighting on a number of factors including the strong mitigating measures the casino applies, the annual on-site inspections by the supervisor, the limited gaming offerings (slot machines and blackjack tables) and the stability in the ownership of the casino which has been more or less the same for decades. The NRA rated the inherent risk as medium and the residual risk as low.
- **Accounting professionals:** while the NRA rated the sector as high risk and acknowledges that accounting professionals can be abused in their activity of recording accounting entries to record entries to ML, assessors considered a number of factors: accounting professionals cannot certify accounts like CPAs, they are prohibited from providing domiciliation services, they do not control or manage funds or assets.

Preventive measures

75. In Luxembourg, AML/CFT preventive measures for all obliged entities are set out in the 2004 AML/CFT Law. The 2004 AML/CFT Law, as amended, covers all FIs, DNFBPs and VASPs required by the FATF Standards. There is no exemption for any sector to the application of FATF Standards. The 2004 AML/CFT Law also covers some entities that are not required under the FATF Standards such as Luxembourg freeport operators, non-life insurance undertakings - reinsurance undertakings and intermediaries where they operate non-life insurance classes credit and suretyship, bailiffs, professional depositaries of assets other than financial instruments and debt recovery, support PFS and Family Offices.

Legal persons and arrangements

76. There are five main types of legal persons that can be created in Luxembourg: commercial companies, civil companies, *Associations sans but lucratif* (ASBLs), *Fondations* and other legal persons (e.g., public institutions). All legal persons incorporated in Luxembourg must be registered with the Trade and Company Register (RCS), which is managed by the Luxembourg Business Registers (LBR). BO information on legal persons is recorded in the RBE (established in 2019), which is also managed by the LBR.
77. Commercial companies are the most frequently used type of legal person, with private limited liability companies (SARL) accounting for over half of all the entities registered with the RCS (see Table 1.3). NPOs in Luxembourg take the form of ASBL or *Fondation*.¹³ Luxembourg investment funds can be established by contract (*Fonds commun de placement*, FCP), without legal personality, or take the form of a legal person (e.g., a *Société d'Investissement à Capital Variable* (SICAV)) – in both instances, they must be registered with the RCS.

¹³ ASBLs are NPOs registered with the RCS and have a legal requirement to yearly file with the RCS the list of their members as well as any change in the composition of the board of directors. ASBLs do not need to submit financial statements unless they accept donations or wills, receive public funds, or are recognised as being of public interest by Grand-Ducal decree, in which case they are treated (and have similar obligations) as *Fondations*. Any person may, subject to approval by grand-ducal decree, allocate by authentic act or by will all or part of his or her assets to the creation of a *Fondation*, which has civil personality. *Fondations* must carry out work of a philanthropic, social, religious, scientific, artistic, educational, sporting or tourist nature. Their income must stem from

Table 1.3. Types of Luxembourg legal persons registered with the RCS

| Legal Form | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 (1 September 2022) |
|---|----------------|----------------|----------------|----------------|----------------|-------------------------|
| Commercial Companies | 124 688 | 128 099 | 132 633 | 121 918 | 121 916 | 126 183 |
| <i>Société à responsabilité limitée (SARL)</i> | 70 871 | 74 093 | 76 763 | 73 226 | 74 461 | 77 357 |
| <i>Société anonyme (SA)</i> | 47 706 | 46 915 | 45 638 | 36 533 | 32 392 | 31 532 |
| <i>Société en commandite simple (SCS)</i> | 1 419 | 639 | 1 737 | 1 697 | 1 849 | 1 944 |
| <i>Société en commandite par actions (SCA)</i> | 1658 | 1 781 | 1 870 | 1 951 | 2 087 | 2 200 |
| <i>Société en nom collectif (SENC)</i> | 419 | 409 | 401 | 167 | 142 | 140 |
| <i>Société coopérative (SC)</i> | 145 | 148 | 151 | 141 | 149 | 149 |
| <i>Société européenne (SE)</i> | 33 | 31 | 36 | 41 | 56 | 56 |
| <i>Société coopérative organisée comme une SA (SCSA)</i> | 76 | 85 | 99 | 114 | 114 | 127 |
| <i>Société par actions simplifiée (SAS)</i> | 102 | 148 | 175 | 185 | 212 | 241 |
| <i>Société en commandite spéciale (SCSPé)*</i> | 1 647 | 2 474 | 3 415 | 4 579 | 6 304 | 7 735 |
| <i>Société à responsabilité limitée simplifiée (SARL-S)</i> | 612 | 1 376 | 2 348 | 3 284 | 4 150 | 4 701 |
| <i>Société coopérative européenne (SCE)</i> | - | - | - | - | - | 1 |
| Civil Companies | 4 752 | 4 975 | 5 178 | 5 478 | 5 845 | 6 044 |
| ASBLs | 10 838 | 11 246 | 11 516 | 8 504 | 8 457 | 8 664 |
| Fondations | 211 | 214 | 217 | 218 | 193 | 193 |
| Other legal persons | 3 255 | 3 177 | 3 182 | 3 096 | 3 019 | 2 997 |
| <i>Association d'Assurance Mutuelle</i> | 6 | 7 | 7 | 6 | 6 | 6 |
| <i>Société créée selon la loi du 28 mars 1997</i> | 1 | 1 | 1 | 1 | 1 | 1 |
| <i>Société créée selon la loi du 24 mars 1989</i> | 1 | 1 | 1 | 1 | 1 | 1 |
| <i>Société d'investissement à capital variable</i> | 1 317 | 1 297 | 1 275 | 1 175 | 1 136 | 1 111 |
| <i>Société européenne d'investissement à capital variable</i> | 1 | 1 | 1 | 1 | 1 | 1 |
| <i>Groupement d'intérêt économique</i> | 80 | 86 | 87 | 80 | 82 | 88 |
| <i>Groupement européen d'intérêt économique</i> | 57 | 55 | 56 | 59 | 58 | 58 |
| <i>Association agricole</i> | 112 | 112 | 118 | 110 | 86 | 89 |
| <i>Association épargne-pension</i> | 13 | 11 | 10 | 10 | 10 | 10 |
| <i>Etablissement public</i> | 54 | 58 | 105 | 118 | 123 | 128 |
| <i>Fonds commun de placement (FCP)*</i> | 1 612 | 1 547 | 1 520 | 1 530 | 1 505 | 1 491 |
| <i>Fonds d'investissement alternatif réservé</i> | 1 | 1 | 1 | 2 | 2 | 2 |
| <i>Mutuelle</i> | | | | 3 | 8 | 11 |
| Total | 143 744 | 147 711 | 152 726 | 139 214 | 139 430 | 144 081 |

Note: *Société en commandite spéciale* (SCSPé) and the *Fonds commun de placement* (FCP) do not have a separate legal personality, but they are registered with the RCS.

the capital assigned to their creation or from the income of their activities (e.g., entrance tickets in a museum) without pursuing a material gain. They must undergo a strict licencing procedure run by the MoJ and receive approval by Grand-ducal decree. Any authentic declaration and any testamentary disposition made by the founder with a view to creating a *Fondation* shall be communicated to the MoJ for approval. Until it is approved, the founder may withdraw his or her declaration. In Luxembourg, no private *Fondations* are allowed (e.g., for organising a family assets' inheritance): all entities must act purely in the public interest and donations (including initial founding) made are irrevocable. *Fondations* must submit their accounts to the MoJ on an annual basis, register with the RCS, and record mandatory information. Two third of the *Fondations* have registered European BOs with the RBE as of March 2021.

78. Luxembourg is not a centre for legal arrangements. Legal arrangements in Luxembourg comprise domestic legal arrangements (domestic *fiducies*) and foreign trusts. Beneficial ownership information of *fiducies* and foreign trusts is recorded in the RFT (established in 2020). This register is maintained by the AED.

Table 1.4. Types and number of legal arrangements

| Legal arrangement sub-sectors | Description | Number registered |
|--|---|---|
| <i>Fiducies</i> and similar legal arrangements | Agreement whereby the settlor agrees with the fiduciary that the latter will become the owner of certain fiduciary assets (the fiduciary estate) under agreed conditions. | 1 430 trusts and <i>fiducies</i> have registered their BO information with the RFT as of 30 September 2022. Out of these 22 are foreign law trusts. |
| Foreign trusts | Trusts created under foreign law administered in Luxembourg. | |

Supervisory arrangements

79. There are three supervisory authorities (CSSF, CAA and AED) and five SRBs (CdN, IRE, OAL, OAD (hereafter, the OAL and OAD are referred to as OAs) and OEC) in charge of AML/CFT supervision covering the different types of professions falling within the scope of the FATF Standards. While the CSSF and the CAA are in charge of the financial sector (including FIs, VASPs and some TCSPs), the AED and SRBs supervise the DNFBP sectors from an AML/CFT perspective. Supervisors have powers to monitor and supervise professionals in their own sectors as well as to take necessary measures, including sanctions, to secure compliance under the 2004 AML/CFT Law (see R.26-R.28 for further details). Table 1.5 summarises the authorities' respective responsibilities for AML/CFT supervision and licensing or registration.

Table 1.5. Luxembourg supervisors and licensing/registration authorities

| Regulated/supervised professionals | Supervisor | Registration/licensing authority |
|---|------------|---------------------------------------|
| Credit institutions (banks) | CSSF | ECB or CSSF (non-EU country branches) |
| Investment firms | CSSF | CSSF |
| Payment Institutions/E-money Institutions | CSSF | CSSF |
| (Alternative) Investment Fund Managers | CSSF | CSSF |
| Life insurance undertakings, insurance intermediaries (i.e., agencies/agents and brokerage firms/brokers and sub-brokers) | CAA | CAA |
| Professionals of the insurance sector (PSAs) | CAA | CAA |
| Specialised PFS | CSSF | CSSF |
| VASPs | CSSF | CSSF |
| Casino | AED | Government Council |
| Real estate agents | AED | MoE |
| DPMS | AED | MoE |
| Accounting professionals | AED | MoE |
| Chartered professional accountants (CPAs) | OEC | MoE |
| Notaries | CdN | Grand Duke |
| Lawyers | OAs | OAs |
| (Approved) statutory auditors and audit firms | IRE | CSSF |

| Regulated/supervised professionals | Supervisor | Registration/licensing authority |
|--|------------|----------------------------------|
| Business/office centres | AED | MoE |
| Professional directors under AED supervision | AED | AED |

International co-operation

80. Luxembourg has a comprehensive legal framework and system allowing it to provide and seek constructive and timely international co-operation on ML, associated predicate offences and TF cases. Due to its international exposure and its status as an international financial centre, the laundering of foreign criminal proceeds constitutes Luxembourg's biggest threat.
81. In line with the risks, international co-operation is at the core of Luxembourg's AML/CFT strategy. Luxembourg provides and seeks international co-operation through international conventions and treaties, national legislation and through bilateral agreements. This is done at the level of the LEAs, the CRF-FIU, the ARO and of the AML/CFT supervisory authorities.
82. Luxembourg's most significant international partners are its neighbouring countries (France, Belgium and Germany), but it also co-operates with many other EU and non-EU jurisdictions.
83. The General State Prosecutor's Office is the central authority for the execution of incoming MLA requests. Investigative judges and PAL/PAD are the competent authorities responsible for outgoing MLA requests. Other forms of co-operation occur more informally between Luxembourg's law enforcement and supervisory authorities and their foreign counterparts. The CRF-FIU has a leading role among all Luxembourg competent authorities in providing and seeking other forms of international co-operation.



Chapter 2. NATIONAL AML/CFT POLICIES AND COORDINATION

Key Findings and Recommended Actions

Key findings

Immediate Outcome 1

1. Luxembourg has a strong understanding of its ML risks and a reasonable understanding of its TF risks informed by a variety of sources (NRAs, VRAs, SSRAs, EU SNRAs). The understanding of ML risks is better than for TF risks as the overall understanding of authorities is focused predominantly on smaller-scale TF and findings relating to larger-scale TF stemming from Luxembourg's status as an international financial centre have not been sufficiently communicated to relevant public and private sector stakeholders.
2. National AML/CFT policies seek to address the risks identified, and objectives and activities of competent authorities generally align with the risks identified. Over the course of four years, multiple national and agency-level action plans have been developed and implemented. This resulted in, for instance, a further harmonization of supervision, access to the beneficial ownership information registers by LEAs and the CRF-FIU, and the establishment of an asset recovery office. However, the prioritisation of action items has not been well-communicated to some government stakeholders critical to their implementation, and the fast-paced implementation of successive action plans required diverting resources from non-AML/CFT priorities for several years, raising the question of sustainability.
3. Luxembourg has very strong domestic co-ordination and co-operation on AML/CFT issues at both policy and operational levels. The collaboration is facilitated through the National Prevention Committee (NPC) which brings together relevant competent authorities, SRBs, professional associations and private sector representatives. The NPC not only develops risk assessments, directly involving FIs, DNFBPs, VASPs and NPOs, discusses and measures progress in the implementation of national strategies and action plans.
4. The Monitoring Committee is the national platform to co-ordinate and co-operate on PF matters. The Monitoring Committee representatives have significant expertise on the designation process at the EU and UN levels. However, they have not disseminated this expertise in a systematic manner to relevant domestic counterparts, who might otherwise be able to leverage information in their possession about potential targets.

5. Luxembourg extensively communicates the results of risk assessments to FIs, DNFBPs and other sectors affected by the application of the FATF Standards in a proactive and consistent manner. However, due to the confidential nature of the 2022 TF VRA working level document, containing more comprehensive and informative findings, private sector stakeholders have not been provided with a detailed assessment of TF risks associated with Luxembourg's status as an international financial centre, and the associated vulnerabilities.

Recommended Actions

Immediate Outcome 1


1. Luxembourg should further develop its understanding of TF risks and vulnerabilities stemming from its role as international financial centre, and transit jurisdiction for foreign TF financial flows and businesses linked to TF activity, including undertaking a qualitative assessment of what Luxembourg legal persons are used for, their links to higher-risk jurisdictions and other intelligence and investigatory materials from law enforcement and other authorities. Authorities should also engage in outreach regarding those findings and other typologies to enhance relevant authorities' and obliged entities' understanding of larger-scale TF.
2. Luxembourg should clearly communicate its AML/CFT priorities to all relevant authorities so that they can appropriately allocate their resources in implementing action items.
3. Luxembourg should ensure that the primary stakeholders in its AML/CFT framework remain staffed at levels that are commensurate to the risks arising from its status as an international financial centre to sustainably maintain, and support further improvements to, Luxembourg's AML/CFT regime.

84. The relevant Immediate Outcome considered and assessed in this chapter is IO.1. The Recommendations relevant for the assessment of effectiveness under this section are R.1, 2, 33 and 34, and elements of R.15.
85. The assessment team's findings on IO.1 are based on a review of national (NRA), supranational (EU SNRA), vertical (VRA) and sub-sectoral (SSRA) risk assessments; review of national and agency level AML/CFT strategies, policies and action plans; discussions with competent authorities, SRBs and representatives from the private sector.

Immediate Outcome 1 (Risk, Policy and Co-ordination)

Country's understanding of its ML/TF risks

86. Luxembourg has a comprehensive and ongoing risk assessment process. It resulted in a strong understanding of ML risks, and a reasonable understanding of TF risks.
87. Overall, most authorities, including the CRF-FIU, LEAs, CSSF, CAA, OEC and IRE, have a strong and well-developed understanding of ML/TF risks, while other authorities, including some DNFBP supervisors (AED, OAs and CdN) had decent but mixed understanding of ML/TF risks. This understanding has been developed through, inter alia, participation in the various NRA exercises, co-operation and co-ordination with domestic and international counterparts, interaction with the private sector (including responses to AML/CFT questionnaires in the course of supervision), and investigatory and supervisory work.
88. Luxembourg is a leading international financial centre with its banking, insurance, and investment funds sectors playing an outsized role in the global financial system, generating significant cross-border financial activity and correspondingly ML/TF exposure to foreign predicate offences. Luxembourg understands that to maintain its reputation, it must take meaningful and durable action to assess and mitigate its ML/TF risks. Accordingly, Luxembourg took wide-ranging steps to increase its ML/TF risk understanding, including the development of two NRAs: the first in 2018 and an update in 2020 (a third NRA is currently being drafted). To further its understanding on ML and TF risks, Luxembourg also conducted topic-focussed assessments: ML/TF vertical risk assessments (VRA) on VA/VASPs (2021), legal persons and legal arrangements (2022), and TF (2022). These assessments are comprehensive, drawing mostly reasonable conclusions regarding risk exposure.
89. Co-ordinated by the National Prevention Committee (NPC), the NRAs involved cross-cutting engagement from government departments, LEAs, the CRF-FIU, supervisory authorities and SRBs, and representatives from the private sector, and drew upon quantitative and qualitative inputs from these stakeholders and external sources such as the EU Supranational Risk Assessments (EU SNRA) and FATF guidance documents. Luxembourg recognises that the largest inherent risks in Luxembourg are driven primarily by exposure to ML of foreign criminal proceeds and vulnerabilities in the financial and non-financial sectors.
90. Luxembourg government departments, LEAs, the CRF-FIU and supervisors share an understanding of the higher risk posed by ML from foreign predicate offences (fraud, forgery, tax crimes, corruption, bribery, drug trafficking); vulnerabilities in the banking (private banking), investment, Payment Institutions (PIs)/E-Money Institutions (EMIs), specialised PFS, real estate agents, TCSPs and the freeport sectors; and risks relating to the use of commercial companies and domestic *fiducies*. This understanding is consistent with the NRAs and the wide range of other risk and threat assessments undertaken by LEAs, supervisors and the CRF-FIU. For example, the FI supervisory authorities (CSSF and CAA) developed a more detailed analysis of sectors considered as highly vulnerable through sub-sectoral risk assessments (SSRAs), such as private banking and collective investment, thus demonstrating a good level of understanding (see IO.3). The national-level risk assessments consider the TF threat as moderate to low and the NPOs carrying out development and humanitarian projects abroad are identified as highly vulnerable to TF.

- 
- 2
91. While Luxembourg authorities demonstrated an overall strong understanding of ML risks, their understanding of the country's TF risk exposure should be further enhanced and communicated to appropriate public and private stakeholders beyond those officials directly involved in the development of the confidential working level document of the 2022 TF VRA. Authorities' methodological approach to the 2022 TF VRA was sound given Luxembourg's minimal historical exposure to both terrorism and TF. It assessed both smaller-scale TF (i.e., individual actors, FTFs) and Luxembourg's inherent exposure to larger-scale TF stemming from its status as an international financial hub.
 92. The resulting confidential working level document of the 2022 TF VRA contains, among other things, a detailed assessment of the terrorist and TF threats facing Luxembourg, including specific conclusions regarding domestic exposure to specified categories of TF threats; case studies derived from financial intelligence with indicators of fund usage to support terrorist acts; and an analysis of the vulnerabilities associated with various activities and sectors in the Luxembourg context. This working level document generally draws reasonable conclusions regarding exposure to both smaller-scale and larger-scale TF and reasonable conclusions about inherent risks.
 93. However, the public 2022 TF VRA adopted by the NPC does not contain much of this valuable granular analysis, even in sanitised form. It principally contains high-level conclusions drawn by authorities, but with insufficient context to provide actionable guidance to authorities (not directly involved in the development and drafting of the working level document), and more critically, to the private sector.
 94. In addition, some conclusions as to the efficacy of mitigating measures are not entirely justified. Under the methodology utilised, mitigating measures play a key role in driving the ultimate determination of residual risk. For example, the assessment team questions the efficacy of mitigating measures in the NPO sector based on its discussions with sector representatives (see IO.10), and what seems to be an assumption in the 2022 TF VRA that robust preventive measures automatically mitigate larger-scale TF. The 2022 TF VRA also cites detection by obliged entities as a key mitigating measure, and notes that over 1 000 TF reports have been filed with the CRF-FIU. However, TF reports are a concern as many of them pertain to terrorism rather than TF, which indicates that obliged entities' may not understand the important distinctions between these two concepts (see IO.6 and IO.4). The absence of indicators that could inform obliged entities' understanding and accordingly refine their reporting compounds the issue; authorities contend that such indicators are often conveyed in the course of outreach, but these indicators are not memorialized in the public VRA itself. Ultimately, this lack of widespread dissemination of actionable typology information undermines the usefulness of obliged entity detection as a mitigating measure.

95. As a consequence, and in light of the significance and materiality of Luxembourg's status as an international financial hub, Luxembourg's public 2022 TF VRA is a good starting point, but would benefit from the publication of more rigorous analysis of, for example, the reports received by the CRF-FIU related to terrorism and TF. The 2022 TF VRA cites the quantity of reports filed to support the proposition that the private sector is aware of the risks associated with their customers; the case studies contained in the working document indicate understanding on the part of the entities that filed those STRs but are insufficient to support the broader conclusion of widespread awareness of risk across the private sector. The 2022 TF VRA does not provide sufficiently detailed indicators to obliged entities to enable them to improve and enhance their reporting. In addition, the fact that obliged entities consistently file far higher quantities of terrorism STRs (versus TF STRs) further indicates that TF risk understanding could be enhanced. Furthermore, the 2022 TF VRA is a more recent assessment (May 2022) and lacks the detail of the confidential working level document, this understanding is not shared uniformly through competent authorities, which results in a misallocation of resources that affects the efficacy of CFT activities against the likely risk exposure. For example, operational authorities interviewed during the on-site visit demonstrated a strong understanding of terrorism risks and the TF risks associated with lone terrorist actors and have provided valuable financial intelligence in response to terrorist acts in neighbouring countries. Their ability to determine whether the focus more on organised and sophisticated TF threat actors (e.g., terrorist organisations rather than lone wolves/individual actors) would be improved by a better understanding by obliged entities and other authorities of these threat actors.

National policies to address identified ML/TF risks

96. National and agency-specific AML/CFT policies and strategies generally seek to address the risks identified in the NRAs. However, there is a concern with the prioritisation of action plan items among some authorities in light of their limited resources and resources being diverted from non-AML/CFT priorities, which could threaten sustainability.
97. The close domestic co-ordination and co-operation, including for ML/TF risk assessments and the development of risk-based policies and action plans, is a key strength of Luxembourg's system. The NPC provides a collaborative forum in which all LEAs, all supervisors, the CRF-FIU, relevant ministries, and the private sector participate. Luxembourg established national AML/CFT policies and activities principally through the mechanism of the NPC. In developing these, Luxembourg took both a bottom-up and top-down approach and drew from the NRAs. Over the course of the last four years, Luxembourg presented three national AML/CFT strategies: the national AML/CFT Strategy 2019-2020, national AML/CFT Strategy 2020-2022, national AML/CFT Strategy 2023-2024. These strategies are supported by agency-level action plans. These national policies are geared to addressing the identified ML/TF risks and vulnerabilities, and gaps in the Luxembourg AML/CFT framework. For example, VASPs have been brought into the licensing and supervisory regime in March 2020 (see IO.3).

- 2
98. The national AML/CFT Strategy 2019-2020 followed the 2018 NRA and consisted of 42 strategic initiatives grouped in four work blocks: 1) enhancing the legal and regulatory framework, 2) enhancing national AML/CFT co-ordination, 3) enhancing supervision, 4) strengthening detection and prosecution of ML and TF, and asset recovery. The initiatives were implemented through the NPC's working and sub-working groups and concretely led to the creation of the Asset Management Office (AMO; see IO.8), direct access by LEAs to the beneficial ownership information registers (RBE and RFT; see IO.5) and an increase in resources of the CRF-FIU and the CSSF.
 99. In response to the 2020 NRA (update), Luxembourg designed the national AML/CFT Strategy 2020-2022 which aimed to address identified ML/TF risks at three levels: through national strategic priorities, a national action plan with seven initiatives and tailor-made agency-level action plans for competent authorities and SRBs. The national strategic priorities relate to enhancing ML/TF prosecution, developing ML/TF investigation capabilities, harmonising DNFBP supervision and improving TCSPs market entry control. The national action plan seeks 1) closer national collaboration and co-ordination, 2) harmonisation of the supervisory approach and practices across agencies, 3) enhancement of internal CRF-FIU capabilities, 4) increased transparency of legal persons and legal arrangements, 5) enhancement of the investigation and prosecution organisation especially of the SPJ, 6) creation of an autonomous and effective ARO, 7) active participation in the international fora. This work resulted in extending supervisory powers to SRBs, including freeport operators as obliged entities based on their high-risk exposure, addressing gaps in the targeted financial sanctions (TFS) framework, increasing resources at various departments, and creating the Inter-ministerial Steering Committee (ISC) as a body to set high-level national objectives.
 100. Luxembourg adopted the national AML/CFT Strategy 2023-2024 a week prior to the on-site visit. Building on the 2020-2022 Strategy, this national plan groups initiatives across four priorities: further enhancing the prosecution of ML/TF; further developing the ML/TF investigative capabilities; harmonizing the supervision of DNFBPs; and improving market entry controls of TCSPs. The plan is a logical next step based on the foundation laid out in the previous strategy. However, it is too recent to assess the effectiveness of any implementation.
 101. The National Coordinator of the NPC and its Executive Secretariat understand national level priorities and are monitoring progress towards these ends. However, there is a mixed understanding amongst other authorities as to how their action plan items advance national AML/CFT priorities or how to prioritise their action plan items. While some stakeholders met, have clearly benchmarked their progress in implementing action items, some authorities were unable to specify which action items were their highest priorities against their identified risks, and were not able to articulate clear milestones to measure their progress in completing actions. Luxembourg's success in making considerable enhancements to its AML/CFT framework over the past five years is attributable in significant part to the diversion of resources from other non-AML/CFT priorities. Therefore, it is unlikely that Luxembourg will be able to maintain this level of resource allotment and attention to AML/CFT reforms on an ongoing basis outside of the context of the mutual evaluation process. Authorities need to clearly articulate their priorities to keep the most significant reforms on a sustainable path.

102. During the on-site visit, NPC members stated that, where there are divergences in standards (e.g., EU Money Laundering Directives versus the FATF Standards), Luxembourg's policy is to implement the strictest standards. They noted that, while they take feedback from the private sector during consultations, it ultimately does not affect this underlying policy choice. This approach is not risk-sensitive and may result in an inefficient allocation of resources for both authorities and the private sector.

Exemptions, enhanced and simplified measures

103. All relevant FIs, DNFBPs and VASPs are required to implement AML/CFT measures and Luxembourg has not granted any wholesale exemptions from AML/CFT requirements. Obligated entities must apply enhanced and simplified measures in line with ML/TF risks (see R.1; IO.4).
104. Luxembourg draws its legal framework for exemptions, enhanced and simplified measures from the EU Anti-Money Laundering legislation, EU SNRAs and NRAs. As such, Luxembourg included sectors in its AML/CFT regime that are not required under the FATF Standards.¹⁴ For instance, Luxembourg's freeport is the only customs free zone in the EU that specialises in storing high-value luxury goods. Following the NRAs, Luxembourg views it as higher risk and consequently, Luxembourg included freeport operators in its AML/CFT legislation. Freeport operators are accordingly required to conduct CDD, including identifying the beneficial owners of those who store goods at the freeport, which resulted in significant loss of business. The inclusion of this high-value sector in its AML/CFT regime, despite commercial disadvantage, demonstrates that Luxembourg is proactively applying measures to mitigate risk in sectors it identifies as high risk in the NRAs. Similarly, nineteen Luxembourg bailiffs – who are public officials – are designated as obliged entities and need to comply with AML/CFT obligations when they carry out valuation and public sales of furniture, movables and harvests.
105. Luxembourg lowered the threshold for conducting CDD for prepaid cards and e-money to EUR 150 from 250 based on an assessment of ML/TF risks associated with anonymous prepaid instruments, particularly when used non-face-to-face. Luxembourg's AML/CFT framework also allows for the application of simplified due diligence measures where there is demonstrated lower risk, though this has not occurred in practice. Based on its risk assessment of certain e-money and payment services, the Luxembourg framework allows for simplified due diligence under specific conditions, including the existence of various mitigating measures and below certain thresholds and aggregate amounts.

¹⁴ In line with the FATF Methodology and FATF precedent, the assessment team did not meet representatives or assess the level of AML/CFT effectiveness in the sectors that are beyond the scope of the FATF Standards.

Objectives and activities of competent authorities

- 2
106. The objectives and activities of competent authorities and SRBs are largely consistent with the evolving national AML/CFT policies and with the ML/TF risks identified. At the policy level, Luxembourg introduced several legislative amendments to address ML/TF risks. Some of these respond to ML/TF risks identified in the EU SNRAs and NRAs, and to the transposition of the EU's Anti-Money Laundering Directives. The changes to the regulatory framework include the introduction of beneficial ownership information registers for legal persons and legal arrangements (RBE and RFT; see IO.5) and harmonization of supervisory powers across the board.
 107. *Supervision* – Supervisory authorities and SRBs use the NRAs and VRAs to inform their understanding of risks and to refocus activities if needed. The FI supervisors (CSSF, CAA) conducted several SSRAs for sectors identified as very high and high risk (e.g., private banking, collective investments, life insurance undertakings and brokers/ brokerage firms). In line with the workplan articulated by the national AML/CFT strategies, supervision of FIs, DNFBPs and VASPs has been further harmonized, with all sectors falling within the FATF Standards now being supervised by one of Luxembourg's eight AML/CFT supervisors.
 108. To align their objectives and activities with the national AML/CFT policies and ML/TF risks identified, supervisors increased resources, developed and improved supervisory tools, and implemented changes to their governance. For example, all supervisors use annual AML/CFT questionnaires to understand risks within their supervised professionals and to develop supervisory plans, the CSSF created a dedicated on-site inspections unit for the investment sector and the AED established a dedicated AML/CFT department responsible for supervision (see IO.3). All supervisors' view of ML/TF risk is aligned to that of the country's risk assessments and supervisors generally apply more focus and resources to the areas of highest risk. However, this picture is not consistent across all supervisors where insufficient supervision and enforcement resources are applied to higher risk areas (e.g., real estate), and conversely, disproportionate resources applied to sectors assessed by the country as low risk (e.g., the annual supervisory visit of the country's sole casino).
 109. *CRF-FIU* – The CRF-FIU played a key role in developing Luxembourg's understanding of ML/TF risks and acts in a manner that is largely consistent with those risks. For example, throughout the review period, the CRF-FIU deployed its limited resources in a risk-sensitive manner using an automated data matching system which determines the level of analysis required. This allowed the CRF-FIU to conduct a more in-depth operational analysis of 4 000 priority SARs/STRs out of a population of 50 000 SARs/STRs subject to initial analysis. This screening was key to the CRF-FIU's ability to produce and disseminate high-quality financial intelligence products to key players in the Luxembourg system (e.g., LEAs) to support their operational needs. The CRF-FIU disseminated ML-related financial intelligence to competent authorities in line with identified risks, conducted strategic analysis on ML/TF in line with identified threats and shared its expertise with supervisors and obliged entities. It was, for instance, responsive to questions that it received regarding reporting on TF and TFS.

110. *LEAs* – The types of ML investigations and prosecutions by LEAs fall within Luxembourg’s risk profile to a large extent. However, Luxembourg has not adequately pursued ML linked to sectors exposed to significant ML risk such as real estate and professionals offering TCSP services. With respect to TF, LEAs tend to consider TF as a secondary matter to terrorism investigations and prosecutions; however, LEAs indicated that they systematically look for the financing element whenever there was intelligence regarding terrorism.

National co-ordination and co-operation

111. National co-ordination and co-operation between agencies on AML/CFT issues is a strength of the Luxembourg system. All relevant competent authorities and SRBs work well together at policy and operational level. This close co-ordination and co-operation is facilitated by strong working relationships and fluid communication among stakeholders, multi-agency bodies (e.g., the NPC, ISC and Monitoring Committee), working groups and, in cases where more formal co-ordination is required, MoUs.
112. The NPC is the main co-ordination mechanism for AML/CFT in Luxembourg and provides a multidisciplinary roundtable to exchange information and co-ordinate national-level actions and decisions. It brings together the national AML/CFT co-ordinator, all LEAs, all supervisors, and a number of ministries (e.g., MoJ, MoF), professional associations of the private sector and obliged entities. It meets every five to six weeks and serves as a platform to develop and co-ordinate implementation of the national strategic priorities. The NPC also organises dedicated working groups that discuss the practical implementation of specific topics resulting from the national AML/CFT Strategy. For example, the work of the working group on TCSPs (consisting of supervisors and the Ministries of Justice, Finance and Economy) led to the legal requirement on all professionals providing TCSP services to register with their respective supervisory authority or SRB.
113. In November 2021, Luxembourg established the ISC to provide high-level policy direction and set high-level strategic objectives on AML/CFT matters that are adopted by the government. These high-level strategic objectives, drawn by senior officials of the MoJ, MoF and MSI, are further refined in operational objectives that are reflected in sectoral action plans and its implementation is tracked by the NPC. The NPC and the ISC are supported by an executive secretariat, whose expertise enhances the effectiveness of these bodies’ co-ordination. It is attached to the MoJ and supervised by the national AML/CFT co-ordinator.
114. National co-operation between agencies is further facilitated by multiple MoUs (e.g., between the CRF-FIU and the AED) and participation in each other’s technical committees. For example, the CAA, AED, IRE and OEC are member of the CSSF’s AML/CFT Advisory Committee (CANTIB) and the CAA’s AML/CFT Technical Committee is attended by the CSSF and IRE. The CSSF also has regular meetings with other TCSP supervisors, notably the AED, OAs and the OEC, in which they discuss supervisory measures and strategy to strengthen TCSP supervision and share individual cases of entities of concern: e.g., negative information about a lawyer’s role in TCSP activities. The co-operation and co-ordination between Luxembourg’s data protection commission (CNPD) and competent authorities is a particularly positive element of domestic co-operation (see box 2.1).

Box 2.1. Co-operation and co-ordination between CNPD and competent authorities

The CNPD is a general data protection authority surveying all sectors. It takes a pragmatic and collaborative approach to working with competent authorities and other stakeholders in ensuring compatibility between data protection and AML/CFT requirements. The CNPD approaches and resolves potential conflicts between these two interests on a case-by-case basis as it views its role to strike the right balance between them. For instance, upon request of the Luxembourg Bar Association, the CNPD reviewed the Code of Conduct for lawyers and law firms. The CNPD meets routinely with the CSSF and other authorities on data protection issues and proactively educates them on data protection.

115. The Monitoring Committee for International Financial Sanctions (Monitoring Committee) provides for good national co-ordination and co-operation on TF-TFS and PF-TFS matters but could improve its awareness-raising with key Luxembourg government stakeholders and the public. Key participants in the Monitoring Committee have significant expertise on the designation process at the EU and UN levels but have not disseminated this expertise in a systematic manner to relevant domestic counterparts, who might otherwise be able to leverage information in their possession about potential targets. The Monitoring Committee has recently started to formally co-ordinate policy decisions and activities to combat PF and would benefit from enhanced co-ordination to better tailor those policies and activities to Luxembourg's context as a global financial centre and major entry point into the EU single market.

Private sector's awareness of risks

116. Luxembourg undertook extensive outreach to ensure that the private sector is aware of the national risk assessments and VRAs. The private sector was directly involved in the NRAs and VRAs processes through bilateral meetings, thematic workshops and conference calls. Furthermore, participation by supervisors and professional associations fed the private sector perspective into these risk assessments, and the 2020 NRA (update) was approved by the NPC which includes obliged entities as members.
117. All NRAs and VRAs are available on publicly accessible websites in English and French. Competent authorities and SRBs pro-actively disseminated the results of the risk assessments through newsletters, presentations and supervisory activity. They organised and participated in conferences to convey information about ML/TF risks to the private sector, which were well received. FIs, DNFBPs, VASPs and NPOs met are aware of the relevant results of the ML/TF NRAs and VRAs. This is in line with the requirement on obliged entities to incorporate the NRA into their risk assessment and when adopting risk mitigating policies, procedures and measures. However, the more comprehensive and informative findings of the confidential document of the 2022 TF VRA providing information related to larger-scale TF stemming from Luxembourg's status as an international financial centre have not been sufficiently communicated to private sector stakeholders. As a result, private

sector stakeholders have not been provided with a detailed assessment of TF risks associated with Luxembourg's status as an international financial centre, and the associated vulnerabilities (see IO.4).

118. In addition to these national and vertical risk assessments, the CSSF and CAA conducted SSRAs which focus on areas identified by the NRA as higher risk¹⁵ and the CRF-FIU produced typologies. During the process of the SSRA, the CSSF used its AML/CFT expert working groups (public-private partnerships of which relevant professional associations and the CRF-FIU are members) to collaborate and discuss with the private sector trends and conclusions emerging before finalising the product. Results were shared with the FIs, DNFBPs and VASPs through training and conferences, and have been published on the CSSF website. In addition, some obliged entities met incorporate the SSRAs in their own entity-level risk assessments (see IO.3). FIs, DNFBPs and VASPs demonstrated an awareness of relevant risks, but their understanding of such risks was mixed (see IO.4).

Overall Conclusion on IO.1

Luxembourg has taken steps to increase its national understanding of ML/TF risks, including through national risk assessments, a range of other risk assessment products (vertical and sub-sectoral), activities and engagement with the private sector. This resulted in a strong understanding of ML risks that stem primarily from foreign predicate offences (e.g., fraud, tax crimes, corruption) and vulnerabilities in FIs (e.g., banking and investment sectors) and DNFBPs (e.g., real estate agents, legal and accounting professionals, and TCSPs). However, there are moderate shortcomings in Luxembourg's overall TF risk understanding. While the TF risk understanding is reasonable at a high level, it only began to mature for most authorities with the process for developing the dedicated 2022 TF VRA (published May 2022), and key findings relating to the particular risks and vulnerabilities inherent to Luxembourg's status as an international financial centre have not been sufficiently communicated to all key public as well as private stakeholders.

National AML/CFT policies, strategies and activities are formulated and implemented in a targeted manner to address identified ML/TF risks; however, additional actions were sometimes added to action plans before pre-existing items were addressed and not all Luxembourg authorities were fully aware of national priorities and how to prioritize action plan items for which they were responsible. The rapid succession of plans and actions to improve the Luxembourg AML/CFT system and significant resources diverted by the government from other non-AML/CFT programs to deliver these improvements result in an approach for some authorities that is not risk sensitive. This is a weighty concern for the assessment team, as this approach is not sustainable.

¹⁵ The CSSF has issued SSRAs in relation to private banking, collective investments and TCSPs provided by specialised PFS. The CAA has issued SSRAs in relation to life insurance undertakings, brokers/brokerage firms and TCSPs services provided by PSAs. See for further details Chapter 6, IO.3.

National co-ordination and co-operation are key strengths of the Luxembourg system. However, in the field of CPF, expertise is limited to a few experts, which undermines the ability of other stakeholders to meaningfully contribute to national co-ordinate and co-operation. Luxembourg has taken positive steps since 2018, the adoption of its first NRA, although many of these efforts remain recent and their full effectiveness is yet to be seen.

Luxembourg is rated as having a Substantial level of effectiveness for IO.1.

Chapter 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

Key Findings and Recommended Actions

Key Findings

Immediate Outcome 6

1. Competent authorities regularly access and use financial intelligence to support investigation of ML/TF and related predicate offences and trace assets for confiscation. The CRF-FIU plays a key role in producing and disseminating a wide range of good quality financial intelligence products, which are widely used by LEAs and other competent authorities to support their operational needs.
2. Annually, the CRF-FIU receives approximately 50 000 reports from obliged entities via goAML and regular information on cash controls from the ADA. The quality and relevance of STRs/SARs and other reports steadily increased over the review period, reflecting increased outreach and feedback by the CRF-FIU. However, the relevance of the information reported by obliged entities in STRs/SARs, including on TF, remains to some extent a concern.
3. The responsiveness and proactivity of the CRF-FIU, including its overall engagement and assistance in ML and predicate offence investigations is commended by all competent authorities. The CRF-FIU plays a central role in Luxembourg's AML/CFT framework that goes beyond the receipt and analysis of SARs/STRs. However, its limited human resources give rise to concerns about the CRF-FIU's ability to continue effectively performing its various functions.
4. The CRF-FIU and other competent authorities regularly and effectively co-operate and exchange information and financial intelligence domestically and with international counterparts using secure channels to protect the confidentiality of the information exchanged or used.

Immediate Outcome 7

1. Luxembourg proactively identifies and investigates ML using a wide variety of sources. Judicial authorities and LEAs use all tools at their disposal to identify and investigate ML cases based on foreign predicate offences, including high risk predicate offences of fraud and drug trafficking. However, the number of ML cases identified in connection with high-risk predicate offences other than fraud and drug trafficking are disproportionately low.
2. Limitations in human resources hamper the ability of investigative and judicial authorities in conducting ML investigations. Strong inter-agency co-operation

among competent authorities, including ad hoc reallocation of resources, mitigates this issue to some extent.

3. Between 2017 and 2022, only a small proportion of cases moved from investigation to prosecution, with an average time lapse of 18 months between investigation and prosecution while files are considered by the Council Chamber. This calls the effectiveness of Luxembourg's prosecution system into question.
4. The types of ML investigations and prosecutions fall within Luxembourg's risk profile to a large extent. However, Luxembourg has not adequately pursued ML linked to sectors exposed to significant ML risk such as real estate and professionals offering TCSP services. Resource limitations, and issues relating to availability of intelligence resulting from underreporting by these segments of the private sector (see IO.4) prevent Luxembourg from pursuing ML cases to the extent that would be expected considering identified residual risks. This is mitigated to some extent, as many judicial investigations of predicate offences include a ML component.
5. Luxembourg prosecutes all forms of ML, including ML originating from foreign predicate offences, although the extent to which it does so is unclear. Based on case studies, ML of proceeds of foreign predicate offences, including third-party and stand-alone ML, are successfully prosecuted. However, data provided by Luxembourg does not disaggregate the different types of ML prosecutions and the assessment team has concerns over the extent to which Luxembourg prosecutes different types of ML more broadly.
6. Although Luxembourg's law provides for proportionate and dissuasive sanctions, frequent application of suspended sentences and the low level of fines imposed are neither proportionate nor dissuasive.

Immediate Outcome 8

1. Luxembourg prioritises confiscation as a prominent feature of its 2019 AML/CFT Strategy and is increasingly targeting assets other than cash. Operationally, Luxembourg authorities are highly committed to implementing the overarching 'crime does not pay' strategy and make full use of the existing tools for freezing, seizing, and confiscating assets domestically and abroad.
2. Luxembourg freezes, seizes and confiscates proceeds of foreign predicate offences and property of equivalent value (save for property of corresponding value to instrumentalities of crime), frequently on its own initiative and as requested by its foreign counterparts. However, Luxembourg cannot demonstrate what portion of the confiscated sums in domestic cases refers to foreign predicate offences, other than the proceeds confiscated from incoming MLA requests. Luxembourg demonstrated firm commitment to repatriation, asset sharing and restitution, paying out more than EUR 13 million to co-operation partners and victims during the review period.
3. Luxembourg effectively uses the range of measures allowing for restitution to victims without conviction-based confiscation. LEAs often intercept funds from ongoing criminality, which allows money to be returned to victims before concluding prosecution of a predicate offence.

4. Luxembourg successfully freezes significant amounts related to domestic cases referred to PAL/PAD. However, statistics on amounts confiscated based on domestic cases do not break down confiscation sums between foreign and domestic predicate offences, or stand-alone ML. Given the limitations in qualitative and quantitative data, the assessment team has concerns regarding how well authorities are confiscating proceeds and instrumentalities involving domestic predicate offences.
5. Luxembourg has limited capacity to preserve and manage the value of assets other than cash and balance on accounts that are seized or confiscated, forcing authorities to focus primarily on liquid assets. A centralised asset management office was recently established under the new AMO legislation.¹⁶ However, the law will not be fully in force until after the on-site visit, so it cannot be considered for the purposes of this evaluation.

Recommended Actions

Immediate Outcome 6

1. Luxembourg should ensure that the CRF-FIU is appropriately resourced to effectively manage its increasing workload, including by accelerating its on-going recruitment programme.
2. Given the complexity of cases analysed by the CRF-FIU, Luxembourg should ensure that newly recruited personnel have significant operational and strategic analysis experience.
3. The CRF-FIU, supervisory authorities and SRBs should increase and diversify their outreach and training activities to target underreporting from non-banking financial and non-financial sectors and reporting of TF. Such activities should focus on improving STRs' quantity and quality.
4. The CRF-FIU should complete the development and implementation of its new IT tool for operational analysis, ensure that it provides effective output and that all analysts receive comprehensive training to use it effectively.
5. The CRF-FIU should expand its information-sharing activities with the private sector, particularly regarding ML/TF typologies about major proceeds-generating foreign predicate offences.

Immediate Outcome 7

1. Luxembourg should increase parallel ML investigations related to all higher risk predicate offences to ensure better alignment of investigations and prosecutions with Luxembourg's risk profile.
2. Luxembourg should clearly prioritise and pursue, in line with identified risks, investigating and prosecuting ML involving corporate legal structures, professional money launderers, and real estate.

¹⁶ Throughout the review period Luxembourg had scattered practices for managing and, when necessary, disposing of property frozen, seized or confiscated.

3. Luxembourg should strengthen resource allocation across the judicial and investigative authorities to ensure competent authorities' ability to adequately prioritise and respond to the increasing number of ML investigations, including major and complex investigations. The principle of proportionality should be considered to avoid the creation of disproportionate workload between the competent authorities.
4. Luxembourg should develop the capacity to measure its own performance in ML prosecutions and convictions, including investigations of predicate offences with ML components, by fully implementing measures to develop and keep reliable, reconciled, and centralised data and statistics on ML investigations, prosecutions and convictions and the risk profiles of the cases.
5. Luxembourg should reconsider the role of the Council Chamber in relation to ML/TF cases. If the Chamber's role is maintained, Luxembourg should increase human resources and enhance ML expertise within the Council Chamber to ensure that ML-related files are appropriately prioritised and reduce the delay between the conclusion of ML investigations and prosecutions.
6. Luxembourg should take steps to enhance the judiciary's understanding of the seriousness of the ML offence and the need for commensurate sentencing through the review of the application of suspended sentences and the current level of sentencing applied in practice to ensure that penalties imposed are proportionate and dissuasive.

Immediate Outcome 8

1. Luxembourg should develop the ARO's capacity to better carry out its new mandate on post-conviction asset investigations and engage in international co-operation.
2. The AMO should implement procedures to manage assets other than cash and balance on accounts. Once the AMO is fully operational, Luxembourg should assess the procedures and staff in place to ensure effective management, and where appropriate disposal, of assets frozen, seized or confiscated.
3. Luxembourg should enhance the ADA's resources for cross-border controls on cash and BNI, including enhancing expertise in detecting ML involving cross-border cash movements.
4. Luxembourg should improve data collection on seizure and confiscation of criminal proceeds, instrumentalities, property of equivalent value and domestic proceeds located abroad to better evaluate their own effectiveness and identify areas for improvement.

119. The relevant Immediate Outcomes considered and assessed in this chapter are IO.6-8. The Recommendations relevant for the assessment of effectiveness under this section are R.1, R. 3, R.4 and R.29-32 and elements of R.2, 8, 9, 15, 30, 31, 34, 37, 38, 39 and 40.

Immediate Outcome 6 (Financial Intelligence ML/TF)

120. In the review period, financial intelligence and all other relevant information was appropriately used by Luxembourgish competent authorities for ML/TF investigations. Luxembourg Financial Intelligence Unit (CRF-FIU) financial intelligence factored in most ML/TF investigations conducted by Luxembourgish investigative authorities. All competent authorities provided numerous case studies demonstrating that reliable, accurate, and up-to-date information fed investigations of ML/TF and associated predicate offences.
121. This assessment was based on statistics; case studies; and interviews with relevant Luxembourgish authorities. Relevant findings on the level of international co-operation which competent authorities are participating in were considered.

Use of financial intelligence and other information

122. Competent authorities regularly access and use financial intelligence and other information to develop evidence and trace proceeds in investigations for ML, TF, and associated predicate offences. The CRF-FIU, the Judicial Police (SPJ), the Office of the Investigative Judge (investigative judge) and the State Prosecutor's Offices of the Luxembourg and Diekirch District Courts (PAL/PAD) can access directly (online), or in few cases indirectly, a wide range of public and private sector databases and information sources, which they regularly use to develop cases. Luxembourg provided extensive data to this effect covering all competent authorities.

Table 3.1. CRF-FIU access to external databases

| Database/Register | Managed by | Access |
|--|---|----------------------------|
| JU-CHA | Judicial authorities | Direct |
| Police databases | Police | Indirect (via SPJ) |
| Register of VAT (indirect taxes) payers | AED | Direct |
| Direct taxes | ACD | Indirect (via ACD) |
| Register of Fiduciary Contracts and Trusts | AED | Direct |
| Electronic Compendium of Companies and Associations (<i>Recueil électronique des sociétés et associations</i> - RESA) | LBR | Direct |
| Register of Beneficial Owners (<i>Registre des bénéficiaires effectifs</i> - RBE) | LBR | Direct |
| Trade and Company Register (<i>Registre de commerce et des sociétés</i> - RCS) | LBR | Direct |
| DOCASH | ADA | Direct |
| CIS+ | OLAF | Direct |
| Business licences register | Ministry of Economy | Direct |
| Mortgages Office (including mortgages, airplanes, and boats) | AED | Indirect (via SPJ and AED) |
| Payment and bank accounts identified by an IBAN and safe registers | CSSF Professionals as defined in Regulation (EU) No 260/2012 | Direct |
| Register of fiduciary contracts and trusts | AED | Direct |
| Real estate registers (<i>Registres fonciers</i>) | The Land and Topology Authority | Direct |
| Register on foreigners living in Luxembourg | Ministry of Foreign and European Affairs | Indirect (via SPJ) |

| Database/Register | Managed by | Access |
|--|--|--------------------|
| Register of asylum seekers | Ministry of Foreign and European Affairs | Indirect (via SPJ) |
| Register of visa applicants | Ministry of Foreign and European Affairs | Indirect (via SPJ) |
| Register of licensed weapon holders | Ministry of Justice | Direct |
| Register of natural persons | National Information Technology Centre | Direct |
| Register of employees, employers and self-employed | Joint Social Security Centre | Direct |
| Register on drivers' licenses | Ministry of Transport | Indirect (via SPJ) |
| Register of vehicles and their owners | Ministry of Transport | Direct |
| Births/deaths/marriages register | Civil Status Office | Direct |

123. The SPJ also provides intelligence support and analysis of data deriving from criminal intelligence operations and ML/TF preliminary or judicial investigations to investigative and judicial authorities. SPJ intelligence and findings triggered and fed a large number of investigations of ML/TF and predicate offences as indicated in various case studies.

Box 3.1. Case study: SPJ intelligence

In July 2020, based on SPJ intelligence, the PAL/PAD opened an ML investigation linked to unexplained/unjustified wealth against Mr. X.

According to the investigation, the SPJ-AB found that Mr. X expanded his activity from fraud to professional ML (third-party ML). The sums involved in this case amount approximately EUR 2.2 million, of which EUR 500 000 were used to create a Luxembourgish company.

Mr. X is suspected of being a professional money launderer, laundering illicit proceeds originating from “country A” and other countries. The proceeds are channelled through countries B, C, D, and F and Luxembourgish accounts before being further dispersed to other countries or used by Mr. X himself for personal expenses (e.g., casinos). SPJ also found that money had further been used from the account of Mr. X and from his company account to pay individuals and companies settled in different jurisdictions, which seem to have no direct link to him or his company. Amounts transferred to individual persons often contain a communication “Family Support” or “Family Assistance”. It is suspected that those transfers possibly represent payments for money mule services.

By the end of the on-site visit, the case was still under investigation.

124. The CRF-FIU produces and disseminates a wide range of high-quality financial intelligence products, which are widely used by law enforcement agencies (LEAs) and other competent authorities to support their operational needs. The CRF-FIU plays a vital role in the development of financial investigations. Statistics indicate that 90% of the white-collar crime cases transferred from PAL/PAD for further financial investigation stem from, or have been supported by, CRF-FIU reports or intelligence products. The CRF-FIU has issued an exhaustive list of criteria that will automatically trigger a report to PAL/PAD (i.e., domestic case under investigation; assets held with a professional are potentially subject to confiscation; indication of standalone ML; indication of self-laundering and/or of an underlying predicate offence; and inadequacy between the declared resources and one's standard of living or the absence of any indication as to the origin of property held). Since 2017, the number of CRF-FIU disseminations to domestic competent authorities doubled.

Table 3.2. CRF-FIU disseminations to domestic competent authorities, 2017-Q3 2022

| CRF-FIU disseminations | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|------------------------|------|------|------|------|------|---------|
| Number of cases | 149 | 263 | 297 | 300 | 335 | 229 |

125. LEAs and investigative authorities regularly sought CRF-FIU input during their investigations. The CRF-FIU provided substantial input and worked closely with investigative authorities in all TF and terrorism related investigations conducted throughout the review period. CRF-FIU intelligence was occasionally requested and provided at prosecution stage. Luxembourg provided numerous cases demonstrating how financial intelligence generated by the CRF-FIU (either based on SARs/STRs and other reports from obliged entities or information from international co-operation) was used by LEAs and investigative authorities to develop evidence for investigations into ML, associated predicate offences and TF. The following is a sample of these cases.

Box 3.2. Case study: The Big Apple

In April 2014, the CRF-FIU received a SAR from an insurance sector professional in relation to a life insurance policy subscribed by a French citizen (the suspect) for an amount of nearly EUR 8 million.

After the suspect submitted a request for partial redemption for the purchase of a property to be transferred to his personal bank account in France, the professional carried out further monitoring of the suspect and found that the New York Regional Office of the United States Securities and Exchange Commission (the SEC) had taken action against him in connection with embezzling considerable amounts from his clients at a US brokerage firm.

In November 2014, upon completion of its analysis and identification of links with France and Switzerland, the CRF-FIU disseminated this information to PAL. The PAL requested a judicial investigation be opened against the suspect and requested, in particular, the seizure of the funds held in the life insurance portfolio and the issuance of mutual

legal assistance (MLA) requests to the US, France and Switzerland. In January 2015, the Office of the Investigative Judge issued a seizure order and addressed an MLA request to the relevant countries. The PGD was mandated with the investigation and execution of the seizure order.

Following a plea bargain, the suspect was sentenced to 18 months of imprisonment and a EUR 250 000 fine. The court also ordered confiscation of approximately EUR 3 million.

Case study: Service-based money launderer

In 2020, a Luxembourg-based EMI filed an SAR about a potential new investor, citizen of “country A”, who was interested to become one of its shareholders.

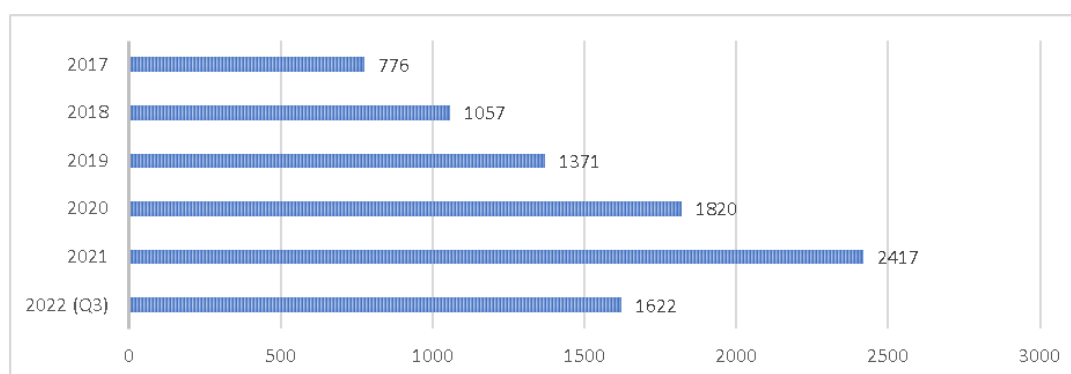
The suspicion was based on publicly available information related to the investor’s activities in “country B”. According to it, the investor and one of his business partners, a citizen of “country C”, participated in a criminal association aiming at committing bank fraud.

To support its analysis, the CRF-FIU engaged in international co-operation with 12 foreign counterparts, as investor and his business partner had links to these jurisdictions. All in all, thanks to the intelligence collected, the CRF-FIU found that:

- The initially reported investor was the BO of two Luxembourg-based companies generating a turnover exceeding EUR 30 million.
- The business activity of the subsidiary consisted in introducing new costumers to foreign payment institutions. The service was remunerated on a commission basis.
- The merchants introduced by the Luxembourg Company (approximately 635 companies opened in foreign jurisdictions) did not have legitimate businesses and operations and that they potentially launder illicit funds.
- Links to the investor’s former business partner, known for being part of the criminal association, which committed bank fraud in another country.
- The customer base seemed to be managed and controlled centrally by a network of third parties. The merchants had no investment or operational expenses, generated a high turnover not consistent with the apparent business activity and considerable outflows of funds in favour of the BO or the previously mentioned investor.
- Indications and suspicions of ML, non-justification of resources and abuse of corporate assets.

126. Given Luxembourg's exposure to foreign predicate offences, information stemming from incoming and outgoing MLA requests, including other forms of international co-operation are crucial channels for intelligence to develop evidence and trace proceeds, particularly related to fraud, corruption and tax crime. As outlined in IO.2, in the review period, the CRF-FIU and LEAs regularly and rapidly exchanged information to good effect with foreign counterparts.
127. Luxembourg provided numerous examples demonstrating the CRF-FIU's effectiveness in developing intelligence from a wide range of sources and successfully tracing proceeds (see box 3.4). Whenever the CRF-FIU established links with foreign jurisdictions, assets (including accounts) and intelligence/evidence crucial for domestic investigations were identified and seized thanks to the numerous international co-operation channels established or used by Luxembourgish competent authorities. On several occasions, CRF-FIU efforts to identify and develop intelligence were aided from its power to freeze assets suspected of ML/TF (see IO.2, core issue 2.4).
128. In line with its legal powers, the CRF-FIU requested and received additional information from obliged entities and other professionals. Between 2017 and 2022, the CRF-FIU made approximately 10 000 requests and received equal number of responses. There is an increasing trend in the volume of requests which follows respective trends in the volume of SARs/STRs, FIU-FIU international co-operation, and domestic co-operation. Over 70% of requests were addressed to banks and entities operating online which is consistent with Luxembourg's profile. The CRF-FIU received timely information on account holders, banking statements, BO declarations, logs of web banking access, etc. Information received from obliged entities were of added-value to CRF-FIU analyses and disseminations. The CRF-FIU requests are not subject to financial or professional secrecy. Obligated entities' replies were provided through goAML using tailored templates for this purpose (RIRA/RIRT), which ensured a standard of good quality and timeliness of responses. On average, the CRF-FIU received additional information within a few hours or directly via phone, in urgent cases. Occasionally, it received information within one week, at the latest, for large and complex requests.

Figure 3.1. Number of requests for information by the CRF-FIU, 2017-2022



129. Obligated entities and professionals are not allowed by law to inform their clients about CRF-FIU requests. CRF-FIU templates for information requests specifically highlight this prohibition.

130. In addition to intelligence from the CRF-FIU, LEAs and investigative authorities regularly open ML/TF files or parallel financial investigations based on information from the ADA and supervisory authorities. Depending on the nature of the case, asset scanning of bank, property, company and business, ownership structures, personal records and travel information routinely occurs in parallel financial investigations. The strong ties and co-operation among Luxembourgish competent authorities have aided to a large extent access to intelligence and development of evidence.

TF intelligence

131. Over the review period, the CRF-FIU was active in developing TF intelligence through reports from obliged entities. All reports on TF are analysed by two specialised analysts (supervised by two magistrates). To ensure adequate prioritisation of these reports, the CRF-FIU established two specific reporting formats: the TF activity reports (TFAR) and the TF transactions reports (TFTR). Many of these reports refer to terrorism rather than TF. Based on these reports, the CRF-FIU undertook its analysis and sought further input from obliged entities. Many of these disseminations relate strictly to terrorism. While these are valuable for terrorism investigations, such disseminations may contribute to some authorities' conflation of terrorism and TF (see IO.1). Table 3.3 breaks down the number of CRF-FIU financial analysis products in relation to TF and terrorism disseminated to the PAL and SRE.

Table 3.3. CRF-FIU disseminations related to terrorism and TF, 2017-Q3 2022

| Authority | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|-----------|------|------|------|------|------|---------|
| PAL TF | 1 | 9 | 1 | 4 | 4 | 2 |
| PAL T | 6 | 7 | 3 | 8 | 13 | 5 |
| SRE TF | N/A | 11 | 3 | 2 | 5 | 2 |
| SRE T | | 29 | 13 | 14 | 14 | 5 |

132. Beyond TFARs and TFTRs, TF-related financial intelligence includes raw financial information, such as bank statements. While most financial intelligence is derived from CRF-FIU reports, TF-related financial information may also have been discovered by SPJ during an investigation into other offences or as a result of a report containing financial information from another competent authority.
133. Overall, Luxembourg effectively develops evidence from a wide variety of intelligence sources, including SARs/STRs, ADA cross-border reports on currency and bearer-negotiable instruments (BNIs), SPJ intelligence; criminal records; supervisory and regulatory information; and information from Luxembourg's Business Register (LBR), the Register of Beneficial Owners of Legal Persons (RBE) and the Register of *Fiducies* and Trusts (RFT). In addition, Luxembourg provided examples of information used from other government agencies, including tax authorities and NPO supervisors; and information obtained through compulsory measures from FIs, virtual asset service providers (VASPs) and designated non-financial businesses and professions (DNFBPs), including customer due diligence (CDD) information and transaction records, as well as information from open sources (e.g., adverse media reports) to develop evidence and trace proceeds.

STRs received and requested by competent authorities

134. The CRF-FIU acts as the central authority for the receipt of SARs/STRs from obliged entities and Luxembourg competent authorities. In the review period, CRF-FIU received annually a very large number of reports (i.e., STRs, SARs, TFARs, TFTRs) from Banks, electronic money and payment institutions, VASPs, licensed operators of the Freeport, including standardised report forms from entities operating online. The quality of these reports and relevancy of information included varied across the financial and DNFBP sub-sectors (see para.116 - 117). The vast majority (99%) of reports were received through the goAML application. By the end of the on-site visit, approximately 6 880 obliged entities (approximately 44% of all obliged entities)¹⁷ were registered with goAML. Between 2017 and 2022, the CRF-FIU, supervisory authorities and SRBs undertook efforts to encourage all obliged entities registration with goAML and optimise submission of reports. However, the registration rate is low for some sectors, which is commensurate with the low reporting rate from certain DNFBPs.
135. The CRF-FIU also received intelligence and ML/TF related reports that contained relevant and accurate information from: (i) judicial authorities and LEAs (i.e., PG; PAL/PAD; the Office of the Investigative Judge; ARO; and SPJ), (ii) national supervisory authorities (i.e., CSSF, CAA, AED), (iii) other authorities (i.e., SRE, ACD), and (iv) SRBs (i.e., IRE, OEC, OAL).
136. In the review period, most reports originated from the e-money/payment institutions, banking, investment, insurance and VASP sectors (see IO.4). The CRF-FIU maintains comprehensive statistics on the underlying criminality of all incoming SARs/STRs per reporting sector. Most reports from these sectors referred to fraud, corruption, tax crimes and illicit trafficking in narcotic drugs and psychotropic substances, which is in line with Luxembourg's risk and context. Reports from these sectors were of good quality and contained relevant and accurate information.
137. Between 2017 and 2022, the CRF-FIU received on average 400 STRs annually from DNFBPs. Accountants, including chartered professional accountants, filed most of these. In recent years, there is an upward trend of reporting from DNFBPs following CRF-FIU awareness-raising campaigns undertaken in co-ordination with supervisory authorities, SRBs and professional associations. However, most DNFBPs, including some high-risk sectors, such as real estate agents provided a low number of SARs/STRs throughout the review period. Reports from these sub-sectors were mainly of poor quality, and some reports related to unanalysed adverse media hits (see IO.4). Because of such reporting, the number of reports actually relating to suspected proceeds of crime and TF are lower and not in line with Luxembourg's risk profile as an international financial hub.

¹⁷ Registration rate with goAML is calculated based on data about the population of obliged entities Luxembourg presented in Chapter 1. More details on the registration rate per category of FI and DNFBPs can be found in IO.4.

138. These issues affected to some extent the overall quantity and quality of information available to the CRF-FIU, and negatively affected its ability to effectively develop financial intelligence regarding ML/TF across all sectors (see IO.4). This issue was more prevalent between 2017 and 2019, leading the CRF-FIU to follow-up requests as a standard practice to ensure completeness and accuracy of reports. The CRF-FIU also worked with supervisory authorities to enhance the quality of the STRs/SARs and strived to develop a better common understanding of the risks related to some specific activities by publishing guidelines, annual reports, and typologies, and by organising various co-ordination meetings and training sessions for obliged entities. Since 2020, the quality and volume of STRs has gradually improved, aiding the CRF-FIU to improve the quality and volume of reports filed with PAL and intelligence shared with other competent authorities.
139. The quality and relevancy of TFARs and TFTRs as submitted across DNFBPs remains a concern for the assessment team. Many of these reports refer strictly to terrorism rather than TF (see IO.4).
140. Following the completion of SAR/STR analysis, the CRF-FIU provides feedback to respective obliged entities through a standardised feedback form. The standard feedback form includes improvement indicators and observations for obliged entities. This approach was followed for every SAR/STR that was closed, indicating whether the SAR/STR was archived, or whether intelligence was used to file a report with PAL/PAD. CRF-FIU experts also provide technical assistance to obliged entities during the SAR/STR submission stage aiming at ensuring adequate and timely outcome. Obligated entities across the board have indicated that the CRF-FIU was very responsive towards their inquiries. This aided in advancing their understanding of their AML/CFT reporting obligations and ML/TF typologies.

Reports on Cross-border Currency and Bearer Negotiable Instruments (CBNIs)

141. In the review period, the ADA requested and received declarations/disclosures for incoming and outgoing cross-border transportation of currency and BNIs (see R.32). The CRF-FIU received ADA reports for all violations of declaration/disclosure requirements. ADA reports were of good quality and contained relevant and accurate information.

Table 3.4. Cash control reports sent to the CRF-FIU, 2017-Q3 2022

| | 2017* | 2018 | 2019 | 2020 | 2021** | Q3 2022 |
|--|-------|------|------|------|--------|---------|
| Volume of reports | 9 | 1 | 7 | 15 | 7*** | 2 |
| Volume of CRF-FIU freezing orders | 5 | 1 | 7 | 15 | 1 | 2 |

*Note: After analysis of the case, the CRF-FIU released its freezing order in two cases in 2017 (as the legal origin of the funds was identified).

**Note: Data captures up to 03 June 2021.

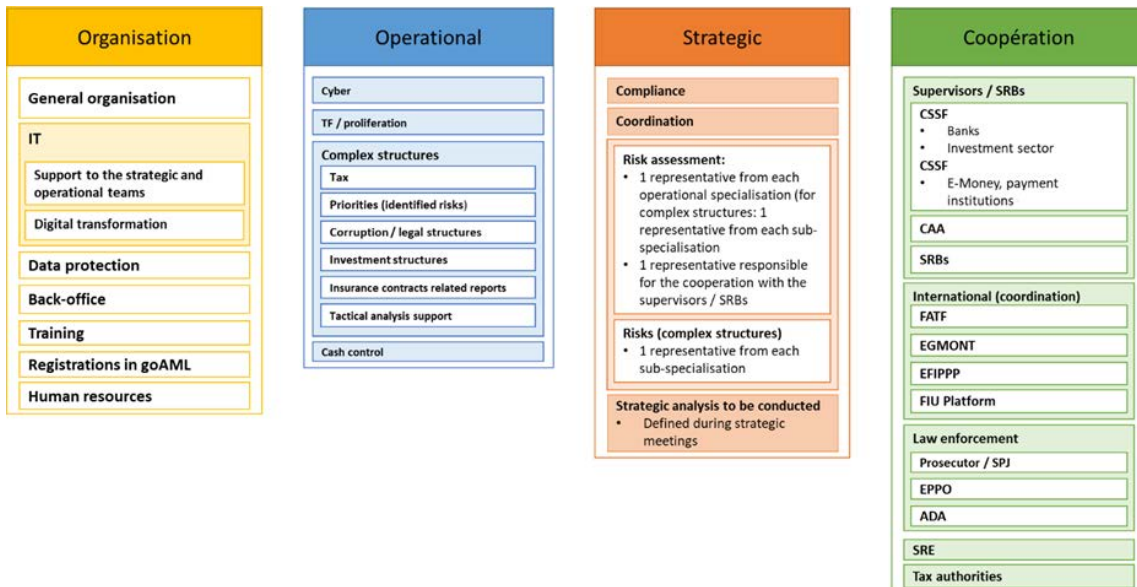
***Note: One report related to two people and to two separate administrative detention decisions. It resulted in six administrative decisions by the ADA and five ADA reports to PAL.

142. The CRF-FIU carried out additional analysis on all ADA reports based on other available databases, obliged entities information requests or requests from other competent authorities, incoming and outgoing requests to/from foreign counterparts. The CRF-FIU considers ADA reports to be of good quality. There is a standardised format for such reports. The CRF-FIU analysis is sent to PAL/PAD together with a copy of the ADA reports.

Operational needs supported by FIU analysis and dissemination

- 143. CRF-FIU analysis and disseminations substantially supported investigative authorities and LEAs’ operational needs. Relevant authorities met on-site confirmed the strong co-operation ties with the CRF-FIU and its ability to disseminate reports of good quality. Luxembourg provided many case studies confirming this fact.
- 144. The CRF-FIU comprises four pillars (i.e., organisation; operational; strategic; and co-operation). The organisation of the CRF-FIU is under the responsibility of the Head of CRF-FIU, the other three pillars under the responsibility of a Deputy Head of the CRF-FIU. The structure of the CRF-FIU meets the needs of domestic competent authorities. Input from the latter and the strong level of domestic co-operation support this finding. Each pillar targets a specific area in the fight against ML/TF (see Figure 3.2). Information on the products of each pillar flows uninterrupted and feeds the work of the other pillars. For example, typologies and trends developed by the Strategic pillar are shared with the Operational and Co-operation pillars, who share these products with domestic competent authorities and foreign counterparts. In addition, the CRF-FIU structure allows for directed communication between CRF-FIU analysts and competent authorities for certain matters (i.e., tax matters).

Figure 3.2. CRF-FIU Organisation chart



Resources

145. The CRF-FIU is the central authority for receipt and dissemination of SARs/STRs and it plays a central role in international co-operation and support to LEAs, intelligence, investigative and supervisory authorities. Despite the gradual increase of CRF-FIU resources throughout the review period (see Table 3.5), the current level of staff is insufficient to continue sustainably supporting its central and multi-faceted role in Luxembourg's AML/CFT framework, particularly considering the size and scope of Luxembourg's FI and DNFBP sectors. The CRF-FIU analysis and support is requested and provided on almost all investigations and incoming MLA requests. Other authorities, such as SRE, rely heavily on CRF-FIU financial intelligence. During the interviews, it was made clear that for all competent authorities, the CRF-FIU is the starting point for every AML/CFT endeavour, including training and awareness raising.
146. Lack of resources, including staff turnover, affected to some extent the quality of CRF-FIU work and responsiveness in the first half of the review period. Up to 2019, the CRF-FIU had only nine analysts, a disproportionately small number, considering both the size of Luxembourg's financial sector, the large volume of SARs/STRs and the volume and frequency of domestic and international requests for the CRF-FIU to conduct transactional analysis. The dedication of CRF-FIU personnel, the systematic investment in analytical tools and software, and occasional resource re-allocation to address complex cases mitigated this shortfall to some degree throughout the review period.
147. Between 2017 and 2020, the total CRF-FIU staff doubled, the number of analysts almost tripled, and the growth trend has steadily increased. At the time of the on-site, greater human resources, combined with increasingly sophisticated technology and analytical tools, enabled the CRF-FIU to handle their workload with reasonable effectiveness. However, the role of the CRF-FIU and its workload continue to increase, and its resources should continue to increase proportionally to keep up and ensure sustainability.

Table 3.5. CRF-FIU human resources, 2017-Q3 2022

| Staff | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|----------------------------|-----------|-----------|-----------|-----------|-----------|-----------|
| Number of Analysts | 5 | 8 | 9 | 14 | 18 | *23 |
| Number of Magistrates | 3 | 4 | 5 | 6 | 6 | 6 |
| Secretariat staff | 5 | 5 | 5 | 5 | 6 | 6 |
| IT staff | 1 | 2 | 3 | 3 | 3 | 3 |
| Total CRF-FIU staff | 14 | 19 | 22 | 28 | 33 | 38 |

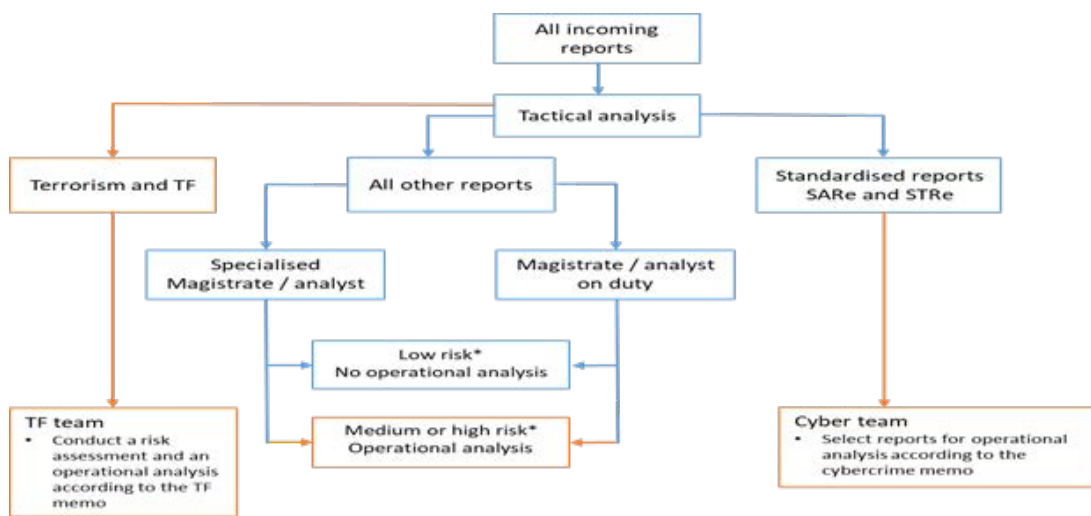
*Note: 18 operational analysts, 3 strategic analysts, and 2 data scientists.

148. The CRF-FIU staff participates regularly in specialised training and continuing education, which meets their current needs. The CRF-FIU staff also received training from the SPJ Training Unit. The CRF-FIU has a training programme that ensures adequate training of its staff. Currently the CRF-FIU is setting up a unit dedicated to training matters. The CRF-FIU provided training on AML/CFT matters to other competent authorities and the private sector. Luxembourg shared with the assessment team a comprehensive list of training events organised or attended by the CRF-FIU personnel.

Operational analysis

149. The CRF-FIU uses an effective automated data matching system for SARs/STRs to support operational intelligence needs. All SARs/STRs were initially screened to determine the level of analysis required. This process includes a quality control of information received and risk assessment. For low and medium risk reports, where no analytical trail could be identified, the analysis was limited to the tactical phase. Medium-risk reports, for which analytical leads were identified, and high-risk reports were subject to an operational analysis. The CRF-FIU shared with the assessment team its criteria and risk matrix based on which it determines the level of analysis required. Upon review, the assessment team considers both as comprehensive.

Figure 3.3. Analysis of incoming reports



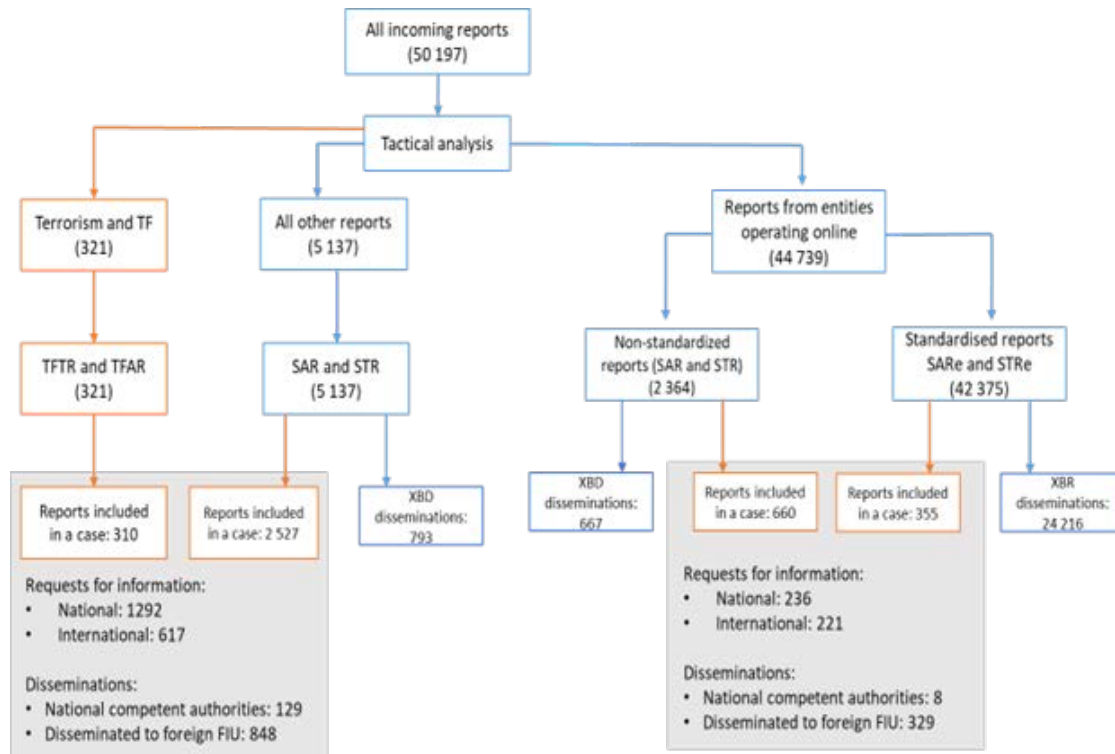
Blue lines: tactical analysis stage Orange lines: operational analysis stage

Note: As described before, for low and medium risk reports, where no analytical trail could be identified, the analysis will be limited to the tactical phase. Medium-risk reports, for which analytical leads could be identified, and high-risk reports are subject to an operational analysis.

150. Between 2017 and 2022, the CRF-FIU received more than 50 000 SARs/STRs per year. The CRF-FIU conducted operational analysis for approximately 4 000 of these SARs/STRs per year. Upon completion of operational analysis, the CRF-FIU took one of the following actions: (i) closed and archived the case; (ii) exchanged the information with its foreign counterparts; (iii) provided specific information to PAL through the “Share system”¹⁸; or (iv) disseminated financial analysis report, including relevant information and documentation to one or more (depending on the professional, sector or offence involved) competent authority(-ies) to support its/their operational needs.

¹⁸ The Share is a secure intranet folder shared only between CRF-FIU and PAL/PAD.

Figure 3.4. CRF-FIU tactical and operational analysis outcome, 2021



Blue lines: tactical analysis stage Orange lines: operational analysis stage

151. Between 2017 and 2022, the CRF-FIU disseminated approximately 1 500 reports (see Table 3.6) to relevant authorities (PAL/PAD; the Office of the Investigative Judge; CSSF; CAA; AED; ACD; and SRE). CRF-FIU reports to PAL and the Office of the investigative judge related to ML through fraud and forgery, tax crimes, drug trafficking and corruption, which is in line with Luxembourg’s main threats (see Table 3.7). The CRF-FIU sent 17 TF-related reports to PAL. All competent authorities acknowledged the quality of CRF-FIU intelligence, which significantly increased over the years of the review period.

Box 3.3. Case study: Misuse of Donations

In 2020, PAL/PAD initiated an investigation of a foreign NPO about misappropriation of funds based on a CRF-FIU report. In the course of the investigation, the CRF-FIU provided additional information to PAL/PAD that proved to be essential. In particular, the CRF-FIU not only provided in-depth analysis of accounts and transactional inflows/outflows, but also provided information on assets held abroad (France, Spain, and Italy).

By the end of the on-site visit, the case was still under investigation and the suspect in pre-trial custody.

Table 3.6. CRF-FIU cases and disseminations, 2017-Q3 2022

| CRF-FIU disseminations | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|--|-------|-------|-------|-------|-------|---------|
| Cases handled in reference year | 1 151 | 1 408 | 1 513 | 1 682 | 2 094 | 1 862 |
| Cases disseminated to domestic competent authorities | 149 | 263 | 297 | 300 | 335 | 229 |

Table 3.7. CRF-FIU disseminations to PAL/PAD / Office of the Investigative Judge per predicate offence, 2017-Q3 2022

| Predicate Offences | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|---|------------|------------|------------|------------|------------|------------|
| Other | 10 | 38 | 35 | 13 | 35 | 18 |
| Standalone money laundering | --- | --- | --- | 45 | 18 | 12 |
| Corruption | 2 | 2 | 3 | 1 | 6 | 1 |
| Counterfeiting and product piracy | | | | | 5 | 4 |
| Cybercrime | 2 | 0 | 7 | 1 | 2 | 1 |
| Extortion | 1 | 0 | 0 | 0 | 0 | 0 |
| Sexual exploitation, including sexual exploitation of children | 0 | 0 | 1 | 2 | 1 | 2 |
| Kidnapping, false imprisonment and hostage-taking | 0 | 0 | 0 | 1 | 0 | 0 |
| Forgery | 16 | 24 | 19 | 13 | 14 | 11 |
| Counterfeiting currency | 1 | 0 | 2 | 2 | 1 | 0 |
| Fraud | 68 | 99 | 137 | 108 | 131 | 78 |
| Tax crimes | 2 | 5 | 4 | 5 | 12 | 11 |
| Participation in an organised criminal group & racketeering | 0 | 0 | 2 | 0 | 1 | 1 |
| Terrorism and terrorist financing | 2 | 7 | 3 | 3 | 2 | 1 |
| Illicit trafficking in narcotic drugs and psychotropic substances | 3 | 5 | 3 | 2 | 7 | 1 |
| Illicit arms trafficking | 1 | 0 | 0 | 0 | 0 | 0 |
| Robbery and theft | 9 | 11 | 3 | 1 | 1 | 1 |
| Total | 117 | 191 | 219 | 197 | 234 | 189 |

Strategic analysis

152. The CRF-FIU undertook strategic analysis that supported and to a large extent met the operational needs of competent authorities. The CRF-FIU conducted strategic analyses on group reports linked to common criminal patterns. Such analyses helped in enhancing competent authorities understanding on new ML/TF indicators and criminals' modus operandi. In the review period, the CRF-FIU issued the following categories of strategic analysis products:
- Strategic analyses carried out for CRF-FIU internal purposes based on recurring SARs/STRs;
 - Strategic analyses carried out for the private and public sector, mainly shared through CRF-FIU annual reports; and
 - Strategic analyses conducted within a specific national or international working group (i.e., Egmont project on BEC-fraud co-chaired by the CRF-FIU or the working groups co-chaired within the Europol Financial Intelligence Public Private Partnership (EFIPPP) on COVID-19).
153. Since 2018, the CRF-FIU carried out strategic analysis in the following areas: (i) TF; (ii) NPOs; (iii) virtual currencies; (iv) tax crime; (v) corruption; (vi) investment funds sector; (vii) real estate sector; (viii) chief executive officer (CEO) fraud; (ix) child sexual exploitation and abuse; (x) fraudulent wire transfers; and (xi) TCSP services. These products assist LEAs to stay current in thematic areas (i) to (xi) and facilitate the conduct of investigations in relevant cases. These strategic analysis products are in line with Luxembourg's main threats and meet LEAs operational needs.
154. The relevant supervisory authorities and SRBs received strategic analyses products through goAML, the CRF-FIU Annual Activity Report, and CRF-FIU guidance to the private sector. These products (i.e., confidential reports and guidance about Covid-19 typologies), were used to support their supervisory activities.
155. The outcome of strategic analyses is also shared during training sessions. The CRF-FIU offered such training courses to PAL/PAD, Office of the Investigative Judge (investigative judge), SPJ, ADA, OEC and the OAs where the outcome of strategic work was included.

Co-operation and exchange of information/financial intelligence

156. In the review period, co-operation and exchange of information and financial intelligence among Luxembourg competent authorities was highly fluid and effective. The assessment team had a first-hand experience during the on-site visit of the strong cooperative spirit that characterises all contacts among Luxembourg's competent authorities. Competent authorities proactively seek co-operation and exchange information at all levels (e.g., supervision, financial intelligence, investigation, etc.). This is also clear from the case studies presented across the different immediate outcomes. Competent authorities spoke about "Luxembourg consensus", the notion that all authorities are generally on the same side even when there are divergent views, and accordingly work to achieve consensus. Luxembourg addresses challenges posed by its size and limited human resources in the CRF-FIU, LEAs and investigative authorities by boosting co-operation among the relevant authorities and working to facilitate resource allocation to help meet the needs arising from major and complex cases.

Table 3.8. CRF-FIU disseminations and PAL/PAD/Office of the Investigative Judge requests, 2017-Q3 2022

| Authority | Proactive co-operation | | | | | | Reactive Co-operation | | | | | |
|--|------------------------|------------|------------|------------|------------|------------|-----------------------|------------|------------|------------|------------|------------|
| | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
| PAL | 117 | 190 | 219 | 189 | 218 | 142 | 44 | 122 | 196 | 225 | 245 | 236 |
| PAD | | | | | | | 1 | 4 | 12 | 20 | 30 | 23 |
| Office of the Investigative Judge | 0 | 0 | 0 | 8 | 18 | 22 | 0 | 0 | 7 | 3 | 12 | 17 |
| Total | 117 | 190 | 219 | 197 | 236 | 164 | 45 | 126 | 215 | 248 | 287 | 276 |

157. As indicated in the table above (see Table 3.8), since 2017, the CRF-FIU responded to an increasing number of requests to support ongoing domestic investigations.

Box 3.4. Case study: Hidden treasure

In March 2016, the SPJ received a complaint of a victim about a theft of bank coupons/securities of EUR 500 000 value.

In parallel, the CRF-FIU received information from an obliged entity that misappropriated securities were cashed through one of their bank accounts. The CRF-FIU identified the beneficiary, including links to other accounts, in four different banks, used by the perpetrator to collect the cash. Overall, the perpetrator (i.e., son of the person in charge of the household of the victim) collected EUR 225 000.

On 18 and 24 March 2016, the CRF-FIU took freezing measures to secure the assets and filed a report with PAL, who requested the seizure of the funds.

On 14 February 2017, the PAL filed an indictment against the suspects. On 22 March 2018, the perpetrator was convicted for standalone ML by conversion, possession and use. He was sentenced to imprisonment for nine months and fined with EUR 3 000. EUR 225 000 was confiscated.

158. Whenever CRF-FIU information suggested ML or underlying predicate offences committed on Luxembourg territory, the CRF-FIU sent its analytical reports to the PAL Economic and Financial Unit. Such reports were comprehensive and contained specific financial and other information, including relevant documentation. Many of these led to convictions and confiscations. The CRF-FIU disseminated analytical reports directly to the investigative judge when information was linked to ongoing judicial investigations.

FIU co-operation and information exchange

159. The CRF-FIU and the PAL Cybercrime unit cooperated on investigations relating to fraudulent foreign account used to commit an offence. Whenever such a case was dismissed or discontinued, information (including account details) was integrated in goAML and immediately forwarded to CRF-FIU foreign counterparts. PAL reopened investigation in some cases of this nature based on information received from CRF-FIU foreign counterparts.
160. Co-operation and information exchange between the CRF-FIU and SPJ was of good quality and produced effective results. Luxembourg provided several case studies where, during an investigation, SPJ requested information analysis from the CRF-FIU to aid in building the case. In addition, both authorities cooperated closely on AML/CFT training matters.
161. The CRF-FIU and CSSF co-operated and exchanged information throughout the review period in a comprehensive manner. Several investigations were initiated from CSSF STRs, from CSSF supervised entities and CSSF activity reports to the CRF-FIU. Between 2017 and 2022, the CSSF made approximately 500 referrals to the CRF-FIU. Many of them resulted into reports to PAL and several triggered disseminations to CRF-FIU foreign counterparts. Both competent authorities worked closely on training matters and awareness raising activities aiming at boosting obliged entities' understating of their AML/CFT reporting obligations. To further facilitate co-operation and information exchange, the CRF-FIU is an active member in several PPP created by the CSSF to produce sector-specific feedback, typologies, risks and AML/CFT obligations. In addition, there was co-operation and information exchange of good quality for the SSRA led by the CSSF (see IO.1 and IO.3).

Confidentiality

162. Throughout the review period, the CRF-FIU protected the confidentiality of the financial and other intelligence it gathered. Physical controls at the CRF-FIU premises and IT security measures are strictly implemented. IT staff dedicated to the CRF-FIU and the State Computer Technology Centre handle, store, and protect access to CRF-FIU information. All CRF-FIU systems were monitored 24/7 and penetration tests were conducted regularly. To ensure the highest data security standards, highly qualified IT specialists dedicated to the CRF-FIU, as well as IT specialists from the Government IT centre handled data security aspects.
163. The assessment team received special authorisation to visit the CRF-FIU physical premises to understand the safeguards put in place. Exchange of intelligence with foreign FIUs took place across secure networks, including FIU.NET and the Egmont Secure Web. Avenues used for communication and information exchange with domestic competent authorities, mainly goAML, were also separate and secure.

164. As with CRF-FIU information, specialised IT staff safeguarded the judicial authorities' database and case management system (JU-CHA). Access to this database was strictly limited to the staff of the judicial administration and certain data were only accessed by specific designated services. Access to JU-CHA was given only to staff with a LuxTrust certificate.¹⁹ LuxTrust allowed management of identities and access rights of all judicial administration employees.

Overall conclusion on IO.6

The CRF-FIU effectively gathers and disseminates a wide range of intelligence. Luxembourg LEAs and investigative authorities made good use of CRF-FIU financial intelligence. There was strong domestic co-operation and information exchange among all competent authorities. However, limitations in CRF-FIU resources throughout the review period, particularly in the first half, and issues pertaining to the relevancy and accuracy of information received from obliged entities, including TFARs and TFTRs, had some impact on the quality of CRF-FIU work and responsiveness. CRF-FIU staff dedication and high-tech analytical tools limit to some extent the overall impact of this issue. However, further resources will be required to keep pace with the CRF-FIU's growing workload. The assessment team has some concerns on gaps in intelligence available to the CRF-FIU from certain non-bank financial and DNFBP sectors. Overall, the identified shortcomings will require moderate improvements to overcome.

Luxembourg is rated as having a Substantial level of effectiveness for IO.6.

Immediate Outcome 7 (ML investigation and prosecution)

165. Given Luxembourg's role in global financial system, most ML investigations have an international component. Luxembourg demonstrates a policy-driven commitment to follow the money by systematic review of MLA requests for potential links to ML offences in Luxembourg. This assessment was based on statistics; case studies; and interviews with relevant Luxembourgish authorities. Relevant findings on ML investigations conducted based on information stemming from incoming formal and informal international co-operation were also considered.

ML identification and investigation

166. Luxembourg proactively identifies and investigates ML through a wide variety of sources. Judicial authorities and LEAs use all tools at their disposal to identify and investigate ML cases based on foreign predicate offences. However, the number of ML cases identified in the course of high-risk predicate offence investigations, other than fraud and drug trafficking are disproportionately low.

¹⁹ LuxTrust is a Certificate Authority authorised to issue public key certificates (i.e., electronic or digital certificates), which can be used for authentication, e-signature or encipherment

Human resources

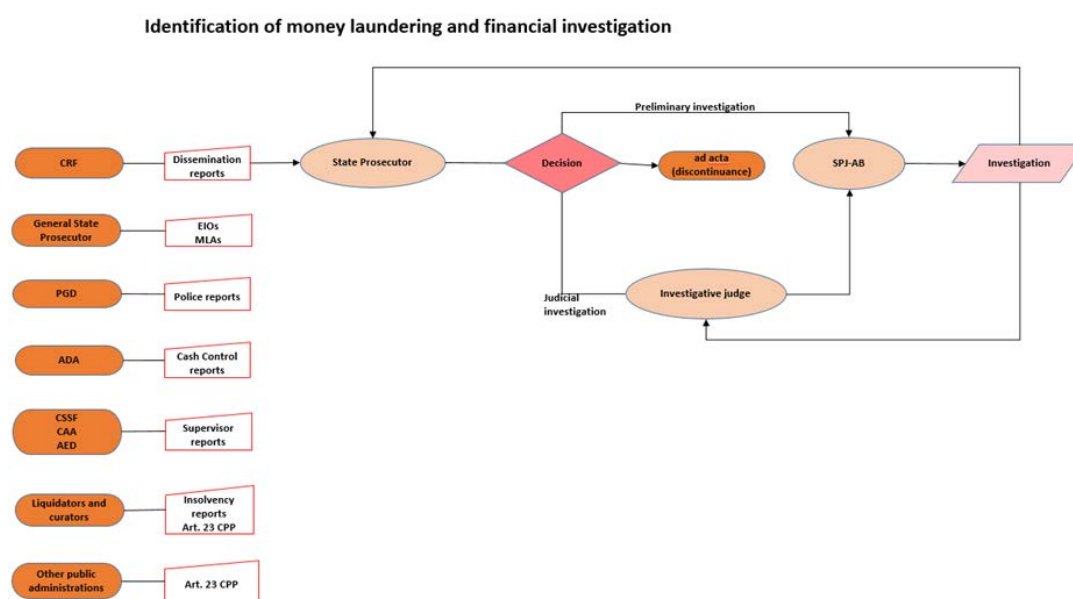
- 3
167. Limitations in human resources impact to some extent the effectiveness of investigative and judicial authorities in conducting ML investigations. Throughout the review period, competent authorities relied heavily on the dedication and professionalism of their personnel to overcome issues pertaining to the increasing volume of ML investigations and incoming MLA requests. Despite Luxembourg's initiatives to increase resources among investigative and judicial authorities, mainly within SPJ, these authorities remain insufficiently resourced.
 168. In an attempt to mitigate this issue, both PAL/PAD and the Office of the Investigative Judge (investigative judge) put significant effort into making the most out of their resources on both international co-operation and investigations. Strong inter-agency co-operation among competent authorities, including ad hoc resource reallocation, addresses this issue to a significant extent. PAL/PAD, the investigative judge and the SPJ meet every three months to discuss resource allocation and prioritisation of ongoing investigations. Such co-operation also includes the addition of specialised support from other SPJ departments and competent authorities to address needs stemming from more sophisticated ML investigations.
 169. Luxembourg investigative authorities are well aware of the country's ML risk and the threat stemming from laundering of foreign predicate offences. In the review period they paid significant attention to AML training of SPJ officers and investigators. The SPJ has a unit dedicated to training that regularly organises training courses on AML and asset recovery. Training also covers technological challenges such as VA-related investigations. The investigative judge and PAL/PAD magistrates all receive comprehensive AML training.
 170. Luxembourg has three competent authorities to investigate ML: the PAL/PAD, the investigative judge and the SPJ. In addition, the ADA, the only non-LEA competent authority in this field, in line with its mandate, detects and records drug-related predicate offences giving rise to ML. Its competence is limited to cases where (a) the predicate offence has clearly been identified as drug trafficking and (b) this predicate offence has not been committed as part of a criminal organisation (1973 Drug Law, Art. 10). The SPJ investigates ML cases. On a case-by-case basis, the PAL/PAD or the investigative judge require the participation of ADA in such investigations. Between 2019 and 2022, the ADA participated in two joint investigation teams. Preliminary investigations are conducted by the PAL/PAD and/or the SPJ when requested by PAL/PAD. Competent authorities have specialised staff and dedicated units responsible for investigating ML.

Table 3.9. Authorities with responsibilities for investigating ML, Q3 2022

| Competent Authority | Human Resources |
|---|--|
| PAL – AML Unit | 39 Magistrates out of which 16 are specialised in white-collar crime investigations, including six specialised in ML investigations. |
| PAD | 7 Magistrates out of which two are specialised in white-collar crimes, including one specialised in ML cases. |
| Office of the Investigative Judge - District Court of Luxembourg | 7 Investigative judges specialised in ML and white-collar crimes |
| Office of the Investigative Judge - District Court of Diekirch | 2 Investigative judges working also on ML and white-collar crimes |
| SPJ – AB Unit | 21 Staff specialised in ML |
| SPJ - Economic and Financial Crime Department | 23 Staff specialised in white-collar crimes |
| ADA | 20 officers |

Identification and Investigation

171. Luxembourg uses a broad range of sources to identify ML cases. These include reports from the CRF-FIU and other Luxembourgish competent authorities, information discovered during investigation of predicate offences, and incoming requests for MLA and international co-operation.

Figure 3.5. Identification of ML and financial investigations

172. The CRF-FIU reports are one of the primary sources triggering ML investigations and parallel financial investigations (see IO.6). Between 2017 and 2022, the CRF-FIU filed more than 1 000 reports with the PAL/PAD (see Table 3.10). Many CRF-FIU reports to PAL/PAD triggered preliminary or judicial investigations. There is a continuing increase of CRF-FIU reports, resulting from the improved quality of STRs from most sectors (see IO.4) and the increase of CRF-FIU resources (see IO.6). CRF-FIU reports are of good quality and rarely require further development for a ML investigation to be initiated. In the review period, the percentage of CRF-FIU reports to PAL/PAD that resulted in investigations increased from 41 % to 71% (see Table 3.10 and Box 3.10). However, investigative and especially judicial resources have not kept pace with the increased capacity in other areas of Luxembourg's AML/CFT regime, which results in delays, particularly with cases moving through the Council Chamber.

Table 3.10. CRF-FIU disseminations to PAL/PAD, 2017-Q3 2022

| | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|---|------|------|------|------|-------|---------|
| Total number of ML notices | 758 | 656 | 836 | 852 | 1 026 | 813 |
| CRF-FIU reports (including after PAL/PAD request) | 117 | 191 | 219 | 197 | 234 | 147 |
| ML notices based on first report by CRF-FIU* | 77 | 113 | 123 | 153 | 160 | 94 |
| Judicial investigations based on first reports | 29 | 43 | 56 | 37 | 63 | 42 |
| PAL/PAD on-going investigations from CRF-FIU reports | 48 | 46 | 90 | 105 | 146 | 105 |

*Note: Although no statistics are maintained to this effect, almost all of these reports were followed by a preliminary investigation.

173. A significant number of ML investigations also arise from information identified by SPJ during investigation of predicate offences. Often, when executing investigative requests from PAL/PAD and investigative judges, SPJ officers discover new facts that are likely to constitute a ML offence, not captured by the initial requests. SPJ officers record these new facts in a separate report and forward it to PAL/PAD, who may decide either to integrate the ML component into the ongoing case or, in the event of a major or complex ML, to open a separate case and entrust the investigation to the SPJ-AB unit. However, Luxembourg neither maintains separate statistics on such investigations, nor takes them into account in the statistical category of pure ML investigations. As such, statistics on ML investigations under-represent the actual number of ML investigations that occur.

174. Incoming MLA requests, including European investigation orders (EIOs) give also rise to ML investigations (see Box 3.5). The PAL AML Unit scans all incoming MLAs/EIOs aiming at identifying links to ML in Luxembourg. Between 2017 and 2022, Luxembourg conducted 36 ML investigations based on information found in executing foreign requests for assistance.

Box 3.5. Case study – ML investigation triggered by incoming MLA

In June 2013, following an incoming MLA request from country A about acts of misuse of corporate assets by Mister Y (director of Co B), the SPJ carried out a search at the premises of a Luxembourg company (LuxCo). The SPJ findings revealed that "clients" of a foreign company (Co B) had contracts and invoices to enable them to take money from companies of which they were directors. The SPJ detected other similar cases.

According to the SPJ findings, Mister X director of Co B, directed the company from offices of another company based in Luxembourg (LuxCo2). Mister X was the manager of LuxCo2 and did not have all the required authorisations to carry out his activities (i.e., domiciliation, company formation and management, chartered accountancy, consultancy and economic consultancy).

In June 2015, based on the SPJ findings, the PAL ordered the opening of a judicial investigation. The investigation uncovered standalone ML, as a company was laundering the proceeds of predicate offences (i.e., misuse of corporate assets) committed by third parties in other countries.

The amounts laundered account for approximately EUR 26.2 million.

Upon completion of the judicial investigation in February 2022, the file was referred to the Council Chamber. The review of the case is pending.

175. Luxembourg has also conducted investigations based on ADA cash control reports. Between 2017 and 2022, PAL/PAD conducted or ordered approximately 40 ML investigations based on such reports. However, none of these cases have resulted in ML prosecutions or convictions.
176. Supervisory authorities' reports to PAL and CRF-FIU may also give rise to ML investigations. Such reports mainly relate to predicate offences, ML suspicion, or violation of AML/CFT obligations by professionals. Most of these reports are filed by CSSF. Since 2017, reporting to PAL from supervisors has doubled or even tripled in some cases. The PAL works closely with supervisors aiming at improving the quality of such reports. The authorities provided cases studies demonstrating the outcome of such co-operation.

Table 3.11. ACD, AED and CSSF reports to PAL, 2017-Q3 2022

| Authority | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|-----------|------|------|------|------|------|---------|
| ACD | 7 | 33 | 23 | 39 | 59 | 31 |
| AED | 14 | 6 | 16 | 27 | 69 | 48 |
| CSSF | 42 | 68 | 73 | 102 | 136 | 74 |

Box 3.6. Case study: VAT Carousel

In March 2020, the AED, in its capacity as tax authority, filed three reports with PAL, following an in-depth inspection of company H by the AED's Anti-Fraud Department.

According to the inspection findings, H was part of a system set up to commit a VAT offence, namely carousel fraud by missing trader, consisting of a mechanism set up between several companies (at least three) established in different EU Member States (Germany, Belgium, the Netherlands), allowing to fraudulently reduce the amount of VAT due to be paid.

In July 2020, PAL requested SPJ to conduct a preliminary investigation.

The AED's investigation as well as the SPJ investigation revealed the following elements that could prove tax fraud:

Company H's profit margins were minimal;

- Absence of a warehouse in the Grand Duchy and non-registration for VAT in Belgium and the Netherlands;
- High number of VAT defaulters;

In April 2022, the District Court ordered the dissolution of company H. for tax fraud and ML.

177. ML investigations can be triggered from reports filed with PAL by liquidators and administrators in the context of their duties given their access to different banking and social documentation. The authorities shared some examples of such investigations with the assessment team. In addition, ML investigations can also arise from open-source information, particularly from the press service of the PG. Although rare, an example was shared with the assessment team.
178. The investigation process as described below is sound and efficient. The assessment team did not identify any obstacles on the process itself other than issues related to the resourcing of competent authorities as noted above:
 - The PAL/PAD (AML Unit) is the primary investigative authority for ML. It receives information from multiple sources and, based on that information and any further investigative measures that should be executed, decides whether to open a preliminary investigation or refer the case to the investigative judge for judicial investigation.
 - Following the PAL/PAD request for judicial investigations, the investigative judge orders any necessary coercive measures to be taken (e.g., search and seizure);
 - The SPJ (AB Unit) conducts preliminary investigations as requested by PAL/PAD and financial and asset investigations in line with the measures ordered by the investigative judge. Upon completion of an investigation, it forwards the file to PAL/PAD.

- After a preliminary investigation for a misdemeanour, PAL/PAD can send the case directly to the District Court for misdemeanours for trial (*citation directe*). In the case of a judicial investigation, PAL/PAD forward the file to the Council Chamber requesting the referral of the case to the competent trial court.
 - The Council Chamber examines cases sent by PAL/PAD, decides whether judicial investigations will result in prosecutions and checks whether there are mitigating circumstances in favour of the defendant. The Chamber then sends cases for trial to either the District Court for misdemeanour matters or the District Court for felony matters.
179. Judicial authorities and LEAs have a wide range of tools at their disposal to identify and investigate ML cases based on both domestic and foreign predicate offences (see R.31). Based on the case studies provided, it is clear that competent authorities make good use of all the available tools.
180. Luxembourg provided examples of successful identification and investigation of ML related to predicate offences, including third-party ML and some complex cases involving cross-border activities, regular use of special investigative techniques, arrests and assets frozen. Investigative authorities conduct a parallel financial investigation for each predicate offence involving large sums of money aiming at identifying any ML elements.

Box 3.7. Case Studies

Case study: Bad banker

In September 2011, Mr. X, a former employee of a Luxembourg bank (Luxbank), misappropriated EUR 3.5 million from customer accounts, which he transferred to his own Swiss account with Swiss bank B (Swissbank).

In December 2011, PAL opened a judicial investigation. An international arrest warrant was issued and executed by the Swiss authorities in December 2012 when Mr. X was arrested. In March 2013, he was extradited to Luxembourg, charged by the investigative judge, and remanded in custody until May 2014. Mr. X was then placed under judicial supervision pending trial.

The SPJ investigations on financial flows uncovered complex ML mechanisms, the set-up and maintenance of which required a high level of expertise in financial engineering. These mechanisms included a circuit of false invoices and foreign structures, directed by nominees, established in different jurisdictions to add opacity to the transactions. In pursuing the money trail, Luxembourg issued 32 MLA requests to 19 jurisdictions, 21 Interpol requests and a request to Europol.

Mr. X and six other individuals involved in the ML mechanisms were put on trial in late 2020. On appeal, Mr. X received 4 years of misdemeanour imprisonment, one of which on probation, and a EUR 500 000 fine.

As for other defendants:

- JM received 2 years of misdemeanour imprisonment and a EUR 200 000 fine.
- YA was acquitted.
- EA was given 24 months of misdemeanour imprisonment and a EUR 150 000 fine.
- MADCM was sentenced to a one-year suspended sentence, and a EUR 60 000 fine.
- PS received a 9-month suspended sentence and a EUR 45 000 fine.

Confiscation of the following was ordered: EUR 300 000; luxury watches.

The defendants were also liable for EUR 3 527 000 in damages.

Case study: Parallel financial investigation

While investigating a robbery that took place in August 2021 in the parking lot of a shopping mall, the SPJ Organized Thefts Unit (RGB) discovered that the victim had made a EUR 70 000 purchase of alcoholic products using cash. However, the RGB investigators found that the vendor had divided the purchase price across several cashier's receipts to conceal the large cash transaction.

Based on SPJ-RGB discoveries, the SPJ Anti-money laundering unit (SPJ-AB) commenced a parallel investigation, which revealed that the vendor launders money for a criminal organisation active in a foreign country. This evidence was found while analysing the books of the vendor and searching to trace back how an amount of EUR 70 000 was included in the accounting of the company (vendor). The investigation triggered MLA requests and co-operation with the other country and several domestic searches and seizures.

By the end of the on-site visit, the case was still under investigation.

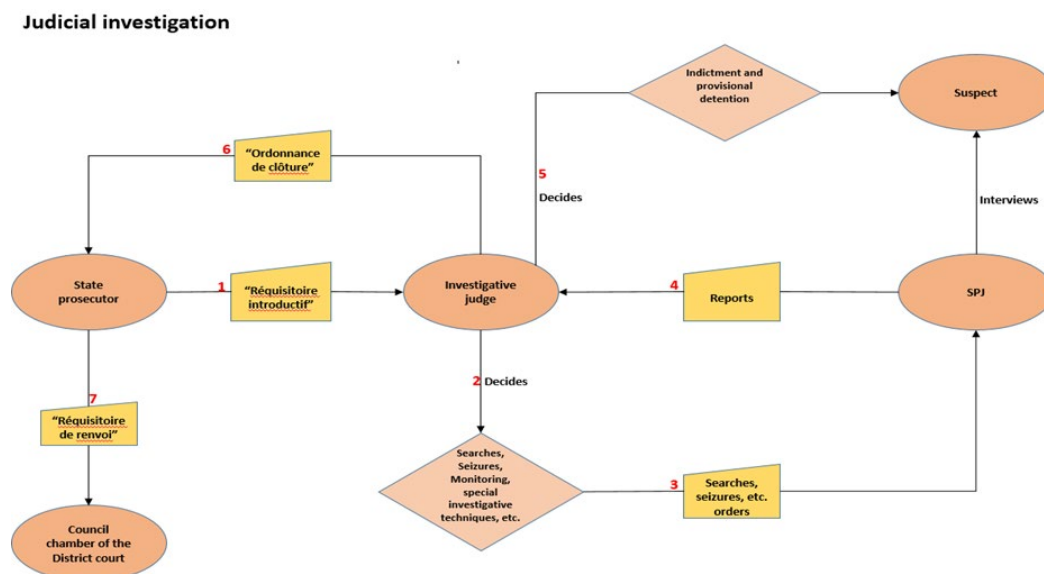
ML investigation

181. The 2019 PG circular on ML investigations (2019 PG circular), which serves as a reference for ML investigations, is carefully followed by competent authorities. The 2019 PG circular provides for: (a) a systematic preliminary or judicial investigation of self-laundering when the laundered amount exceeds EUR 1 000; and (b) requires the PAL/PAD to consider investigating other forms of ML, including third-party ML, when the value of proceeds exceeds EUR 5 000. Both provisions apply equally to domestic and foreign predicate offences.

182. The Luxembourg PG developed a procedure where specific steps are taken to decide whether there is reason for an investigation. The procedure is comprehensive and has assisted the authorities in pursuing ML investigations. The specific steps are: (a) recognising indicators of a potential predicate offence; (b) observing proceeds or financial benefits; (c) determining whether there is a potential act of ML; (d) determining whether the proceeds exceed or might exceed the thresholds identified in the 2019 PG circular; (e) distinguishing between self-laundering and third-party/stand-alone ML.
183. During a general investigation, the PG instructs PAL/PAD to determine whether a financial investigation is needed. If a financial investigation is needed, the initially identified proceeds must meet the EUR 1 000/5 000 threshold (for self-laundering or third-party/stand-alone ML cases, respectively) and determine whether coercive measures are needed. When coercive measures are needed, a judicial investigation will ensue, otherwise, a preliminary investigation will be launched.
184. The investigation will seek to: (a) determine the extent of the criminal network and/or the scale of criminality; (b) identify and trace the proceeds of crime or any other assets that are, or may become, subject to confiscation; and (c) develop evidence, which can be used in criminal proceedings. In more complex cases, the ML component might be dissociated from the proceedings of the predicate offence, and a separate ML case might be opened for a parallel financial investigation by SPJ-AB, while another unit investigates the predicate offence (see box 3.7).
185. The entire ML investigation process is reflected in Figure 3.6. Competent authorities involved in the investigation process are comfortable with their role in it and the assessment team did not identify any difficulties arising from overlap or confusion; co-operation and co-ordination between the different investigative bodies is strong.
186. PAL/PAD in case of a preliminary investigation, or the investigative judge in case of a judicial investigation, decide on the measures to be taken and may, in particular, instruct the SPJ-AB to carry out an asset investigation as part of a broader financial investigation. The SPJ-AB unit carries out the ordered measures and sends them an execution report. The investigative judge has exclusive jurisdiction to order coercive measures (e.g., searches, seizures, special investigative techniques), except in *flagrante delicto*²⁰ cases, where PAL/PAD can order coercive measures. Where appropriate, PAL/PAD takes coercive measures in the form of a “summary” judicial investigation. In line with this approach, on several occasions, PAL/PAD petitioned the investigative judge to order a search, seizure, witness hearing, or expert testimony without opening a judicial investigation for any misdemeanour.
187. When a judicial investigation is completed, the Council Chamber can: (a) dismiss the case; (b) refer the case for trial to the District Court for misdemeanour matters; (c) refer the case for trial to the District Court for felony matters.
188. In case of a preliminary investigation, PAL/PAD can: (a) refer the case directly to the District Court for misdemeanour matters; (b) refer the case to the Council Chamber. The latter must indicate whether it has found mitigating circumstances in favour of the defendants before referring them to the District Court for misdemeanour matters.

²⁰ Cases including those where a suspect is observed in the act of committing the crime, as defined under article 30 of the CPP.

Figure 3.6. ML investigation process



189. Given Luxembourg's context, most ML investigations have an international component. Many of these investigations involve complex corporate structures that appear to have legitimate purposes. Luxembourg prioritises and invests significant resources to pursue such investigations.
190. The main challenges faced by the competent authorities is collecting evidence from abroad and tracing illicit funds that have transited through Luxembourg. Money trails usually involve many jurisdictions and require numerous outgoing MLA requests to collect evidence, trace, freeze and seize assets and locate suspects. The international elements often result in investigations going on for years (see Box.3.7). Competent authorities understand that such delays are problematic, and they use all legal avenues available to them, including informal co-operation, to try to speed up the investigation process (see IO.2).
191. As in the "Bad Banker" case (Box 3.7), many of the cases reviewed by the assessment team provide good examples of joint investigations and effective co-operation among domestic agencies. Relevant investigative and judicial authorities have considerable expertise in financial crimes, with specialised units in several branches of the law enforcement system. Investigators rapidly obtain valuable information from a variety of domestic sources and use teamwork and co-ordination to maximise available resources.

WIKI-ECOFIN

192. The SPJ has established an internal tailored encyclopaedia, the WIKI-ECOFIN, that provides valuable assistance in the conduct of investigations both in terms of procedural guidance, and archive. The tool retains institutional memory and assists new investigators to keep current. Every member of the economic and financial crimes department and every local agent specialised in economic and financial investigations has access to it. The SPJ has granted access to a limited number of investigative judges, magistrates and CRF-FIU officers.

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

193. The types of ML investigations and prosecutions are largely consistent with Luxembourg's threats and national policies. The 2020 NRA (update) lists laundering of proceeds of foreign crime (i.e., fraud and forgery; tax crimes; corruption and bribery; and drug trafficking) as the main threat to Luxembourg's financial centre. Qualitative data (case studies and the NRA) indicate that domestic ML often takes place using professionals and legal entities. ML cases arising from drug trafficking and fraud/forgery cases are consistent with identified threats. However, the volume of ML investigations pursued by Luxembourg, unlike the volume of predicate offence investigations, is not entirely in line with its other main threats as identified in the NRA (see Table 3.12). Resource limitations have prevented Luxembourg from pursuing other types of ML cases to the extent that would be expected considering Luxembourg's risk and context.

Table 3.12. ML investigations – by predicate offence, 2017- Q3 2022

| Predicate offence | Total Investigations | Prosecution | Discontinuance (after preliminary investigation) | Other Status/Ongoing investigations |
|---|----------------------|-------------|--|-------------------------------------|
| Fraud and forgery | 1090 | 213 | 285 | 592 |
| Tax & excise evasion | 53 | 5 | 18 | 30 |
| Corruption and bribery | 12 | 2 | 2 | 8 |
| Illicit trafficking in narcotic drugs and psychotropic substances | 521 | 460 | 12 | 49 |
| Counterfeiting and piracy of products | 7 | 1 | 1 | 5 |
| Counterfeiting currency | 10 | 5 | 4 | 1 |
| Cyber-criminality | 89 | 3 | 17 | 69 |
| Environmental crimes | 10 | 2 | 3 | 5 |
| Extortion | 26 | 14 | 4 | 8 |
| Illicit arms trafficking | 51 | 39 | 4 | 8 |
| Illicit trafficking in stolen and other goods | 257 | 118 | 57 | 82 |
| Kidnapping, illegal restraint, and hostage taking | 6 | 5 | 0 | 1 |
| Murder, grievous bodily injury | 3 | 3 | 0 | 0 |
| Participation in an organised criminal group & racketeering | 86 | 35 | 13 | 38 |
| Robbery or theft | 518 | 310 | 64 | 144 |
| Sexual exploitation, including sexual exploitation of children | 5 | 3 | 2 | 0 |
| Trafficking in human beings and migrant smuggling | 17 | 5 | 7 | 5 |
| Total | 2761 | 1220 | 493 | 1045 |

194. In the review period, Luxembourg conducted many investigations on predicate offences (see Table 3.13). These are in line with Luxembourg's main threats, risk profile and national AML policies. As mentioned previously in this chapter, many of the investigations reflected in table 3.13 included an ML component. However, these cases were not included in the statistics regarding the overall number of ML investigations.

Table 3.13. Status of new notices* by predicate offence, 2017-Q32022

| Predicate offence | Notices to PAL/PAD | Prosecution | Dismissals (Council Chamber) | Discontinuance after preliminary investigation | Other Status/Ongoing investigations |
|--|--------------------|-------------|------------------------------|--|-------------------------------------|
| Fraud and forgery | 16705 | 1294 | 191 | 6568 | 8652 |
| Tax & excise evasion | 389 | 40 | 0 | 132 | 217 |
| Corruption and bribery | 117 | 24 | 2 | 70 | 21 |
| Illicit trafficking in narcotic drugs and psychotropic substances | 1732 | 435 | 20 | 982 | 295 |
| Counterfeiting and piracy of products | 34 | 0 | 3 | 19 | 12 |
| Counterfeiting currency | 489 | 16 | 0 | 231 | 242 |
| Cybercriminality | 3487 | 14 | 6 | 389 | 3078 |
| Environmental crimes | 1316 | 131 | 2 | 573 | 610 |
| Extortion | 784 | 87 | 8 | 198 | 491 |
| Illicit arms trafficking | 1708 | 468 | 9 | 886 | 345 |
| Illicit trafficking in stolen and other goods | 1086 | 239 | 6 | 460 | 381 |
| Kidnapping, illegal restraint, and hostage taking | 283 | 58 | 7 | 154 | 64 |
| Murder, grievous bodily injury | 3016 | 583 | 69 | 1682 | 682 |
| Participation in an organised criminal group & racketeering | 196 | 41 | 3 | 57 | 95 |
| Robbery or theft | 95562 | 4774 | 168 | 16395 | 74225 |
| Sexual exploitation, including sexual exploitation of children | 860 | 116 | 41 | 323 | 380 |
| Smuggling | 10 | 10 | 0 | 0 | 0 |
| Trafficking in human beings and migrant smuggling | 254 | 12 | 6 | 55 | 181 |

*Note: A new notice is created at the detection stage, when the PAL/PAD receives a report stating that an act that could constitute a criminal offence might have been committed

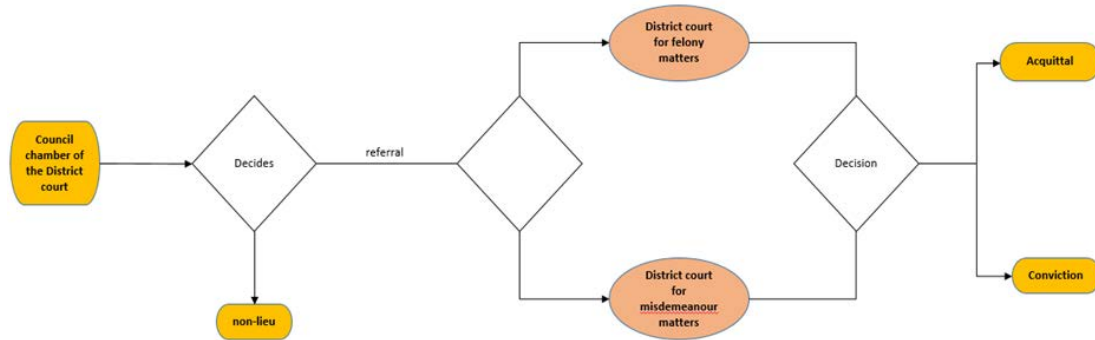
195. Statistics and case studies provided demonstrate that ML investigations and prosecutions correspond to some of Luxembourg's main threats. Luxembourg also maintains annual statistics that demonstrate a steady increase of ML investigations and prosecutions of the main predicate offences relevant to its risk and context. As indicated in the tables above, investigations and prosecutions related to fraud and forgery are significantly higher compared to other significant offences in Luxembourg's context. As explained by Luxembourg, the category of fraud and forgery encompasses a broad range of offences such as, among other, abuse of corporate assets, fraudulent bankruptcy, insurance fraud, forgery of documents, abuse of trust, which accounts for the higher numbers.

ML investigations vs prosecutions

196. Except for ML connected with drug trafficking offences, only a small proportion of cases moved from investigation to prosecution between 2017 and 2022 (see Tables 3.13 and 3.12). Regarding the other main threats (i.e., fraud and forgery; tax & excise evasion; and corruption and bribery) only 20% of investigations led to prosecution; 30% were dismissed or discontinued. Approximately 50% of cases remain under judicial investigation or remain in the hands of the Council Chamber for review. Several reasons explain this phenomenon.

197. As outlined in the previous section, all cases go to the Council Chamber for review once the judicial investigation is complete. This often results in significant time lapse between the conclusion of a ML judicial investigation and prosecution. Many ML cases remain under review by the Council Chamber for more than 18 months. This issue is caused by lack of prioritisation in the review of ML cases by the Council Chamber over other matters that may be of less strategic importance. This issue is further exacerbated due to the limited resources available to the Council Chamber (three magistrates and three clerks) to perform a very wide range of duties. In particular, over the review period the Council Chamber issues several thousands of orders pertaining to: (a) matters without oral hearings; (b) matters with oral hearings; and (c) penal orders in its capacity as a trial judge. In addition, the Council Chamber conducted in depth review of all MLA requests and completed judicial investigation files.

Figure 3.7. Council Chamber decision-making process



ML-related fraud and forgery

198. Fraud and forgery were the main categories of predicate offences triggering ML investigations. Unlike other categories of predicate offences, the use of forged documents, which is one of the most common forms of criminality, is always fully committed in Luxembourg. In the period from 2017-2022, the judicial authorities received 350 ML-related MLA requests arising from fraud and forgery. Case studies and interviews with the investigative and judicial authorities indicate that fraudulent bankruptcy is also a recurring offence (see Box 3.8).

Box 3.8. Case study: The car is mine

This case study illustrates how a businessman was prosecuted, convicted and sentenced for fraudulent bankruptcy committed in Luxembourg and for laundering the proceeds of fraudulent bankruptcy, including fraudulent bankruptcy committed in Belgium.

In 2016, the Luxembourg District Court declared company R insolvent and appointed a curator.

In August 2016, the curator filed a criminal complaint with PAL because some vehicles registered in the name of company R could not be found, while other vehicles and material were not remitted to the curator. In addition, company's R bank account statement showed suspicious transactions (i.e., wire transfers to a newly incorporated German company belonging to the same BO than the insolvent company R, as well as unexplained cash withdrawals).

At the same time, CRF-FIU filed a report with PAL, including a CD-ROM containing the details of bank documentation.

PAL requested SPJ to conduct an in-depth financial investigation into Mr. Z (BO of company R) and his German/Belgian activities. The investigation revealed many more unexplained cash withdrawals that occurred before the insolvency through the personal accounts of Mr. Z. The precise analysis of those incoming transactions raised the suspicion that Mr. Z used his private account to divert assets from both his Belgian business (also declared insolvent) and from his Luxembourg company R.

PAL opened a judicial investigation on the counts of fraudulent bankruptcy, misuse of company assets, forgery, use of forged invoices and ML from fraudulent bankruptcy.

The investigative judge issued an EIO to the Belgian and the German judicial authorities to conduct a search for company R's assets, seize documents and interview witnesses.

During the criminal procedure, Mr. Z absconded. A European arrest warrant (EAW) was issued against him and, in May 2020, following an intensive search, Mr. Z was located, arrested and returned to Luxembourg.

The trial took place in September and October 2020.

In April 2021, following the defendant's appeal, the Court of Appeal sentenced Mr. Z to 24 months of imprisonment, 6 months of which on probation. In addition, the seized vehicles were confiscated and returned to the curator. The decision against Mr. Z was published. As to the civil aspect, Mr. Z was held liable to pay the amount of approximately EUR 155 000 to the curator of the insolvent company R.

ML-related tax crimes

199. The SPJ Economic and Financial Crimes Unit (IEF) is responsible for the investigation of ML-related tax offences. IEF was established in 2018 to assist SPJ's work in this area and the increasing number of tax notices to PAL/PAD triggered from the extension of the criminalisation of tax offence in 2017. IEF is adequately staffed (13 police and 10 civil investigators) with specialised investigators in tax crimes. Given Luxembourg's context, ML-related tax crime investigations are often linked to predicate offences committed abroad. Despite the increasing number of tax-related ML investigations, the data provided show that Luxembourg did not adequately pursue such investigations, comparing to investigations on other less important ML threats identified by Luxembourg.

Box 3.9. Case study: Fruit and vegetables

On 24 July 2019, the CRF-FIU filed a report with PAL based on suspicious facts in the context of company G S.à.r.l. Suspicious activity indicated ML, tax fraud, misuse of corporate assets, false balance sheets, and failure to comply with professional obligations.

By indictment, on 30 July 2019, PAL requested the opening of a judicial investigation. An asset investigation was carried out by the SPJ-AB to determine the assets likely to be confiscated at a later date (if necessary, by equivalent value).

In the context of this judicial investigation, searches were carried out at the auditor P., G. S.à.r.l. and a Luxembourg bank with which G. S.à.r.l. had a hidden account.

On 17 and 19 February 2021, RG and AG (managers of G. S.à.r.l.) admitted to the facts of the case, which were misuse of corporate assets, tax fraud in relation to direct taxes and VAT, false balance sheets and ML.

On 06 May 2022, the District Court sentenced the two directors to a nine-month suspended sentence and a fine of EUR 150 000 each. The directors had already paid EUR 920 000 corresponding to the taxes evaded, totalling EUR 1.27 million. The decision is final.

ML-related drug trafficking

200. Luxembourg competent authorities investigated 521 and prosecuted 460 ML cases related to drug trafficking (see Box 3.11). This caseload is consistent with the level of threat that Luxembourg faces, and the prosecution rate is impressive. The 2020 NRA (update) assessed Luxembourg's external exposure to drug trafficking threat as high. Luxembourg is exposed to this threat externally via financial flows from abroad, including its proximity with countries estimated to have a large drug trafficking activity (i.e., Germany, France, the Netherlands). Over the review period, Luxembourg received approximately 180 MLA requests related to drug trafficking, of which approximately 40 were linked to ML.

ML-related corruption and bribery

201. Luxembourg also conducts ML investigations and prosecutions of proceeds of corruption and bribery. Between 2017 and 2022, competent authorities conducted 12 ML investigations related to corruption and bribery, arising from foreign predicate offences. In the same period, Luxembourg received approximately 60 MLA requests on ML linked to corruption. Even though NRA identifies this category as one of the main ML threats, the number of ML cases involving corruption is low.
202. The 2020 NRA (update) identifies professionals providing TCSP services and real estate and associated construction sectors as high risk for ML in Luxembourg. Case studies and discussions with investigative authorities confirmed that the authorities understand the sectoral risk. However, outside of major and complex ML cases, Luxembourgish authorities do not often pursue ML cases arising in these sectors.

Types of ML cases pursued

203. Based on qualitative information provided, Luxembourg prosecutes all types of ML, including self-laundering, stand-alone ML, third-party ML and ML originating from foreign predicate offences. However, data maintained by competent authorities does not distinguish between the different types of ML that are prosecuted. This prevents any granular analysis on the extent to which each of these specific types of ML are prosecuted or the extent to which they are consistent with Luxembourg's threats, risk profile or national AML/CFT policies.

Stand-alone ML

204. ML can be prosecuted in the absence of a conviction, or even a charge, for the predicate offence. PAL/PAD regularly prosecuted alleged offenders for stand-alone ML. Although Luxembourg did not provide any quantitative data on this issue, Luxembourg did provide some successful examples of such cases, including the following:

Box 3.10. Case study: Namaste

In December 2018 and February 2019, CRF-FIU filed two reports with PAL about suspected ML activities connected to internet fraud through a fake website in Germany.

The CRF-FIU analysis revealed that Luxembourg bank accounts, opened by several foreign students who attended the same Private School, present significant inflows and outflows, mainly from Germany and Switzerland to Turkey, where the funds were withdrawn in cash.

PAL requested the investigative judge to conduct a full-fledged judicial investigation, including the seizure of assets. The subsequent investigation and judicial co-operation with the German competent authorities: (a) confirmed the CRF-FIU findings; and (b) allowed to gather sufficient evidence on the predicate offence in Germany (i.e., organised Internet fraud). Investors were presented profitable offers via a fake Internet shop of a well-known German gold trader. The payments were made on Luxembourg bank accounts. However, the purchased gold was never delivered.

The accounts in Luxembourg were held by Nepalese students, registered at the same school, allowing the fraudsters to access their accounts via web banking against a small commission. They were thus acting as third-party money-launderers (money mules).

The investigative judge seized assets of EUR 30 000 and issued arrest warrants against the suspects.

In March 2019, one of the suspects was arrested by the SPJ-AB and indicted by the investigative judge.

The suspect was convicted for standalone third-party ML and sentenced to two years of suspended imprisonment. The seized assets were confiscated and given back to the victims who attended the trial. This sentence occurred independently

of any proceeding, trial or conviction for the predicate offences committed abroad.

Following a European arrest warrant that was issued against the second suspect, the latter was surrendered to the judicial authorities.

In December 2020, the second suspect was convicted for ML (third-party ML - money mule) and sentenced to two years of misdemeanour imprisonment, 18 months of which on probation. The amount of approximately EUR 21 000 that had been seized during the investigation was confiscated and returned to the victims.

A European arrest warrant was issued against the third suspect (money mule), who was arrested and surrendered to Luxembourg in September 2022.

Convictions

205. Luxembourg provided statistics on the number of convictions obtained in ML cases.

Table 3.14. Total penalties imposed for ML(natural persons), 2017-Q3 2022

| | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 | TOTAL |
|---|------|------|------|------|------|---------|-------|
| Number of prison sentences imposed | 187 | 228 | 236 | 209 | 210 | 211 | 1 281 |
| Number of suspended custodial sentences | 131 | 187 | 181 | 140 | 171 | 140 | 950 |
| Number of fines imposed | 103 | 170 | 145 | 84 | 134 | 123 | 759 |

206. In line with its risk profile, Luxembourg achieved many prosecutions and convictions in relation to ML-related fraud and forgery and drug trafficking. ML-related prosecutions and convictions of tax crimes are low following the number of respective investigations for the reasons noted earlier.

Table 3.15. ML-related prosecutions and sanctions on the top 4 predicate offences, 2017-Q3 2022

| Predicate offence | ML Prosecutions Cases | ML Sanctions* 2017- Q3 2022 | |
|------------------------|--------------------------|-----------------------------|----------------------------|
| | | Prison sentences | Suspended prison sentences |
| Fraud and forgery | 389 | 86 | 213 |
| Tax crimes | 9 | 0 | 1 |
| Corruption and bribery | 5 | 0 | 4 |
| Drug trafficking | 511** | 328 | 586 |

*Note: The sanctions referred to in this table are custodial sentences. Other sanctions imposed may include tax redress, fines, etc.

** Note: Multiple cases may be tried in a single prosecution; therefore, number of cases and number of prosecutions will differ.

Effectiveness, proportionality and dissuasiveness of sanctions

207. In Luxembourg, criminal offences are divided into three categories: crimes (felonies), *délits* (misdemeanours) and contraventions (petty offences). Following the conviction of an offender, the Court looks at various aspects that must be taken into account to hand down a sentence that is appropriate and just (e.g., seriousness of the offence committed, the personal situation of the offender, criminal record, etc.).

208. The maximum punishment for ML is five years' imprisonment, including a maximum fine of EUR 1 250 000. Sentences may also be doubled in the event of recidivism within five years and could be raised to imprisonment of 15 to 20 years (see R.3). Although such serious penalties are available, Luxembourg shared statistics indicating that the large majority of defendants convicted received an average of 1.5 to 2 years' imprisonment. In 2022, this practice changed, and the average prison sentence increased to 3.5 years (see Table 3.16). Most custodial sentences were accompanied by fines, the average level of which has increased since 2019. These increasing combined penalties would seem to demonstrate the judiciary's emerging understanding of the need to impose more stringent penalties as a deterrent to ML.

Table 3.16. Sanctions imposed for ML, 2017-Q3 2022 (natural persons)

| | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|--|---------|--------|--------|---------|--------|---------|
| Number of prison sentences imposed* | 187 | 228 | 236 | 209 | 210 | 211 |
| Average length of prison sentences imposed (years) | 1.5 | 1.5 | 1.5 | 2 | 1.5 | 3.5 |
| Highest custodial sentence (years) | 10 | 18 | 12 | 18 | 8 | 8 |
| Lowest custodial sentence (years) | 2 | 3 | 3 | 1 | 1 | 3 |
| Number of suspended custodial sentences | 131 | 187 | 181 | 140 | 171 | 140 |
| Average length of suspended custodial sentences (years) | 1 | 1 | 1 | 1 | 1 | 2 |
| Number of fines imposed | 103 | 170 | 145 | 84 | 134 | 123 |
| Average level of fines imposed (EUR) | 3 658 | 2 617 | 2 902 | 6 800 | 2 823 | 7 182 |
| Highest fine (EUR) | 100 000 | 20 000 | 50 000 | 250 000 | 70 000 | 150 000 |
| Lowest fine (EUR) | 300 | 50 | 100 | 500 | 200 | 100 |

*Note: Partly suspended prison sentences are counted in both categories. In some cases, the convicted individual is sentenced simultaneously both to actual prison and given a suspension.

209. However, many sentences are suspended. The suspension of the execution of sentences is reserved for first-time offenders who had not been convicted and handed a final custodial sentence before their prosecution, or a misdemeanour or felony fine in the case of a legal person. Suspended sentences may be accompanied by probation measures consisting of supervision or social assistance measures (Article 629 et seq. of the CPP). As indicated by the number of prison sentences imposed in the table above, this measure is not particularly dissuasive in the first instance. However, based on Luxembourg's low recidivism rate (see discussion in paragraph 196 below), there does appear to be some dissuasive value. Suspension of the execution of sentences or probation carries a dissuasive element of its own: in the event of a repeat offence within seven years (for a felony) and five years (for a misdemeanour), the sentenced individual must serve both the entire suspended sentence and any new custodial sentence for which suspension or probation is not permitted.²¹ Over the review period, less than 5% of suspended sentences were revoked on annual basis (see Table 3.17).

Table 3.17. Suspended sentences, 2017-Q3 2022

| | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|--|------|------|------|------|------|---------|
| Number of suspended custodial sentences | 131 | 187 | 181 | 140 | 171 | 96 |
| Suspensions revoked | 15 | 13 | 18 | 6 | 8 | 1 |

210. Luxembourg has also applied sanctions to legal persons for ML in a limited fashion (see Table 3.18). Such fines do not appear to be proportionate or dissuasive.

Table 3.18. Total penalties imposed for ML (legal persons), 2017-Q3 2022

| | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|------------------------------|---------|--------|--------|--------|-------|---------|
| Number of cases | 1 | 3 | 2 | 3 | 3 | 2 |
| Level of fine imposed | 100 000 | 11 667 | 30 750 | 12 667 | 7 167 | 53 750 |

211. The court may apply a method known as "*concours d'infractions*" (several offences), in cases where a defendant has committed more than one offence and has yet to be convicted of any one of them. Luxembourg provided some examples where this approach was effectively applied, including the following case involving a bank that breached professional obligations in connection with a ML case.

²¹ As the revocation can take place during the whole probation period, a suspended sentence handed in 2017 may therefore not necessarily be revoked only in 2017 but also later on, until the end of the relevant probation period. This explains why the more recent the suspension, the lower the number of revocations.

Box 3.11. Case study: Bankers & Bikers

For more than four years, the SPJ investigated a drug trafficking organisation importing large quantities of heroin and cocaine in Luxembourg. The judicial investigation involved exceptional resources in terms of number of officers involved, including an undercover agent, and technical means used (GPS beacons, sophisticated systems to intercept communications, police observations). Among the suspects were members of the Hells Angels motorcycle club, including Z.

The investigation headed into three directions: (a) predicate offence (i.e., drug trafficking on an international scale); (b) domestic ML; (c) AML/CFT breaches of a local bank (relevant for this case study).

All three branches led to convictions.

SPJ began its investigation based on information from its Belgian counterpart. The investigation revealed that the drug trafficking in Luxembourg, was linked to the Belgian/Dutch criminal structure specialised in the production and distribution of marihuana.

The production facilities of this group were located at: (a) Trooz (B), searched in February 2014; (b) Court-Saint-Etienne (B), burnt down in December 2012; (c) Estaimburg near Tournai (B), searched by the Belgian Police in April 2014, seizure of 3 000 cannabis plants and 16 kilograms of marihuana.

The extent of the drug trafficking activity in Luxembourg was estimated at least 160 kilograms of marihuana having generated a profit of approximately EUR 528 000 for Mr. X.

In October 2015, the SPJ arrested Mr. Z and X's girlfriend. It also searched Mr. Z's home in Luxembourg and seized prohibited weapons and a vehicle. A further search of X's girlfriend's home in Luxembourg was carried out, where many luxury goods, expensive clothing and a vehicle were seized.

Mister X was sentenced to 10 years of imprisonment, and a fine of EUR 10 000. Three other suspects were convicted for standalone ML by conversion.

In March 2016, PAL received a report from SPJ-AB in the context of this case. The report referred to possible breaches by a local bank of its professional obligations. Several employees of the local bank were privately associated with members of the motorcycle club, including Z. Mr. Z and another member of the motorcycle club had accounts with the local bank.

In March 2017, PAL initiated a new case against the local bank for failing its AML obligations and opened a judicial investigation.

After plea bargaining, the local bank was sentenced, in March 2019, to a fine of EUR 60 000.

212. Statistics (including those set out in the table above), case studies and interviews with competent authorities indicate that courts are beginning to increase sanctions to be more effective, proportionate, and dissuasive. It should be noted that Luxembourg often imposes a broad range of sanctions in addition to imprisonment and fines. In many cases, the sentences include confiscation (see IO.8), and a prohibition against holding office or a professional licence. Higher sentences are reserved for very serious and complex cases and repeat offenders. The latter has not often been applied, given the low recidivism rate.
213. The recidivism rate for persons convicted of ML is approximately 7%. This indicates that, despite somewhat light or suspended sentences, penalties are dissuasive in Luxembourg's context. Between 2017 and 2022, 1 859 persons were convicted of ML once; 132 persons were convicted twice. Only 14 persons were convicted three times and 2 persons were convicted four times. However, despite the availability of much higher penalties for repeat offenders, the fines imposed in practice are quite low and not proportionate, ranging between EUR 2 500 and 7 500.

Use of alternative measures

214. Luxembourg can apply alternative criminal justice measures. The decision to prosecute a case for ML, or for a different criminal charge lies with PAL/PAD depending on the level of proof and the underlying offences. In the presence of an identified predicate offence, PAL/PAD could opt to prosecute for the underlying offence, despite the suspicion of ML. In addition, PAL/PAD occasionally offer a concession to defendants in exchange for plea bargain. Very often Luxembourg prosecutes individuals based on non-compliance with professional obligations. Luxembourg shared several cases demonstrating this approach (see Box 3.7 and 3.9). Between 2017 and 2022, Luxembourg sentenced 18 professionals for violations of their professional obligations. Fines ranged from EUR 1 200 to EUR 100 000, with an average fine of approximately EUR 33 750. These fines are neither proportionate nor dissuasive, particularly in the context of high risk/vulnerable professions such as TCSPs.

Table 3.19. Fines imposed for violation of professional obligations, 2017-Q3 2022

| Year | Number of fines | Average in EUR |
|---------|-----------------|----------------|
| 2017 | 2 | 52 500 |
| 2018 | 3 | 15 000 |
| 2019 | 2 | 33 750 |
| 2020 | 4 | 10 125 |
| 2021 | 3 | 28 333 |
| Q3 2022 | 2 | 57 500 |

Box 3.12. Case study: The investment firm -suspicious client

In December 2016, during a first AML/CFT on-site inspection of investment firm A, the CSSF identified a legal entity client named "X", for which there was a series of elements giving rise to ML suspicion. X is a foreign maritime entity registered in Liberia (the official country of the registered office) and in Nevis (as a foreign maritime entity under Nevis law).

CSSF established that the origin of the funds of company X was not fully known by the investment firm A at the time of the on-site control.

The review of the onsite inspection report was completed in August 2018 by the OSI department of the CSSF. On 24 October 2018, the CSSF filed a SAR, including a supplementary SAR on 5 April 2019.

In November 2018, CSSF conducted a second on-site inspection to further investigate the issues raised by the SAR in question. Following the on-site verification, the CSSF initiated a non-litigation administrative procedure.

On 17 December 2018, PAL requested, after having sought additional information from CRF-FIU, the opening of a judicial investigation.

The District Court sentenced the investment firm A to a EUR 100 000 fine. Firm A was found guilty for contravening the provisions of article 3 (customer due diligence); article 4 (adequate internal management requirements); and article 5 (co-operation requirements with competent authorities and self-regulatory bodies) of the 2004 AML/CFT Law.

The judgment is final.

215. In addition, PAL/PAD shared information on some cases with tax authorities for fiscal or administrative settlements, when a criminal approach is not opportune, or a fiscal settlement is more efficient.

Overall conclusion on IO.7

Luxembourg proactively identifies and investigates ML and different types of ML through the systematic use of financial intelligence, investigative techniques, and strong co-operation between LEAs. However, the number of ML investigations is somewhat inconsistent with Luxembourg's risk and context. This is mitigated to some extent, as many predicate offence investigations include an ML component.

Many cases remain in the stage of investigation for several years, either due to the level of complexity and evidence pursued abroad, resource limitations or delays caused by the Council Chamber. Limitations in resourcing the investigative judge and PAL/PAD have impacted to some extent the volume and length of ML investigations. Impact of resource limitations is mitigated to a large extent by the strong co-operation and co-ordination among relevant investigative authorities.

Luxembourg prosecutes all types of ML, including self-laundering, stand-alone ML, third-party ML and ML originating from foreign predicate offences. However, limitations in Luxembourg's data collection prevent any granular analysis on the extent to which each of these specific types of ML are prosecuted or the extent to which they are consistent with Luxembourg's threats, risk profile or national AML/CFT policies. Luxembourg has a low rate of recidivism, indicating some level of effectiveness; however, the frequent application of suspended sentences is not dissuasive and financial penalties are not proportionate.

Luxembourg is rated as having a Moderate level of effectiveness for IO.7.

Immediate Outcome 8 (Confiscation)

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

216. Confiscation of criminal proceeds, instrumentalities (see R.4) and property of equivalent value is a high priority for Luxembourg, and it is actively pursued as a policy objective. Confiscation is a prominent feature of its 2019 AML/CFT Strategy, based on which competent authorities increasingly target assets other than cash. Operationally, Luxembourg competent authorities (i.e., PG, PAL/PAD, Office of the Investigative Judge (investigative judge), SPJ, CRF-FIU, ARO, AMO and ADA) are highly committed in implementing the overarching "crime does not pay" strategy and made full use of the existing tools for freezing, seizing, and confiscating assets domestically and abroad.
217. Luxembourg's 2019 AML/CFT Strategy focused on three policy goals: (a) setting up SPJ guidelines to generalise and standardise the practice of asset investigations and provide relevant training; (b) enabling the detection and tracing of property to be confiscated even after a final conviction; (c) setting up a specialised asset management office (AMO) to ensure the adequate management of property frozen, seized or confiscated, including maintenance of comprehensive statistics.

218. Based on the overarching national policy of “crime does not pay”, Luxembourg pursues asset confiscation through the conduct of parallel financial investigations from the outset of every case as part of its overall investigation process. This policy is in line with Luxembourg’s risk profile. If assets are found and there is a risk of dissipation before assets can be confiscated, steps are taken to freeze or seize the assets immediately.
219. The asset recovery working group of the NPC is responsible for policy matters for asset confiscation and implementing law with operational policies. Its work entailed two initiatives: (a) expanded the scope of measures to preserve the value of seized assets; and (b) provided a specific legal basis for the Asset Recovery Office (ARO). The implementation of these initiatives confirmed the working group’s significant role in improving Luxembourg’s asset confiscation framework. All authorities with competency on asset confiscation matters are members of the working group, including PG, PAL/PAD, the investigative judge, SPJ, ARO and AMO. MoJ and other authorities can join the working group upon invitation (e.g., the ADA).

Guidelines

220. In mid-2019, the SPJ set up comprehensive guidelines to generalise the practice of asset investigations (e.g., establishing an inventory of the suspect’s assets), including templates on how to proceed with asset investigations. The guidelines facilitated competent authorities work in pursuing effective results in asset investigation and reducing the length of investigations. In addition, the guidelines not only addressed issues from the condition to have property identified beforehand, but it also ensured a common understanding and drafting of asset investigation reports to PAL and the Office of the Investigative Judge. In mid-2022, the Asset Management and Recovery Law allowed for value confiscation, where no property liable to confiscation has been identified, or where the property identified is insufficient to cover the object, or direct or indirect proceeds of an offence or any pecuniary advantage derived from the offence.
221. In October 2019, PAL issued a note to strengthen guidelines on the ML prosecution and repeat the importance of financial asset investigation in every economic crime and all kinds of offences. In October 2022, PAL issued circulars to address asset management and confiscation and outlined the value of engaging CRF-FIU in asset investigations. This signalled a need for a general note on asset investigation and confiscation to ensure that all authorities involved in this area have the same overarching knowledge and understanding of processes when conducting asset investigations.
222. Luxembourgish competent authorities, particularly SPJ that undertook the actual investigations, have adequate experience in financial investigations. The SPJ applied a flexible approach in resource allocation that allowed to cover needs for additional human resources and specialised expertise in the context of complex investigations. Whenever required by the circumstances, the SPJ drew expertise from other competent authorities, such as the AED and ACD for tax offences, or the CSSF for complex financial structures. Case studies and interviews with competent authorities when onsite confirmed this finding. Co-operation among competent authorities is strong. This supports information and experience sharing, including optimal practices, among them.

Training

223. The SPJ regularly receives and delivers asset investigation training. Luxembourg provided an all-inclusive list of training activities, which were intensified beginning in 2018. The SPJ-AB unit regularly provides asset investigation training to all SPJ departments, including to some extent to PGD uniformed police officers. Such training was occasionally held in co-operation with other competent authorities (e.g., in 2020 the SPJ-AB in co-operation with the CRF-FIU, delivered training to members of other police departments on asset investigation and data protection). Training was also available to the investigative judge. WIKI-ECOFIN (see IO.7) also offers instructions on asset investigation and confiscation matters, including training.
224. The CRF-FIU also provided training to judicial authorities and SPJ, as its role in asset tracing and financial investigations became increasingly significant in the review period. CRF-FIU developed guidelines for the judicial authorities to improve the effectiveness and the quality of bilateral co-operation in this field and delivered training both to judicial authorities and SPJ in relation to, among other things, business e-mail compromise (BEC) fraud that was a recurrent typology identified in asset investigations.

Resources

225. ARO is headed by a PAL magistrate, who is assisted by investigators from the SPJ-AB unit to conduct asset investigations including post-sentence asset investigations, since July 2022. However, the ARO is inadequately resourced to perform these functions effectively. The magistrate in charge, although highly experienced and specialised, must carry out all of ARO's work, including asset tracing and investigation and representing ARO in various international fora such as CARIN. Lack of resources impacted to some extent ARO's ability to effectively provide support in asset investigations, particularly between 2017 and 2018, given the overall issue of resources across competent authorities during this period. More recently, this issue was mitigated to a large extent by Luxembourg's policy of close co-operation and resource reallocation, with the magistrate receiving support from SPJ-AB investigators. However, this resourcing model is not sustainable given the increasing workload as other investigative authorities continue to improve their effectiveness.

Asset investigation

226. PAL/PAD and the investigative judge have a good understanding of the need to deprive criminals of proceeds and instrumentalities of crimes or property of equivalent value. This was shared as a common goal and was one of the highest priorities in criminal investigations throughout the review period. The decision to launch asset investigation lies with PAL/PAD and the investigative judge. The SPJ is the authority that conducts the actual investigation. Throughout the review period, the SPJ effectively applied a five-step strategy to identify assets (i.e., intelligence gathering; registration of findings; interview and interrogation; initiation of international co-operation to locate assets abroad; report to PAL). Whenever links to other jurisdictions were identified, CRF-FIU and ARO effectively used the channels of information at their disposal to seek further evidence with asset investigations (see IO.2).

227. Over the review period, Luxembourg's efforts to freeze, seize and recover assets have provided increasingly effective results. Partial statistics kept in relation to freezing, seizure and confiscation demonstrate a positive trend in confiscation activities. Confiscation of proceeds and benefits of crime is seen as having a deterrent effect and is therefore actively pursued.
228. Improvements on the type of information collected, for example, the value of criminal instrumentalities confiscated, including confiscation per crime category, will provide Luxembourg with granular data on the outcome of its confiscation efforts and help remain in line with its policy objective to confiscate instrumentalities of crime.

Confiscation of proceeds from foreign and domestic predicate offences, and proceeds located abroad

229. Based largely on successful MLA requests and international co-operation, the assessment team concludes that, since 2020, Luxembourg actively confiscates the proceeds of foreign predicate offences and property of equivalent value, including complex multinational cases. Changes made to its legal regime in recent years have been successful in increasing the amount of assets confiscated. However, in statistics on domestic ML cases (see Table 3.20), Luxembourg does not disaggregate foreign and domestic predicate offences. Therefore, Luxembourg cannot demonstrate what portion of the confiscated sums relates to domestic and foreign predicate offences, other than the proceeds confiscated based on incoming MLA requests. Likewise, Luxembourg's data on confiscated amounts does not disaggregate proceeds of crime, instrumentalities, and property of corresponding value.
230. Assets confiscated were mainly cash and balances on accounts. Throughout the review period, the system in place for registration of confiscated assets does not record the nature of the objects confiscated. For instance, when real estate property is seized, there is no provision for a valuation or estimate of the real property for the purpose of entering that value into the system. When such property is confiscated, the PG's Office instructs AED to conduct the sale of the property. However, the price of the transaction is not recorded. This issue will be rectified when the Asset Management Office becomes fully operational. Some case studies indicate that Luxembourg confiscated assets other than cash and balances on accounts. However, the focus of competent authorities remained on confiscation of cash and balances on accounts, at least, until the adoption of the 2019 AML/CFT Strategy.
231. Confiscation of the assets is carried out by the prosecutor using criminal, civil or administrative mechanisms in accordance with the law. Between 2017 and 2022, Luxembourg confiscated approximately EUR 26 million based on domestic ML cases. However, these sums do not all refer to final confiscations, as some represent court judgments where the defendant has not yet received notice of the confiscation order. Luxembourg also confiscated approximately EUR 30 million (final confiscation) based on foreign MLA requests.

Table 3.20. Volume and value of confiscation, 2017-Q3 2022

| | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|--|---------|-----------|------------|---------|---------|---------|
| Number of confiscation orders | 2 | 114 | 96 | 29 | 25 | 19 |
| ...of which (convictions by final decision) | 2 | 93 | 74 | 26 | 24 | 19 |
| Value of domestic confiscation (EUR) | 302 000 | 4 333 000 | 20 637 000 | 305 000 | 810 000 | 20 000 |

Table 3.21 MLA based asset-sharing and restitution, 2017-Q3 2022

| | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|--|------------------------|----------------------------------|--------------------------|--|---------------------------|---|
| Number of confiscation orders received per year | 5 | 7 | 4 | 11 | 12 | 13 |
| Number of confiscation orders considered admissible by the court and executed from the same year* | 0 | 0 | 0 | 1 | 1 | 6 |
| Value of incoming MLA confiscation orders considered admissible by the court executed from the same year (EUR)* | 0 | 0 | 0 | 13 000 | 2 000 | 8 000 000 |
| Shared with Requesting State (EUR) | 0 | 0 | 0 | 6 600 | 0 | 549 000 |
| Retained by Luxembourg (EUR) | 0 | 0 | 0 | 6 600 | 2 000 | 549 000 |
| Restitution to victims (EUR) | 0 | 0 | 0 | 0 | 0 | 7 000 000 |
| Number of confiscation orders considered admissible by the court and executed from previous years | 3 (2015, 2x2016) | 4 (2015, 2x 2016, 2017) | 4 (2x2017, 2x2018) | 4 (2016, 2017, 2018, 2019) | 11 (2x2019, 9x2020) | 8 (2012, 2016, 2019,20 20, 4x2021) |
| Value of incoming MLA confiscation orders considered admissible by the court and executed from previous years (EUR) | 9 762 000 | 1 567 000 | 1 777 000 | 160 934 | 4 100 000 | 4 670 000 |
| Shared with Requesting State (EUR) | 9 741 000 | 783 371 | 880 833 | 39 780 | 754 664 | 14 110 |
| Retained by Luxembourg (EUR) | 21 311 | 783 371 | 880 833 | 42 829 | 758 709 | 14 110 |
| Restitution to victims (EUR) | 0 | 0 | 14 833 | | 1 458 53 0 | 4 641 43 3 |

*Note: The term “executed” means that the assets are confiscated, seized or otherwise permanently taken away from the criminal.

232. Incoming MLA requests on confiscation from EU countries, which are Luxembourg’s main counterparts, are executed and assets are shared equally and in a timely manner (generally, between three to six months). Requests, from non-EU countries usually take between one and three years, as special agreements for asset sharing are required on a case-by-case basis. The origin of incoming requests and the types of criminality entailed are in line with Luxembourg’s risk and context. Luxembourg prioritises the execution of confiscation requests that include all necessary information. Incomplete incoming requests are executed once Luxembourg receives all required clarifications.

233. Following the adoption of the 2019 AML/CFT Strategy, Luxembourg made confiscation a policy objective. Accordingly, Luxembourg’s efforts to confiscate assets from domestic cases and execute all incoming confiscation requests increased.

Non-conviction-based confiscation

234. Luxembourg has a conviction-based regime whereby, upon conviction of a specified offence, the court can order confiscation of defendant's property, for the equivalent value of his/her benefits. Despite Luxembourg's regime being conviction-based, foreign non-conviction-based confiscation orders are enforceable (see Box 3.13).

Box 3.13. Case study: Enforceability of an NCB confiscation - share and repatriation

In September 2014, the UK National Crime Agency (NCA) requested that Luxembourg execute a judgment and a subsequent confiscation/recovery order issued by the High Court of Justice, Queen's Bench Division. Although the suspect had not been convicted for the offence generating the criminal proceeds, the UK court explained expressly in its decision that the funds, seized in Luxembourg pursuant to a MLA request, originated from drug trafficking activity. It was therefore clear that the funds transferred to Luxembourg had been generated by a criminal activity.

In January 2015, ARO filed a petition to render this confiscation order enforceable in Luxembourg and reasoned its request according to the judgment of the High Court of Justice. To render the confiscation order duly enforceable, the District Court ruled that the assets seized in Luxembourg were the proceeds of an illicit activity, namely drug trafficking and ML.

In April 2015, following that decision approximately EUR 0.2 million were repatriated to the requesting State.

235. In addition, Luxembourg law allows the enforcement of foreign non-conviction-based confiscation orders, including circumstances where the perpetrator is not available by reason of death,²² flight, absence or the perpetrator is unknown. Luxembourg provided comprehensive statistics to this effect (see below). Approximately 650 confiscations following judgments in absentia were completed over the review period. Most were linked to drug trafficking, theft and other predicate offences.

²² There were no instances involving death over the review period.

Table 3.22. Confiscation Orders (Judgment in absentia), 2017-Q3 2022

| | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|--------------------------------------|------|------|------|------|------|---------|
| Number of confiscation orders | 140 | 188 | 125 | 91 | 61 | 49 |

Table 3.23. Confiscations (Judgment in absentia) by predicate offence*, 2017-Q3 2022

| Predicate offence | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|--|------|------|------|------|------|---------|
| Environmental crimes | 0 | 1 | 0 | 0 | 0 | 0 |
| Extortion | 0 | 1 | 0 | 1 | 1 | 0 |
| Forgery | 5 | 3 | 3 | 2 | 1 | 1 |
| Fraud | 6 | 4 | 2 | 1 | 1 | 0 |
| Illicit arms trafficking | 5 | 6 | 4 | 2 | 1 | 1 |
| Illicit trafficking in narcotic drugs and psychotropic substances | 11 | 26 | 19 | 19 | 8 | 5 |
| Illicit trafficking in stolen and other goods | 2 | 3 | 1 | 2 | 2 | 0 |
| Kidnapping, illegal restraint, and hostage taking | 0 | 0 | 1 | 0 | 0 | 0 |
| Murder, grievous bodily injury | 1 | 2 | 2 | 1 | 1 | 0 |
| Participation in an organised criminal group & racketeering | 3 | 3 | 1 | 0 | 0 | 0 |
| Robbery or theft | 11 | 25 | 23 | 9 | 2 | 3 |
| Sexual exploitation, including sexual exploitation of children | 1 | 1 | 0 | 0 | 1 | 0 |
| Smuggling | 0 | 0 | 2 | 0 | 1 | 0 |

*Note: Individual confiscation orders may relate to multiple predicate offences.

Proceeds located abroad

236. Luxembourg indicated that ML offences based on foreign predicate offences are investigated as domestic cases. Some of these cases have generated important seizures in Luxembourg and abroad. As a result, Luxembourg requested the seizure of approximately EUR 4 million from its foreign counterparts. This amount had not yet been confiscated by the end of the on-site. The underlying ML criminality for these seizures is in line with Luxembourg's main threats. However, considering the total amount of assets frozen domestically, there is room for improvement to further the proactive pursuit of proceeds located abroad. Overall, Luxembourg uses the exequatur procedure (with non-EU countries) or the confiscation certificate (with EU countries) to request confiscation of proceeds located abroad. Any amount below EUR 10 000 would be kept by the requested foreign country. Larger amounts would be shared between the two parties.

Provisional Measures

237. Luxembourg effectively uses its range of provisional measures to ensure that criminals are deprived of the proceeds of crime from the earliest possible time. These provisional measures include the CRF-FIU freezing powers, powers of the investigative judge to order seizure of assets, and a measure referred to as interception.

238. The CRF-FIU effectively uses its freezing powers²³ to halt the flight and dissipation of assets when ML/TF suspicions were raised and prior to any formal restraint procedures (see Box 3.14). Even though the CRF-FIU has no explicit mandate in asset recovery, it plays a fundamental role in tracing and securing criminal assets. Between 2017 and 2022, the CRF-FIU issued 345 freezing orders in 201 cases disseminated to PAL/PAD to secure a total amount of more than EUR 181 million. Most freezing orders relate to fraud; however, the highest sums derive from participation in an organised criminal group & racketeering, stand-alone ML and fraud, which is at somewhat in line with Luxembourg's profile. Most funds were seized after a request of the investigative judge; however, a comparatively small amount was eventually confiscated or restituted (see Tables 3.24 and 3.25). Competent authorities stated that the main challenge to final confiscation is the various stages until the conclusion of a cases (e.g., investigation, MLA requests, appeals).

Table 3.24. Assets frozen, seized and confiscated or restituted by CRF-FIU*, 2017-Q3 2022

| Amount frozen | Amounts seized | Amounts confiscated | Amounts restituted |
|-------------------------|-----------------|---------------------|--------------------|
| approx. EUR 181 000 000 | EUR 117 000 000 | EUR 3 000 000 | EUR 8 500 000 |

*Note: Freezing/seizing orders remain active for some of these amounts.

Table 3.25. Volume and value of assets frozen by CRF-FIU in disseminated cases, 2017-Q3 2022

| Predicate offence | Frozen assets in EUR | # Freezing orders |
|---|----------------------|-------------------|
| Participation in an organized criminal group and racketeering | 57 653 026 | 2 |
| Others* | 30 121 071 | 43 |
| Standalone money laundering | 33 101 508 | 39 |
| Fraud | 26 722 699 | 185 |
| Corruption | 25 212 435 | 7 |
| Cash control | 2 682 480 | 26 |
| Counterfeiting and product piracy | 1 001 020 | 27 |
| Forgery | 589 053 | 5 |
| Criminal tax offences | 164 502 | 3 |
| Cybercrime | 38 759 | 4 |
| Illicit trafficking in narcotic drugs and psychotropic substances | 340 262 | 3 |
| Thefts | 490 | 1 |
| Total | 181 549 298 | 345 |

*Note: Refer to sums where no predicate offence could be identified at first instance and there was an indication to ML/TF. As of 2020, these sums are included in the category stand-alone ML.

²³ As of 2018, CRF-FIU can freeze assets for an indefinite period, thus giving time to PAL/PAD to apply for the seizure of the frozen assets.

239. Overall, including international co-operation requests, in the same period the CRF-FIU made 656 freezes, amounting approximately EUR 700 million, including VAs (see Table 3.26). However, the volume and value of freezing orders, related to foreign requests, is unclear. Subsequently, the sum from CRF-FIU freezing orders that became subject to final confiscation is unknown, as Luxembourg does not maintain such data.

Table 3.26. VA-related asset freezes by CRF-FIU, 2017-Q3 2022

| Year | Frozen assets in EUR | No. Of freezing orders |
|--------------|----------------------|------------------------|
| 2017 | 329 688 | 3 |
| 2018 | 87 404 | 2 |
| 2019 | 148 977 | 3 |
| 2020 | 281 377 | 7 |
| 2021 | 2 565 211 | 8 |
| Q3 2022 | 7 994 | 1 |
| Total | 3 619 632 | 25 |

Box 3.14. Case study: Abuse of weakness

In April 2019, the CRF-FIU received information about a potential abuse of a weak or vulnerable person, fraud and breach of trust. The 84 years old victim had received approximately EUR 0.7 million on his account from a sale of property. Thereafter, the amount was transferred to the account of his daughter, who had a proxy on her father's account.

The CRF-FIU analysis revealed that the victim's daughter was abusing the proxy on her father's account for her own benefit. More than EUR 0.8 million vanished in that way.

To avoid the dissipation of the victim's properties by his daughter, the CRF-FIU issued freezing orders on the respective accounts, including on other beneficiary accounts identified. In that way, the CRF-FIU secured more than EUR 0.5 million. In May 2019, the CRF-FIU filed a report with PAL. PAL requested seizures, which were ordered by the investigative judge and executed by SPJ.

In June 2019, the District Court for civil matters, on PAL request, placed the victim under guardianship and appointed a legal guardian.

In 2020, the judicial investigation was concluded, and the file was handed out to the Council Chamber.

In October 2022, the perpetrator was handed a community sentence.

240. In the review period, the CRF-FIU froze large sums of assets related to foreign predicate offences (i.e., tax crimes) on its own initiative because of ML suspicion. Upon freezing, the CRF-FIU informed the relevant foreign counterpart of the existence of sums in Luxembourg. On several cases, assets frozen by CRF-FIU did not become subject to seizure and confiscation in Luxembourg. The CRF-FIU explained that in these cases, it was requested from its foreign counterparts to lift its freezing orders, as its foreign counterparts had come to an agreement with the relevant suspect(s) to pay his/her/their taxes. Despite the absence of statistics on the frequency of this cases, the CRF-FIU shared relevant case studies the assessment team to this effect.
241. The investigative judge is the competent authority competent to seize any property in relation to criminal proceeds, instrumentalities, or property of equivalent value in Luxembourg. Throughout the review period, Luxembourg made extensive use of seizure orders as a precautionary measure to ensure final confiscation (see Box 3.15). Seizure orders are provisional until confiscation, distribution or restitution is ordered in a final decision. Additional seizure orders were made where further evidence of property was identified during an investigation (e.g., proceeds of crime, property of equivalent value, etc.). Between 2017 and 2022, Luxembourg seized approximately EUR 224 million (approximately EUR 177 million related to ML) all in line with its main threats.

Box 3.15. Case study: Fake invoices

Between January 2002 and December 2005, the secretaries of the accountancy firm X issued fake invoices, which were not related to any real service. These invoices were issued in the name of offshore companies aiming at reducing the profits of companies taxable in Luxembourg. These forged invoices were issued following consultation with the BO of the Luxembourg company to ensure that they do not exceed 20% of the company's turnover.

In 2006, Luxembourg competent authorities commenced an investigation.

In May 2022, following the investigation findings, the investigative judge ordered the seizure of the following assets: (a) EUR 2.75 million; (b) EUR 3 450 on the current account; (c) securities of an equivalent value of EUR 51 954 and EUR 106 392; (d) the amount of EUR 230 681 and EUR 939 from the *Caisse de Consignation*; and (e) a sum of approximately EUR 326 000 from various other accounts.

In June 2022, the Court found the defendant guilty of forgery, use of forged documents and abuse of corporate assets. The Court ordered the confiscation of EUR 3.5 million as proceeds. The defendant has appealed the judgment.

242. Beyond ML-related MLA seizures, Luxembourg effectively seized large sums based on incoming MLA requests on foreign predicate offences. Seized amounts are mainly funds and insurance policies.

Table 3.27. Amounts seized following an MLA request, 2017-Q3 2022

| Type | Currency | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|---|-------------|-------|-------|--------|--------|-------|---------|
| Account, cash | USD million | 0.33 | 23.70 | 165.16 | 121.20 | 33.12 | 0.243 |
| | EUR million | 12.35 | 61.61 | 38.99 | 70.33 | 94.72 | 67.84 |
| | GBP million | / | 0.06 | / | / | / | 0.448 |
| | CHF million | 0.04 | / | / | / | 0.18 | / |
| Insurance | EUR million | 2.03 | / | 0.27 | 3.63 | 0.07 | 0.01 |
| | CHF million | 0.93 | / | / | / | / | / |
| Other forms of value (car, property, value of drugs, other values, value of bitcoins) | EUR million | 0.03 | 29.00 | 2.50 | 0.04 | 1.48 | / |

243. One of Luxembourg's provisional measures deprives the criminals of the proceeds of their crimes before they obtain the asset. Since 2019, Luxembourg competent authorities systematically seek to intercept the flow of illicit money as it is transferred from the victims' accounts. This policy was mainly followed in fraud and forgery cases (e.g., email fraud), which is Luxembourg's primary ML-related predicate threat. The CRF-FIU is Luxembourg's main weapon in pursuing this policy, given its ability to swiftly engage in international co-operation and issue freezing orders. In the review period, Luxembourg reported approximately 122 cases that required emergency freezing of accounts. Luxembourg provided several case studies and some statistics demonstrating the effective use of this approach.

Box 3.16. Case study: CEO

On 17 January 2019, a company filed a complaint with SPJ in relation to a CEO fraud. Following a transfer order allegedly issued by the company's treasurer whose e-mail box had been hacked, the sum of EUR 1.8 million was fraudulently transferred to an account in Romania.

The same day, CRF-FIU was contacted by the victim, via the Judicial Police, and carried out an urgent international exchange with its Romanian counterparts to identify the destination of the flows and secure the assets. This exchange revealed that the funds were subsequently transferred to three accounts in Hong Kong. Thereafter, CRF-FIU contacted its Hong Kong counterpart and managed to repatriate approximately EUR 1.4 million.

On 18 January 2019, CRF-FIU filed a report with PAL, who opened a file. The investigation did not identify the perpetrators.

244. Luxembourg demonstrated a firm commitment to repatriation, sharing and restitution, paying out over EUR 13 million to co-operation partners and victims. Luxembourg provided case examples, including complex multinational cases, where proceeds and property of equivalent value were successfully frozen, seized, and confiscated. However, in the absence of more detailed quantitative data, the assessment team cannot determine how well authorities are confiscating instrumentalities, and proceeds of domestic predicate offences. Confiscation of property of corresponding value to instrumentalities of crime is also an issue, as there is lack of measures to enable it. This issue does not carry much weight given Luxembourg's context.
245. Luxembourg's confiscation regime allows for repatriation of seized assets (through MLA) even in the absence of a final foreign confiscation decision. In the review period, such decisions were taken on a case-by-case basis, provided that the foreign judicial authorities had entered into an agreement with a suspect (i.e., suspect's agreement that seized assets derive from criminal activity and should become property of the requesting state) without formally prosecuting the file. Seizures were lifted only upon receipt of an MLA request from foreign counterparts and executed by the investigative judge and ARO. This is a popular policy among EU countries. On several occasions, Luxembourg became subject to the so-called "passive sharing" of assets (i.e., the requesting state shared repatriated assets), as an acknowledgement of Luxembourg's efforts and costs incurred during the identification, seizure and repatriation stage of criminal assets.
246. PAL/PAD systematically pursued victim compensation (restitution) as part of the criminal or confiscation case. Whenever a convict possessed illegally obtained gains and an injured third party existed, PAL/PAD issued a request for a confiscation order. Between 2017 and 2022, Luxembourg courts returned EUR 8.5 million to victims based on domestic cases, and EUR 1.2 million based on incoming MLA requests. Luxembourg provided some examples and statistics to this effect.

Table 3.28. Value and volume of restitution orders, 2017-Q3 2022

| | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|--|-----------|-----------|-----------|-----------|-----------|-----------|
| Number of cases | N/A | 52 | 50 | 22 | 15 | 5 |
| Value of restitution (in million) | N/A | EUR 0.274 | EUR 0.429 | EUR 3.217 | EUR 0.208 | EUR 0.116 |
| Value of MLA restitution (in million) | EUR 0.828 | | EUR 0.130 | EUR 0.014 | EUR 1.008 | EUR 0.190 |

247. Despite Luxembourg having a conviction-based regime, on several occasions, it returned frozen property to victims without court confiscation decision based on the EU Regulation 2018/1805 that allows for pre-conviction restitution (see Box 3.17). Statistics on the overall number of cases and amounts returned to victims based on this mechanism are not maintained.

Box 3.17. Case study: Fake e-mail address

In December 2020, the Luxembourg-incorporated company B fell victim of an internet / social fraud for an amount of approximately EUR 400 000.

The victim detected the fraud when the genuine long-standing business partner complained that its invoices have still not been paid.

On 29 December 2020, the director of company B filed a complaint with the police of country A (country of residence).

On 4 January 2020, the Prosecutor's office of country A transmitted the complaint to its Luxembourg counterpart. The Prosecutor informally informed his Luxembourg counterpart that the receiving account in country C had already been frozen at CRF-FIU own initiative (CRF-FIU and FIU country C co-operation).

The same day PAL requested the investigative judge to open a full-fledged investigation against unknown individuals in connection with forgery, use of forged documents, fraud and ML.

In January 2020, PAL received a comprehensive report from the CRF-FIU. The report contained a description of the money flows, including the flows which occurred at the two receiving accounts level. The report not only confirmed the informal information from the prosecutor of country A that the receiving account in country C has been frozen at the initiative of the CRF-FIU with the remaining balance of EUR 56 405 (of the total amount defrauded, EUR 338 864), but also informed that the rest of the defrauded money has already been transferred to: (a) another bank account in country C (EUR 45 072); (b) a bank account in country D (EUR 170 000) both with the same account holder; and (c) 3 bank accounts in country E (for a total amount of EUR 67 500).

On 5 January 2020, the investigative judge issued an EIO and a freezing order to the country C and the country F judicial authorities.

On 9 February 2021, the investigative judge sent an assistance request to the Judicial authorities in country D to freeze the account identified by the CRF-FIU and obtain all the relevant information thereof.

In conformity with Article 29 of Regulation (EU) 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders, the seized money was transferred to the Luxembourg bank account of the victim Company B. The restitution of the frozen money to the victims explains that no confiscation decision was taken.

There are ongoing proceedings.

Tax measures

248. Luxembourg also relies to some extent on tax and administrative measures, in addition to criminal confiscation measures, as a tool to recover criminal assets, by levying taxes, imposing tax fines, or seizing wages or benefits. However, competent authorities did not provide statistics or case studies demonstrating the effective application of this tool.

249. Between 2017 and 2022, taxes valued at approximately EUR 11 million were evaded and recovered by the tax authorities. Reimbursement of taxes and duties evaded as part of prosecution for tax offences, is a measure that aims to oblige the offenders to pay the full amount of taxes and duties evaded before the PAL offers them a plea bargain.

3

Table 3.29. Reimbursement of taxes and duties, 2017-Q3 2022*

| Year | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|----------------|------|---------|-----------|-----------|-----------|-----------|
| Amounts in EUR | / | 438 899 | 1 065 132 | 1 159 194 | 2 372 031 | 7 920 003 |

*Note: The table does not distinguish whether the tax offence was completed or remained at the attempt stage.

Asset management

250. Until 2019, Luxembourg pursued mainly confiscation relevant to liquid assets (e.g., cash, bank accounts, securities, etc.), given the absence of a comprehensive asset management mechanism. This approach changed with the adoption of the 2019 AML/CFT Strategy. Until October 2022, neither PAL, the investigative judge nor the ARO could dispose of non-liquid assets to preserve their value for future confiscation. Limited mitigating measures were developed to enable, to a certain extent, the management of seized property that would deteriorate if it were kept as such. The investigative judge, often the ordering authority, provided a discretionary management mandate to banks (i.e., as a prudent person) to maintain the value of portfolios, when assets were held by them.
251. In October 2022, Luxembourg enacted the 2022 Asset Management Law, establishing the AMO as the competent authority for managing, and when necessary, disposing of property seized, frozen or confiscated. Under this law, professionals should transfer all seized assets to AMO and an electronic reporting system for banks is being developed. However, there were no administrative or operational measures in place to manage assets and the law was not yet in force by the end of the on-site visit. Accordingly, these developments cannot be considered in analysing the effectiveness of Luxembourg's confiscation regime.

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

252. Luxembourg competent authorities are well aware of the risks related to the cross-border transportation of cash and valuable goods associated with criminal activities and demonstrated their ability to seize assets at the borders, including Luxembourg's international airport and courier express facilities. However, only partial confiscation²⁴ of the seized cash is permitted (see R.32).

²⁴ The non-confiscated part is returned to the offender, save for when ML is also prosecuted. In that case, the remaining part can also be seized, and the court can confiscate it.

253. Luxembourg implements a declaration system that is broadly in line with the FATF Standards (see R.32). Luxembourg exercises approximately 15 000 cash and bearer-negotiable instrument (BNI) controls per year. The ADA averaged approximately 160 cross-border currency and BNI declarations per year, all of which were available to the CRF-FIU through the DOCASH database. The ADA detects an annual average of 10 cases of non-declared or falsely declared cash.

Table 3.30. Regular cash control declarations and cases of missing or falsely declared cash, 2017-Q3 2022

| Year | Cross-border transportation of currency and bearer negotiable instruments | | | | | |
|---------|---|---------------------------------|-----------------------------------|---|---|--------------------------------|
| | Number of declarations or disclosures Incoming/Outgoing (intra EU & extra EU) | | | Cross-border cash transport - infringements | Assets frozen/detained by ADA* (Value in EUR) | CRF-FIU Freezes (Value in EUR) |
| | Currency | Bearer negotiable instruments** | Highly-liquid stores of value**** | False or missing declarations/disclosures | | |
| 2017 | 162 | NAV | / | 9 | 436 900.43 | 343 665 |
| 2018 | 156 | NAV | / | 1 | 13 490 | 13 490 |
| 2019 | 198 | 7 | / | 7 | 166 912 | 166 912 |
| 2020 | 126 | 1*** | / | 15 | 2 076 638 | 2 076 638 |
| 2021 | 125 | 0 | 0 | 6 | 185 075 | 185 075 |
| Q3 2022 | 104 | 0 | 1 | 2 | 59 954 | N/A |

*Note: The amounts relate to the cash detected by ADA in cases where the legal provisions of Regulation 1889/2005 and 2010 Cash Law were infringed and led to the temporary freeze of the cash for up to 24 hours, respectively, as of 3 June 2021 (entry into force of the EU Regulation 2018/1672) and 27 July 2021 (entry into force of the 2021 Cash control law), to a 30-day detention following an administrative decision by ADA.

**Note: Statistical data from 2015 – 2018 includes declarations for both, currency and BNIs. In 2019, the statistics differentiate between both categories of cash after ADA internal instruction.

***Note: BNI of EUR 1.6 million.

****Note: Goods that presents a high ratio between their value and volume. These can easily be converted into currency through accessible trading markets, while incurring only modest transaction costs. These are coins with a gold content of at least 90 %; and (b) bullion such as bars, nuggets or clumps with a gold content of at least 99.5 %.

254. The ADA is empowered to temporarily freeze²⁵ any undeclared or falsely declared cash.²⁶ All infringements detected are reported by ADA to PAL and CRF-FIU. The low number of infringements is in line with Luxembourg's cross-border context given its geographical position and strong controls in place. Out of 38 cases reported to PAL in the review period, there were 17 convictions, 1 acquittal, 2 cases were dropped in absence of evidence/suspicion, whilst there are ongoing procedures for 22 cases (see Table 3.31). Courts issued confiscation orders and imposed fines proportionate to the seriousness of underlying offence on a case-by-case basis.

Table 3.31. Follow-up action by PAL, 2017-Q3 2022

| Year | Reports filed by ADA | Action taken | Fines (EUR) | Confiscations (EUR) |
|---------|----------------------|--|-------------|---------------------|
| 2017 | 9 | Ongoing procedure: 1 Dropped cases: 1 Acquittal: 1 Convictions: 6 | 11 500 | 328 450 |
| 2018 | 1 | Convictions: 1 | 1 500 | 13 490 |
| 2019 | 7 | Ongoing procedures: 4 Dropped cases: 1 Convictions: 2 | 1 300 | - |
| 2020 | 15 | Ongoing procedures: 8 Dropped cases: / Convictions: 7 | 13 700 | 110 075 |
| 2021 | 6 | Ongoing procedures: 5 Dropped cases: / Convictions: 1 | 251 | - |
| Q3 2022 | 4 | Ongoing procedures: 4 Dropped cases: / Convictions: / | N/A | N/A |

255. Since 2017, the ADA has been actively building its capacity for detecting cross-border movement of cash and BNIs. By the end of the onsite, the ADA had 2 cash detection dogs, a scanner van for baggage and parcels, and a scanner truck for the x-ray inspection of trucks and containers. The ADA also invested in training on cash control matters, and many agents received training. However, some of these resources were only recently acquired or are mainly stationed at the airport. The ADA could benefit from further increase of its resources, including training to more effectively detect falsely or non-declared cross-border movement of cash.

²⁵ The ADA can detain cash for 30 days. The decision may be appealed at the administrative tribunal within 3 months. Detention can be extended up to a maximum period of 90 days from the time of the finding. The extension is intended to give the CRF-FIU or/and PAL additional time to conduct investigations.

²⁶ It is possible to challenge that decision before the Administrative Tribunal. By the end of the on-site visit, no administrative appeals were notified.

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

256. In line with Luxembourg's low domestic crime rate and identified higher risk of ML arising from foreign predicate offences, confiscation of proceeds involving foreign predicate offences carries significant weight. Given the absence of comprehensive quantitative and qualitative information, the assessment team cannot confirm that confiscation results are consistent with Luxembourg's risk profile. Following the adoption of the 2019 AML/CFT Strategy, Luxembourg intensified its efforts to execute all incoming confiscation orders systematically and expeditiously.
257. Regarding domestic cases, fraud and tax crimes, which are the main proceeds-generating crimes in Luxembourg's context, represent a significant portion of the assets recovered. However, in the absence of more comprehensive data on instrumentalities, proceeds of domestic predicate offences and proceeds that have moved abroad, the assessment team cannot confirm, at this stage, that confiscation results from domestic predicate offences are consistent with identified risks.
258. Some actions described in Luxembourg's AML/CFT policies and priorities were recently completed, thus more time is required to demonstrate whether confiscation results are in line with them. However, as acknowledged earlier, the SPJ guidelines to generalise the practice of asset investigations (i.e., one of the three policy goals), have already provided positive results.

Overall conclusion on IO.8

Confiscation of criminal proceeds, instrumentalities (save for confiscation of property of corresponding value to instrumentalities of crime) and property of equivalent value is a high priority for Luxembourg, and, since 2019, it was actively pursued as a policy objective.

Luxembourg has a solid legal regime that enabled competent authorities to freeze and seize all relevant forms of assets. However, in the absence of an asset management mechanism, value of non-liquid assets could not be preserved and competent authorities focused on seizure and confiscations of cash, balance on accounts and securities, unless otherwise required by an incoming MLA.

Luxembourg has a range of measures in place that allowed, on numerous occasions, restitution to victims without conviction-based confiscation. LEAs largely applied policy allowing them to intercept ongoing criminality (i.e., email fraud), which allows to return money to victims before the conclusion of a predicate offence.

Given the absence of comprehensive statistics, the assessment team cannot confirm that confiscation results are consistent with identified risks.

Cash controls are in place and ADA is active in pursuing cross-border cash movements. However, the absence of ML infringements detected leaves room for some improvement both in training and resources. Overall, major improvements are required.

Luxembourg is rated as having a Moderate level of effectiveness for IO.8.

Chapter 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

Key Findings and Recommended Actions

Key Findings

Immediate Outcome 9

1. During the review period, Luxembourg had no prosecutions or convictions for TF due to the mitigating measures in place. This is somewhat in line with Luxembourg's risk profile.
2. Luxembourg does not pursue prosecution in absentia for TF purposes, as the investigative judge can order coercive measures, red notices, EAWs and extradition requests. Regarding stand-alone TF cases where substantial evidence was found, Luxembourg issued several red notices solely for terrorism.
3. The CRF-FIU has specialised analysts dedicated to analysing TF-TRs. Case studies illustrate its continuing efforts to identify potential TF links.
4. PAL analyses all incoming MLA requests seeking information that could trigger domestic TF investigations. Despite the absence of domestic prosecutions on TF, case studies demonstrate that Luxembourg contributes significantly to successful foreign TF investigations, prosecutions, and convictions.
5. LEAs have adequate experience and tools to identify and investigate possible TF activity.
6. TF investigations are integrated and support Luxembourg's national CTF strategy and national counter-terrorism strategies. Competent authorities have a good coordinating mechanism and rapidly share all information linked to potential T/TF.
7. Sanctions available under Luxembourgish legislative framework would be proportionate and dissuasive in the event of a conviction. Luxembourg regularly employs alternative measures, such as de-radicalisation programmes, to prevent and disrupt terrorism and TF.

Immediate Outcome 10

1. Between 2017 and 2020, Luxembourg relied upon the EU framework as well as supplemental domestic legislation and regulations (the 2010 UNSCR Implementation Law and related regulations) for implementing TF-related TFS. Under this framework, UN and EU designations were transposed via ministerial regulation, generally within one working day. Since then, Luxembourg has put measures in place to transpose by reference and

address other deficiencies in the prior regime, by, among other things, requiring all natural and legal persons to freeze the assets of designated persons without delay and without prior notification. These measures, several of which were only recently put in place, require further development to demonstrate effective implementation.

2. Despite the comprehensive framework for border controls, the ADA has a limited understanding of the steps required to freeze funds or other assets of designated persons (e.g., identification of designated persons in complex cases, such as those involving BOs as designated persons).
3. Luxembourg has identified 91 NGOs that engage in development and humanitarian projects abroad (DNGOs) that are likely to be at risk of TF abuse. However, the MoFA does not apply a risk-based approach in its supervision of the sector. Since 2019, the MoFA has enhanced its contacts with the sector. However, the sector's understanding of TF risk remains very low.
4. Luxembourg considers its exposure to terrorists, terrorist financiers, and terrorist organisations to be limited. Nevertheless, Luxembourg has taken appropriate steps to deprive them of assets and instrumentalities related to TF activities.

Immediate Outcome 11

1. Between 2017 and 2020, Luxembourg relied solely upon the EU framework for implementing PF-related TFS, and accordingly did not implement PF-related TFS without delay during that period. Following passage of the 2020 Sanctions Implementation Law and implementing regulations, it now applies the same TFS framework for both TF and PF. Thus, shortcomings identified under IO.10 related to the current framework equally apply to the implementation of PF-related TFS. Luxembourg provided a case study about a proposal to designate persons under a relevant EU sanctions regime, which illustrated the value of all-source intelligence in identifying sanctions evasion.
2. Luxembourg does not have any notable links to North Korea, but it maintains a limited trade relationship with Iran (i.e., medical equipment). Luxembourg has made some effort to examine trade and direct financial flows. However, this examination has not considered common sanctions evasion techniques. Although this is a challenging exercise, it is critical for Luxembourg given its size and reach, which inherently has greater potential exposure to PF activities.
3. Currently, Luxembourgish obliged entities have frozen considerable assets pursuant to TFS, but none of these relates to UNSCR 1718 or UNSCR 2231. Although not a FATF requirement, obliged entities have filed PF-related SARs, which the CRF-FIU examined thoroughly, including soliciting input from foreign counterparts. This is a good practice.
4. Awareness of PF-related TFS in the private sector varies. The financial sector generally has a strong understanding of its TFS obligations; however, this is not the case in some non-bank financial sectors. VASPs understand

their TFS obligations and their vulnerability to potential violations of DPRK sanctions in light of the prevalent use of virtual assets in ransomware attacks. DNFBPs' understanding varies significantly.

5. All Luxembourg supervisory authorities assess FIs' and DNFBPs' compliance with TFS-obligations during on-site and off-site inspections, but some of the gaps identified in IO.3 regarding risk-based supervision have an impact here.

Recommended Actions

Immediate Outcome 9

1. Where there is sufficient evidence of TF on stand-alone TF cases, Luxembourg should make effective use of red notices and extradition requests to ensure that individuals can be prosecuted for TF.
2. Luxembourg should proportionately strengthen resource allocation across the judicial and investigative authorities to ensure competent authorities' ability to effectively conduct TF investigations.
3. Intelligence sharing between the SRE and TF investigative authorities should be further strengthened, to ensure that, where available, SRE intelligence is systematically supporting investigations on TF.
4. Luxembourg should leverage from the role of the CSSF in monitoring cross-border payments to strengthen identification of TF cases.

Immediate Outcome 10

1. Luxembourg should refine its high-level guidance on the designation process into clear and operationalised procedures and communicate these procedures to the relevant competent authorities so that they can leverage this important tool.
2. The MoFA should develop and implement procedures to apply the risk-based approach to its oversight of the NPO sector. Authorities should improve their outreach to NPOs aiming at enhancing the sector's poor understanding of TF risk, including the application of mitigating measures.
3. The ADA should develop its understanding of the steps required to freeze funds or other assets of designated persons, and put in place controls at the borders, other than the airport, with a view to implementing TF-related TFS.
4. The MoF should provide additional guidance on the TF TFS regime to the public, aiming at ensuring effective implementation of TF-related TFS by DNFBPs relying on its website for manual sanctions screening.

Immediate Outcome 11

1. Recommended actions 3 and 4 listed in IO.10 relating to improvement of the TFS regime also apply here.
2. Luxembourg should expand and enhance its assessment of its potential exposure to PF activities beyond an analysis of direct financial flows in light of the significant vulnerability inherent in its context as an international financial centre.
3. The MoF and supervisory authorities should enhance their outreach and training activities aimed at improving FIs and DNFBPs' understanding of PF-related TFS obligations by increasing the frequency, diversity and reach of current outreach and training activities.

259. The relevant Immediate Outcomes considered and assessed in this chapter are IO.9-11. The Recommendations relevant for the assessment of effectiveness under this section are R. 1, 4, 5-8, 30, 31 and 39, and elements of R.2, 14, 15, 16, 32, 37, 38 and 40.

Immediate Outcome 9 (TF investigation and prosecution)

260. Luxembourg has a strong CTF framework to counter TF, but deficiencies in understanding of TF risk (see IO.1) impact application of the framework in line with risks. Luxembourg has never been subject to terrorist attacks and no active terrorist cells have been identified in its territory. Given its role as a global financial centre and past terrorist incidents in the territory of its direct neighbouring countries, Luxembourg has strong prevention-based policies and commences international co-operation for any suspicion linked to terrorism or terrorism financing. Luxembourg's Financial Intelligence Unit (CRF-FIU) and the Judicial Police (SPJ) are primarily responsible for implementing these policies.
261. This assessment was based on statistics; case studies; and interviews with relevant Luxembourgish authorities. The assessment team considered relevant findings on international co-operation sought and provided by Luxembourg competent authorities.

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

262. In the review period, there was one conviction for terrorism and 30 TF investigations (preliminary and judicial).. At the same time, Luxembourg did not prosecute or convict any offender for TF. The assessment team considers this somewhat consistent with Luxembourg's TF risk as assessed in the 2022 TF VRA.
263. Luxembourg competent authorities demonstrated a good understanding of some different types of TF activity, mainly drawing on information available to the CRF-FIU and SPJ-SAT (Anti-Terrorism Section). However, this understanding does not extend to potential TF activities stemming from Luxembourg's risk as a transit country for TF, attributable in the view of the assessment team to deficiencies in dissemination of detailed TF risk information across authorities (see IO.1).

264. Luxembourg has criminalised TF in line with the FATF Standards (see R.5). Interviews with competent authorities indicate that it is a challenge to identify the intended recipient of the funds or make a specific link between the recipient and terrorism. The authorities explained that it may be simple to identify the origin of a financial flow; however, it is difficult to identify the beneficiary.
265. In some stand-alone TF investigations, the evidence gathered by the investigative judge was sufficient to justify criminal proceedings, but the defendant had not yet returned from the combat zones. In these cases, competent authorities did not initiate procedures for prosecution in absentia because of the impossibility to notify defendants of the indictments. In addition, enforceability of the judgments would not be possible because of the defendants' right to request for recourse. Given the power of the investigative judge to issue coercive measures, including red notices, EAWs and extradition requests, competent authorities consider it useful to keep these investigations open. Luxembourg indicates that in relation to these stand-alone TF investigations, several red notices were issued, but solely for terrorism. The assessment team considers this is an issue given the stand-alone nature of the said cases and the possibility to issue red notices on TF too.

Human resources

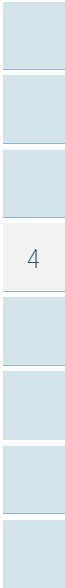
266. Limitations in human resources impact to some extent the effectiveness of investigative and judicial authorities in conducting TF investigations. Throughout the review period, competent authorities heavily relied on CRF-FIU analyses and intelligence to advance TF investigations. As with ML, despite Luxembourg's initiatives to increase resources among investigative and judicial authorities, mainly within the SPJ-SAT, these authorities remain insufficiently resourced (see Table 4.1).

Table 4.1. Authorities with responsibilities for investigating terrorism and TF, Q3 2022

| Competent Authority | Human Resources |
|--|--|
| PAL/PAD | Three Magistrates |
| Office of the Investigative Judge | Two investigative judges, including the Chief Investigative judge. |
| SPJ - SAT | 13 investigators |

Experience and training

267. The State Prosecutor's Offices of the Luxembourg and Diekirch District Courts (PAL/PAD), the Office of the Investigative Judge (investigative judge) and the SPJ have attended numerous training events on TF investigation and prosecution, both domestically and abroad, and have built sufficient experience to conduct comprehensive TF investigations. Luxembourgish competent authorities successfully leverage their strong international co-operation ties with neighbouring and EU counterparts, pursuing opportunities to draw on experience and best practices on TF investigations from them.



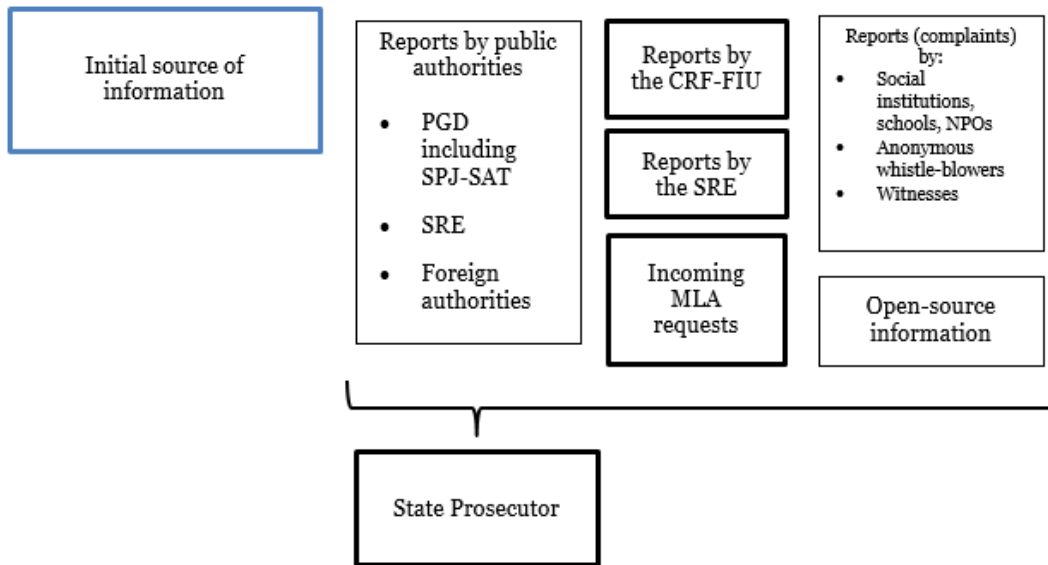
TF identification and investigation

268. Luxembourg has robust mechanisms in place to detect potential TF activity, in line with TF risks as identified, arising both domestically and abroad. There is close co-operation and co-ordination between the competent authorities in charge of terrorism and TF investigations. PAL acts as a central authority that receives terrorism and TF-related reports and intelligence from all competent authorities and decides whether to commence TF investigations. In the review period, Luxembourg investigative authorities sought to identify a TF component for every terrorism related investigation.

TF Identification

269. Luxembourg competent authorities proactively identified and assessed TF-related elements throughout the review period. The main sources of TF investigations were CRF-FIU reports and incoming MLA requests. Other sources of information relate to SPJ and SRE reports, reports by other public authorities, complaints by obliged entities, reports by foreign counterparts, etc. The following flow chart reflects this process.

Figure 4.1. Identification of TF cases



270. The CRF-FIU has specialised analysts and adequate tools to identify TF. The CRF-FIU has put a system in place to prioritise the processing of TF-related reports (i.e., TF activity reports (TFARs)²⁷ and TF transaction reports (TFTRs)²⁸). Between 2017 and 2022, the CRF-FIU received approximately 450 TFARs and TFTRs per year, 95% of which were submitted from entities operating online and banks. Many of these reports refer strictly to terrorism rather than TF (see IO.6). In addition, most TFARs and TFTRs were related to clients of Luxembourg-based payment and e-money institutions providing services in other EU countries. However, given its sensitivity towards TF and terrorism, the CRF-FIU conducted an analysis on most of these reports to ensure that there were no missed TF elements. The CRF-FIU reports were shared with the relevant foreign FIUs, which provided positive feedback on the completeness and relevance of such reports.
271. The CRF-FIU conducts an initial assessment of all incoming TFARs/TFTRs (see IO.6). Based on this assessment, the CRF-FIU specialised analyst selects the reports that require further analysis based on an exhaustive list of indicators (see Table 4.2). Most TF-related STRs/SARs referred to adverse information²⁹ and compliance.³⁰

Table 4.2. Indicators that triggered reports, 2017-Q3 2022

| Indicators / other elements that triggered reports | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|--|------|------|------|------|------|---------|
| Behaviour of the customer / transaction monitoring | 12 | 26 | 79 | 71 | 48 | 35 |
| Purchase of suspicious goods | 5 | 8 | 38 | 59 | 28 | 23 |
| Multiple indicators | 7 | 17 | 40 | 12 | 20 | 12 |
| Cash withdrawals in high-risk regions | - | 1 | 1 | - | 0 | - |
| Fundraising | 10 | 17 | 30 | 45 | 43 | 16 |
| Fundraising / crowdfunding | 2 | 7 | 19 | 25 | 25 | 8 |
| NPO | 8 | 10 | 11 | 20 | 18 | 8 |
| Requests from law enforcement | 7 | 12 | 4 | 6 | 7 | 4 |
| Money remittance* | 24 | 24 | 1 | / | / | / |
| Sanctions lists | 44 | 12 | 10 | 14 | 77 | 12 |
| Adverse information | 98 | 140 | 110 | 98 | 42 | 48 |
| Open source | 3 | 8 | 7 | 11 | 20 | 9 |
| Compliance database | 95 | 132 | 103 | 88 | 22 | 39 |
| Additional information | 98 | 178 | 149 | 177 | 106 | 37 |

*Note: As a result of refinement of CRF-FIU methodology in maintaining statistics, it stopped collecting statistical information on "Money remittance" in 2020 and 2021, as other statistical indicators were more conclusive.

²⁷ The TFAR model is used particularly for refusals to enter into a business relationship or clients who are on sanctions lists, but whose financial transactions show no anomalies.

²⁸ TFTRs include transactions conducted by the suspect. Obligated entities may immediately flag certain transactions as suspicious, or include them in the TFTR, to make as much financial information as possible available to the CRF-FIU.

²⁹ Under the category "adverse information", the CRF-FIU classifies reports that have been triggered by publicly available information on SPJ or investigative judge investigations, court proceedings, press articles or information published by other media (including through Internet).

³⁰ Reports linked to compliance databases (e.g., World-check).

Box 4.1. Case Study - Detection of wire transfers to NPOs suspected of terrorism or TF

In June 2019, following adverse media articles and a suspicious wire transfer from a non-EU citizen of country A, an obliged entity placed the bank accounts belonging to certain NPOs from country B on an internal "blacklist" and filed a report (TFTR) with the CRF-FIU. Immediately, the CRF-FIU TF experts commenced analysis of the report and contacted the concerned FIUs (Countries A and B) to receive information related to the involved persons, accounts and the NPOs.

A few days after the first denunciation, the obliged entity intercepted and refused a further transfer from another account to one of the blacklisted accounts. The FIU of Country A responded that the beneficiary account was indeed known to be in connection with the targeted NPOs and that the latter were mentioned in several STRs with suspicions of misuse of donations. Between June and November 2019, there was continuous communication on this case between the CRF-FIU and the FIU of Country A. In November 2019, the Country A FIU informed the CRF-FIU that the suspected NPO was the subject of an investigation in their country.

The NPOs were suspected of using at least some of the generated funds for possible TF or extremist groups.

Outcome: Following the CRF-FIU requests for information to the Country B FIU, it received information indicating that the account holder was a third NPO and that neither the third NPO, nor its accounts/members were adversely known to their FIU. The Country B FIU explained that it had no information indicating that the NPO, or its accounts/members, could be involved in any TF activities. The other two NPOs were unknown to their FIU.

In line with the input received from its foreign counterparts and the analysis of accounts and transactions executed by the Luxembourgish obliged entity, the CRF-FIU did not reveal any TF links. In absence of TF elements, the authorities did not open a judicial investigation.

272. The CRF-FIU co-operates closely with the SPJ-SAT to leverage further intelligence to assess the ground and merit of TFARs and TFTRs received from obliged entities. This co-operation has a positive effect in filtering and eventually limiting the number of reports sent to PAL. Between 2017 and 2022, the CRF-FIU sent 19 reports to PAL (see Table 4.3). PAL ordered an investigation for all of them, but so far, no specific links to TF were found.

Table 4.3. CRF-FIU reports sent to PAL, 2017-Q3 2022

| | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|---|------|------|------|------|------|---------|
| Number of reports sent to PAL stemming from TFARs & TFTRs | 2 | 7 | 3 | 3 | 2 | 2 |
| Number of reports requested by PAL | 5 | 0 | 1 | 9 | 15 | 8 |

273. Over the review period, PAL filtered all incoming MLA requests to identify TF elements. PAL commenced co-operation with the CRF-FIU in the cases containing a link to a Luxembourg-based obliged entity. PAL systematically sent known/unknown requests to the SPJ-SAT about individuals mentioned in incoming MLA requests. For instance, in addition to the statistics contained in Table 4.4, between 2020 and 2021, PAL commissioned national checks on foreign natural and legal persons linked to terrorism and TF in the context of 21 incoming MLA requests. Overall, PAL conducted six preliminary investigations on TF based on MLA requests. None of these investigations revealed links to TF.

Table 4.4. Number of cases opened based on an MLA request, 2017-Q3 2022

| | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|---|------|------|------|------|------|---------|
| Number of national cases opened for TF | 1 | 0 | 4 | 0 | 0 | 1 |
| Number of national cases opened for terrorism | 0 | 2 | 1 | 1 | 4 | 4 |

274. The CSSF reviews cross-border flows and the related geographical risks. These data specify the country of origin and the country of destination of the transaction and thereby allow to see exposure to international and/or high-TF risk jurisdictions countries. These reviews were considered in the 2022 TF VRA. However, competent authorities did not use them as a tool to assist them in identification of TF cases.

TF investigation

275. Investigative authorities and LEAs have adequate experience and tools to identify and investigate possible TF activity. Competent authorities engage proactively with foreign counterparts to identify potential TF activity. Over the review period, Luxembourg conducted 30 investigations solely on TF, seven of which were developed to judicial investigations.³¹ However, none of these investigations led to prosecution to date,³² often because no specific links to TF were found.

³¹ Between 2017 and 2022, Luxembourg conducted approximately 345 investigations of TF, TF linked to other offences and terrorism investigations.

³² Luxembourg informed the assessment team that a TF case is ongoing. This case involves a pre-trial detention and may result in prosecution. However, this will fall outside the review period.

276. TF investigations are entrusted to the SPJ-SAT and, where appropriate, the SPJ-AB unit. Irrespective of which magistrate leads an investigation, be it PAL or the investigative judge, the SPJ is responsible for its execution. Over the review period, PAL informed the CRF-FIU and requested its support on all incoming TF-related reports. The CRF-FIU was mainly requested to screen person(s) under investigation. To this end, the CRF-FIU also actively engaged with the SPJ in consultation PAL. The investigative judge also contributed to TF investigations to the extent that coercive measures were deemed necessary.
277. Preliminary investigations conducted by SPJ-SAT and SPJ-AB make extensive use of data hubs to gather as much information as possible on the subjects in a timely manner (see IO.6). When onsite, the SPJ investigators informed that in many TF investigations, including ongoing ones, they often deployed special investigative techniques (i.e., surveillance), including early engagement with domestic and foreign counterparts to identify terrorist financiers and domestic links or international TF networks. The SPJ can also conduct undercover operations for TF.
278. During a TF investigation SPJ-SAT investigators can always rely on specialised economic and financial investigators (SPJ-AB) for assistance. In addition, each investigator has direct contact with the magistrates in charge of the investigations, both during preliminary investigations and judicial investigation. These exchanges often led to timely orders for the seizure of documents and search for evidence. SPJ-SAT investigation of TF were also supported by analysts and specialists in new technologies, where necessary. This additional resource allowed in-depth research in TF investigations involving VAs.
279. Luxembourg is aware and highly sensitive to the devastating effect any act of terrorism would have on such a small jurisdiction. Accordingly, competent authorities act immediately if there is any indication of TF or terrorism threat. At these early stages, all investigative and intelligence agencies rely on the CRF-FIU to systematically analyse the financial aspect of each case to attain a clear indication on the nature of each case and whether it related to TF or terrorism. Case studies shared with the assessment team demonstrate that financial intelligence from the CRF-FIU has led to terrorism and TF-related prosecutions in other countries (see the following two case studies).

Box 4.2. Case Study – Terrorist attacks in Europe

The following case study mirrors the CRF-FIU modus operandi in all terrorist incidents that happened in its neighbouring countries since 2015.

Following a terrorist attack in a neighbouring country to Luxembourg, the CRF-FIU began financial analysis to gather intelligence in relation to the assaults and the perpetrators of the attacks.

Urgent requests for information were sent to most obliged entities, focusing on payment and e-money institutions. Obligated entities provided relevant information within a matter of hours. Several e-money accounts, IP addresses, as well as credit card records linked to the individuals involved in the attacks were identified.

Even if the information received did not show a connection to TF, the financial intelligence collected made it possible to understand the behaviour of suspects and related persons. The intelligence received was promptly shared with the relevant foreign FIUs and analysed by a team of senior CRF-FIU analysts and magistrates. Working in collaboration with the other FIUs, the original information was continuously enriched and further intelligence gathered. Links to additional potential suspects were shared and analysed as a top priority.

To avoid tipping off, the suspicious accounts and credit cards were not frozen, but subject to close monitoring and the CRF-FIU provided timely updates to advance foreign LEAs investigations into identifying and locating the suspects.

Status: Three suspects were killed in a raid carried out by the foreign authorities. All other suspects are currently either in prison or under judicial supervision or sought after by arrest warrants. The main suspect has been convicted to a life prison sentence without possibility of parole. The other 19 suspects were convicted to high prison sentences.

280. Overall, the intelligence-led identification and investigation efforts undertaken by Luxembourg competent authorities are recognised by the assessment team. Intelligence from Luxembourg has contributed to investigations in other countries, especially in the region, some of which have led to TF prosecutions in other countries.

TF investigation integrated with – and supportive of - national strategies

281. TF investigations are integrated in, and supportive of, Luxembourg's national strategy of aggressively preventing radicalisation, terrorism and TF. Most competent authorities in this area regularly coordinate their actions to ensure the best possible mitigation of TF risk. Competent authorities provide input from TF investigations at the development stage of national strategies. Potential medium or higher TF risks identified were mitigated by countermeasures based on the following five pillars: (i) national strategy and coordination, (ii) prevention and supervision, (iii) detection, (iv) prosecution, investigation and asset recovery, and (v) international co-operation.

282. The CRF-FIU and LEAs use financial intelligence and investigation to support Luxembourg's national counter-terrorism strategy of prevention and de-radicalisation. Case studies indicate that information from Luxembourg was used in other jurisdictions to identify and disrupt terrorist financing and terrorist organisations. NPOs suspected of radicalisation or at risk for TF were administratively closed (see Box 4.3).

Box 4.3. Case Study - NPO dissolved based on an administrative order

In March 2017, the CRF-FIU received a TFTR about a foreign-based NPO. In the period between May 2017 and August 2022, the CRF-FIU received additional SARs about the said NPO. The CRF-FIU conducted extensive operational analysis on TF-related SARs, involving approximately 1 200 individuals. Given the common elements in these reports (i.e., date of birth; financial information; etc.) SARs were centralised to detect common patterns.

The analysis revealed that payments, or potential donations, were credited on payment and e-money institution's accounts through money pools, which were advertised on an NPO's website, including specific campaign codes and phone numbers.

The CRF-FIU analysis indicated that the collected funds were systematically withdrawn from a specific EU Member State bank account.

Given the seriousness and complexity of findings, the CRF-FIU initiated international co-operation with its European counterpart. In the period between March 2017 and August 2022, there was continuous communication between the CRF-FIU and its foreign counterpart. This co-operation led to the discovery of additional evidence that resulted in searches and seizures in Luxembourg's territory.

In addition, PAL and its foreign counterpart engaged in discussions aiming at establishing a common *modus operandi* for the collection of financial evidence.

In May 2021, the NPO of concern was dissolved based on an administrative order.

283. At the operational level, there is regular co-ordination and co-operation among all competent authorities in charge of terrorism and TF investigations, as described above. Several cases shared with the assessment team demonstrate the full integration and importance of financial intelligence in Luxembourg's overarching counter-terrorism strategy.

Effectiveness, proportionality and dissuasiveness of sanctions

284. Luxembourg's legal framework allows TF prosecution of both natural and legal persons; however, there have been no convictions to date. Sanctions for natural persons and legal persons as foreseen by the Penal Code (see R.5) would theoretically be proportionate and dissuasive, if applied in a manner consistent with the gravity of the offence and the statutory range in case of a future prosecution and conviction. The assessment team extensively discussed this matter with competent authorities.

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

285. Luxembourg demonstrated its ability to use alternative measures (such as de-radicalisation programmes and dissemination of financial intelligence products to supplement on-going investigations and administrative procedures) to mitigate TF risk at a grass-roots level. Since 2015, Luxembourg has in place a programme to raise awareness at schools and community centres intended to fight radicalisation at the early stages and diminish the appeal of contributing to radicalised groups.
286. Where a conviction for TF could not be secured, the investigative judge, upon PAL's consent, can issue red notice or EAW. In the review period, Luxembourg issued a number of red notices for terrorism. In addition, the CRF-FIU disseminated relevant information collected to its international counterparts. This led to prosecution and conviction of individuals for other offences, which disrupted the suspected TF activity.

Box 4.4. Case Study - Preventing the abuse of NPOs for TF

In 2017, based on an incoming request from a foreign FIU, the CRF-FIU conducted analysis of a foreign-based NPO's account for potential TF. The transactional analysis revealed that from February 2018 to April 2019, a total amount of approximately EUR 3 million passed through the said account.

General KYC information, identification data of the authorised user of the account, and open-source data were gathered and analysed.

An injunction to freeze the NPO's assets was issued by the EU Member State (not applicable in Luxembourg), and a freezing order was issued by the CRF-FIU. Hence, approximately EUR 1 million were frozen in Luxembourg.

In parallel, the CRF-FIU duly documented the findings and shared them with its EU counterparts, including information on the freezing order to allow foreign judicial authorities to pursue seizure of the funds.

In May 2021, the NPO was already under judicial liquidation and the funds remain frozen. By the end of the on-site visit, there were still on-going procedures abroad.

Overall conclusions on IO.9

Investigative authorities and LEAs have adequate experience and tools to identify and investigate possible TF activity and Luxembourg demonstrated that TF activities are identified and investigated. All counter-terrorism investigations also include a TF component. The number of TF cases investigated and the prosecutions is somewhat in line with Luxembourg's self-assessed risk profile. Competent authorities act immediately on any indication of TF or terrorism threat and systematically analyse the financial aspect of each case. However, often no specific link to TF is ultimately found. While sufficient evidence was found in some stand-alone TF investigations, Luxembourg has only issued red notices for terrorism, and excluded mention of TF. This is an issue considering the stand-alone nature of these cases. Limitations in human resources have impacted to some extent the effectiveness of investigative authorities in conducting TF investigations. The comprehensiveness of TF intelligence gathering, save for TF-related STRs/SARs, and investigations, and competent authorities' regular practice of sharing information with foreign counterparts to support TF investigations and prosecutions weigh in Luxembourg's favour. Intelligence from Luxembourg has contributed to investigations in other countries, especially in the region, some of which have led to TF prosecutions there. Overall, moderate improvements are required.

Luxembourg is rated as having a Substantial level of effectiveness for IO.9.

Immediate Outcome 10 (TF preventive measures and financial sanctions)

287. Luxembourg is a global financial centre that attracts a large number of multinational firms (financial and non-financial) to establish branches or subsidiaries in its domestic market. Most of these companies have a well-established understanding of their TF risk and TF-related TFS obligations, based on e.g., group-level rules that are in place for their global operations. This, coupled with Luxembourg's assessed medium-low risk of TF overall, and its recent efforts to enhance the domestic CFT regime for NPOs and the framework for implementing of TFS without delay, indicate an overall framework that is generally technically sound; several enhancements to the framework are quite recent and have not been in place long enough to assess their effectiveness.
288. This assessment was based on a review of the Luxembourgish and EU legal framework on TFS; statistics on assets frozen; case studies; interviews with relevant competent authorities; and discussions with FIs, DNFBPs, VASPs and NPOs.

Implementation of targeted financial sanctions for TF without delay

289. Luxembourg does not have a national sanctions list and relies wholly upon the UN and EU regimes; this is in line with its TF risk profile. Between 2017 and 2020, Luxembourg implemented TF-related TFS in accordance with the EU Council Decisions and Regulations and supplemental domestic legislation and regulations (the 2010 United Nations Security Council Resolution (UNSCR) Implementation Law and related regulations) for implementing TF-related TFS. Under this framework, UN and EU designations were transposed via ministerial regulation, generally within one working day. This framework also had some other systemic deficiencies (e.g., lack of obligation to freeze without delay and without prior notice; gaps relating to the scope of freezing obligations), though entities supervised by the CSSF and the CAA were subject to clear regulatory obligations to freeze without delay and without prior notice for the duration of the review period. Luxembourg rectified these issues to a large extent in late 2020 and 2022 through: (a) legislation that automatically transposes UN and EU designations directly into the Luxembourg framework by reference to listing by those entities (the 2020 Sanctions Implementation Law); and (b) regulation requiring all Luxembourg persons to freeze the assets of these designated persons without delay and without prior notification (see R.6). In practice, Luxembourg provided a UNSCR 1267 designation, demonstrating that updates pursuant to UNSCR 1267 and its successor resolutions were transposed to Luxembourg Law without delay (and in a maximum of 24 hours) (2020 Sanctions Implementation Law).

Table 4.5. Transposition of UNSCR 1267 designations and updates to Luxembourg law

| Date listed by UN | Name | Communication date by UN | Date of transposition to Luxembourg | Date of transposition to EU |
|-------------------|--|--------------------------|-------------------------------------|-----------------------------|
| 04/02/2020 | Amadou Koufa | 04/02/2020, 22h37 | 05/02/2020 | 11/02/2020 |
| 23/02/2020 | Islamic State West Africa Province (ISWAP) | 23/02/2020, 22h56 | 24/02/2020 | 28/02/2020 |
| 23/02/2020 | Islamic State in The Greater Sahara (ISGS) | 23/02/2020, 22h56 | 24/02/2020 | 28/02/2020 |
| 04/03/2020 | Jamaah Ansharut Daulah | 04/03/2020, 23h01 | 05/03/2020 | 10/03/2020 |
| 04/03/2020 | Islamic State in Iraq and The Levant – Libya | 04/03/2020, 23h01 | 05/03/2020 | 10/03/2020 |
| 04/03/2020 | Islamic State in Iraq and The Levant – Yemen | 04/03/2020, 23h01 | 05/03/2020 | 10/03/2020 |
| 21/05/2020 | Amir Muhammad Sa'id Abdal-Rahman Al-Mawla | 21/05/2020, 23h27 | 22/05/2020 | 26/05/2020 |
| 16/07/2020 | Noor Wali Mehsud | 16/07/2020, 23h46 | 17/07/2020 | 22/07/2020 |
| 08/10/2020 | Jamal Hussein Hassan Zeiniye | 08/10/2020, 22h59 | 09/10/2020 | 13/10/2020 |

Designations

290. Luxembourg has neither identified nor proposed or made any designations pursuant to United Nations Security Council 1267/1989 and 1988 sanctions regimes, nor UNSCR 1373. In the review period, Luxembourg did not receive any request from other jurisdiction to designate individuals or entities pursuant to UNSCR 1373. This is generally consistent with Luxembourg's assessed TF risk exposure.
291. Luxembourg communicates designations and relevant updates through the MoF website (there is a dedicated section on UN and EU sanctions) and through the MoF's newsletter sent via email, which requires a (free) subscription. Luxembourg provided samples of newsletters. In practice, most FIs, VASPs and large DNFBP sectors use commercial automated screening mechanisms (updated timely) to avoid business relationships and transactions with designated persons and entities. Small DNFBPs rely on manual checks via publicly available sources such as the MoF's and other official websites.

Listing and De-listing

292. The MoF's internal guidance for listing and de-listing articulates high-level principles about these processes. While some relevant officials have sufficient expertise to be able to execute listing or de-listing, this expertise has not been memorialised in a way to be easily replicable by those lacking such expertise. And these principles have not been sufficiently operationalised to be user-friendly for other authorities who are critical sources of potential designations. For example, in the review period, LEAs identified subjects of interest for whom designation at the UN or EU level might had been an appropriate action, but they were unfamiliar with the availability of this option as a possible tool.
293. Discussions onsite with the Monitoring Committee revealed that competent authorities consider de-listing procedures as a critical protection against government power that assuaged stakeholders concerned about the enhancements to the TF-TFS regime introduced by the 2020 Sanctions Implementation Law. However, for the vast majority of the review period, these procedures were not clearly communicated to the public. Authorities noted that Luxembourg law provides for two administrative procedures that domestically designated persons can use to challenge their designations, but the MoF website did not provide any guidance to this effect, in a manner that would be clear to the general public until one week before the conclusion of the onsite visit.

Understanding of TF-related TFS

294. FIs (with few exceptions) and VASPs have a sophisticated understanding of TF-related TFS obligations. As for DNFBPs, their understanding varies across the different sub-sectors. Lawyers and approved statutory auditors have a good understanding of TFS. Other sub-sectors' understanding is less developed. Screening of BOs and senior managers of corporate entities against UN sanctions lists is not always applied across the DNFBP sector. This was confirmed by the interviews conducted during the onsite visit.

Implementation of TFS and freezing obligation

295. In the review period there were no instances where Luxembourg could have frozen assets related to TF-TFS. However, Luxembourg provided examples to the assessment team, where FIs reacted immediately to designations under other UN sanctions regimes and froze substantial amounts of assets (i.e., cash and securities).
296. During the interviews held on-site, the assessment team identified that, despite Luxembourg's comprehensive framework for border controls, the ADA has a limited understanding of the steps required to be taken in relation to the obligation of freezing funds or other assets of designated persons (e.g., identification of designated persons in complex cases, such as involving BOs as designated persons). This gap is mitigated to some extent, as TFS controls at the airport are automatic. However, this is not the case at the borders.
297. Compliance with TF-related TFS forms part of the CSSF and CAA routine AML/CFT on-site inspections. This was also confirmed in interviews with competent authorities and obliged entities. In 2019, the CSSF applied a sanction and a pecuniary penalty against a FI for failure to comply with TF-related TFS obligations. Supervisors for smaller DNFBPs have not to date taken remedial action to address gaps in TFS implementation by smaller DNFBPs such as small real estate firms and DPMS. Follow-up actions by supervisors confirm private sector compliance with this policy. The CSSF receives information from obliged entities and others on the implementation of TF-related TFS on an annual basis. Since 2020, CSSF did not identify any instance of non-compliance with TFS from supervised obliged entities.

Guidance

298. The CSSF and the CAA provide clear and timely guidance to its supervised entities about their obligations via their websites, as well as other outreach. Luxembourg provided a list of outreach activities conducted by the supervisory authorities. MoF, the authority responsible for TFS, has a website on TFS, but the guidance to the public about their obligations, as well as to listed persons regarding options for delisting, is not always clear and is sometimes cursory. For example, as of the conclusion of the onsite visit, the MoF website did not provide clear guidance to Luxembourg persons that they have an obligation to freeze assets under their control without delay and without prior notification. This is attributable in part to the fact that a clear regulatory requirement for all persons in this regard is a very recent development.

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

299. In 2020, Luxembourg identified the subset of organisations falling within the FATF definition of NPO. Based on this assessment, the DDCOM (MoJ), the Directorate for Development Cooperation and Humanitarian Affairs (CD) of MoFA and LBR collaborated and conducted a detailed analysis, which identified 91 NPOs that engage in development and humanitarian projects abroad (DNGOs) that are likely to be at risk of terrorist financing abuse (see R.8).

Supervision and risk understanding

300. MoFA, the competent authority for the supervision of DNGOs, demonstrated only a minimal understanding of the risk-based approach (RBA). There is no formal procedure or criteria for risk-based supervision. To the extent that supervision considers misuse of funds as a factor, it relies upon self-reporting, which is unlikely to uncover DNGOs subject to TF misuse. Since 2020, MoFA has enhanced its contacts with the sector. This will likely have a positive impact on the sector's understanding of TF risk, which is currently very low.
301. NPOs are aware of the existence of relevant risk assessments. Many of them have participated in outreach events convened by authorities. MoJ and MoFA shared with the assessment team a list of awareness-raising and training events for DNGOs starting from 2019, focusing on CDD, de-risking and TF risk. However, NPOs interviewed at the onsite did not demonstrate an understanding of TF risk. The sector applies mitigating measures, but such mitigation is only based on a general understanding of the need to implement financial controls.

Use of regulated channels

302. The MoJ encourages NPOs to conduct transactions via regulated financial channels. Cash donations are rare and are only accepted in very small amounts (for instance through anonymous collection boxes). All other monetary donations are received through the financial system. DNGOs' main donors are Luxembourg residents followed by a small percentage of EU residents.
303. Donations to DNGO's above EUR 30 000 are subject to MoJ's approval. In 2021, MoJ submitted two STRs to the CRF-FIU concerning requests for approval of donations. The CRF-FIU conducted analysis of the two STRs received and exchanged information with the FIUs of the jurisdictions concerned. Based on CRF-FIU analyses, the MoJ refused one of these requests, whereas the donation with charge in favour of a *fondation* was unrelated to the *fondation's* purpose and the exact amount of this donation was undetermined at the time of its attribution. The MoJ receives on an annual basis approximately 85 requests for approval, 90% of which are approved.

Oversight and sanctions

304. MoFA has a range of sanctions available for NPOs. Sanctions for failure to abide by the disclosure obligations include liquidation and criminal penalties for both the responsible legal and natural persons (see R.8). Although sanctions, such as liquidation, have been applied by MoJ to a number of ASBLs and *fondations*, MoFA has not applied any sanctions to DNGOs given that supervision of the subset is at early stages.³³

³³ Currently, one DNGO is in the process of a liquidation procedure opened by judicial decision.

305. The CRF-FIU, investigative authorities and LEAs are aware of the TF risk carried by DNGOs. In the review period, the CRF-FIU received and analysed 75 NPO-related STRs, all but one related to foreign NPOs. Most referred to donations made by residents of Luxembourg to foreign suspicious NPOs. Between 2017 and 2022, six investigations were conducted concerning TF suspicion on domestic NPOs. Information was received by the CRF-FIU that carried out analyses and filed reports to PAL. All the analyses were related to suspicions of religious radicalisation. None of these investigations revealed actual links to TF.

Box 4.5. Case study: Donations to foreign religious NPOs active in high-risk areas

In June 2018, the CRF-FIU filed two reports with PAL based on STRs received from a local bank. According to the reports, suspicion was raised based on transactions, including the purchase of numerous flight tickets, to a religious NPO in EU Member State A, operating in high-risk regions.

SPJ investigations revealed no links to terrorist or TF offence. In both cases, SPJ investigations were substantially supported by its foreign counterparts.

Deprivation of TF assets and instrumentalities

306. Luxembourg has mechanisms in place to deprive terrorists, terrorist associates, or terrorist financiers of assets and instrumentalities, including preventive measures, and mechanisms to freeze and seize terrorist property. Despite its limited exposure to terrorists, terrorist financiers, and terrorist organisations, where presented with the opportunity, Luxembourg has undertaken appropriate steps to deprive them of assets and instrumentalities related to TF activities. This is consistent with Luxembourg's assessed TF risk and context (see IO.1).
307. In the review period, the CRF-FIU received approximately 20 false-positives related to TF-TFS and analysed approximately 1 850 terrorism and TF-related STRs. The CRF-FIU imposed eight freezing orders³⁴ in relation to terrorism and TF. Most were initiated after FIU analyses of STRs or incoming MLA requests.

Table 4.6. CRF-FIU freezing orders on terrorism and TF, 2017-Q3 2022*

| Date of receipt of the initial report | Date of the freezing order | Amount |
|---------------------------------------|----------------------------|------------------|
| 07/10/2021 | 08/10/2021 | EUR 1 604 347.20 |
| 01/09/2021 | 02/09/2021 | EUR 1 876 428.71 |
| 01/09/2021 | 02/09/2021 | EUR 0.00 |

³⁴ These freezing orders are a CRF-FIU authority distinct from obliged entities freezing obligations under the Sanctions Implementation Law.

| Date of receipt of the initial report | Date of the freezing order | Amount |
|---------------------------------------|----------------------------|----------------|
| 03/06/2021 | 03/06/2021 | EUR 99 049.00 |
| 16/10/2020 | 10/12/2020 | EUR 987 824.00 |
| 16/04/2018 | 28/12/2018 | EUR 43 954.11 |
| 23/01/2018 | 12/04/2018 | EUR 66 398.11 |
| 25/04/2017 | 02/05/2017 | EUR 12 345.76 |

*Note: There were no freezing orders up to the end of Q3 2022.

308. As indicated under IO.9, there has been one terrorist conviction in Luxembourg. SRE has not identified any threats or vulnerabilities about domestic terrorist cells or terrorist attacks.
309. There was no criminal seizing or confiscation orders in relation to TF ordered, other than confiscation of a document stemming from an incoming MLA request. Currently, there is one ongoing TF investigation.

Consistency of measures with overall TF risk profile

310. Luxembourg has assessed its overall TF risk profile as medium-low, which is reasonable. As described in IO.1, however, findings about TF risks relating to exposure that may arise out of Luxembourg's status as an IFC (e.g., serving as a destination for funds from organised terrorist organisations) have not been sufficiently disseminated to relevant stakeholders. Despite the technical gaps in Luxembourg's TF-TFS framework for most of the review period, the assessment team is of the view that the absence of TF prosecutions, convictions and funds frozen related to TF-TFS, are in line with the self-assessed TF risk profile of Luxembourg.
311. The level of supervision and monitoring of the NPO sector varied throughout the review period and has been significantly enhanced since 2020. Luxembourg has not applied risk-based supervision of DNGOs consistent with the risks of TF abuse. This was also acknowledged by Luxembourg authorities during the on-site visit.

Overall conclusions on IO.10

Between 2017 and 2020, Luxembourg transposed UN and EU designations usually within one business day, but its overall framework for TF TFS had some significant deficiencies, including gaps in the scope of freezing obligations, and lack of obligations to freeze without delay and without prior notification. With changes to the framework in 2020 and 2022, Luxembourg has instituted a mechanism for automatic transposition of UN and EU designations and addressed these deficiencies; some of these more recent changes have not been fully implemented in a manner that demonstrates their effectiveness. Understanding of TF-related TFS obligations varies across the private sector, with FIs and VASPs having a sophisticated understanding of their obligations. Most private sector entities rely on commercial automated software to screen against UN sanctions lists.

MoFA's understanding of RBA is underdeveloped and DNGOs are not subject to risk-based supervision. Despite MoJ and MoFA outreach and training activities to enhance NPOs understanding of TF risk, this remains low. Luxembourg competent authorities have taken actions against NPOs that were not found compliant with their obligations.

Overall, in the review period, Luxembourg undertook appropriate steps to deprive terrorists, terrorist financiers, and terrorist organisations of assets and instrumentalities related to TF activities.

Luxembourg is rated as having a Moderate level of effectiveness for IO.10.

Immediate Outcome 11 (PF financial sanctions)

312. Luxembourg is exposed to potential PF activities given the relative ease of company formation, and the misuse of legal persons and financial channels, as well as the magnitude of the financial sector. Competent authorities acknowledge this potential exposure and are currently undertaking a PF risk assessment that demonstrates their willingness to go one step further than what the Methodology for the 4th FATF round of mutual evaluations requires.³⁵ Luxembourg is neither a weapons manufacturing jurisdiction nor a market of proliferation goods. The jurisdiction has a freeport, which applies strong AML/CFT/CPF controls. Overall, Luxembourg is geographically distant from both Iran and DPRK and there are no trade relationships with DPRK. There are negligible export activities with Iran that are subject to special authorisation (e.g., medical equipment).
313. This assessment was based on a review of the Luxembourgish and EU legal framework on TFS; statistics on assets frozen; case studies; interviews with relevant competent authorities; and discussions with the private sector.

³⁵ The findings in these paragraphs reflect the current situation in Luxembourg. However, the assessment team did not take into account findings in relation to the understanding of PF risks by FIs/DNFBPs in the conclusions, weighting or rating of IO.11 since recent changes to the FATF Standards related to risk of PF sanctions evasion will not be assessed until FATF's 5th round of Mutual Evaluations.

Implementation of targeted financial sanctions related to proliferation financing without delay

- 4
314. Between 2017 and 2020, Luxembourg relied solely on the EU framework for PF TFS implementation. As of 2020, applied the same framework for the implementation of TFS pursuant to UNSCRs 1718 and 2231 as it does for TF TFS. Thus, shortcomings discussed under IO.10 regarding the current framework equally apply to the requirements of IO.11.
 315. Luxembourg has yet to propose a listing to the UN pursuant to UNSCR 1718 and UNSCR 2231 and it has not frozen any funds or assets in relation to these Resolutions. However, on one occasion³⁶ related to DPRK (beyond UNSCR 1718), Luxembourg proposed and achieved the designation of four individuals at EU level.³⁷ This demonstrates the important role that all-source intelligence can play in supporting designations under international sanctions regimes and underscores the importance of systematically disseminating information about designation procedures to all relevant authorities (see IO.10). Luxembourg competent authorities did not receive any international request (formal or informal) linked to PF activities, movement of funds or other assets.
 316. Since 2010, Luxembourg has a permanent working group, the Monitoring Committee on International Financial Sanctions, that oversees the implementation of TFS (see Chapter 2, core issue 1.5). In 2022, CPF was included in the Committee's mandate. However, in practice, the Committee discussed CPF-related matters throughout the review period. The Committee allows for quick exchanges of PF-related information between competent authorities. Up to the on-site visit, the Committee discussed, among other things, updates on TFS regimes on DPRK and Iran, and the identification of areas where improvement in the implementation of PF-related TFS is required.

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

317. Luxembourg does not have any notable links to North Korea. However, Luxembourg maintains a limited trade relationship with Iran (i.e., medical equipment). Luxembourg has undertaken basic efforts to examine trade/financial flows to some extent based on supervisory data, through an assessment of direct financial flows. The methodology has not, however, accounted for the assessment of indirect financial flows indicative of common sanctions evasion techniques; competent authorities recognise the importance of undertaking such an analysis, but have found it difficult to identify such flows based on the data analysed to date. This is a challenging exercise, but critical for Luxembourg given the size and reach of the IFC; this status alone means that its exposure to PF activities is likely to be much higher.

³⁶ To this effect, Luxembourg shared granular information with the assessment team on a confidential basis.

³⁷ Designations occurred on 20 April 2018 through Council Decision 2018/611.

318. The CSSF provided data that demonstrate the low direct exposure of obliged entities under its supervision to potential PF activities. Luxembourg banks maintain 22 accounts with individuals, 4 accounts with legal entities, and 10 UBO's that reside in Iran. In 2021, there were 4 banks that received or sent payments from/to Iran (47 payments received for a total amount of EUR 765 507 and 14 payments sent for a total amount of EUR 3 875 373). A small number of clients residing in Iran is also found in other FIs. None of these relationships/transactions has a direct link to designated persons and entities pursuant to UNSCR 1718 and 2231. None of the shareholding and BO relationship of FIs under CSSF supervision was established in Iran or DPRK.
319. In addition, according to CSSF data, very few banks offer trade finance transactions. None of these banks has VOSTRO accounts³⁸ held by respondent banks established in relevant Iran, DPRK or other countries under UN sanctions regimes.
320. Between 2017 and 2022, there were no hits identified by the private sector or Luxembourg competent authorities. This is also confirmed by findings of supervisory authorities. Most FIs, VASPs and large DNFBPs use commercial automatic software (updated in real time) to screen against PF-related TFS. Some medium/small DNFBPs noted that they lacked the resources to subscribe to such databases. Accordingly, they rely upon publicly available sources, both international and domestic, to screen their customers for TFS. This underscores the need for MoF to improve its targeted financial sanctions website as noted in IO.10.
321. Currently there are sizeable amounts of funds frozen³⁹ in relation to DPRK, but none of these relates to UNSCR 1718 and UNSCR 2231, which is consistent with Luxembourg's low exposure to PF activities. All operators holding funds and economic resources under freezing regime submit a quarterly report to MoF on the frozen assets, including information on the value, legal basis of freeze, designated person(s) and entity(ies) concerned.
322. Despite not being a requirement under the FATF Standards, the CRF-FIU received a few PF-related SARs. CRF-FIU examined these SARs thoroughly, but no trace of PF activity was identified. The CRF-FIU sought also input from foreign counterparts before completing the analysis of these SARs.

FIs, DNFBPs and VASPs' understanding of and compliance with obligations

323. Awareness concerning PF-related TFS of the private sector varies. The financial sector largely has a strong understanding of its TFS obligations, but understanding is not as strong for some non-bank sectors. For example, in the interviews held when onsite, all representatives of one sub-sector (i.e., investment firms) were unable to identify the correct authority to notify following an asset freeze under the TFS framework. VASPs understand their TFS obligations, including their vulnerability to potential violations of DPRK sanctions (i.e., prevalent use of virtual assets in ransomware attacks).

³⁸ A VOSTRO account is a bank account held by a foreign bank with a Luxembourg bank.

³⁹ Up to the end of the on-site visit, Luxembourg had two active cases of assets freeze. The value of the assets frozen is EUR 1 000 604 (market value of securities as at 31 December 2021), EUR 294 036 (cash as at 31 December 2021). Both cases were reported by FIs and freezing measures were implemented by these institutions.

324. DNFBPs' understanding of their PF-related TFS obligations varies significantly comparing to FIs. Large DNFBPs have a good understanding, unlike medium/small professionals that have a less developed or immature understanding of their obligation to report and freeze assets of designated persons and entities.
325. Findings of competent authorities' supervisory activities demonstrate that, across the review period, there was an increasing compliance culture with TFS, that is particularly strong within the financial sector. Some obliged entities across different sectors were found non-compliant with their TFS obligations (i.e., gaps in internal procedures for TFS and non-systematic screening of TFS). Such gaps were immediately rectified by the obliged entities of concern.

Competent authorities ensuring and monitoring compliance

326. All Luxembourg supervisory authorities assess FIs' and DNFBPs' compliance with TFS-obligations during on-site and off-site inspections, but some of the deficiencies in risk-based supervision from IO.3 accordingly cascade here (e.g., resource constraints; limitations in implementation of risk-based supervision by some authorities). Financial supervisors also monitor obliged entities compliance with TFS through annual questionnaires that include comprehensive questions based on PF indicators (i.e., geographic risk exposure; origin of clients; financial flows with DPRK and Iran; products and services exposed to PF; training of TFS, etc.).
327. Financial supervisors provide clear guidance to obliged entities regarding their TFS obligations. Supervisory authorities have dedicated sections on TFS, including PF, in their websites. These sections host all types of guidance and circular letters and newsletters on PF-related TFS that are shared with the obliged entities on a regular basis. Guidance addressed matters about several issues, including the following: (a) measures for DPRK and Iran related business relationship with clients or transactions; (b) CSSF's supervisory expectations on asset/name screening; (c) trade finance, including PF risk factors.
328. In ensuring obliged entities compliance with PF-related TFS CSSF and CAA have provided feedback to the former about TFS related deficiencies found in inspections either bilaterally or through annual reports, organised events with the industry to discuss PF-related TFS obligations and sent alert on UN sanctions list to obliged entities through email. The CSSF and the CAA co-operate and co-ordinate with the MoF to ensure that guidance provided to obliged entities remains current.

Box 4.6. Case study: Investment Firm

In February 2017, the CSSF carried out an on-site inspection on the AML/CFT framework of an investment firm headquartered in Luxembourg and authorised to carry out the activities of investment adviser, broker in financial instruments, commission agent, private portfolio manager and family office.

The inspection team reviewed more particularly the investment firm's AML/CFT process, its AML/CFT procedures and issued remedial actions. Several minor AML/CFT breaches were discovered, including, (i) formalisation and control of name-screening, (ii) follow-up and closure of name-screening alerts, (iii) AML/CFT procedures.

In the aftermath of the inspection, the investment firm confirmed in writing to CSSF that all the necessary remedial actions have been taken. The formalization and control of the name-screening was improved as well as the formalization and closure of the name-matching alerts. Finally, the AML/CFT procedures were updated according to the latest AML/CFT regulations.

Off-site supervisory activities in 2017 and 2018 also confirmed that the identified issues had been remediated in a satisfactory manner.

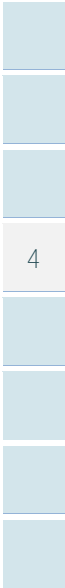
329. DNFBP supervisors and SRBs' communication in this regard is more mixed. The MoF's communication in this regard could be improved. The OEC is the most active DNFBP supervisor on PF-related TFS, as it systematically provided training to this effect to chartered professional accountants throughout the review period. Overall, the OEC's policy had a positive effect on this sector's level of compliance.

Overall conclusion on IO.11

Between 2017 and 2020, Luxembourg relied wholly on the EU PF TFS framework, and accordingly did not implement without delay. Currently, the mechanism implementing PF-related TFS is the same as the one for TF. Thus, shortcomings listed under the IO.10 findings equally apply to the implementation of PF-related TFS.

No funds or other assets have been frozen in relation to designated persons or entities under the PF-related TFS regime, as no matches were identified. A large part of the financial sector, including VASPs, and a smaller part of DNFBPs understand their PF-related TFS obligations and performs sanctions screening. Most of the obliged entities have internal procedures on the implementation of PF-related TFS. Financial sector supervisors undertook significant efforts through onsite/offsite inspections, outreach activities and guidance to boost obliged entities understanding and compliance with PF-related TFS. The assessment team is of the view that the main financial supervisors adequately monitored and supervised obliged entities compliance with PF-related TFS. This cannot be said for a number of DNFBP subsectors.

Luxembourg is rated as having a Moderate level of effectiveness for IO.11.



Chapter 5. PREVENTIVE MEASURES

Key Findings and Recommended Actions

Key Findings

Immediate Outcome 4

1. Understanding of ML risks and AML/CFT obligations is strong for FIs, good for VASPs (although the understanding of ML threats focuses on certain but not all ML threats) and mixed among DNFBPs. Generally, for all sectors, there is a need to further develop the understanding of TF risk, particularly in light of Luxembourg's risk profile as an international financial centre.
2. REAs and DPMS have a weak understanding of ML/TF risks and application of AML/CFT obligations resulting in weaker risk-based mitigating measures.
3. Interviews with obliged entities in most sectors did not reveal any serious concerns about the implementation of their AML/CFT requirements and they have appropriate mitigation measures in place that are commensurate to their risks. Implementation is stronger for FIs, specialised PFS and PSAs (TCSPs) than for other DNFBPs and VASPs. Smaller DNFBPs face challenges implementing AML/CFT measures effectively. For DNFBPs (with the exception of specialised PFS and PSAs) good AML/CFT mitigating programmes are more recent and investment firms and DNFBPs, with the exception of Specialised PFS and PSAs and few other TCSPs and lawyers, did not fully understand their TFS obligations.
4. While important remediation work and blocked investor accounts were observed during the review period, CDD and record-keeping measures improved much by the time of the on-site visit. Overall, there was a good understanding of beneficial ownership identification, except by REAs and DPMS, and adequate awareness on handling complex structures that include legal persons and legal arrangements.
5. Compliance with reporting obligations is divergent. There are low number of reports filed by most DNFBPs, and a large proportion of reports are driven by adverse media hits which not all FIs, DNFBPs and VASPs properly analyse to establish if there are grounds for suspicion before filing the report. Furthermore, the quality and relevancy of TF-related reports submitted by most obliged entities remains a concern.
6. FIs, DNFBPs and VASPs apply tools and controls such as internal policies and procedures, business and customer risk assessments and training (including for group compliance). These measures are more sophisticated and more effective for FIs, VASPs and larger DNFBPs.

Recommended Actions

1. Luxembourg should enhance guidance, training or other forms of outreach by the relevant authorities and supervisors to ensure that:
 - a) FIs, DNFBPs and VASPs have a better understanding of their foreign TF risk, methods and exposure, relevant to Luxembourg's status as a significant international financial centre with very significant cross-border activities which terrorist funds may be utilising;
 - b) VASPs and medium and small-sized DNFBPs have a more detailed understanding of ML threats to which they are exposed;
 - c) Investment firms and DNFBPs have properly understood the scope of their obligations regarding TFS, including informing the MoF of a TFS positive match;
 - d) REAs and DPMS improve their understanding of ML/TF risks and AML/CFT obligations and implementation of risk-based mitigating measures;
2. The CRF-FIU and supervisors should enhance outreach activities to ensure that remaining FIs, who have not registered, and DNFBPs register with goAML and obliged entities properly understand the scope of their obligations to identify, analyse and report suspicious activity and transactions to raise the level and quality of reporting.
3. Luxembourg should continue to develop tools such as e-learning for raising awareness of AML/CFT obligations and for enhancing the training offering for DNFBPs supervised by SRBs.
4. Luxembourg should continue working closely with VASPs to ensure the effective transposition and implementation of the travel rule on wire transfers.

330. The relevant Immediate Outcome considered and assessed in this chapter is IO.4. The Recommendations relevant for the assessment of effectiveness under this section are R.9-23, and elements of R.1, 6, 15 and 29.

Immediate Outcome 4 (Preventive Measures)

331. The implementation of preventive measures by the relevant sectors is weighted as **most heavily** for banks, Investment Fund Managers (IFMs) and specialised PFS (TCSPs); **heavily** for investment firms, notaries, lawyers, Chartered Professional Accountants (CPAs) and real estate agents (REAs); **moderately heavily** for Payment Institutions (PIs), E-Money Institutions (EMIs), life insurance undertakings and brokers, PSAs (TCSPs), DPMS, TCSPs (provided by professional directors supervised by the AED, business/office centres and statutory auditor and audit firms), and VASPs; and **less heavily** for the casino and accounting professionals. This weighting is based on the relative importance of each sector and Luxembourg's risks, context and materiality, as explained in Chapter 1. TCSP activities offered by specialised PFS and PSAs are considered as part of the FI sections as they are supervised by the CSSF and CAA, other professionals with TCSP activities are covered in the DNFBP section.
332. The assessment team's findings on IO.4 are based on interviews with private sector representatives, statistics, findings from enforcement actions, input from supervisors, and information from the Luxembourg national authorities (including the NRAs). The assessors met with a wide range of FIs, DNFBPs, VASPs and professional associations. These meetings included foreign and domestic owned banks (which offer private banking, retail banking, banks servicing the collective investment scheme sector and those providing fiduciaire activities), investment fund managers and investment firms, PIs, EMIs, life insurance undertakings and brokers, VASPs, lawyers, notaries, accountants, TCSPs (provided by specialised PFS, statutory auditors and audit firms, business/office centres, and professional directors supervised by the AED), REAs, DPMS and the casino. Meetings with the private sector representatives indicated that the implementation of preventive measures varies across and within sectors.

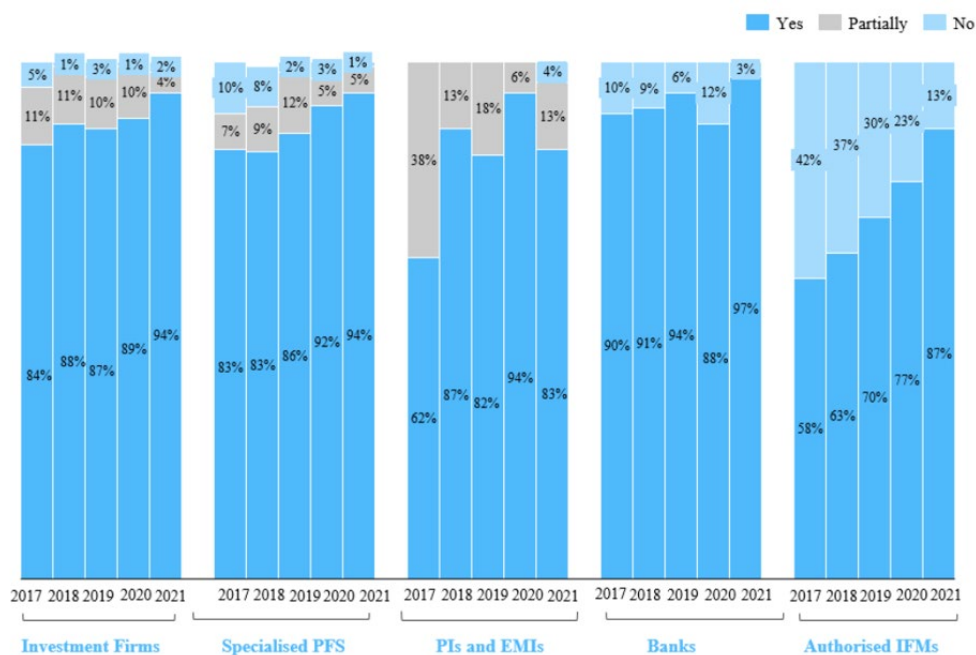
Understanding of ML/TF risks and AML/CFT obligations

FIs

333. FIs have a good understanding of their ML risks, but how much they understood their TF risks varied. All FIs met demonstrated a sound knowledge of their AML/CFT obligations. However, all investment firms met were unable to identify the correct authority to notify following an asset freeze under the TFS framework, indicating a deficiency relating to communication about TFS obligations to this particular sector.
334. Widespread industry participation in risk assessments and extensive engagement with supervisors (CSSF and CAA) helped to develop FIs' understanding of ML/TF risk and AML/CFT obligations. Methods of engagement include firm specific supervisory activities and sectoral level engagement (e.g., participation in expert working groups, work of professional associations and supervisory/industry-led events). The CSSF and CAA observed positive trends in increased understanding and noted that the self-assessment element within the annual supervisory AML/CFT questionnaires helps FIs identify gaps in their internal AML/CFT compliance procedures, thus continuously increasing FIs' understanding of AML/CFT obligations.

335. FIs regard the NRAs, VRAs and SSRAs as useful guides in developing their own enterprise-wide risk assessment. These enterprise-wide assessments, which must be updated annually, focus on the risk posed by customers, products, services, delivery channels and geographical locations. FIs use the NRA to determine the risk levels within each of these categories. In the past years, FIs lessened their risk appetite following the Panama Papers reports and changes to Luxembourg law making tax crime an ML predicate offence (see IO.3). There has been a sharp decrease in the number of foreign corporate clients at Luxembourg banks. For example, the number of Panamanian and BVI companies decreased from 1 300 and 4 200 in 2016 to 428 and 1 900 in 2021 respectively. Most non-corporate clients are EU-residents and most corporate clients are Luxembourg legal persons, which FIs regard as lower risk. FIs are required to document their risk appetite and to have this approved at board level. Compliance with this requirement is high (see Figure 5.1). FIs refuse potential clients if they cannot satisfy themselves on *inter alia* tax compliance, identification of source of funds or if there are discrepancies in beneficial ownership (BO) information.

Figure 5.1. Have the ML/TF risk appetite and KRIs been defined, approved by the Board, communicated to the employees and monitored on a regular basis? Indicative data 2017-2021



Source: CSSF data for the financial sector

336. Banks regard their main ML exposure in line with national and sectoral risk assessments: high risks stemming from tax crimes, corruption (particularly where they have PEPs as clients), fraud, and private banking. IFMs and investment firms share this view. IFMs, banks and specialised PFS providing depository, administration and transfer agency services to Luxembourg investment schemes are well attuned to the ML risk posed by investors and how risk arise through schemes' promoters and from the underlying investments. These FIs scrutinise investment fund transactions to ensure they are satisfied about the origins of the investment opportunity and that tax obligations are complied with, particularly when dealing with investments in alternative asset classes such as private equity, infrastructure and real estate, which are regarded as higher risk assets. Such control includes understanding the tax implications, screening the buyer and seller and considering whether the asset value reflects the market. In line with the NRAs, banks consider PEPs, complex corporate structures, residency in high-risk jurisdictions, high asset value and certain commercial activities as high-risk factors. They also consider the cumulative effect that each of these factors can have on the risk rating. Private banking, IFMs and investment firms met consider their TF exposure as low. While this is reasonable given their client bases (e.g., for private banking clients mainly consist of high-net worth individuals from the EU) and in line with the vertical and sectoral risk assessments, they demonstrated a weaker understanding of their TF risks in relation to TF levels stemming from international organisations using Luxembourg's IFC status.
337. PIs and EMIs met explained that their main ML threat comes from fraud, including tax fraud and more recently PPE fraud, and the main TF threat from movement of funds and purchases. These entities serve EU buyers and marketplaces although sellers on those platforms can be located worldwide. PEPs and connections to higher risk jurisdictions are regarded as high-risk factors but the proportion of clients from non-EU countries is relatively small.
338. The life insurance sector considers the main ML exposure to be from tax offences and entities met understand and are aware of the potential TF risk arising from individual terrorists taking out policies to benefit their families.
339. Overall, following national work on TF risks, such as the 2022 TF VRA, reflective of Luxembourg's status as a significant international financial centre, as well as its exposure to low-level TF (e.g., lone wolves), a more in-depth TF risk understanding by FIs is beginning to develop. However, this development is in the early stages as the public version of the 2022 TF VRA was published recently (in May 2022) and does not give the necessary details to provide actionable guidance to obliged entities for them to understand the TF typologies and methods within their business activities, services and products (see IO.1).

VASPs

340. Registered VASPs have a good understanding of their ML risks and AML/CFT obligations and demonstrated a careful approach to risk, including to risks emerging from new products and patterns. However, their understanding is more limited for some of the ML threats such as drug trafficking and TF risk which tends to focus on the risk of listed terrorists conducting transactions rather than risks stemming from for instance lone actors, small cells and FTFs using virtual assets to channel funds for TF purposes. VASPs met regularly assess their risks and ensure that their risk assessment is approved by management. They were also aware of the various national and vertical risk assessments and used these in developing their own risk assessments. They have a good dialogue with the CSSF, even though the VASP registration regime only started in March 2020.

DNFBPs

341. Understanding of ML risks and AML/CFT obligations among DNFBPs varies depending on the sector and size of the entity and the risk exposure, while the understanding of TF risk and TFS obligations is generally limited across all DNFBPs. This is due to their limited exposure to TF risks and some confusion regarding the responsible authority to whom TFS positive matches should be reported, especially among REAs, DPMS and some medium and small-sized DNFBPs supervised by SRBs.
342. Larger firms in the accounting, audit and legal fields have a stronger understanding of risks and obligations, using the various risk assessments to inform their own client risk analysis, and have more sophisticated internal AML/CFT policies and processes in place. Smaller firms met tend to avoid risks instead of mitigating them because their risk understanding is more recent and limited. For instance, they would refuse business when dealing with PEPs or clients from abroad. A risk-averse approach may be effective in mitigating the risks in some situations. However, it does create vulnerabilities as the level of risk of clients and products may fluctuate over time.
343. Generally, TCSPs have developed a good understanding of their inherent risk factors in the last two years and in line with the NRA (e.g., complex ownership structures with a high number of foreign owners, the potential for products and services being abused and the use of intermediaries). This is due to the adoption of the CSSF's 2020 SSRA for specialised PFS providing corporate services (TCSP activities), CSSF's leadership and the development of risk-based supervision for most sectors around the same time. TCSPs also have a good, but recent, understanding of their AML/CFT obligations. The NRAs and SSRAs, especially the CSSF's 2020 SSRA, assisted professionals in obtaining a deeper risk understanding and improving their compliance levels. This led to a decrease of risk appetite for complex structures with links to jurisdictions perceived to be higher risk. Similarly, the OAs observed a sharp decrease of high-risk services in the legal profession, including servicing companies with complex structures that are difficult to understand and may not have a clear economic purpose. Notaries take a risk-averse approach: they tend to assess their clients and activities as higher risk than the NRA findings.

344. Among entities supervised by the AED, the casino has a very good risk understanding, and a good understanding and application of its AML/CFT obligations. The level of risk understanding is limited for REAs and DPMS as many of them have not started reflecting on their risks and could not articulate what their higher risks are. When it comes to the understanding and application of AML/CFT obligations, the assessment team noted, through the material provided by Luxembourg and on-site interviews, that REAs, DPMS and accounting professionals have a significant degree of deficiencies related to assessing risks, including the absence of formalized risk assessments in a majority of firms or low-quality risk assessments for the firms that had one.

Application of risk mitigating measures

FIs

345. A vast majority of FIs apply appropriate mitigating measures to manage ML/TF risks. Supervisory data for 2020 shows that about 80% of banks, IFMs and investment firms have measures commensurate with their risks, whereas for PIs and EMIs this figure is lower, closer to 50% and improving. FIs generally invested significantly in compliance over the last five years. FIs met sufficiently showed how they apply risk sensitive measures to various customer situations. Most FIs, except the PI and EMI sectors, do not apply simplified measure to low-risk situations, but apply EDD to a variety of higher risk situations, indicative of a cautious approach to risk management within most FI sectors.
346. There is some room for improvement in the application of AML/CFT measures in the insurance sector. This is reflected in the responses to the AML/CFT qualitative questionnaires which indicate that resourcing challenges (due to a tight labour market) are having an impact on the application of commensurate risk-based controls (see Table 5.1). The CAA attributes this to short-term fluctuations, i.e., turnover within compliance departments at these FIs, and ongoing investment in IT compliance tools.

Table 5.1. Compliance Officer self-assessment of supervised entity's consistency between ML/TF risks and mitigation measures, 2018-Q3 2022

| Qualitative Questionnaire | Answers | Life insurance undertakings | Brokers | Life insurance undertakings | Brokers |
|---|---------|-----------------------------|---------|-----------------------------|---------|
| | | 2018 | 2019 | Q3 2022 | |
| Question 7.1: Does the Compliance Officer (AML/CFT) consider that the professional has sufficient qualified human resources to properly assess, manage and mitigate ML/TF risks? | Yes | 97% | 98% | 84% | 95% |
| | No | 3% | 2% | 16% | 5% |
| Question 7.2: Does the Compliance Officer (AML/CFT) consider that the professional has sufficient and appropriate IT tools / technological | Yes | 89% | 84% | 73% | 92% |
| | No | 11% | 16% | 27% | 8% |

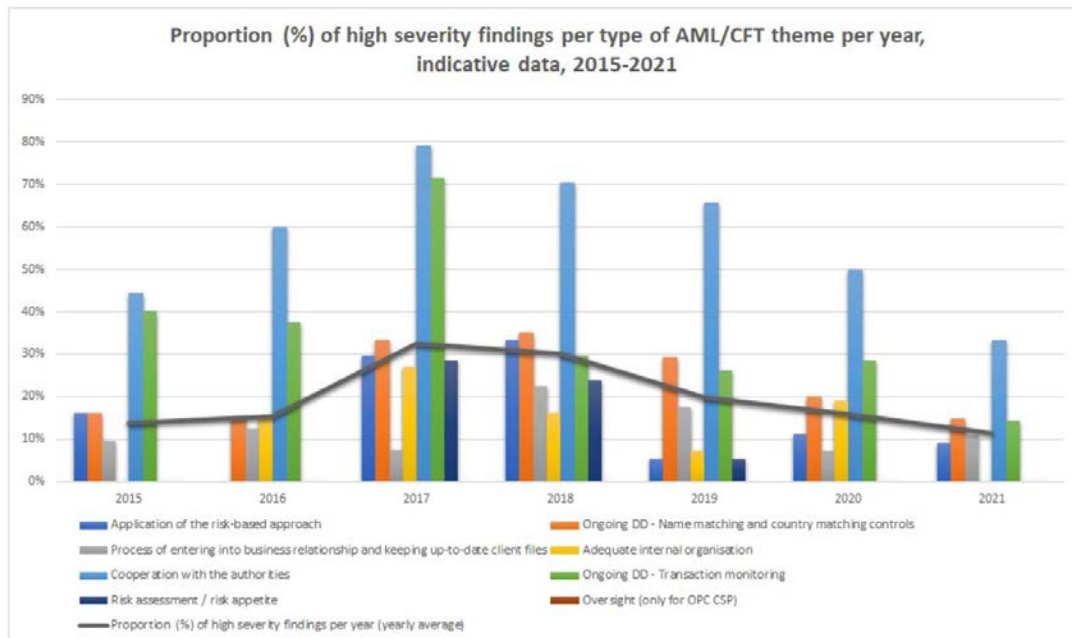
| Qualitative Questionnaire | Answers | Life insurance undertakings | Brokers | Life insurance undertakings | Brokers |
|--|-----------|-----------------------------|---------|-----------------------------|---------|
| | | 2018 | 2019 | Q3 2022 | |
| means to properly assess, manage and mitigate ML/TF risks? | | | | | |
| Question 7.5: In the opinion of the Compliance Officer, are all the measures put in place sufficient to mitigate ML/TF risks? | Yes | 89% | 88% | 68% | 91% |
| | No | 0% | 0% | 0% | 1% |
| | Partially | 11% | 12% | 32% | 8% |

Source: CAA data for the insurance sector.

Note: The CAA issues these self-assessments at predefined times, i.e., in 2011, 2018 and 2022 for life insurance undertakings, and in 2019 and 2022 for brokers.

347. Supervisory work, which has become more frequent and intense over the past years, indicates continued improvement in FIs’ controls and a decline in the severity of supervisory findings since 2017. Specifically, it observed that the severity of weaknesses in the application of AML/CFT measures decreased (see Figure 5.2). There is a vast improvement in FIs’ co-operation with Luxembourg national authorities. All FIs met noted they acted on audit recommendations from their statutory auditors, and many indicated an increasingly tougher regulatory regime evolving over the past years.

Figure 5.2. Proportion (%) of high severity findings per type of AML/CFT theme per year, indicative data, 2015-2021



Source: CSSF data for the financial sector. Data for 2022 is not available as on-site inspections have not all been finalised.

Note: the black line represents the proportion of findings regarded as 'high severity' while the vertical columns represent the type of AML/CFT issue. Therefore, in 2017 32% of all findings were highly severe, and this is 30% in 2018, 20% in 2019 and 16% in 2020.

VASPs

348. VASPs have comprehensive controls and sophisticated tools in place that are designed to mitigate risks. This is also observed by the CSSF through its supervisory work (see IO.3). During the registration process, the CSSF assists the applicant VASP in setting-up internal AML/CFT policies and measures that are proportionate to the risks VASPs are exposed to. VASPs assess the risks before listing any new product on their platform. They also consult the CSSF and adapt the level of mitigation measures to be applied based on the client risk (e.g., whether it has a complicated legal structure), distribution channel, activity and service provided.

DNFBPs

349. Generally, DNFBPs have put in place good AML/CFT programmes designed to mitigate ML/TF risks. These are more recent for some sectors (accounting professionals, business/office centres and professional directors supervised by the AED). However, in the REAs and DPMS, risk mitigation controls and policies need further maturing. DNFBP supervisors observe an upward trend in the compliance rate among their supervised professionals, and all firms met had good co-operation with the authorities and did not hesitate to reach out to them in case of doubt.
350. Smaller entities across all DNFBP sectors met indicated a very limited risk appetite for foreign clients, complex structures with no clear economic purpose and high-risk products (e.g., the use of virtual currency), while larger firms had a higher risk appetite. Both small and large firms invest significant resources in applying good mitigating measures with small firms struggling with the high resource requirements. The casino applies very strong mitigation measures that go beyond the risks identified in Luxembourg and are commensurate with the risks generally identified in casinos abroad, even though the game offerings by the Luxembourg casino are limited to slot machines and a few blackjack tables.
351. In relation to TCSPs, outreach by the CSSF to other TCSPs supervisors and TCSPs themselves contributed significantly to the application of good mitigating measures commensurate with risks across the TCSP sector, though this is very recent for professional directors, as the AED has not fully developed the supervision of the latter. Nonetheless, professional directors supervised by the AED have limited activities and therefore pose a lesser ML/TF risk than other TCSP professionals, notably the specialised PFS who are supervised by the CSSF.
352. Lawyers, CPAs, notaries and statutory auditors and audit firms have risk assessments, policies and procedures in place for the implementation of due diligence measures which are generally in line with the risks identified for their activity, such as risks related to international clients and real estate transactions. Most firms met presented a limited risk appetite and owners of small firms keep a close control on their businesses. Several firms also noted that although they have access to good IT tools, they conduct additional analysis, including manual checks, to ensure that they have a full understanding of the business structure and its economic reason. However, in some cases SRBs noted issues relating to the level of quality and documentation of risk assessments, which can be considered a limited deficiency.

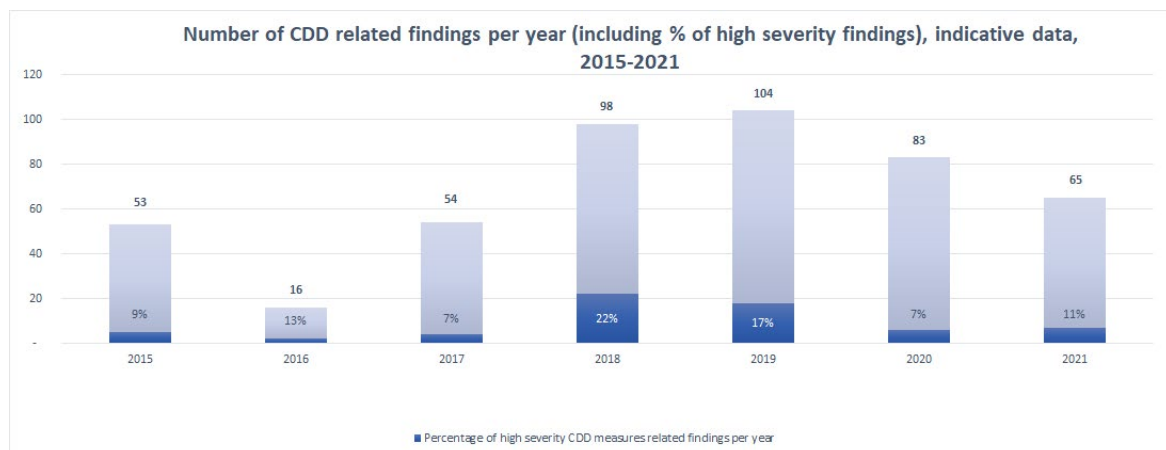
353. The implementation of risk-based mitigation measures by REAs and DPMS is more limited. None of the professionals met were able to demonstrate the implementation of mitigation measures adapted to the risks and vulnerabilities specific to their sector, apart from some mitigating measures in certain risk situations. The AED's on-site inspections in 2020 showed that the DPMS sector had no risk-based approach. While approximately 22% of REAs had some form of a risk-based approach, most of these had significant deficiencies. Nevertheless, both sectors indicated to the assessment team that they have put in place some mitigation measures. For example, DPMS apply thresholds for limiting the use of cash at EUR 7 000 or conduct some level of CDD for cash transactions above EUR 2 500. REAs met noted that they do not accept cash, usually avoid non-face-to-face transactions, conduct additional Internet searches when facing a foreign client or check the history of the client for very high-value purchases. Although helpful, these measures do not replace systematic risk-based mitigation measures.

Application of CDD and record-keeping requirements

FIs

354. The CSSF and CAA report that FIs generally have effective CDD and record-keeping measures in place, with little to no variation across the sectors. Based on interviews with FIs met during the on-site visit, the assessment team shares this view. Where gaps in these requirements are identified through supervisory activities and the long-form report/special (AML/CFT) report prepared by the statutory auditors, they are mostly minor and non-systemic (see Figure 5.3).

Figure 5.3. Number of CDD related findings per year (including % of high severity findings), indicative data 2015-2021



Source: CSSF data for the financial sector.

355. FIs have effective processes in place for onboarding customers and conducting CDD. Depending on the services provided, they use different modes to onboard new customers with no simplification of the type or depth of CDD applied. Banks mostly have face-to-face interaction. For example, private banking clients are met through the bank's client relationship managers and a large share of clients come from the EU or neighbouring countries who go to branches in other EU countries or travel to Luxembourg to open an account. PIs and EMIs use remote onboarding with some relying on verification services offered by technology companies. A number of FIs, across all sectors, rely on CDD undertaken by a third party. For instance, in the life insurance sector, one-third of undertakings rely on the brokers for the execution of some CDD measures. Also, a small proportion of the specialised PFS rely on third parties who do the CDD to introduce new customers (none relate to high-risk TCSP activities). Within the investment sector, 70% of IFMs have cross-border intermediaries in the funds they manage (these relationships are considered as correspondent services: see section 5.2.4). Supervisory work shows that FIs using a third party for CDD apply appropriate oversight and monitoring which includes a review of the third party's procedures and spot-checks to ensure that the third party applies appropriate controls.
356. The CDD application for natural persons includes checks of official identity documents and, when appropriate, proof of CV to establish if funds being deposited are from savings, inheritance or other sources. For legal persons, FIs require corporate structure charts to understand the BO and control arrangements and for complex structures also the rationale behind the multiple layers used. Complex structures are generally regarded as containing three or more layers or including a trust or *fondation*. FIs met accurately identify beneficial owners when dealing with legal persons (with some FIs lowering the thresholds from 25% to 10% for higher risk relationships) and arrangements. When seeking to establish if there is BO without legal ownership, FIs explained their measures include scrutinising structure charts to understand the multiple layers in a structure and the role of any legal arrangement, and consider information on source of funds for individuals being presented as the beneficial owner, and corroborate this information with the registers (i.e., the RCS, RBE, RFT). FIs benefit from the specific guidance issued by the CSSF in 2019 on BO and they train staff on how to perform effective controls when handling corporate clients. FIs providing administration, depository and transfer agency services to collective investment schemes undertake CDD on the scheme's management company, including its beneficial owners. This approach is also applied to "seed" investors which can include third-party asset managers in advance of the scheme's launch as well as to investors after launch.

357. FIs take a risk-based approach to monitoring their customers on a periodic basis to identify any changes in the relationship which would alter the risk and ensure CDD remains up to date and relevant. On a real-time basis, they also review if a proposed transaction or an activity creates a trigger to review the customer file. FIs met conduct, depending on their size, daily or monthly screening of their entire clients list against government and commercial databases, including TFS and PEPs lists. The CSSF observed a positive trend of adequate and timely periodic reviews. Of the 161 on-site inspections performed in the period 2017-2021, only 23 breaches related to issues with periodic review. FIs review high-risk clients every year with the banking and PI/EMI sectors reviewing them more frequently, at six-month intervals. Medium-risk clients are in principle reviewed every three years and low-risk every 5-7 years. In 2021 15% of Luxembourg banks reported they review medium-risk files every 3-5 years and 13% reported that low risk files were reviewed at least 5-7 years, with the remaining 85% and 87% reviewing clients in shorter time frames. The CSSF has been working with banks to reduce the timeframe to within five years.
358. FIs also undertake ad-hoc reviews following mergers, supervisory action or regulatory changes (e.g., tax crime becoming a predicate offence for ML in Luxembourg in 2017) and they implement remediation programmes where CDD deficiencies have been identified. In the collective investment sector, there are a significant number of accounts, where transfer agents have “blocked” investors’ access to the funds arising from redeeming units in a scheme or from a dividend distribution. This is for a number of reasons including deficient CDD as well as prudential reasons. For blocks imposed on investor accounts in a scheme which is liquidating, investor CDD is reviewed before final pay-out or trading is suspended. The number of blocked investors compared to the total number of investors in Luxembourg investment funds are as follows (see Table 5.2).

Table 5.2. Accounts Blocked, 2018-2021

| Year | No. of blocked accounts | Total no. of investors in Luxembourg investment funds | Portion of no. of accounts blocked of the total no. of investors in % |
|------|-------------------------|---|---|
| 2019 | 89 814 | 861 108 | 10.43% |
| 2020 | 85 241 | 978 654 | 8.71% |
| 2021 | 85 822 | 1 029 035 | 8.34% |

359. Whilst some of these remediation programmes and blocked accounts may stem from inadequacies in the application of CDD in the years prior to the review period or arise from regulatory changes, it would appear that inadequate CDD has been held by FIs for a significant number of customers, including investors in Luxembourg collective investment schemes, during the review period. There have been CDD deficiencies on customer relationships (including investors into collective investment schemes whose accounts have been blocked) as well as in the life insurance sector which are still being managed. For the insurance and investment sectors, the risks are however mitigated as no pay-outs or redemptions to investors would be made if the CDD is incomplete.

360. FIs met refuse business or terminate business relationships when CDD is incomplete or when the BO information provided does not correspond with that in the RBE. Statistics from the CSSF show that banks reported 1 225 instances to the CRF-FIU where business was refused on ML/TF grounds (between 2018 and 2020). The CAA recorded a refusal rate of 0.03% per year: e.g., in 2021, of the 56 new contracts refused for ML/TF reasons, including concerns with the CDD, 24 were reported to the CRF-FIU.

VASPs

361. VASPs adequately apply CDD and record-keeping measures. CDD includes identifying, verifying and screening the beneficial owner for new and existing customers. Checks also capture the identity, address and VPN of clients. VASPs use blockchain analytics software to monitor and analyse ongoing customer transactions and conduct manual checks on clients classified as high-risk, such as PEPs. VASPs met explained that it is considered challenging to ensure on-going monitoring and implementation of the travel rule as the sector is fast-moving and technologically dynamic.

DNFBPs

362. Compliance with CDD and record-keeping measures by DNFBPs is mixed. The extent and degree of CDD, as well as the type of documents collected, varies among sectors. The majority of DNFBPs have a good level of CDD application and verification and ongoing monitoring. They use sophisticated (IT) tools and regularly consult the basic and BO registers (RCS and RBE). In general, DNFBPs do not enter a business relationship when CDD is incomplete.
363. Business/office centres and professional directors supervised by the AED (TCSPs) conduct good CDD, verify beneficial owners and do on-going monitoring. When dealing with sophisticated clients and structures, these DNFBPs find it sometimes challenging to understand the source of funds, and to confirm who the beneficial owners are and how they control the structures. Professionals met explained that if they note that the risk of tax crime is high and they do not fully understand the structure of the company, they conduct additional checks until they are satisfied. Supervisors observed limited issues relating to incomplete documentation of information, insufficient scrutiny of transactions throughout the course of the business relationship and keeping information up to date.

364. The assessment team observed that REAs and DPMS conduct limited checks on clients: they ask for the client ID and in some cases conduct client verification through Internet searches, especially when the client is from abroad. They check the source of funds and the client's financial capacity for certain large transactions. In case of doubt, some entities met noted that they consult with the CRF-FIU. One larger real estate firm, that also has investors as clients, mentioned that they may consult the RCS and RBE. Supervisory observations by the AED revealed deficiencies related to the actual identification of customers and frequency of checking the identity of customers and beneficial owners, keeping sufficient documentation and ongoing due diligence. Accounting professionals verify the client ID, the beneficial owners of clients interested in real estate investments (usually corporate clients) and whether the lifestyle of the clients would be in line with the business expectations. The casino verifies client ID and ensures that casino personnel understand the details of a potential player playing on behalf of someone else and the relationships between players.
365. When it comes to the sectors supervised by the SRBs (lawyers, notaries, CPAs and statutory auditors), these conduct significant checks when onboarding new customers to ensure that they have a good understanding of the client, the origin and destination of funds, the geographic context, and they analyze the full structure of the business and the economic reasons behind it. For instance, notaries met explained they perform checks on the source of funds and the financial capacity of the buyer and the seller's reasons for selling when conducting real estate transactions, which are assessed as higher risk activities. Lawyers monitor higher risk clients on a frequent basis: depending on the size of the firm and risk of the clientele that they serve, these range from weekly checks to checks every six months, which is commensurate to the risk.

Application of EDD measures

FIs

366. Application of EDD measures vary among FIs depending on the EDD measure but is now generally sufficient.
367. *PEPs*: Almost all FIs have formulated policies and measures for identifying PEPs and entering or continuing a business relationship with a PEP. This includes senior management sign-off for new or continuing a PEP relationship, screening on a monthly if not daily basis for large firms and monitoring of transactions at a lower monetary threshold than for standard risk. Once a customer is no longer a PEP, the FIs met explained they will declassify the PEP status only if lower risk can be established. They also noted that most PEPs they service, are nationals from Luxembourg or come from other EU Member States. Overall, the CSSF and CAA identify few deficiencies in the FI sectors. However, there had been significant deficiencies within some private banks – which is considered as a higher risk sector – as shown by substantial penalties levied by the CSSF between 2018 and 2021. These gaps in the application of the EDD measures concerned for instance not sufficiently understanding and verifying the source of funds and wealth, which have been remediated in recent years.

368. *Correspondent banking:* Luxembourg banks offer limited correspondent banking service and no payable-through accounts. Correspondent banks apply appropriate controls to their correspondent banking relationships. Out of thirteen banks offering correspondent services to 264 correspondent banks, mainly based in Europe, six banks offer correspondent relationships to correspondent banks within the group and seven offer correspondent relationships to external banks (non-group). Five Luxembourg banks dominate the market, serving about 85% of the total correspondent banks. Relationships with correspondent banks are subject to EDD utilising for instance the Wolfsberg Groups CBDD questionnaire.
369. There is significant use of correspondent services in the investment sector which relies on professional intermediaries for fund distribution. Data from the CSSF indicates that at the end of 2021, 53% of investor holdings in Luxembourg collective investment schemes were held by cross-border credit institutions, mostly within Europe. Banks and other FIs providing transfer agency services apply robust CDD to the intermediaries and risk rate those relationships taking into account the intermediary's investor base. Their distribution agreements include caveats that the intermediary must inform the transfer agent of any material matters regarding underlying investors including if there is a TFS-listed person. There was evidence that these contracts are effective as intermediaries were giving notice of PEPs or persons designated under EU, US or UK sanctions lists. This enabled the transfer agent to apply appropriate controls and block or ring-fence affected share/unit holdings. Some transfer agents also sought the identity of any underlying beneficial owner for whom the intermediary is acting and who owns 10% or more of the intermediary's investment in the scheme. Supervisory findings from 2020 show that 99% of the IFMs apply EDD on cross-border intermediaries.
370. *New technologies:* FIs analyse new technology products and services for ML/TF risks prior to their introduction to the market. This includes assessing their impact on transparency of the identity of the customer, the beneficial owner or source of funds, complexity of technology as well as security concerns. There were some minor deficiencies in the insurance sector: in 2020 and 2021, the CAA observed an insufficient formalization of the ML/TF assessment prior to the launch of new products or the use of new technologies at two life insurance undertakings and one broker. FIs met noted that they have little to no appetite to provide services in connection with virtual assets but are considering or piloting the use of biometrics and artificial intelligence respectively for verification within remote customer onboarding and ongoing monitoring.
371. *Wire transfers:* banks, PIs and EMIs use automated tools to screen wire transfers and have specific procedures to deal with missing information from a transfer. The CSSF identified breaches in two banks in 2018 relating to a failure to identify missing information of incoming payments and a lack of formal procedures. The assessment team shares the view of the CSSF that FIs apply appropriate controls to wire transfers. In 2020, FIs rejected more than 70 000 incoming transfers for missing information which represent less than 0,05% of the total incoming transfers.

372. *TF-TFS*: FIs met are aware of the obligation to freeze without delay and many use automated tools to screen the UN and other sanction regimes. They explained that their monitoring and screening identifies sanctioned persons within 24 hours after a designation and if a hit appears, they know to report. Most FIs will report to the MoF, as required under the TFS regime, but the investment firms met did not know to which authority these reports should be made. For banks and most other FIs daily screening of the client database covers customers, beneficial owners and any other related party. For FIs providing investment services, such as administering investment schemes or providing transfer agency services, the screening also includes investors, the promoters and service providers of the investment scheme and assets held by those schemes. For collective investment schemes, where transfer agents, advised by an intermediary that one of its clients is sanctioned, the shareholding would be segregated and blocked in case of a hit. The CSSF identified weaknesses in some sectors, but deficiencies were not significant (mainly concerned the frequency of screening) and mostly dealt with through observation letters rather than injunctions, and promptly remediated by FIs. However, the CSSF did for example sanction one bank in 2019 and issued an injunction letter against one specialised PFS in 2020 over IT failures which adversely affected the automated screening of the FI's client database.
373. Approximately 40% of insurance brokers, and a few undertakings, have no automated screening tools and instead conduct manual checks or outsource screening to other FIs. The CAA identified a few brokers who do not regard sanctions to be applicable to them, which it has been addressing through guidance provision. The CAA has issued a small number of injunctions against life insurers and brokers.
374. *Higher-risk countries*: FIs met satisfactorily apply EDD to transactions, customers and related parties and beneficial owners when there is a connection to a higher-risk country identified by the FATF, the EU or the FI's own listing. This is also confirmed by the CSSF and CAA. PIs and EMIs met indicated that they prohibit sellers from higher-risk jurisdictions such as Iran and DPRK.

VASPs

375. VASPs interviewed implemented EDD measures on an ongoing basis, including PEP screening, requesting more information from higher risk customers and monitoring customers and transactions against TFS lists. One VASP indicated that they complement the use of IT tools with manual checks. They are aware of their obligations regarding virtual assets transfer rules and explained the measures that they are working on to that effect.

DNFBPs

376. Implementation of EDD measures vary among the DNFBP sector but is generally done well except for REAs and DPMS but their customers are mainly based in Luxembourg. Most DNFBPs (business/office centres, professional directors, statutory auditors and audit firms, lawyers, notaries, CPAs, the casino) screen against PEPs, TFS and higher-risk countries lists using automated IT tools, which some obtained from their supervisors (e.g., lawyers and notaries), supplemented by manual controls (e.g., CPAs, lawyers, notaries). Where the customer is a legal person, the corporate structure is also checked against these lists. Depending on the size of the firm and the client base, checks are carried out on a daily, monthly or three-monthly basis, with several DNFBPs also frequently testing the accuracy of the lists (e.g., CPAs).
377. A few DNFBPs (TCSPs, lawyers) met explained that their regular monitoring led to hits of clients on or linked to non-UNSCR TFS lists. In those circumstances they liaised with the MoF. Smaller entities, whose clients are mostly based in Luxembourg, also do not screen against TFS lists and are not fully aware where to go when they have a hit – instead they submit an STR with the CRF-FIU or seek advice from the CRF-FIU or the Chamber of Commerce.
378. Some DNFBPs have lowered their risk appetite and therefore go beyond the FATF's designation of higher-risk countries and consequently refuse business (e.g., notaries, CPAs). REAs and DPMS experience difficulties in verifying PEPs and rely on the relationship with their clients. Most REAs and DPMS met had a limited awareness of lists of high-risk countries, but this concern is limited as most of their clients are based in Luxembourg. Accounting professionals met were small firms that had no dealings with PEPs and had no clients from higher-risk countries; only one firm has a few clients from other EU countries. During the interviews, a majority of REAs and DPMS noted that they had known a large part of their clients for a long time and that when they were unsure about a client, they conducted Internet checks. Although their understanding of EDD was theoretical, the assessment team considers it to be proportionate to their risk exposure.

Reporting obligations and tipping off**Table 5.3. Number of STRs received by the CRF-FIU, 2017-Q3 2022**

| Reporting Entities | 2017 | | 2018 | | 2019 | | 2020 | | 2021 | | Q3 2022 | |
|--|-----------|-----|-----------|-----|-----------|-----|-----------|-----|-----------|-----|-----------|----|
| | ML | TF | ML | TF | ML | TF | ML | TF | ML | TF | ML | TF |
| Banks | 1 650 | 15 | 2 050 | 20 | 2 542 | 19 | 2 392 | 25 | 2 552 | 15 | 2 054 | 8 |
| Insurance sector | 176 | 2 | 202 | 1 | 247 | 3 | 220 | 2 | 305 | 5 | 273 | 0 |
| Securities sector | 128 | 1 | 169 | 1 | 173 | 1 | 243 | 5 | 254 | 1 | 231 | 1 |
| Investment firms | 26 | 0 | 39 | 1 | 41 | 0 | 54 | 0 | 106 | 1 | 56 | 0 |
| Other professionals of the financial sector | 261 | 2 | 304 | 1 | 282 | 0 | 291 | 12 | 319 | 3 | 241 | 1 |
| Entities operating online | | | | | | | | | | | | |
| Banks (operating online) | 3 879 | 219 | 3 623 | 370 | 3 339 | 352 | 2 550 | 342 | 2 627 | 198 | 2 315 | 92 |
| Electronic money institution* | 31 334 | 92 | 47 020 | 45 | 42 411 | 58 | 26 761 | 57 | 30 099 | 52 | 11 924 | 38 |
| Payment institution* | 50 | 2 | 136 | 1 | 388 | 1 | 1 178 | 1 | 8 783 | 7 | 22 | 8 |

| Reporting Entities | 2017 | | 2018 | | 2019 | | 2020 | | 2021 | | Q3 2022 | |
|-------------------------------------|---------------|------------|---------------|------------|---------------|------------|---------------|------------|---------------|------------|---------------|------------|
| | | | | | | | | | | | 821 | |
| VASP** | 294 | 1 | 1 040 | 1 | 1 648 | 4 | 5 445 | 6 | 3 230 | 31 | 1 381 | 13 |
| Total financial institutions | 37 798 | 334 | 54 583 | 441 | 51 071 | 438 | 39 134 | 450 | 48 275 | 313 | 41 296 | 161 |
| DNFBPs | | | | | | | | | | | | |
| Casino | 26 | 0 | 25 | 0 | 32 | 0 | 17 | 0 | 22 | 0 | 35 | 0 |
| Real Estate | 3 | 0 | 4 | 0 | 10 | 0 | 6 | 0 | 8 | 0 | 18 | 1 |
| Dealers in goods (including DPMS) | 6 | 0 | 3 | 0 | 6 | 0 | 11 | 0 | 26 | 0 | 8 | 0 |
| Lawyers | 19 | 0 | 72 | 1 | 56 | 0 | 124 | 0 | 92 | 1 | 47 | 1 |
| Notaries | 4 | 0 | 6 | 0 | 51 | 0 | 40 | 0 | 57 | 1 | 60 | 1 |
| Accountants | 116 | 1 | 135 | 2 | 166 | 0 | 173 | 0 | 218 | 2 | 147 | 3 |
| (Approved) statutory auditors | 46 | 0 | 42 | 0 | 39 | 0 | 39 | 0 | 22 | 0 | 48 | 2 |
| Tax advisors | 4 | 0 | 3 | 0 | 8 | 0 | 8 | 0 | 13 | 0 | 9 | 0 |
| Total DNFBPs | 224 | 1 | 290 | 3 | 368 | 0 | 418 | 0 | 458 | 4 | 372 | 8 |
| Other reporting entities*** | 349 | 38 | 592 | 39 | 491 | 6 | 776 | 4 | 1143 | 4 | 647 | 3 |
| Grand Total | 38 371 | 373 | 55 465 | 483 | 51 930 | 444 | 40 328 | 454 | 49 876 | 321 | 42 315 | 172 |

*Note: Luxembourg explained that the fluctuation in numbers between 2021 and Q3 2022 for EMIs and PIs arises from a further refinement of the reporting process on a firm-by-firm basis by the CRF-FIU for EMIs and PIs, and the structural changes due to Brexit.

**Note: The VASPs registration regime came into effect in 2020. Prior to this, some obliged entities, licensed as a bank or PI, were providing VA services and as such they are counted for in the table under the VASP heading for 2017-2019.

***Note: Reports submitted, and explicitly flagged as such in goAML, by business/office centres and professional directors supervised by the AED are part of this category.

379. Annually, EMIs, PIs and banks report the most. About 99% of reports have been received through goAML. By the end of the on-site visit, approximately 44% of all FIs⁴⁰ and DNFBPs were registered with goAML. The CRF-FIU and supervisors encourage all obliged entities to register with goAML and optimise the submission of reports. In general, the quality and relevancy of TF-related reports submitted by most obliged entities remains a concern as the level of TF reporting is extremely low. It is not clear whether there are reports that include the aspect of financing or if they are all related to terrorism itself. This links back to the need for the private sector to further develop its TF risk understanding (see section 5.2.1; IO.1). Adverse media is a valuable indicator for suspicion, particularly when analysed by the obliged entity to establish an actual suspicion of ML/TF. The CRF-FIU provided statistics indicating that most of the STRs filed based on adverse media hits included some level of analysis. However, some FIs and a large number of DNFBPs and VASPs met by the assessment team, indicated that they provided STRs based on adverse media without further analysis of the client file.

⁴⁰ This percentage does not include the intermediaries in the insurance sector as STRs related to intermediaries are filed by life insurance undertakings and brokerage firms. For the financial sector under the supervision of the CSSF, 95% of the obliged entities are registered with goAML.

FIs

380. The CRF-FIU received more than 48 000 SARs/STRs from FIs in 2021 (see Table 5.3). FIs generally understand their reporting obligations and their filing pattern is in line with the transactional levels associated with different products and services offered. Data on FI reporting demonstrates that high frequency transactional services (e.g., by retail banks, banks operating online and EMIs) have a higher reporting level than low frequency transactional services (e.g., by life insurance undertakings, investment and private banking, where many services are provided on a discretionary management basis by the FI). However, FIs met submit SARs/STRs driven by adverse media hits, which can be a valuable indicator for suspicion, but they do not always make a link between the adverse media and actual suspicion of ML/TF. The CRF-FIU and the CSSF regard the quality of reports submitted by FIs as good. However, the CRF-FIU issued the report quality feedback letters to about 270 FIs and DNFBPs in the first 14 months of an initiative introduced in June 2021 which indicates that there is room for improvement.
381. More than half of the reports are submitted by EMIs with a portion relating to forged documents (e.g., identity documents, BO declarations, loan or consultancy agreements). One bank also files a large number of SARs which is consistent with the volume and type of customers they service. In the insurance sector, there has been a significant increase since 2017: FIs filed 56% more reports in 2017 compared to 2016. Authorities explained that this is due to the legislative change making tax crime a ML predicate offence in Luxembourg as of 2017. Fraud and tax offences are the most common drivers for reports, with a small percentage (2-4%) of these filings concerning clients of FIs being a victim of fraud rather than a suspected perpetrator.
382. Many FIs met file SARs based on their clients being negatively featured in the press (adverse media). Luxembourg authorities explained that the CRF-FIU largely encourages FIs to consider negative media reports as an indicator of suspicion and to report their analysis to the CRF-FIU. While some FIs submit reports without further analysis of the client file to determine if there is cause for an actual suspicion, supervisory authorities and the CRF-FIU have insisted on the necessity for FIs to assess and integrate all relevant information (e.g., CDD, transactions) in a SAR/STR. The CRF-FIU acknowledges, where reports result from adverse media hits, it works with FIs and supervisors to further develop reporting based upon an analysis of the business relationships and transactions. The CSSF encourages FIs to report if in doubt. For example, the CSSF department dedicated to the specialised PFS (PSF-SP) focused its efforts in 2020 on clarifying that SAR/STRs are required when activities are only dubious, and do not require certainty/proof of illicit activity. FIs established internal procedures and provide regular training to staff on the reporting obligations, including on red flags, the internal escalation process before a suspicion is reported to the CRF-FIU and on measures to prevent tipping-off.

VASPs

383. VASPs are aware of the requirement to submit SARs/STRs. This is due to the extensive outreach by the CSSF and the CRF-FIU. VASPs have been filing a large number of SARs/STRs: one VASP submitted eight hundred reports in 2021 alone. Many of the SARs/STRs are batch reports concerning forged ID documents or an adverse media hit where VASPs have not always made a link to an actual suspicion of ML or TF. Authorities report that these reports are of good quality. No tipping-off issues have been noted so far.

5

DNFBPs

384. There is an upward trend in reporting by DNFBPs in recent years. However, the levels are low for all DNFBPs, except for the casino and accountants, when compared to the size of the sectors and Luxembourg's exposure to ML as an international financial centre. For example, REAs have a very low reporting activity, with only eight SARs/STRs submitted in 2021, which is not in line with the high vulnerability and turnover of the sector. The CRF-FIU and AED recognize that this is an issue and are providing additional guidance and training to the sector. Also, the CRF-FIU is vigilant and requests information about clients and transactions directly from REAs.
385. Supervisory inspections by the AED reveals that REAs, DPMS and TCSPs (business centre/office) have difficulties submitting timely reports. The AED and SRBs encourage and verify that all obliged entities sign in to goAML so that reporting can be conducted quickly if a suspicion arises. The quality of reporting by REAs is low.
386. DNFBPs follow the instructions and recommendations of their supervisors on reporting obligations. A large number of submitted STRs concern forged documents or are triggered by hits with adverse media articles discovered in CDD processes and ongoing client monitoring, which can be a valuable indicator for suspicion. However, a large number of DNFBPs met by the assessment team submit such STRs without further analysis. Supervisors and the CRF-FIU undertake outreach activities, including providing feedback, to ensure that reporting obligations and expectations regarding the quantity and quality of STRs/SARs is understood and improves, and provide some level of guidance (see section 6.2.6). However, some DNFBPs, notably the REAs and DPMS, met during the on-site visit would welcome sector-specific practical guidance, which could include red-flag indicators, typologies reports and concrete examples of suspicious activities to allow them to develop a better understanding of suspicious transactions and activities, and raise the quality of reporting. DNFBPs are aware of their obligation to avoid tipping off customers when they make an SAR/STR.

Internal controls and legal/regulatory requirements impending implementation**FIs**

387. Many of the FIs met had strong internal control and group-wide policies in place adapted to Luxembourg's obligations where requirements differ. FIs that were part of a group confirmed that there were no barriers to sharing information at group-level. Many FIs indicated how stringent the regulatory environment in Luxembourg had become.

388. FIs generally have good risk-based and up-to-date internal controls and procedures, which are regularly reviewed. To this effect, FIs invested significant resources establishing the three lines of defence model (operations, compliance and internal audit), with the external statutory auditor being the fourth line of defence. Internal policies and procedures include guidance to staff on red flag indicators that would prompt reporting to the CRF-FIU, and dedicated AML/CFT training to staff. Most FIs vet their staff and have established internal controls regarding professional conduct such as conflict of interest for management functions.

VASPs

389. VASPs have good internal AML/CFT controls and procedures, including a compliance officer and a permanent control team. VASPs met have group-wide policies and adapted their compliance procedures to their business in Luxembourg and the Luxembourg regulatory requirements. VASPs also provide regular mandatory and non-mandatory AML/CFT training to all staff.

DNFBPs

390. Most DNFBPs have compliance programmes, including checks when hiring staff, ongoing AML/CFT training programs and internal audit functions. They explained that their internal compliance procedures are regularly reviewed and updated. However, for some sectors these internal procedures have been put in place more recently. Large firms have group-wide procedures in place and appoint compliance officers while in smaller obliged entities the compliance function is usually exercised by the owners, who take their responsibilities seriously. Some supervisors noted issues relating to insufficient documentation of procedures or staff training. The REAs and DPMS, irrespective of their size, often lack good quality internal compliance programmes. The AED noted that these professionals often rely on procedures prepared by consultants and are not adapted to their businesses. The REAs and DPMS also provide limited training to their staff and there is a lack of awareness of the training offered by the AED.

Overall conclusions on IO.4

Preventive measures by FIs, DNFBPs and VASPs are steadily improving, and this largely correlates to the increasing robustness of supervisory activities for most sectors or from sharing of good practices for example by the CSSF for sectors offering TCSP services. Implementation is stronger for FIs, including the heavily weighted sectors, than for DNFBPs and VASPs. In particular, smaller DNFBPs and the REAs and DPMS face challenges implementing AML/CFT measures effectively, which likely arises from a less developed understanding of their ML/TF risks and AML/CFT obligations. The assessment team gave more weight to the issues concerning professionals in higher risk sectors.

There are major shortcomings in the understanding of TF risks across the private sector, in terms of awareness of TF exposure and the TF methods used. This is not in line with Luxembourg's risk profile as a jurisdiction with very significant cross-border financial flows, large sectors and high number of entities having a significant non-resident client base.

Furthermore, there are major shortcomings in compliance with reporting obligations. In addition, the quality and relevancy of TF-related reports submitted by most entities is low and many reports are driven by adverse media hits, which can be a valuable indicator for suspicion. The CRF-FIU provided statistics indicating that most of the STRs filed based on adverse media hits included some level of analysis. However, some FIs and a large number of DNFBPs and VASPs met by the assessment team indicated that they provided STRs based on adverse media without further analysis.

When it comes to the application of EDD measures, they are generally adequately applied, except by REAs and DPMS. However, the processes to report TFS positive matches are not well understood by some investment firms and DNFBPs, and some smaller DNFBPs do not screen against TFS lists.

Luxembourg is rated as having a Moderate level of effectiveness for IO.4.

Chapter 6. SUPERVISION

Key Findings and Recommended Actions

Key Findings

1. In recent years, Luxembourg undertook steps to harmonize DNFBP supervision and the CSSF became responsible for registering and supervising VASPs. The quality of supervision varies among the eight AML/CFT supervisors with the CSSF and CAA performing stronger than DNFBP supervisors. All regulated activities under the FATF Standards are supervised for AML/CFT compliance in Luxembourg; with the supervision of professional directors (TCSPs) by the AED just started.
2. Luxembourg has robust market controls to prevent criminals and their associates from entering the market and supervisors routinely check to ensure that unlicensed or unregistered activity is detected.
3. Supervisors identify and maintain an understanding of ML/TF risks in their supervised sectors and individual professionals. The CSSF and CAA have a well-informed ML/TF risk understanding at a national, sectoral and firm-specific level. DNFBP supervisors have varied levels of ML understanding and a less sophisticated TF risk understanding, which is starting to evolve with the recent May 2022 TF VRA that would need further integration into their work.
4. All supervisors use a range of supervisory tools, including on- and off-site inspections, with varying degrees of effectiveness. The CSSF has the most advanced use of its tools, which it shares with other supervisors, and uses a multipronged approach by combining off-site monitoring with on-site inspections. DNFBP supervisors are in the early stages of developing their methodology for a risk-based approach to supervision. Limited resources and organisational set-up impede AED's, CdN's and OEC's ability to carry out their supervisory tasks.
5. Where enforcement measures to address non-compliance are used, principally by the CSSF, these have been dissuasive but public statements on enforcement cases convey very limited information on the nature of breaches to assist FIs in understanding what would constitute significant deficiencies thereby undermining the effectiveness. Also, sanctions against individuals are rarely public. The CAA applies a very small number of enforcement measures. As for the DNFBP sectors, there is a mixed landscape, with sanctions that are not considered to be sufficiently dissuasive or effective for REAs and DPMS, and not imposed for the notary sector.

6. FI and some DNFBP supervisors demonstrate the positive impact of their actions and outreach on supervised entities in promoting general understanding of their risks and obligations, curbing their risk appetite, and developing internal procedures and controls. However, some supervised sectors would benefit from further guidance on the understanding of TF risks and TFS obligations.

Recommended Actions

1. Improve risk understanding
 - a) The AED and SRBs should deepen their understanding of TF risks at national and sectoral levels.
 - b) The CSSF and CAA should consider updating their SSRAs following the 2022 TF VRA.
 - c) The AED should deepen its understanding of ML/TF risks of the real estate, DPMS and TCSP sectors by conducting more thorough and systematic risk assessments for each sector it supervises.
2. Enhance risk-based supervision
 - a) The AED should start AML/CFT supervisory inspections of professional directors under its supervision.
 - b) The AED and OEC should increase staffing to enhance risk-based supervision. The AED, in particular, could revisit its approach towards Luxembourg's one casino, while ensuring good performance is sustained.
 - c) Luxembourg should take further steps to increase the independence and strength of CdN, including by hiring more independent compliance officers to conduct off-site and on-site inspections.
3. Enhance remedial actions and sanctions
 - a) The CSSF should ensure that public statements on enforcement measures contain sufficient information for FIs to understand the nature of deficiencies and should publish sanctions on individuals on a case-by-case basis.
 - b) The CAA should make use of the sanctions available for non-compliance including sanctions on individuals where appropriate.
 - c) The AED, should increase remedial actions for the DNFbps it supervises to ensure that they are effective, proportionate and dissuasive and CdN should consider using all remedial actions that are available to them, including fines to ensure that they use the appropriate tool in all cases.

4. Improve awareness

- a) The AED and some SRBs should increase guidance on AML/CFT risk assessments and obligations, including the provision of concrete examples where appropriate, and a heightened focus on obligations related to TFS.
- b) Supervisory authorities should develop typologies and conduct outreach to further raise awareness and understanding of TF among obliged entities.

391. The relevant Immediate Outcome considered and assessed in this chapter is IO.3. The Recommendations relevant for the assessment of effectiveness under this section are R.14, 15, 26-28, 34, 35 and elements of R.1 and 40.

Immediate Outcome 3 (Supervision)

392. The conclusions in IO.3 are based on statistics and examples of supervisory activities and actions provided by Luxembourg; guidelines and guidance issued by the supervisors, documents used to monitor the different reporting sectors; discussions with the CSSF, CAA, AED and SRBs, as well as FI, DNFBP and VASP sector representatives and professional associations.
393. The assessment team weighted positive and negative aspects of supervision **most heavily** for banks, Investment Fund Managers (IFMs) and Specialised PFS (TCSPs); **heavily** for investment firms, notaries, lawyers, Chartered Professional Accountants (CPAs) and real estate agents (REAs); **moderately heavy** for Payment Institutions (PIs), E-Money Institutions (EMIs), life insurance undertakings and brokers, PSAs (TCSPs), DPMS, TCSPs (provided by professional directors and business/office centres supervised by the AED as well as statutory auditors and audit firms), and VASPs; and **less heavily** for the casino and accounting professionals. This weighting is based on the relative importance of each sector and Luxembourg's risks, context and materiality, as explained in Chapter 1.
394. The CSSF supervises the majority of FIs (e.g., banks, investment firms and IFMs, EMIs/PIs) and VASPs. The CAA supervises the insurance sector.⁴¹ The AED supervises REAs, DPMS, the casino and accounting professionals. Self-regulatory bodies (SRBs) supervise notaries (CdN), lawyers (OAs) and CPAs (OEC). Trust and company services are provided by various professionals and are therefore supervised by multiple supervisors: banks (CSSF), investment firms (CSSF), specialised PFS (CSSF), PSAs (CAA), lawyers (OAs), statutory auditors and audit firms (IRE), CPAs (OEC), business/office centres and professional directors supervised by the AED. See Chapter 1 for an overview and description of the licensing/registration authority and supervisor for each sector. TCSPs offered by banks, investment firms and specialised PFS and PSAs are considered as part of the sections on FI supervisors as these professionals are supervised by the CSSF and CAA respectively. Other professionals with TCSP activities are covered in sections on the AED or SRBs, unless otherwise stated.

⁴¹ Note that some intermediaries are supervised by both the CAA and CSSF or the AED depending on the activities provided: e.g., a credit institution under the supervision of the CSSF which has also been licensed to act as an insurance brokerage firm. Some pension fund management companies licensed and supervised by the CAA (i.e., PSAs) are also licensed as liability managers under the CSSF.

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

395. Market entry controls are robust across the board. Licensing, registration and fit and proper tests to prevent criminals and their associates from entering the market are generally strong. Also, supervisors routinely conduct checks to ensure that unlicensed or unregistered activity is detected, and professionals promptly report any suspicion of unlicensed or unregistered activity.

CSSF (FIs, VASPs, specialised PFS and statutory auditors)

396. The CSSF examines the market entry of banks, investment firms, IFMs, PIs/EMIs, VASPs, specialised PFS, statutory auditors and audit firms. Fit and proper checks are done upon application; when there is a change in business model prompting a new or additional license (e.g., investment fund managers are required to apply for an extension to manage a new set of asset classes); and when there are changes to the authorised managers, directors, key function holders (e.g., the AML/CFT compliance officer) and beneficial owners. Applications are handled within the dedicated sectoral departments at the CSSF. For banks, except branches of non-EU foreign banks, the ECB decides on license applications based on the CSSF's recommendations.
397. The licensing regime has five main steps: (1) pre-application interaction, (2) formal application, (3) assessment of the application by the CSSF, (4) decision and (5) post-application checks. The CSSF engages with the potential applicant before the formal application to discuss and understand the projected business plan. This pre-application interaction serves as a filter to discourage licensing requests that are not likely to be successful. When assessing the formal application, the CSSF conducts several prudential and AML/CFT-related checks, including adequacy of mitigating measures and assessment of ML/TF risks. Fit and proper tests of the management, shareholders, beneficial owners and AML/CFT compliance officer, cover at a minimum screening of the CV, criminal records, TFS and PEP lists and adverse media. Additional checks through open-sources and consultations with domestic (e.g., CRF-FIU) and foreign competent authorities are carried out, if relevant. The CSSF conducts a *visite d'accueil* within the year after the license has been granted, verifying the appointed management and compliance with the licensing requirements. Since 2020, the CSSF screens daily against Luxembourg Regulatory Enforcement, TFS and PEPs lists. Overall, there are limited number of refusals as the process is quite robust and comprehensive, and less credible applicants are discouraged during the pre-application phase to proceed with their application (see Figure 6.1).

Figure 6.1. Summary and breakdowns of licensing applications and outcomes 2015-2021

| Outcome | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 |
|---------------------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| No. applications received | 50 | 44 | 37 | 56 | 50 | 44 | 24 |
| No. applications reviewed | 52 | 47 | 34 | 50 | 49 | 45 | 33 |
| of which withdrawn | 16 | 11 | 12 | 15 | 13 | 20 | 11 |
| of which rejected | 4 | 1 | 1 | 1 | 3 | 1 | - |
| of which approved | 32 | 35 | 22 | 34 | 33 | 24 | 22 |
| Banks | | | | | | | |
| No. applications received | 2 | 7 | 3 | 3 | 4 | 1 | 1 |
| No. applications reviewed | 5 | 4 | 3 | 2 | 4 | 2 | 2 |
| of which withdrawn | - | 2 | 1 | - | - | - | 1 |
| of which rejected | - | - | - | - | 1 | - | - |
| of which approved | 5 | 2 | 3 | 2 | 3 | 2 | 1 |
| PIs & EMIs | | | | | | | |
| No. applications received | 7 | 8 | 7 | 11 | 17 | 11 | 7 |
| No. applications reviewed | 3 | 5 | 7 | 7 | 13 | 14 | 12 |
| of which withdrawn | 2 | 2 | 5 | 5 | 9 | 6 | 7 |
| of which rejected | - | - | - | - | - | - | - |
| of which approved | 1 | 3 | 2 | 2 | 4 | 8 | 5 |
| Specialized PFS | | | | | | | |
| No. applications received | 5 | 2 | 8 | 9 | 3 | 9 | 6 |
| No. applications reviewed | 6 | 6 | 3 | 10 | 6 | 3 | 5 |
| of which withdrawn | - | - | - | 3 | - | 1 | - |
| of which rejected | 1 | 1 | 1 | 1 | 2 | - | - |
| of which approved | 5 | 5 | 2 | 6 | 4 | 2 | 5 |
| Investment Firms | | | | | | | |
| No. applications received | 6 | 4 | 2 | 9 | 6 | 7 | 3 |
| No. applications reviewed | 8 | 9 | 4 | 7 | 6 | 10 | 7 |
| of which withdrawn | - | 1 | 1 | 2 | - | 6 | 3 |
| of which rejected | 3 | - | - | - | - | 1 | - |
| of which approved | 5 | 8 | 3 | 5 | 6 | 3 | 4 |
| Authorized IFMs | | | | | | | |
| No. applications received | 30 | 23 | 17 | 24 | 20 | 16 | 7 |
| No. applications reviewed | 30 | 23 | 17 | 24 | 20 | 16 | 7 |
| of which withdrawn | 14 | 6 | 5 | 5 | 4 | 7 | - |
| of which rejected | - | - | - | - | - | - | - |
| of which approved | 16 | 17 | 12 | 19 | 16 | 9 | 7 |

Source: CSSF data for the financial sector.

398. Rejections and withdrawals are often related to insufficient AML/CFT procedures and inappropriate business plans. In the case of banks, it may also relate to financial soundness of the parent to protect Luxembourg's deposit guarantee scheme. The CSSF also considers the quality of home supervision and the extent to which the institution has a good working relationship with the home supervisor, and geographical risks.
399. To detect unauthorized activity, the CSSF co-operates with other domestic competent authorities and foreign supervisors, investigates reports received from obliged entities, service providers and whistle-blowers, and uses its own supervisory work. The CSSF often discovers fraudulent websites impersonating Luxembourg FIs. These cases are referred to the Public Prosecutor, and the CSSF publishes a warning on its website and sends a notification to its mailing list.

400. Since March 2020, the CSSF is responsible for the registration and supervision of VASPs. A similar market entry process for FIs applies to VASPs, including robust fit and proper assessments for managers, beneficial owners and compliance officers. There were nine VASPs registered in Luxembourg at the end of the on-site visit, with five of these already having a bank or PI/EMI license in Luxembourg. No applications were rejected, but several applicants withdrew their applications due to a change of business strategy, termination of business, or the lengthy registration process. To detect unregistered operations, the CSSF searches the Internet, the Trade and Company Register (RCS) and media. It also meets and exchanges with the CRF-FIU on a quarterly basis and liaises with the Luxembourg House of Financial Technology which acts as the first contact point for Fintech companies. The CSSF wrote to thirteen entities it suspected of providing virtual asset services. Out of these, four confirmed that they provide services based on reverse solicitation; the CSSF is still assessing the others. To confirm that the registered VASPs are conducting activities in line with their permits, the CSSF visits them six to twelve months after their registration and requires that they submit quarterly reports. So far, the CSSF has carried out four post-registration meetings in which it looked at the activities and the AML/CFT framework in place. When an entity would like to provide an additional virtual asset service, it must first update its registration with the CSSF.
401. For statutory auditors and audit firms the same fit and proper controls as described above are applied by the CSSF. Furthermore, for statutory auditors, the CSSF inspects the professional qualifications and administers the exams to become a statutory auditor. The CSSF communicates the list of statutory auditors and audit firms to the IRE on a weekly basis. The IRE (the AML/CFT supervisor) also carries out an on-site visit within two years post-registration and informs the CSSF of the results.

CAA (FIs and PSAs – insurance)

402. The CAA handles the licensing for life insurance undertakings, intermediaries (i.e., agencies, agents, brokerage firms, brokers and sub-brokers), professionals of the insurance sector (PSAs) and pension funds. The CAA meets with life insurance and pension fund applicants before a formal licensing request so the CAA can pre-screen applications that are likely to fail. As part of these pre-application meetings, the CAA scrutinises ownership structures to ensure stability of the proposed applicant given the longevity of life insurance and pension contracts. Consequently, no formal applications have been refused within these sub-sectors. A significant number of natural person applicants within the intermediary sector are largely refused based on failing to pass the required CAA exam.

403. The CAA applies fit and proper tests to all authorised managers, key function holders and beneficial owners across the sectors which include inspecting criminal records, declarations of non-bankruptcy and of honour, and screening names against TFS and PEP lists and adverse media. The fit and proper checks also cover shareholders and legal entities (including their natural person directors) acting as directors and are carried out on a regular basis (i.e., daily screening checks, periodical criminal record checks and annual supervisory reporting). Between 2017 and November 2022, the CAA received one application for life insurance activities. To detect unlicensed activities, the CAA regularly exchanges with competent authorities and insurance professional associations (ACA, APCAL, Reinsurance Managers Association), screens the RCS, uses whistleblowing reports and out-of-court complaint resolution.⁴²

Ministry of Economy (REAs, DPMS, accountants, TCSPs – business/office centres)

404. The Ministry of Economy (MoE) oversees the market entry controls and licensing process of REAs, DPMS, accounting professionals, CPAs and business/office centres. Before issuing the business license, the MoE examines the professional integrity of a wide range of stakeholders: the managing director, persons identified as “*gérant*” or administrator, board members that are officially listed on the RCS, majority shareholders and any person having significant influence on the management of the business, beneficial owners and possible associates when appropriate. The MoE checks criminal records and screens names against TFS and PEPs lists. The managing director and additional managers/board members/owners also need to complete a declaration on companies they were managing or had a major influence in during the previous three years. Internal checks are conducted to determine if the managing director already has one or more business licenses. Applications are routinely rejected on grounds of debt or lack of professional integrity, especially for real estate agents. No license request has been refused due to AML/CFT reasons specifically. The AED conducts additional checks in relation to potential tax issues (e.g., to ensure that managers, who may have managed other companies previously, do not owe any tax to the AED). For CPAs, once cleared by the MoE, they need to register with the OEC. The OEC then conducts full information check and due diligence (including TFS and PEP lists screening) on individual CPAs and structures.⁴³

⁴² The CAA receives and examines any claim from a natural person acting for purposes outside of his trade, industrial, craft or liberal activity and concerning insurance contract concluded or negotiated by any natural or legal person under its supervision.

⁴³ The OEC cannot refuse the registration once the license has been issued. However, if the CPA does not meet the requirements, it will not be registered as active and therefore the CPA will not be able to carry out business as one of the requirements is to be employed by a CPA firm.

AED (TCSPs- professional directors)

405. Fit and proper checks of professional directors started in February 2021, with the AED conducting full scope checks only as of 2022. Professional directors are natural persons and need to be registered with the AED, which maintains a list. The AED checks the ID documentation, criminal records, professional fiscal behaviour and screens against TFS and PEP lists. So far, no registration request has been rejected. AED uses checks against VAT registration to find possible professional directors that are not registered.

CdN (notaries)

406. Notaries are appointed by the Grand Duke on the proposal of the MoJ following the opinion of the General State Prosecutor and CdN. The number of notaries in Luxembourg is capped at 36 and no external ownership of notary firms is allowed. When a notary passes away, retires or is removed from office, a vacancy is issued. The MoJ co-ordinates the application and approval process, and consults the General State Prosecutor, for criminal background checks, and CdN to confirm the good character of the applicant. As supervisor, CdN checks twice a year whether notaries still fulfil good repute standards (including TFS screening and open-source searches). There was one case of an unlicensed notary providing notarial services, which CdN reported to the General State Prosecutor and the business subsequently ceased.

OAs (lawyers)

407. Lawyers must be sworn in before the Luxembourg Supreme Court and register with a Bar Council (OAs): either the Luxembourg Bar Council (OAL) or the Diekirch Bar Council (OAD). Both OAs check the fit and proper of the applying lawyer by inspecting qualifications, ID documents and criminal records. Both OAs also screen names against TFS and PEP lists, adverse media and incompatible commercial ties. If there is doubt, the person is called for a hearing before the Bar Council. Ten applications were refused during the review period. Once a year, all OAs' members are screened against TFS and PEP lists and adverse media. Law firms operating as legal entities must also be approved by the OAs and only registered lawyers can be owners or shareholders of the law firm. On an annual basis, both OAs review the managers, shareholders and beneficial owners of all firms.

Government Council (casino)

408. There is one licenced land-based casino in Luxembourg, with limited activities, since the 1980s. When an application is received, the MoJ prepares the file and sends it to the Government Council who is in charge of issuing the license. The authorization is for twenty years, with the last one granted in 2021: a license extension requires the same full process as a new application. The MoJ examines the professional integrity (including criminal record checks) of new directors, management, staff working in the gaming room of the casino and in direct contact with the customers, beneficial owners and shareholders (who have largely remained unchanged). The authorities have not received an application for more than a decade, as Luxembourg law requires casinos to be set up in the interest of tourism.

409. Online casinos are not permitted to operate in Luxembourg and authorities monitor to ensure such activities are not offered in the country. To this effect, the AED (the supervisor) annually checks URL addresses, using the central register for website addresses, against possible illegal domestic gaming offering. Geo-blocking prevents access from within Luxembourg to online casinos based outside of Luxembourg.

Supervisors' understanding and identification of ML/TF risks

410. Supervisors broadly have a better understanding of ML risks present in their respective sectors than for TF risks which has been improving through the development of the 2022 TF VRA, published in May 2022. This national-level work has not yet been fully integrated into the work of supervisors. Supervisors build their understanding through a range of information including NRAs, EU SNRAs, VRAs, SSRAs, annual AML/CFT questionnaires, supervisory work, regular interaction with the private sector, and documents published by the FATF, IMF and Europol. All supervisors participated in the 2020 NRA (update) by providing statistics, case studies and typologies, and continue to co-ordinate amongst each other and with other competent authorities on a regular basis (see IO.1).

CSSF

411. The CSSF has a good ML/TF risk understanding. At sectoral level, the CSSF assessed the risks of its higher ML/TF risk sectors, namely private banking, collective investments, TCSPs provided by specialised PFS, and agents and e-money distributors of PIs and EMIs established in other EU Member States. The CSSF is particularly attuned to the ML risks arising from tax crimes, which is one of the key ML threats identified in the NRA. It has published a guidance on tax crimes for FIs and recruited in-house tax specialists to provide training and to assist in supervision, including scrutinising proposed shareholder structures from a tax perspective. When it comes to TF risk, the CSSF demonstrated it assesses and understands risks stemming from FI products, services and clients, and low-level and high-level TF. This understanding has been gradually improving in the past years through national (NRAs, 2022 TF VRA) and supervisory work (SSRAs, off- and on-site supervision). Its supervisory work includes regular analysis of data collected from the Luxembourg Central Bank and from FIs from which links with certain jurisdictions can be discerned. For example, data on the origin and destination of financial flows assist its understanding of TF risks at sector and firm level as well as between banks. Its annual AML/CFT questionnaire requires FIs to provide geographical information of the client and assets held in the portfolio which the CSSF discusses issues in its annual meetings with bank compliance officers. It has also undertaken ad hoc exercise to understand the TF exposure of certain products for example analysing in January 2021, the controls within the collective investment sector to manage the TF risks stemming from charitable payments by Sharia funds, finding no major concerns. The CSSF also scrutinized PIs/EMIs flows, which showed extremely low level of direct financial flows to and from TF associated countries.

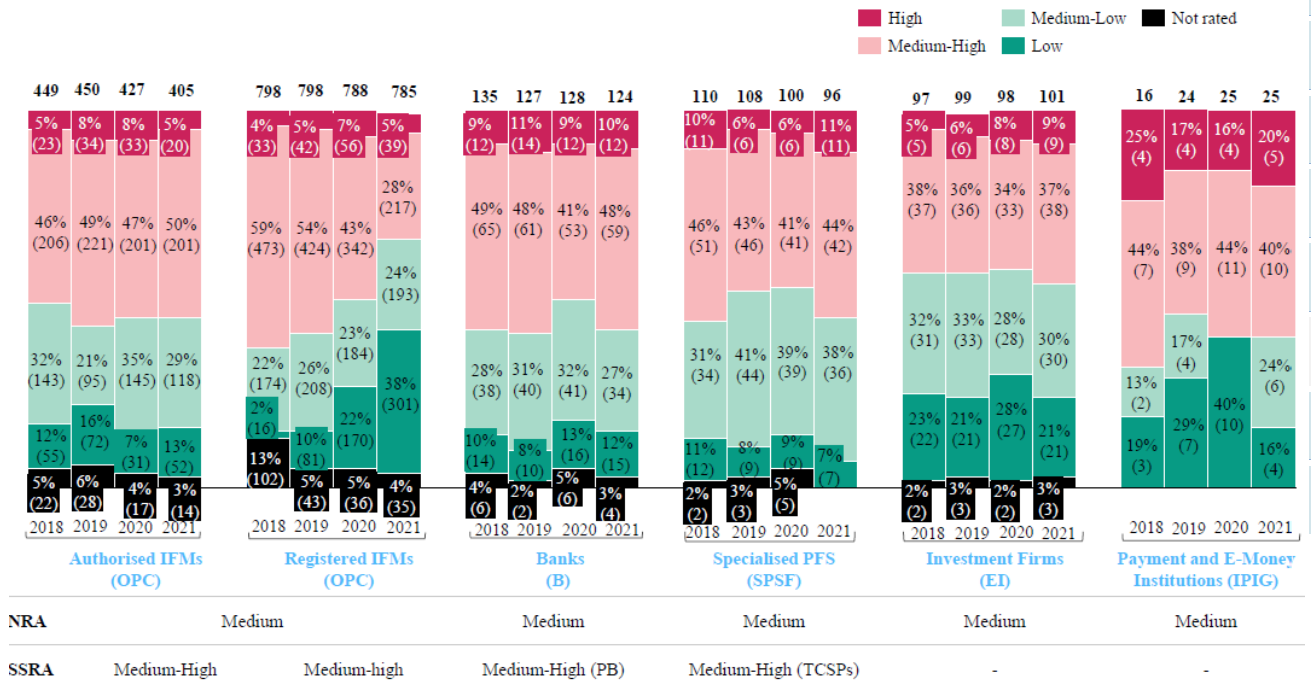
412. At the individual FI level, the CSSF risk assesses through comprehensive annual AML/CFT questionnaires tailored to each sector and which are adapted annually to take into account new threats and vulnerabilities. It also draws from the various risk assessments, guidance from international organisations, and its own supervisory experience and risk analysis. This model leads to a final risk scoring, which the assessment team considers sound. The risk score of an FI is re-assessed during the year in response to major events or changes. For example, in 2022 the risk score for 21 FIs was modified following acquisitions, whistleblowing reports, adverse media and outcomes of on-site inspections.
413. The CSSF started using its current model in 2017 for banks (utilising 2016 data) and in 2018 for other sectors (using 2017 data). In 2019, 106 FIs across all supervised sectors (7%) were categorised as high-risk, while the year following, in 2020 this figure increased to 119 FIs, representing 8% of the CSSF's supervised population (see Table 6.1). By 2020, the assessment covered over 1 500 CSSF supervised FIs. The IFM sector has the largest number of high-risk professionals (see Figure 6.2).

Table 6.1. High-risk professionals by sector, 2019-2021

| | 2019 | 2020 | 2021 |
|--------------------------------------|------|------|------|
| Total no. high-risk entities | 106 | 119 | 96 |
| % share of total entities | 7% | 8% | 6% |
| o/w Authorised IFMs | 32% | 28% | 21% |
| o/w Registered AIFMs | 40% | 47% | 41% |
| o/w Banks | 13% | 10% | 13% |
| o/w Specialised PFS | 6% | 5% | 10% |
| o/w Investment Firms | 6% | 7% | 10% |
| o/w Payment and E-Money Institutions | 4% | 3% | 5% |

Source: CSSF data for the financial sector

Figure 6.2. Residual risk distribution by sector, 2018-2021



Source: CSSF entity-level risk assessment results 2018-2021.

- 414. For VASPs, the CSSF uses various means to identify and understand the ML/TF risk exposure, including the dedicated 2020 VRA VA/VASP, meetings with VASPs and quarterly reporting by VASPs to the CSSF.
- 415. To further build and maintain its understanding, the CSSF established AML/CFT public private partnership (PPP) expert working groups,⁴⁴ involving various competent authorities (e.g., the CRF-FIU and for some the AED and a few SRBS) and professional associations representing a large portion of the supervised entities. These PPP working groups conduct ad-hoc risk analyses and produce outputs in response to trigger events such as the Panama Papers reports (see Box 7.1) and the COVID-19 pandemic.

⁴⁴ Collective Investment Expert Working Group (November 2018), Private Banking Expert Working Group (March 2019), Expert Working Group regarding Specialised PFS (September 2022).

CAA

416. The CAA understands the ML/TF risks for the insurance sector and at entity level to a good degree. The main ML threat is from tax and the TF risk is considered as low. The CAA explained that life insurance clientele largely comes from the EU (France, Italy, Belgium) and that products have a limited TF vulnerability. Various factors contribute to reducing the risk including the discretionary management of investments within policies by a professional who reports the assets to the CAA that the assets are deposited with a CAA approved custodian bank, and CAA approval is required for a life insurance undertaking seeking to distribute in a non-EU country. Furthermore, all insurance contracts include an exclusion clause from payout for participation in an armed conflict or suicide. The inherent ML/TF risk in the insurance sector is assessed as medium but the risk attributed to each sub-sector varies (see Table 6.2).⁴⁵ The CAA has further developed its actions to identify and maintain ML/TF risk understanding in recent years, becoming more structured since 2019 and now taking a similar form and process as that of the CSSF.

Table 6.2. Inherent and residual risk from the insurance sector and sub-sectors

| Sector | Inherent risk outcome | Residual risk outcome | Sub-sectors | Inherent risk Outcome | Residual Risk Outcome |
|-----------|-----------------------|-----------------------|--|-----------------------|-----------------------|
| | | | | | |
| Insurance | Medium | Low | Life insurers | High | Medium |
| | | | Intermediaries | High | Low |
| | | | Professionals of the insurance sector (PSAs) | Low | Low |
| | | | CAA-supervised pension funds | Very low | Very low |

417. For life insurance undertakings, the CAA collects AML/CFT data through annual questionnaires and, as of 2021, draws additional data from its prudential supervision reporting to get a granular understanding of the premia written by country of residency of the policy holders and jurisdictions of originating/destination banks of the insurance premium and pay-outs. For intermediaries, the CAA uses both prudential supervision reporting and the outcome of AML/CFT qualitative questionnaires, which have been completed for the first time in 2019 by the brokers to improve its ML/TF risk understanding. The CAA also issues ad hoc questionnaires on specific topics, such as tax crimes, cyber insurance and marine insurance. As a result of Brexit, several insurance undertakings moved to Luxembourg, including non-life business writing marine and kidnap for ransom insurance. The CAA closely co-operates with domestic competent authorities (e.g., CSSF, CRF-FIU) and foreign competent authorities (with other supervisors through supervisory colleges).

⁴⁵ The CAA produced SSRAs on life insurance, which is the highest risk sector within Luxembourg's insurance sector, brokers/brokerage firms and PSAs when providing TCSP services. No specific risk assessment has been carried out for insurance agents and agencies as their business is indirectly captured through CAA's supervision of insurance undertakings, from whom and behalf of whom they act. As intermediaries do not issue premiums, their residual risk is considered low.

AED

418. The AED has a mixed understanding of ML/TF risks of its supervised entities at sector-level but a good understanding at entity level. The AED piloted annual AML/CFT questionnaires in 2019 and started using them more broadly in 2020. These questionnaires have a well-rounded risk scoring. The questionnaires are used to assess risk of some supervised entities in the high-risk sectors (i.e., REAs, accounting professionals, TCSPs-business/office centres). The AED's comprehension of ML/TF risks is strong in relation to Luxembourg's only casino but is more recent and still developing for other sectors. For the REAs, the AED draws from the annual AML/CFT questionnaires; however, the quality of responses is low translating into a weaker risk understanding for the supervisor. When it comes to DPMS, the AED demonstrated a fair understanding overall, with a better understanding regarding the business and large cash transactions. The AED's ML/TF risk understanding of services provided by business/office centres is good, both at sectoral and entity level. This is mainly due to AED's supervisory work and regular contacts with the CSSF. The AED also benefitted from the CSSF's SSRAs on TCSPs. However, the AED has not fully developed its ML/TF risk understanding of TCSP activities provided by professional directors, as supervision began in 2022.

SRBs (OEC, IRE, OAs, CdN)

419. The OEC (CPAs) and IRE (statutory auditors and audit firms) generally understand the risks present in their supervised sectors and individual entities. For instance, the OEC observed ML threats and vulnerabilities in line with the 2020 NRA (update): i.e., fraud, forgery and TCSPs (which is offered by 47% of the independent CPAs and 66% CPA firms). Both the OEC and IRE see a change in private sector risk appetite, with a noticeable decline of TCSP services being provided by CPAs and by statutory auditors (60% reduction in the period 2018-2022).
420. The OAs (lawyers) and CdN (notaries) demonstrated an adequate but more recent ML/TF risk understanding in the legal profession and notary sectors. The OAs and CdN recognize the main vulnerabilities for lawyers (i.e., a large, fragmented profession, broad clientele, role as AML/CFT gatekeeper) and notaries (i.e., role as AML/CFT gatekeeper, including in real estate transactions and constituting legal persons) as identified in the NRAs. However, some additional work is needed to internalize their understanding and monitor the evolution of the risks so that they can refine their risk-based approach to supervision.

Risk-based supervision of compliance with AML/CFT requirements

421. There is an uneven level of sophistication in the development of risk-based models for supervision among the public sector and professional body supervisors. Luxembourg's supervisory regimes, particularly DNFBP supervision, started maturing in 2018 with, in 2020, the powers of DNFBP supervisors (AED and SRBs) standardized and aligned with the CSSF powers and VASPs included in the supervisory framework. The CSSF has the most mature and extensive approach and has acted as an example for other supervisors by sharing its model. As a result, all supervisors now use a comprehensive annual AML/CFT questionnaire to inform their supervisory work and risk classify their supervised entities. Since then, the off-site and on-site AML/CFT inspections of all sectors are more focused.

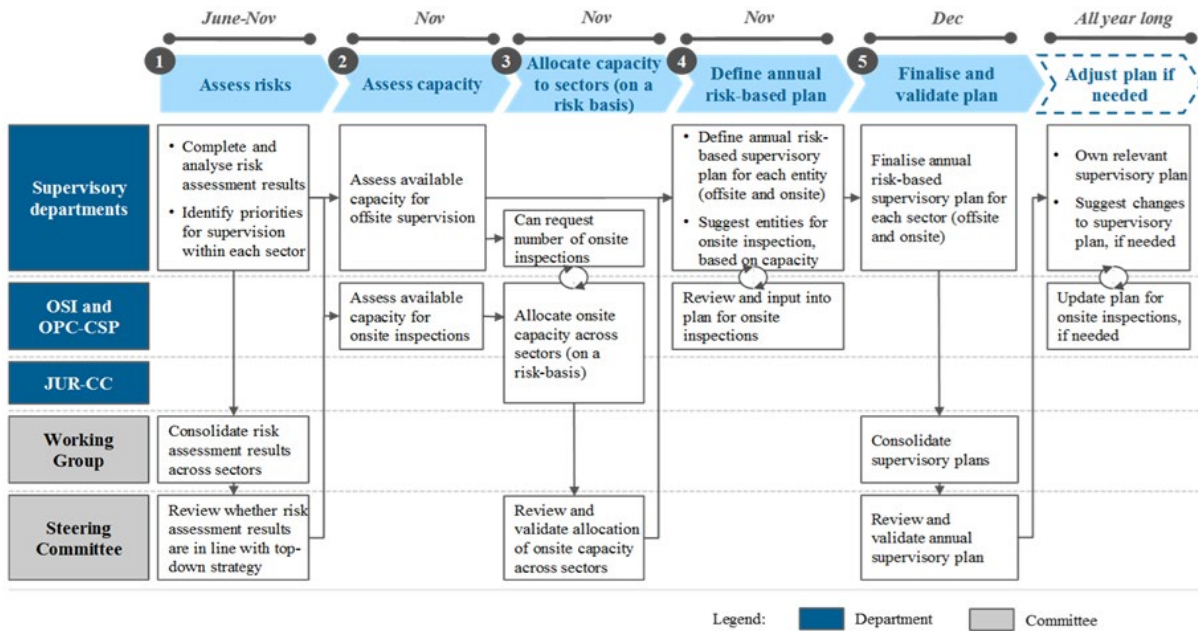
CSSF

422. The CSSF has a risk-based approach dedicated to AML/CFT supervision of FIs, separate from prudential supervision. As of the end of 2021, the CSSF's AML/CFT supervisory population comprised of 1 562 professionals with the investment and banking sectors making up 85% of the FIs.
423. Over the review period, the CSSF has been improving its supervisory work by increasing staff, dedicating resources to higher risk sectors, refining its existing tools and introducing new ones. The CSSF takes a multi-pronged approach to supervision. It reserves more intrusive supervisory measures (i.e., on-site inspections) for medium-high and high-risk firms, and all FIs are subject to monitoring through adverse media screening, supervisory review of statutory audit reports, compliance reports and annual AML/CFT questionnaires. Off-site reviews are also drawing on the technology and automatization deployed to supervise remotely since COVID-19. Although there is no fixed cycle for on-site inspections for medium-high and high-risk firms, the CSSF monitors intervals between on-site inspections, including through off-site sample testing of due diligence and face-to-face meetings to discuss the FI's AML/CFT framework. The assessment team is of the view that in totality and the level of off- and on-site supervision and monitoring is commensurate with the risks within each sector.
424. The CSSF is organised into six off-site supervisory departments⁴⁶ (which have dedicated AML/CFT experts working alongside prudential supervisors), two departments leading AML/CFT on-site inspections⁴⁷, three dedicated AML/CFT coordinators providing support and co-ordination amongst the departments and teams on AML/CFT matters, and ten legal experts within the AML/CFT division of the legal department (JUR-CC) providing legal and policy support and representing the CSSF at international and national levels on AML/CFT matters. Annual AML/CFT supervisory plans are produced by the CSSF's off-site supervisory departments based on the risk scoring of each entity (see section 6.2.2) and the available supervisory resources for off-site and on-site supervision (see Table 6.3). Each department proposes FIs for on-site inspections, and the OSI and OPC-CSP use an allocation tool to determine the number of on-site inspections per sector it could perform with the resources available. The CSSF increased its AML/CFT staff resources significantly from 45 in 2018 to 71 in 2022, with a larger number devoted to higher risk areas including a dedicated on-site team for IFMs (given the sector's size and higher risk profile) and an ad-hoc on-site team. On top of dedicated AML/CFT staff, AML/CFT supervision is augmented by input on AML/CFT matters such as FI governance, risk management and operations, by the CSSF's prudential supervisors. Its IT specialists also contribute for example by joining on-site inspections to FIs utilising technology in their AML/CFT framework. The assessment team considers that the CSSF has sufficient resources dedicated to the supervision of FIs and VASPs.

⁴⁶ These are 1) banks, 2) IFMs (OPC), 3) PIs/EMIs and VASPs (IPIG), 4) investment firms (EI), 5) specialised PFS (PSF-SP), 6) market operators (MAF).

⁴⁷ There is a dedicated team for IFMs (OPC-CSP) and a team for the other FIs (OSI).

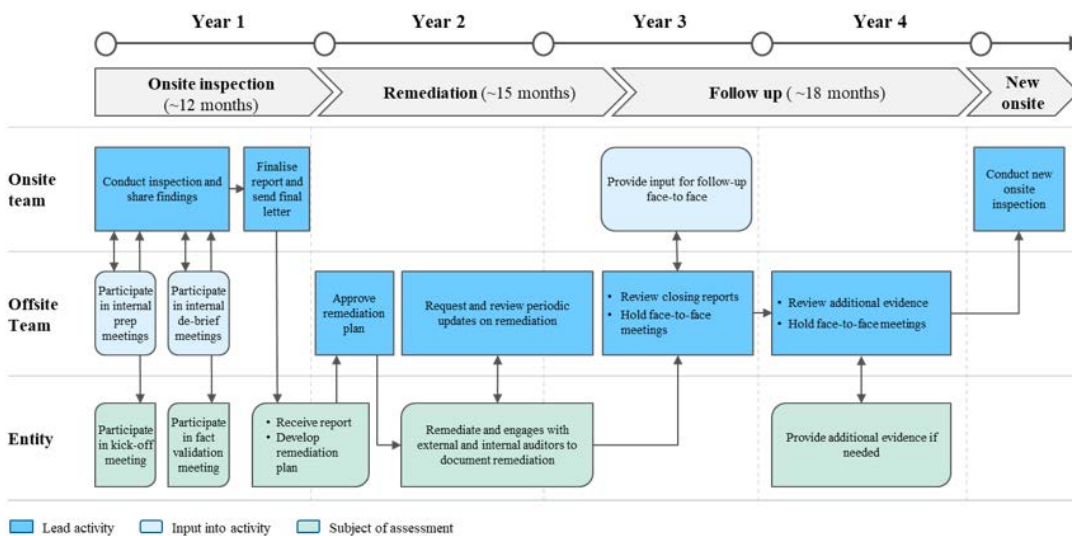
Figure 6.3. CSSF supervisory planning process



On-site inspections

425. On-site inspections can consist of full scope, partial scope, thematic, and, when immediate action is required, ad-hoc and follow-up inspections. The intensity of full scope inspection will be attuned to risk, with a high-risk FI being subject to full testing and more CDD sampling than during a full scope inspection to a low or medium risk FI, where the time allocated will be reduced by 50%. Full scope on-site inspections to high-risk FIs can last for extended periods of time. Figure 6.4 shows the supervisory timeline for high-risk professionals:

Figure 6.4. Overview of a typical risk-based supervisory timeline for high-risk professionals



426. The number of on-site inspections has increased from 29 in 2015 to 54 in 2021 following a significant and steady increase in AML/CFT staff resources at the CSSF since 2018. More resources for on-site inspections are devoted to high-risk sectors. The annual on-site programme is weighted towards higher risk sectors of private banking and IFMs. The proportion of on-site inspections within each sector is also weighted towards high and medium-high risk FIs and the programme also includes a smaller number of medium-low and low risk FIs. The following table illustrates the number of CSSF's AML/CFT on-site inspections across the risk spectrum per sector in 2019, 2020 and 2021.

Table 6.3. Coverage of sector (%) and number of on-site measures, 2019-2021

| | On-site inspections | | | | | | | | | | | | | | |
|--------------------|---------------------|-------|-----------|---------------|----------|------|-------|-----------|---------------|----------|------|-------|-----------|---------------|----------|
| | 2019 | | | | | 2020 | | | | | 2021 | | | | |
| | IFMs | Banks | Spec. PFS | Invest. Firms | PIs/EMIs | IFMs | Banks | Spec. PFS | Invest. Firms | PIs/EMIs | IFMs | Banks | Spec. PFS | Invest. firms | PIs/EMIs |
| High | 9% | 33% | 45% | - | 50% | 11% | 21% | 67% | 17% | 50% | 12% | 14% | 20% | 14% | 50% |
| | 5 | 4 | 5 | 0 | 2 | 8 | 3 | 4 | 1 | 2 | 10 | 2 | 2 | 1 | 2 |
| Medium High | 1% | 22% | 6% | 11% | - | 5% | 15% | 11% | 6% | - | 2% | 15% | 11% | 8% | - |
| | 6 | 14 | 3 | 4 | 0 | 10 | 9 | 5 | 2 | 0 | 13 | 10 | 6 | 3 | 0 |
| Medium Low | 3% | 11% | 3% | 10% | 100% | 3% | 3% | - | 3% | 50% | 1% | 3% | 3% | 3% | - |
| | 8 | 4 | 1 | 3 | 2 | 3 | 1 | 0 | 1 | 2 | 3 | 1 | 1 | 1 | 0 |
| Low | 1% | 7% | - | 5% | - | 1% | 10% | 11% | - | - | 1% | - | 11% | - | - |
| | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 |
| Not Rated | - | - | 50% | - | - | - | - | - | - | - | - | - | - | - | 4% |
| | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| Total | 2% | 17% | 9% | 8% | 25% | 2% | 11% | 9% | 4% | 17% | 2% | 10% | 10% | 5% | 8% |
| | 20 | 23 | 10 | 8 | 4 | 22 | 14 | 10 | 4 | 4 | 27 | 13 | 10 | 5 | 3 |

427. The CSSF increased its partial on-site inspections, which are more targeted, allowing more in-depth analysis on specific areas but are less resource intensive as full scope inspections. The CSSF also undertakes thematic on-site inspections to compare practices across sectors or deep dive into a topic.⁴⁸ Themes are selected by the CSSF management based on risk or trigger events and inspections involve generally five to nine FIs, which is low. For example, in 2022, the CSSF started analysing the involvement of PEPs and corruption, as this is a main threat to Luxembourg, with the participation of so far seven FIs. In 2016 and 2017, the CSSF undertook a thematic analysis of banks' corporate accounts after the publication of the Panama Papers report. This wide-ranging review covered 30 banks, five investment firms, three specialised PFS and two IFMs, resulting in nine FIs being fined a total of EUR 2 million in 2017. This exercise shows that thematic work can be effective in identifying deficiencies and administrative fines can and are applied.

⁴⁸ The CSSF carried out 42 thematic inspections under twelve topics, two of which resulted in public best practices reports between 2017 and 2021.

428. The CSSF also runs ad-hoc on-site inspections when significant information against an FI requires immediate action to mitigate a very significant ML/TF risk. There are between 1 and 3 cases a year and three case studies provided by the CSSF showed effective actions to reduce the risk and, where appropriate, apply sanctions (see Box 6.1).

Box 6.1. Case Study: Bank fined after an ad-hoc on-site inspection based on adverse media

The CSSF was informed about investigations regarding a high-profile fraud case and that one of the major suspects had accounts at a private bank in Luxembourg. In response, CSSF performed an ad-hoc on-site inspection to review the internal governance system and the bank's relationship with the client involved.

The inspection identified that the bank's internal governance systems were not adequate. This notably covered the compliance policy and compliance with AML/CFT professional obligations. The CSSF therefore imposed a fine of EUR 8.985 million which was published via a press release. The CSSF also withdraw the good repute/honourability of a former senior manager because of his role and responsibility in the non-compliance by the bank of its AML/CFT obligations. Subsequently, the bank's senior manager will be considered as no longer being fit to exercise a function requiring CSSF's approval for a period of ten years.

429. While the CSSF supervisory responsibilities for VASPs is relatively recent (i.e., March 2020), it has undertaken on-site inspections to FIs that are authorized as both VASPs and PIs/banks. In that context, the CSSF supervised FI VASP activities even before they were registered as VASPs. These three entities currently service 99.1% of the clients of the VASPs registered, process 99.5% of the transactions in terms of volume in EUR equivalent and process 99.9% of the total of transfers in VA.

Off-site supervision

430. Regardless of the risk classification, every FI will be subjected to a defined set of supervisory measures annually. At a minimum, this will include, where applicable, a review of the annual long form report prepared by the statutory auditor, the report of the FI's AML/CFT compliance officer, the FI's internal audit report and the AML/CFT questionnaire.⁴⁹ For IFMs, except for high-risk IFMs, all documents are not systematically analysed but rather reviewed on a sample basis. As for specialised PFS, all documents are reviewed for high-risk and medium-risk entities.

⁴⁹ For IFMs: 1) internal audit reports are not applicable to registered IFMs; 2) AML/CFT external report by the statutory auditor have been applicable to all IFMs since 31/12/2021. For VASPs: 1) the annual statutory auditor report and the internal audit report are not applicable; 2) the first AML/CFT questionnaire will be submitted in 2023 for the figures as of end 2022; 3) for VASPs that are also PIs/EMIs (3 out of 9 entities as of November 2022) or banks (2 out of 9 entities as of November 2022): the report of the AML/CFT compliance officer shall cover the VA activities; 4) VASPs established outside of Luxembourg (3 out of 9 entities) are also supervised by their home competent authority.

Statutory auditors are required to identify within the long form report or, for IFMs, specific AML/CFT reports, any areas of non-compliance with AML/CFT obligations, enabling the CSSF to consider follow-up action. Statutory auditors may also be requested to perform additional risk-based controls beyond the reports they already prepare annually. These baseline desk-based reviews increased from 387 FIs in 2015 to all FIs by 2019 and the assessment team considers this an effective way of identifying and following up on findings⁵⁰ arising from these reports and questionnaires. For example, the interventions by the CSSF's banking department increased from 633 in 2017 to 1 321 in 2021. For VASPs, as this is a recent area of supervision, the CSSF reviews the level of activities of its registered VASPs on a quarterly basis.

- 6
431. Further off-site measures are applied based on the risk rating of the individual FI and include face-to-face meetings or calls with FIs (authorised managers, compliance officer, internal auditor) or the statutory auditor. The CSSF banking department conducted the highest number, as there are annual meetings with higher risk banks' chief compliance officer (see Table 6.4). The assessment team was informed by banks it met that these meetings are lengthy (lasting 3 hours) and require good preparation and presentation on specific AML/CFT issues. In the assessment team's view, off-site measures applied to banks and IFMs are strong. In 2021, there were 27 on-site inspections to IFMs (1 190 professionals) and 184 meetings with IFMs, out of which 44 full scope face-to-face AML/CFT meetings with IFMs representing 26.25% of total assets under management. While the number of AML/CFT meetings with the collective investment sector is considerably smaller, despite having the largest number of high and medium-high risk FIs involved, they are complemented by the large number of direct calls with the professionals. Furthermore, the investment sector is supervised by the CSSF through a chain of operators that includes depositary banks, managers and specialised PFS.

Table 6.4. Total number of face-to-face meetings and calls conducted by department, data only indicative, 2015-Q3 2022

| | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 | Total |
|--------------------------------|----------|------------|------------|------------|------------|------------|------------|------------|--------------|
| OPC – Calls (est.)* | - | - | - | 2 046 | 2 936 | 6 938 | 5 427 | 5 592 | 22 939 |
| OPC – F2F meetings | - | - | - | 2 | 29 | 42 | 44 | 41 | 158 |
| B | - | 144 | 232 | 339 | 223 | 141 | 156 | 72 | 1 307 |
| PFS-SP | - | - | 2 | 6 | 3 | 5 | 12 | 12 | 40 |
| EI | - | 7 | 4 | 2 | 4 | 12 | 5 | 5 | 39 |
| IPIG | 2 | 6 | 4 | 21 | 55 | 65 | 63 | 42 | 258 |
| Total (excl. OPC calls) | 2 | 157 | 242 | 370 | 314 | 265 | 280 | 172 | 1 802 |

Note: CSSF internal data, until Q3 2022. Data of years 2015-2017, are not necessarily complete because of lack of data recorded.

*Note: OPC figures include an estimated number of calls with supervised professionals, with whom they are in contact on a frequent basis and for whom total call volumes are not systematically tracked.

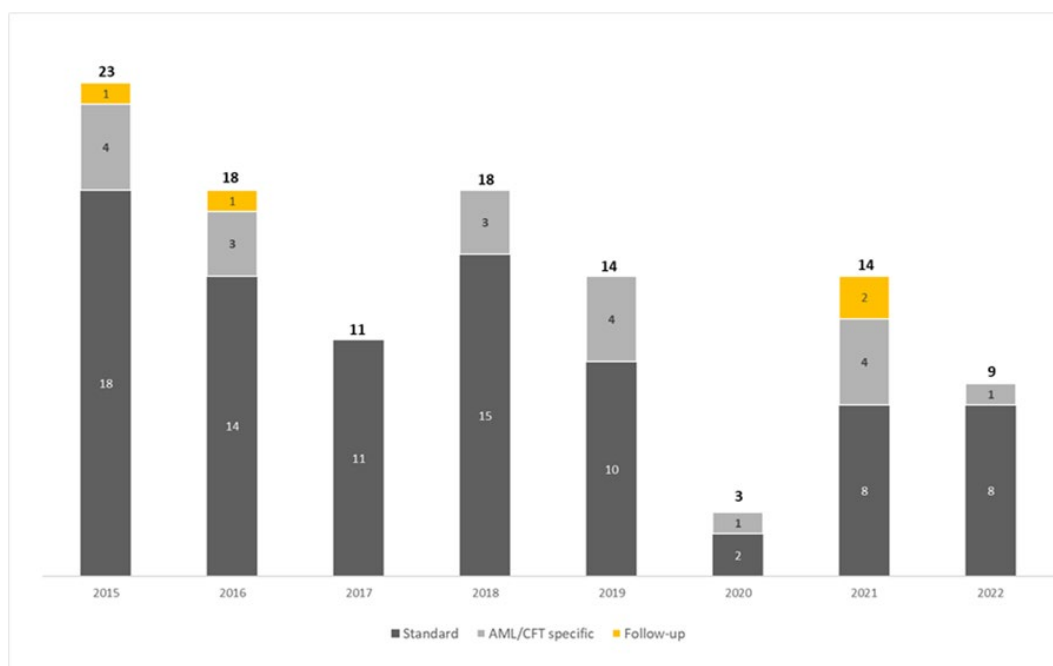
⁵⁰ Note that “findings” in this context do not necessarily indicate a breach of AML/CFT obligations and include areas for enhancement identified by professionals (e.g., as part of the Internal Audit report), external auditors and CSSF.

432. There are a range of sources which can trigger off-site and on-site CSSF supervisory intervention including whistle blowers, adverse media, management changes within an FI, information from the ECB, and through a supervisory college. It also draws on information from its prudential supervision which, in one case, resulted in a EUR 4.6 million fine and public statement on a bank where CSSF's prudential supervisors had raised concerns about its high ML/TF risk appetite.

CAA

433. The CAA supervises for AML/CFT purposes 37 life insurance undertakings and 109 brokerage firms.⁵¹ It has a risk-based approach to supervision of its insurance professionals using a combination of both desk-based reviews and on-site inspections. AML/CFT supervision of the life insurance sector is carried out by six dedicated AML/CFT experts and the prudential team.
434. The CAA AML/CFT supervisory plan is informed by annual quantitative and qualitative AML/CFT questionnaires which lead to a risk scoring of each FI: low, medium, medium-high, high. The CAA's risk model is similar to that of the CSSF. The supervisory plan is approved by the CAA Directorate and can be adjusted if the CAA becomes aware of facts that require further investigations. Aside from vertical inspections, in which a single FI is inspected, the CAA also conducts horizontal inspections to corroborate the information provided by a broker with that of the life insurance undertaking with which the business has been placed and vice versa. There are two types of on-site inspections: standard on-site inspections and targeted on-site inspections (see Figure 6.5). Standard on-site inspections are part of the general prudential supervisory work and are conducted by prudential experts. These inspections cover AML/CFT checks (e.g., existence of adequate AML/CFT procedures and compliance with reporting obligations), and the final general report covers both prudential and AML/CFT findings. Targeted on-site inspections (see Table 6.5) cover higher risk FIs and are performed by AML/CFT experts with the assistance, in limited cases, of prudential experts. Such targeted on-site inspections always include a review of a sample of insurance contracts. Since 2021, the CAA prudential agents only perform AML/CFT checks for low and medium ML/TF risk professionals in the context of their prudential controls, which are performed every three to four years. Prudential and AML/CFT supervision plans are co-ordinated annually.

⁵¹ The insurance sector has over 4 000 intermediaries of which most are insurance agents/agencies (i.e., 3 428) engaged in insurance intermediation for and on behalf of one or several Luxembourg-based insurance undertakings and sub-brokers (i.e., 464). They distribute to a domestic market, largely non-life insurance products, collect no premium and act under the responsibility and on behalf of brokerage firms or brokers.

Figure 6.5. Number of on-site inspections with an AML/CFT component by type, 2015-Q3 2022**Table 6.5. Targeted AML/CFT on-site inspections, 2018-2021**

| | Life insurance undertakings | | Brokers | |
|------|-------------------------------------|---------------|-------------------------------------|---------------|
| | No. of targeted on-site inspections | Inherent risk | No. of targeted on-site inspections | Inherent risk |
| 2018 | 1 | Low* | 2 | NA** |
| 2019 | 2 | High | 2 | High |
| 2020 | 1 | High | 0 | - |
| 2021 | 2 | High | 2 | Medium-high |

* Note: Following further investigations, the CAA re-categorized this entity as high-risk.

**Note: The CAA explained that information was not available as the first risk assessment was finalised in November 2018.

435. The CAA also uses off-site supervision; this includes a review of the annual AML/CFT questionnaire and the special report prepared by the statutory auditor of the FIs, by the AML/CFT experts who request further information or amendments if the information provided is incorrect. PSAs submit an annual report on the TCSP services provided. Since 2020, the CAA increased its focus on improving the content and quality of the special reports prepared by the statutory auditor as they are an important element in the CAA's monitoring of FIs. The CAA is also in regular dialogue with the CSSF, CRF-FIU and foreign supervisors. Because of the COVID-19-related health and sanitary restrictions, no FI was inspected through in-person or remote/virtual on-sites from February 2020 to March 2021. In this period, the CAA undertook two surveys of the life insurance sector regarding the impact of the pandemic and tax crimes and performed its desk-based supervisory activities.

AED

436. The AED supervises over 3 000 DNFBPs representing various sectors and uses a combination of on-site inspections and off-site measures. The AED has bolstered its risk-based approach to supervision by introducing annual AML/CFT questionnaires for most sectors in 2020. However, the risk-based supervision is not yet fully mature; measures to improve the risk-based approach are somewhat recent, and not completely risk-sensitive. The AED only has seven supervisors for on-site inspections, and this appears to be a low number considering the supervisory population and the need to sustain recent efforts (such as inspecting professional directors). The AED is further improving its approach, tools and resources.
437. The AED conducts good off-site supervision. It includes pre-screening (based on factors such as fiscal compliance and turnover), collecting and analyzing data from AML/CFT questionnaires and complementing this with information provided by other authorities, databases and open sources. However, the quality of responses by REAs is low (see section 6.2.2) and digitization of the supervisory activities is only beginning – resorting to technology to a larger extent would increase the efficiency of AED as it would free up resources for reallocation to other supervisory activities.
438. On-site inspections focus on selected higher-risk entities, while other entities are visited if certain criteria are met, such as not responding to the AML/CFT questionnaire or other administrative measures from the authorities (e.g., requests related to tax issues), not following up on an AED observation, being at risk of tax crime or being the object of a whistleblowing report. The AED conducted 135 on-site inspections in 2021, with REAs being visited the most (see Table 6.6). This is broadly in line with the high risk this sector poses. For the DPMS sector, the AED focusses on professionals with the highest turnover and with large cash transactions above EUR 10 000, well complementing the off-site work (although the implementation of these measures is recent). The AED recently increased inspections of business centres and conducted none for professional directors (as the AED just started the supervision). Although these TCSP professionals are less material, the supervision levels are low. Each year, the AED carries out an on-site inspection at Luxembourg's only casino. The casino has limited game offerings (slot machines, blackjack tables), applies strong mitigation measures (see IO.4) and has been licensed since the 1980s. The annual on-site inspection of the casino is not in line with the lower risk the casino represents and takes away the limited resources of the AED to supervise other sectors with more risks.

Table 6.6. Number of on-site inspections, 2019-2021

| Supervised Sector | 2019 | | 2020 | | 2021 | |
|---|--------------------------------------|-------------|--------------------------------------|-------------|--------------------------------------|-------------|
| | Supervised entities | Inspections | Supervised entities | Inspections | Supervised entities | Inspections |
| Real estate agents | 2 329 (352 in scope*) | 43 | 2 559 (380 in scope*) | 22 | 2 767 (400 in scope*) | 66 |
| Accounting professionals and tax advisors | 671 | 16 | 695 | 39 | 641 | 56 |
| TCSPs | 78 business centres 661 directors | 1 | 60 business centres 627 directors | 6 | 63 business centres 688 directors | 7 |
| DPMS | 153 (20 in scope**) | 1 | 123 (20 in scope**) | 4 | 133 (20 in scope**) | 6 |

*Note: The AED considers 400 REAs in scope as they likely present higher ML/TF risk given these account for 90% of the market/annual turnover.

**Note: The DPMS sector consists of professionals having a business license while in scope refers to the DPMS carrying out cash transactions in excess of EUR 10 000.

SRBs (OAs, CdN, OEC, IRE)

439. All SRBs conduct risk-based supervision which has matured significantly in recent years with the use of annual AML/CFT questionnaires. These questionnaires combined with information provided by other authorities, assessments by internal supervisory boards and open-source information assist risk classification of entities and inform SRBs' supervisory plans.
440. The OAs use a combination of in-house dedicated staff and peer-review to conduct the risk-based supervision of the legal profession. Since 2020, the OAL, which also conducts supervision for the OAD members, uses an AML/CFT questionnaire to inform its supervisory plan. The OAL has three in-house supervisors and nine lawyers appointed as supervisors by the OAL management for three to six years. The OAL focuses on-site inspections on high-risk lawyers and law firms: between 2020 and November 2022, they inspected 1 000 lawyers and all law firms with more than 50 lawyers.⁵² There was a small dip in 2019-2020 due to COVID-19 and a significant campaign of inspections was conducted in 2020-2021 as 29% of lawyers were inspected (i.e., 877 lawyers and 35 law firms, see Table 6.7). Although recent, the controls are becoming effective and include a review of the quality and effectiveness of the work of the lawyer or law firm to provide useful recommendations. The OAL needs to sustain these efforts.

Table 6.7. Statistics of number of AML/CFT on-site inspections, 2016-Q3 2022

| Judicial year | Nb of on-site inspections | Law firms inspected | Lawyers inspected | % lawyers inspected | Total number of lawyers registered at the end of the relevant judicial year |
|---------------|---------------------------|---------------------|-------------------|---------------------|---|
| 2016-2017 | 12 | 12 | 289 | 12% | 2 376 |
| 2017-2018 | 32 | 27 | 819 | 32% | 2 576 |

⁵² Luxembourg has total of 547 law firms and 3 230 lawyers. There are nine law firms that have 50 or more lawyers and these employ 1 122 lawyers.

| Judicial year | Nb of on-site inspections | Law firms inspected | Lawyers inspected | % lawyers inspected | Total number of lawyers registered at the end of the relevant judicial year |
|------------------------|---------------------------|---------------------|-------------------|-----------------------------|---|
| 2018-2019 | 21 | 19 | 282 | 10% | 2 790 |
| 2019-2020 | 17 | 16 | 176 | 6% | 2 946 |
| 2020-2021 | 35 | 35 | 877 | 29,0% | 3 023 |
| 2021-Q3 2022 | 28 | 28 | 126 | 4% | 3 112 |
| TOTAL | 145 | 137 | 2 569 | | 82.6% |
| Excl. Duplicate | | 103 | 1 943 | 62.4% | |
| | | | | OA members inspected | |

441. Like the OAs, CdN uses a peer review mechanism to supervise the notary sector. CdN started using the AML/CFT questionnaire in 2019 to develop its risk-based approach to supervision. The NRA has helped them develop their risk-based approach which was more basic in the past. The process of reviewing questionnaires is manual but allows CdN to arrive at a good risk scoring. For 2021, about 50% of notaries were considered medium-risk, 31% high-risk and 13% low-risk. These percentages are fairly stable. Annual off-site checks are conducted on all notaries, and all have been visited. The CdN works closely with the notaries so that they address any issues that are highlighted but have not yet issued any penalties. As there are only 36 notaries in Luxembourg and they know each other, the assessment team has concerns about the independence of this supervisory function, especially considering that notaries have not been fined at all while serious breaches calling for tougher measures were detected (see section 6.2.4). The assessment team notes that in 2021 CdN hired one compliance officer who is not a notary to assist CdN in its supervisory activities and this action aims at increasing independence. However, having a more balanced mix of personnel or a fully independent function is still needed to strengthen the function further.
442. OEC conducts risk-based supervision of CPAs. Before 2019, the controls were executed by peers and were not efficient as they were long and less focused. Since then, supervision has been professionalized and becoming more effective. OEC conducts approximately 100 controls per year and expects to have controlled all high-risk entities (22% of the approximately 1 200 CPAs) by the end of 2022, so that all high-risk entities have been visited in the last five years. They also conduct some controls of medium-risk and low-risk firms. However, OEC only has three in-house staff. These resources are limited and may not be sustainable to conduct effective and in-depth supervision of the CPA sector, especially considering the risks of CPAs and their TCSP activities (even if the number of TCSPs and domiciliation activities are decreasing due to a change in risk appetite reinforced by the Panama Papers and related negative association to certain jurisdictions and complex structures).

443. IRE uses a strong risk-based approach to identify approved statutory auditors and audit firms to be inspected on-site. It supervises professionals that are highly sensitized to AML/CFT and compliance issues. IRE performed 40 controls in 2020-21 and 38 controls in 2021-22. Very high-risk firms are inspected every two years and all firms are inspected at least every six years. IRE has 2.5 full time equivalent persons dedicated to AML/CFT supervision with approximately eight external controllers who are appointed by the IRE Council upon recommendation from the AML/CFT Committee. They must be experienced and not subject to conflict of interest and they work within IRE for several years. IRE has thorough on-site inspections and good off-site supervision.
444. There is good co-operation between the OEC and IRE to supervise joint members. However, there is also some duplication between the two SRBs, as different risks can apply to a statutory auditor and to a CPA. A formal exchange of information related to AML/CFT controls exists since the beginning of 2022.⁵³ Further measures could be taken to limited the burden on joint members who need to respond to two questionnaires.

Remedial actions and effective, proportionate, and dissuasive sanctions

445. Luxembourg's supervisors use a range of remedial actions and sanctions to encourage compliance. However, the use is not proportionate, effective or dissuasive for the AED and CdN, and the CAA has made little use of sanctions.

CSSF

446. The CSSF has a range of supervisory measures which are applied in practice including: observation and injunction letters, warnings and fines. The CSSF uses observation and injunction letters to address most deficiencies in AML/CFT processes. Where significant failings are identified, the CSSF has applied more severe measures: 78 administrative fines totalling EUR 14.68 million⁵⁴ were imposed between 2017 and 2021 following AML/CFT inspections.

⁵³ As of 3 March 2022, 205 statutory auditors and approved statutory auditors (of a total of 593) as well as 27 audit firms and approved audit firms (of a total of 67) also hold the CPAs' license and are subject to AML-CFT dual supervision by the OEC and by the IRE. They are in general (but not automatically as this is decided on a case-by-case basis) not controlled by the two SRBs at the same time. OEC and IRE exchange the names of joint members who are in scope of the AML/CFT supervision plan and who have a dual registration. They also exchange information on the results of on-site controls which may be relevant for the other. However, OEC determines internally (and on a case-by-case basis) if a programmed AML/CFT control is maintained or not. Both organisations, however, send their own RBA questionnaires to these firms, and these require a lot of resources to be filled properly.

⁵⁴ In December 2022, the CSSF fined a bank EUR 1.56 million at the conclusion of a complex AML/CFT onsite inspection that began in late 2019. However, since this fine was not imposed until after the end of the on-site visit, it was not taken into account for the purpose of analysis or rating.

447. Deficiencies are assessed against specified criteria and classified through a standardised decision matrix to determine the appropriate response: e.g., severity and duration of the deficiencies identified, degree of responsibility of the supervised professional, previous deficiencies or breaches by the supervised professional. This helps to ensure that the CSSF takes a consistent approach in the application of supervisory measures. The CSSF mostly issues observations to convey requirements or suggestions for improvements. The implementation of the observations is monitored by the CSSF and augmented by the FI's statutory auditor confirming to the CSSF if the deficiencies have been remediated. These are effective in returning the FI to compliance. The CSSF can also issue injunctions and fines, for example for non-filing of AML/CFT questionnaires. Where there is non-compliance with the terms of an injunction letter, the CSSF can issue penalties. The use of these measures has had a positive impact on compliance. For example, twelve reminders were issued to specialised PFSs in 2018, reducing to three in 2019 (including one injunction), no reminders were needed for 2020 and 2021. The proportion of FIs who have been required to re-submit these questionnaires because of data issues has significantly improved over the period.
448. The CSSF has formal procedures for dealing with cases where a sanction would be appropriate. Sanctions must ultimately be approved by the CSSF executive board, and the FI has a right to challenge the proposed action before a final decision is made. This formal process helps to ensure proportionality and consistency and is based on the EU legislation. The CSSF is making increasing use of sanctions (see Table 6.8) and from the cases studies provided to the assessment team the penalties appear proportionate.

Table 6.8. Number of sanctions imposed per year of inspection (legal and natural persons), 2017-2021

| | 2017 | 2018 | 2019 | 2020 | 2021 | Total |
|-----------------------------|-----------|-----------|-----------|-----------|-----------|------------|
| By type of sanction | | | | | | |
| Total | 18 | 23 | 31 | 13 | 15 | 100 |
| Warning | 0 | 4 | 1 | 0 | 0 | 5 |
| o/w natural persons | 0 | 0 | 0 | 0 | 0 | 0 |
| Reprimand | 1 | 1 | 4 | 0 | 1 | 7 |
| o/w natural persons | 1 | 0 | 1 | 0 | 0 | 2 |
| Administrative fines | 17 | 16 | 19 | 12 | 14 | 78 |
| o/w natural persons | 1 | 0 | 0 | 1 | 0 | 2 |
| Temporary bans | 0 | 0 | 1 | 0 | 0 | 1 |
| o/w natural persons | 0 | 0 | 0 | 0 | 0 | 0 |
| Withdrawal or suspension | 0 | 2 | 6 | 1 | 0 | 9 |
| o/w natural persons | 0 | 2 | 6 | 1 | 0 | 9 |
| By department/sector | | | | | | |
| Total | 18 | 23 | 31 | 13 | 15 | 100 |
| B | 4 | 10 | 3 | 1 | 0 | 18 |
| OPC | 6 | 7 | 21 | 8 | 14 | 56 |
| PFS-SP | 4 | 3 | 7 | 1 | 0 | 15 |
| EI | 4 | 3 | 0 | 2 | 0 | 9 |
| IPIG | 0 | 0 | 0 | 1 | 1 | 2 |

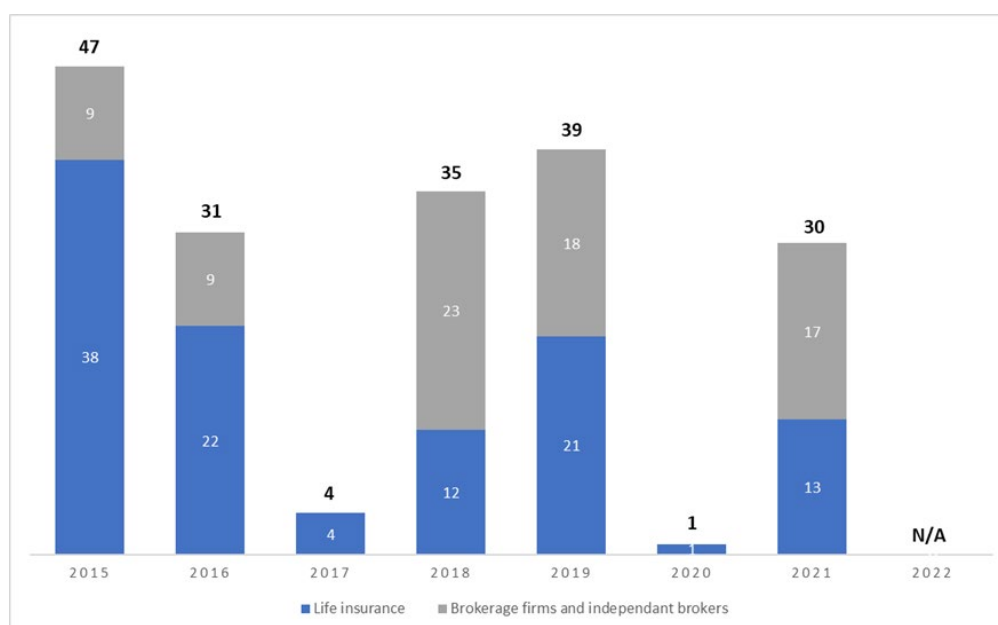
Source: CSSF internal data. Data indicative only since remediation processes are still ongoing.

449. Sanctions are published in public statements on the CSSF's website. For the period 2017-2021, 90% of measures taken were made public. The assessment team considers that publication serves as a deterrent and FIs met generally described them as dissuasive. However, the assessment team believes that the effectiveness elements of sanctions is undermined as these statements are extremely short (covering the legal provisions which were not met with no further information explaining the nature or seriousness of the breach(es)). Additionally, they do not always identify the level of fine or sanctioned FI (and the reason for not identifying the FI is unexplained in the public notice which do not set clear messages for industry on the CSSF's expectations in terms of compliance). While the CSSF advised that more information is given in annual reports and conferences, this information is high-level and not sufficiently detailed, and, in the absence of one permanent document record of the deficiencies, there is reliance on the conference attendee to accurately feed the information back to the FI.
450. The CSSF took action against thirteen individuals including nine suspensions, two fines and two reprimands but only one prohibition case against an individual is public. The CSSF found that the individual was no longer of good repute and has prohibited them from holding a management position for ten years (see Box 6.1). It is a short statement identifying the individual failed in their obligation to ensure that the FI respects its professional obligations in relation to the fight against ML and TF.
451. The CSSF also co-operates with LEAs. It has referred a large number of cases to the Prosecutors Office: 452 between 2016 and 2021, of which 198 covering 113 entities have been for violations of professional AML/CFT obligations. The CSSF liaises with PAL to ensure no action it takes would jeopardise a criminal case. In a majority of such cases, the CSSF pursued applying its own sanctions. There was good evidence of parallel investigations by the CSSF alongside criminal investigations to establish regulatory failings and effect change (to ensure timely management on a forward-looking basis of ML/TF risks posed by FIs) on cases which are under criminal investigation.

CAA

452. The CAA has the same range of remedial actions and sanctions at its disposal to address AML/CFT breaches as the CSSF. The CAA imposes remediation action orders (injunctions) where deficiencies in AML/CFT obligations are identified (see Figure 6.6). For these injunctions to be closed, the FI must inform the CAA of the action it has taken and its statutory auditor is also required to assess compliance with the injunction and report its findings to the CAA. The CAA will follow up with an on-site inspection or a disciplinary hearing in cases where an FI does not inform the CAA of the action taken or the statutory audit report reflects non-compliance with the injunction. This is an effective mechanism for ensuring that an FI remediates the deficiency, and there have been very few cases of non-compliance with an injunction.

Figure 6.6. Number of AML/CFT injunctions following on-site inspections for life insurance undertakings and brokers, 2015-Q3 2022



Source: CAA data for the insurance sector

Note: In 2017: The shift between the number of injunctions is explained by the number of OSIs performed by life insurance undertakings and brokers. In 2020: The low level of injunctions in 2020 is explained by the low number of OSIs performed this year due to the Covid-19 pandemic. In 2021 and 2022: The related reports of 4 OSIs initiated in 2021 and all OSIs initiated in 2022 are still in progress.

453. Until 2021, the only sanctions the CAA had imposed were four administrative fines of EUR 3 000 on brokers for breaches of AML/CFT training requirements. In 2021, the CAA initiated its sanctioning process in four cases where non-compliance was detected during an on-site inspection, including in one case where non-compliance with a previous injunction letter was identified. At the time of the on-site visit, these cases were being challenged or appealed by the FIs. There has been limited use by the CAA of its sanctioning power against FIs and no sanction of an individual.

AED

454. With the broadening of its sanctioning powers in 2018, the AED increasingly imposed warnings, fines and reprimands since 2019. The number of fines issued to the REAs, DPMS, business/office centres and accounting professionals have increased from 8 in 2018 to 58 in 2022, with a peak of 135 in 2021, which is due to a large number of fines issued to REAs and the accounting professionals (see Table 6.9). These remedial actions are becoming more dissuasive, but non-compliance rates underline the need for further actions. For example, non-compliance of REAs with the implementation of RBA requirements has decreased from 89% (2020) to 70% (2021), non-compliance with general AML/CFT obligations has decreased from 56% (2020) to 44% (2021), and as a result partial compliance has increased from 11% (2020) to 22% (2021). Non-compliance and partial compliance remain considerable and REAs and DPMS met do not seem to be aware of the AED's actions.

Table 6.9. AED Sanctions by sector, 2018-Q3 2022

| | 2018 | 2019 | 2020 | 2021 | Q3 2022 | Total |
|---------------------------------|----------|-----------|-----------|------------|-----------|------------|
| REAs | 2 | 43 | 22 | 66 | 44 | 177 |
| Warning | 1 | 4 | 2 | 3 | - | 10 |
| Fine | 1 | 30 | 15 | 45 | 28 | 119 |
| Reprimand | - | 5 | - | 11 | 8 | 24 |
| DPMS | 1 | 1 | 4 | 6 | 2 | 14 |
| Warning | 1 | - | - | - | - | 1 |
| Fine | - | 1 | 1 | 6 | 1 | 9 |
| Reprimand | - | - | 2 | - | - | 2 |
| TCSP – B/O Centres | 2 | 1 | 6 | 7 | 4 | 20 |
| Warning | - | - | 1 | - | - | 1 |
| Fine | 1 | 1 | 3 | 3 | 3 | 11 |
| Reprimand | - | - | - | 1 | 1 | 2 |
| Accounting professionals | 3 | 16 | 39 | 56 | 8 | 122 |
| Warning | - | - | 1 | 2 | - | 3 |
| Fine | 3 | 15 | 21 | 35 | 4 | 78 |
| Reprimand | - | - | 3 | 6 | 1 | 10 |
| Total | 8 | 61 | 71 | 135 | 58 | 333 |

455. No sanctions have been applied by the AED to professional directors, as supervision has only recently started. There have been no remedial actions for the casino, except for minor recommendations about language that they use in their AML/CFT documents. The authorities have not observed any material deficiencies, and this is in line with the low risks and stability of the casino.

SRBs (OAs, CdN, OEC, IRE)

456. The OAs have a number of remedial actions and sanctions for non-complying lawyers and law firms, such as injunction, warning, fine and disbarment (see Table 6.10). These have been used more often since their AML/CFT powers were broadened in early 2020 and have started to become more proportionate and dissuasive since then.

Table 6.10. OAs Sanctions AML/CFT, 2018-Q3 2022

| | 2018-2019 | 2019-2020 | 2020-2021 | 2021-Q3 2022 | Total |
|------------|-----------|-----------|-----------|--------------|-------|
| Injunction | 0 | 0 | 0 | 5 | 5 |
| Warning | 1 | 1 | 2 | 1 | 5 |
| Fine | 0 | 0 | 4 | 3 | 7 |
| Disbarment | 0 | 0 | 13 | 1 | 14 |
| Total | 1 | 1 | 19 | 10 | 31 |

457. The CdN can issue observations, recommendations and, through its Disciplinary Council, fines. It detected 42 shortcomings for which it made observations in 2020. However, no financial penalties have been imposed on notaries in the past five years. During 2021 and 2022, following on-site inspections, three cases called for more severe action from the CdN as the notarial offices concerned did not sufficiently apply any AML/CFT policies, controls or procedures. The CdN required rectification of these shortcomings immediately and was satisfied with the manner and timeliness of the corrections. They also noted that the nature and severity of the shortcomings detected during the last five years did not justify the application of other sanctions. However, the assessment team is concerned that there may be situations where the CdN did not apply the most appropriate remedial actions. The CdN seems to be reluctant to impose strong measures and the burden of going to the Disciplinary Council raise questions about the independence of CdN and the effectiveness of its remedial actions.
458. The OEC has a range of remedial actions, such as close monitoring, warnings, disciplinary instructions and fines. Since March 2020, the OEC evolved its sanctioning powers with the OEC having a faster process to issue fines than before. It mainly uses close monitoring controls and appearance before the President of the Board as to address deficiencies. In the period 2015-2021, the OEC resorted to close monitoring 35 times and appearance before the President of the Board 8 times. Only two fines related to an AML/CFT breach were issued in May 2022. Although some of the changes and measures are more recent, they seem sufficiently robust and increasingly proportionate and dissuasive.
459. The IRE has various remedial actions and sanctions at its disposal, but uses injunctions accompanied by close monitoring as the main remedial action, but has not issued fines so far. This is proportionate and dissuasive as it has generally led to remediation of all deficiencies within a few months.

Impact of supervisory actions on compliance

460. Supervisors observed that AML/CFT compliance by their supervised professionals is maturing as a result of their supervisory actions. This trend is stronger for the FI sector than the DNFBP and VASP sectors. The introduction of the annual AML/CFT questionnaires, remedial actions and sanctions, and guidance and outreach (see section 6.2.6) has had a positive impact on increasing compliance by FIs, DNFBPs and VASPs.

CSSF

461. The CSSF shared many case studies demonstrating its actions had a positive impact on compliance by individual FIs and sub-sectors (see Box 6.2).

Box 6.2. Case Study: CSSF's measures taken at parent bank level X

Following the remediation actions taken by bank X, the CSSF has been able to see a clear change in the mindset of the management of the bank, such as there is a better co-operation with the CRF-FIU (increase of STR/SAR filed), enhanced due diligence performed on high-risk clients and new screening tool implemented.

The CSSF shared the outcome of the AML/CFT on-site inspection and remediation plan of bank X with two other EU supervisory authorities responsible for the AML/CFT supervision of the bank's branches established in their respective countries. One authority explained that they were surprised to see major changes in the statistical data provided by the branch (number of name screening alerts was multiplied by 10 compared to the previous years; number of declarations to the foreign FIU also increased significantly). So far, the authority had not discussed the issue with the branch but based on the information exchanged by the CSSF during the AML/CFT college, they understood that the reasons for these shifts derive from the implementation of a new group wide name screening tool in 2019 and the change of tone at the top from the head office in Luxembourg.

462. There has been an overall decrease of regulatory breaches identified through AML/CFT on-site inspections since 2018. The CSSF also observed a change in the nature of inspection findings over time, with the number of high severity breaches⁵⁵ declining since 2017 despite increased focus on higher-risk FIs and more on-site inspections (see Table 6.11).

Table 6.11. AML/CFT related regulatory breaches identified through on-site inspections, indicative data, 2017-2021

| | 2017 | | 2018 | | 2019 | | 2020 | | 2021 | |
|----------------------|------------|-----------|------------|------------|------------|-----------|------------|-----------|------------|-----------|
| | Total no. | o/w high | Total no. | o/w high | Total no. | o/w high | Total no. | o/w high | Total no. | o/w high |
| TOTAL* | 197 | 64 | 425 | 130 | 403 | 80 | 261 | 39 | 205 | 23 |
| o/w high risk | 74 | 40 | 99 | 28 | 102 | 20 | 123 | 26 | 56 | 3 |
| o/w medium high risk | 59 | 14 | 214 | 77 | 165 | 44 | 111 | 10 | 136 | 18 |

⁵⁵ Typical examples of high-severity breaches are delaying the review of the name matching alerts, inadequate frequency of name matching controls, delayed periodic reviews, lack of information and/or documentation on the origin of funds; examples of medium-severity breaches are missing data in the client database (e.g., missing country of residence, date of birth, some related counterparties missing), inadequate clients' ML/TF risk assessment (some ML/TF risk factors not entirely taken into account i.e. without major impact on the monitoring of the relationship), lack of verification of the identity of some representatives; examples of low-severity breaches are procedural deficiencies, lack of controls of the effectiveness of the transaction monitoring system/ name matching system, insufficient formalisation of transaction name matching alerts.

| | 2017 | | 2018 | | 2019 | | 2020 | | 2021 | |
|-------------------------|-----------|-----------|------------|-----------|------------|-----------|-----------|-----------|-----------|-----------|
| Banks | 65 | 32 | 223 | 86 | 113 | 20 | 87 | 23 | 71 | 10 |
| o/w high risk | 49 | 29 | 90 | 25 | 5 | 0 | 47 | 17 | 5 | 0 |
| o/w medium high risk | 7 | 2 | 133 | 61 | 83 | 15 | 30 | 4 | 62 | 10 |
| IFMs | 46 | 12 | 97 | 17 | 134 | 21 | 96 | 3 | 88 | 7 |
| o/w high risk | 16 | 5 | 0 | 0 | 60 | 9 | 32 | 0 | 37 | 1 |
| o/w medium high risk | 16 | 3 | 61 | 9 | 24 | 5 | 52 | 3 | 48 | 5 |
| Specialised PFS | 31 | 10 | 35 | 10 | 51 | 19 | 34 | 4 | 39 | 6 |
| o/w high risk | 9 | 6 | 9 | 3 | 20 | 5 | 8 | 0 | 14 | 2 |
| o/w medium high risk | 4 | 2 | 6 | 1 | 28 | 14 | 21 | 3 | 19 | 3 |
| Investment Firms | 55 | 10 | 39 | 7 | 34 | 7 | 13 | 1 | 7 | 0 |
| o/w high risk | 0 | 0 | 0 | 0 | 0 | 0 | 5 | 1 | 0 | 0 |
| o/w medium high risk | 32 | 7 | 14 | 6 | 20 | 5 | 8 | 0 | 7 | 0 |
| PIs/EMIs/VASPs | 0 | 0 | 31 | 10 | 71 | 13 | 31 | 8 | 0 | 0 |
| o/w high risk | 0 | 0 | 0 | 0 | 37 | 6 | 31 | 8 | 0 | 0 |
| o/w medium high risk | 0 | 0 | 0 | 0 | 10 | 5 | 0 | 0 | 0 | 0 |

*Note: The total no. in this table covers five categories (high risk, medium-high risk, medium-low risk, low risk, not rated). The table provides a further breakdown of only the first two categories: i.e., high risk and medium-high risk. The reference to “o/w high” in the row on top refers to the number of high severity breaches.

463. Improved compliance is also observed in off-site inspections, through the annual AML/CFT questionnaires. Timely filing of the AML/CFT questionnaires is mandatory and the CSSF's use of injunctions and fines for non-filing has had a positive impact. For example, the CSSF issued a warning against a registered alternative investment fund manager (AIFM) for failing to submit on time its AML/CFT questionnaire for 2018. The CSSF closely monitored the AIFM's filing for 2019 and noted that the AIFM was amongst the first to respond to the annual AML/CFT questionnaire. In the specialised PFS sector, twelve reminders were issued in 2018, three in 2019 (including one injunction) and none for 2020 to 2022. Equally, the proportion of FIs required to re-submit questionnaires because of data issues has significantly decreased over the period.
464. Extensive supervisory work and outreach by the CSSF has also led to a clear change in the risk appetite of its supervised FIs. For example, since the Panama Papers report and the following CSSF thematic analysis, there has been a large reduction in banking services to foreign legal entities: e.g., the number of Panamanian companies fell from 1 300 in 2016 to 428 in 2021 and BVI companies from 4 200 to 1 900 over same period. A similar trend and impact are also observed in the specialised PFS sector (see Box 6.3). Evidence from a survey by the CSSF's private banking expert working group indicates that FIs are using the CSSF SSRAs in their own assessments. Furthermore, there is a significant decline in FIs offering depository services for bearer shares (see IO.5).

Box 6.3. Case Study: Specialised PFS and the “Panama Papers” exercise

In 2017, following the publication of the Panama Papers, all specialised PFS were contacted by CSSF to collect information on their offshore clients (i.e., the client companies which are not domiciled in Luxembourg) following which three on-site inspections were launched. This resulted in a fine of EUR 76 000 for one specialised PFS providing TCSP services and this sanction was published on the CSSF website. Based on the interview with and information provided by the specialised PFS, the CSSF noted that the entity improved its AML/CFT compliance culture as the entity reviewed its STRs filing policy and the number of STRs filed with the CRF-FIU increased, and the entity showed a better understanding of the risks associated with offshore companies and subsequently reduced the number of offshore companies.

Furthermore, the publication of the sanctions related to the Panama Papers on the CSSF's website increased the awareness of the sector regarding the risks related to offshore companies. Several specialised PFS advised CSSF that they have consequently reduced the number of offshore companies serviced.

465. Although the CSSF's competence vis-à-vis VASPs is recent (i.e., March 2020), its actions did have some impact on compliance by VASPs. However, it is too early to draw conclusions. VASPs met appreciate the regular dialogue with the CSSF that helps to improve the level of understanding of technical aspects and risks of business.

CAA

466. The CAA observed, through its review of the annual AML/CFT questionnaires, that insurance professionals take into account guidance the CAA has issued in its circular letters. It also noted the continued development of internal AML/CFT procedures based on the annual statutory audit reports of life insurance undertakings. With tax crime becoming a predicate offence for ML in 2017, the CAA instructed all its life insurance undertakings to implement remediation programmes for customers onboarded prior to 2017. Furthermore, the CAA's active encouragement of its supervised professionals to register with goAML resulted in all life insurance undertakings and 75% of brokerage firms being signed up to goAML.⁵⁶

DNFBPs supervised by the AED and SRBs (OAs, CdN, OEC and IRE)

467. The AED and SRBs are starting to see the positive effects of their supervisory actions on compliance by DNFBPs entities they supervise. This relates to the fairly recent introduction of the risk-based supervision of the majority of the sectors, with the supervision of professional directors by the AED having commenced only recently – thus, not allowing for a clear impact assessment.

⁵⁶ Percentage corresponds to the brokers/brokerage firms registered with goAML and therefore excludes the other intermediaries i.e. agents/agencies engaged in insurance intermediation for and on behalf of one or several Luxembourg-based insurance undertakings and sub-brokers which distribute insurance products under the responsibility and on behalf of brokerage firms or brokers.

468. The AED reports that inspection findings show improvements of the internal AML/CFT policies since 2019, in particular in the area of AML/CFT procedural manuals, appointment of an AML/CFT compliance officer and provision of staff training. However, major shortcomings across the board remain such as in relation to assessing risks. The casino has been supervised for decades and it shows that supervisory actions led to a strong level of understanding of AML/CFT requirements and compliance by the casino.
469. The impact of SRBs' actions is also noticeable for lawyers, CPAs and statutory auditors and audit firms, and led to greater awareness of their important AML/CFT role and their risks. This translated into a reduced appetite for high-risk products and clients and complex structures with no clear economic purpose. The OAs reported a decrease in technical breaches, such as non-registration with goAML, and a decline in offerings of high-risk TCSP activities. The OEC observed an increased compliance of CPAs with AML/CFT obligations, while the CdN noted improved reporting obligations by notaries.

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

470. All supervisors undertake a range of outreach activities to promote a clear understanding by FIs, DNFBPs and VASPs of their AML/CFT obligations and ML/TF risks. These include issuing guidance, well-attended (annual) conferences, training and ongoing feedback as part of supervisory activities. However, a large number of STRs are based on adverse media hits, which can be a valuable indicator for suspicion when analysed by the obliged entity to establish an actual suspicion of ML/TF. . CRF-FIU provided statistics indicating that most of the STRs filed based on adverse media hits included some level of analysis. However, some FIs and a large number of DNFBPs and VASPs met by the assessment team indicated that they provided STRs based on adverse media without further analysis. Furthermore, guidance from the authorities on TF risks and methods to the private sector would be beneficial to ensure obliged entities get a better understanding of TF risks (see IO.4).

CSSF

471. The CSSF has an extensive range of outreach activities which also benefit obliged entities supervised by other supervisors. These activities include issuing AML/CFT regulations accompanied by FAQs, guidance (circulars), monthly newsletters, annual reports and results of thematic reviews (see section 6.2.3), seminars and regular dialogue on an individual basis with its supervised FIs (including as part of the licensing process), and use of social media (e.g., the SSRA for the specialised PFS providing TCSP activities was complemented by a publicly available podcast). The CSSF website (available in English and French) contains specific pages on the regulatory requirements, including guidance, and entities (FIs and others) can subscribe for automatic alerts. Many FIs met appreciated the ability to easily contact the CSSF with questions.

472. The CSSF advises FIs through its circulars on emerging issues and trends on general and sector-specific levels. For instance, at the general level, the CSSF published guidance on the impact of the COVID-19 pandemic on the application of AML/CFT measures, VA-related risks, implications of tax crime becoming an ML predicate offence and application of BO requirements. It also issued sector-specific circulars giving more granularity on risks relating to private banking and the investment fund sector. However, there are no guidance or circulars specifically issued for VASPs to understand their AML/CFT obligations, other than registration requirements. The CSSF did undertake awareness raising activities to inform the private sector of the new VASP regime. VASPs met appreciated the regular dialogue and the ability to easily contact the CSSF. However, they also explained that there is a need for the CSSF to get a better understanding of the VASP business and new technology to provide the appropriate level of supervisory guidance.
473. The CSSF has an ongoing dialogue with the private sector (e.g., meetings, calls, webinars) and collaborates via the CSSF AML/CFT advisory committee (CANTIB) and public private partnerships (i.e., the three CSSF AML/CFT expert working groups⁵⁷). The CANTIB⁵⁸ serves as a platform to exchange information and consult experts before the adoption of a CSSF regulatory text or guidance, while the three CSSF AML/CFT expert working groups focus on the sectors found to be highly vulnerable to ML/TF risks. All these initiatives have been well-received and appreciated by FIs met. The CSSF also host its own events and takes part in seminars organised by the private sector. At these conferences, the CSSF presents general and specific topics, including the CSSF's SSRAs, trends and observations made during its supervisory inspection work (e.g., what breaches of AML/CFT obligations it has detected and what enforcement measures it took).

CAA

474. The CAA undertakes a range of outreach aimed at promoting a clear understanding of AML/CFT obligations and ML/TF risks. These include providing advice, since 2011, through circulars, information notes, training and other engagement activities. Since 2019, it provides annual AML/CFT training. The CAA issued regulations to support the application of the 2004 AML/CFT Law and published circulars letters, information notes and annual reports. These documents are available on its website and professionals can subscribe for automatic alerts. The CAA organises and participates in public events, and has regular meetings with individual FIs and professional associations. The CAA has a public private partnership platform (the CAA AML/CFT Technical Committee) allowing it to engage with its supervised entities, professional associations and other supervisors on AML/CFT matters including new regulations and circular letters.

⁵⁷ These are collective investments (OPC EWG), private banking (PB EWG) and specialised PFS (EWG PFS-SP, only established in September 2022), and are attended by relevant professional associations, the CRF-FIU and other competent authorities, and meet on a monthly (OPC EWG) or quarterly basis (PB EWG).

⁵⁸ It consists of senior compliance experts from supervised FIs, professional associations, the CRF-FIU and relevant ministries.

475. Like the CSSF, the CAA uses the licenses process and its supervisory work to promote a clear understanding of AML/CFT obligations and ML/TF risks in the insurance sector. For example, the CAA organised meetings with prospective applicants relocating from London to Luxembourg to ensure that regulatory requirements were understood.

AED

476. The AED undertakes various forms of outreach: through guidance (e.g., *guichet.lu* provides an easily accessible and simple summary of the AML/CFT obligations and the questionnaires), annual conferences, a webinar, newsletters for all sectors and bilateral meetings with its supervised entities and professional associations. The AED issued specific guidance for all sectors apart from the casino (as this is covered by the regular dialogue between the casino and the AED, and strong understanding of AML/CFT obligations by the casino). While guidance is thorough for REAs, for the other sectors the documents provide high-level information repeating the legislation and obligations with no concrete examples. However, the AED started issuing newsletters as of January 2020, which contribute to informing these sectors on AML/CFT issues such as the NRA outcomes and the importance of reporting obligations and registration with goAML.
477. With the real estate sector being highly vulnerable to ML/TF risks and having a limited understanding of risks and obligations, the AED increased its efforts in recent years: it sent a series of specific newsletters in 2021 and 2022, which provided additional guidance on AML/CFT obligations and the NRA outcomes, presented at a webinar and the Chamber of Commerce. These events elaborated on the AML/CFT requirements, including how to assess risks and organise internal controls, and main deficiencies in the sector observed through supervisory work. Professionals interviewed during the on-site visit were generally aware of these outreach activities. However, some REAs and DPMS felt that they would benefit from more detailed and practical guidance, with concrete examples, on how they can be misused for ML/TF and how to respond to recurring deficiencies found across the sector.

SRBs (OAs, CdN, OEC, IRE)

478. All SRBs have prioritized outreach and training activities for the sectors they supervise. These activities include regular conferences, webinars, training and bilateral meetings with entities as well as issuing FAQs and close follow-up interventions. Most obliged entities met appreciated and were satisfied with the outreach actions organised by their supervisors. However, some indicated that they would have an interest in more e-learning activities that they could follow at their own pace.

Overall conclusion on IO.3

Luxembourg's supervisory regime has been steadily maturing in recent years, although many of these efforts remain recent and their full effectiveness is yet to be seen, particularly for DNFBPs. In 2020, the powers of DNFBP supervisors (AED and SRBs) were standardized and aligned with the CSSF powers and VASPs were included in the supervisory framework. For professional directors (TCSPs) supervised by the AED, supervision only started in 2022.

Market-entry controls are robust across the board. All supervisors have been increasingly improving their supervisory tools and approaches, such as the use of annual AML/CFT questionnaires to inform their understanding of risks in their sectors and at entity level to inform risk-based supervision. As a result, FI supervisors have a good understanding of ML/TF risks. This is more mixed for DNFBPs supervisors as they are enhancing their risk-based approach. Weight is given to the level of understanding by supervisors of the TF risks and vulnerabilities in their sectors, which is less granular than for ML risk but improving with the TF VRA of May 2022 and needs to be further integrated in the work of supervisors.

Off-site supervision and monitoring, and on-site inspections are becoming increasingly focused, which links back to the evolution kick-started in 2020. While the CSSF has a risk-sensitive multi-pronged supervisory approach, improvements are needed for the DNFBP supervisors, and some weight is given to the recency of the supervision of VASPs by the CSSF and professional directors (TCSP) by the AED. The AED, supervising high-risk sectors like REAs, does not have a fully mature risk-sensitive approach. Furthermore, several supervisors (AED and OEC), in charge of several higher risk sectors (such as CPAs providing TCSP activities), have limited resources to effectively conduct supervision and the CdN, supervising a high-risk sector (notaries), uses mainly a peer review mechanism (with the exception of a lawyer hired as a supervisory officer in 2021) and the lack of fines calls into question whether independence of the supervision function is sufficient.

Major improvements are needed in the use and application of supervisory sanctions. The CSSF uses a variety of remedial actions and sanctions; however, weight is given to the brevity of its public statements, by virtue of which no one clear documented messages about the deficiencies are set for the vast financial industry. The CAA has used its sanctioning power in a very limited manner. The AED broadened its powers in 2018 and remedial actions have been steadily increasing since 2019. These actions are becoming more dissuasive, but non-compliance rates remain high. The CdN is reluctant to impose sanctions on notaries.

FI supervisors' work demonstrates an increased compliance culture; however, this is less the case for DNFBPs, given the recent introduction of the risk-based approach of the majority of sectors.

Luxembourg is rated as having a Moderate level of effectiveness for IO.3.

Chapter 7. LEGAL PERSONS AND ARRANGEMENTS

Key Findings and Recommended Actions

Key Findings

1. Luxembourg demonstrates a good understanding of the ML risk posed by legal persons and legal arrangements, including through a dedicated vertical risk assessment (VRA), while the TF risk understanding is less developed.
2. Luxembourg relies effectively on a wide range of mitigating measures, including the establishment of the Beneficial Ownership Registers for Legal Persons (RBE) and Legal Arrangements (RFT), restrictions on bearer shares and involvement of obliged entities in the creation, maintenance and operation of most legal persons and legal arrangements.
3. In performing their tasks, competent authorities have unrestricted and direct access to, and make effective use of, the Trade and Company Register (RCS), beneficial ownership information of legal persons register (RBE), and beneficial ownership information of legal arrangements register (RFT) to obtain basic and BO information. They also access CDD information from obliged entities in a timely manner. Competent authorities and obliged entities, who also have access to the RCS and RBE, clearly understand their obligation to file discrepancy reports to the registrars should they discover inaccurate, missing or out of date information, which helps ensure accuracy.
4. There are a limited number of legal arrangements in Luxembourg (domestic *fiducies* or foreign trusts), and their BO information can be directly obtained by the competent authorities and obliged entities through the RFT. The competent authorities can also access information from or the fiduciaires or trustees. For Luxembourg or EU corporate settlors or corporate beneficiaries, information would be available through the RBE or similar EU registers, and for non-EU incorporated legal persons being a settlor or beneficiary the beneficial owner would be registered in the RFT. While the registrar (AED) does not conduct verification, obliged entities acting as fiduciaires are to investigate and record beneficial owners as part of their CDD process.
5. While a range of administrative and criminal measures and sanctions are available to address non-compliance with information requirements, they have been applied to varying extent. Only criminal penalties are available for violation of legal person BO disclosure requirements, which sharply limits the proportionality, timeliness and effectiveness of sanctions. Moreover, it requires involvement of the State Prosecutor, which detracts resources from higher AML/CFT priorities. Also, only limited criminal fines have been imposed for not maintaining or updating lists of members or a register of shares.

Recommended Actions

1. Luxembourg should provide the LBR with powers to administratively sanction non-compliance with the BO information requirements relating to legal persons.
2. Luxembourg should review and update its range of available sanctions for failure to maintain or update lists of members or a register of shares to ensure that sanctions are effective.
3. Luxembourg should advance its proposal to reduce the timeframe for the LBR to proactively investigate corporate non-filing in the registers from ten to five years.

7

479. 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 40.⁵⁹
480. The assessment team's findings are based on discussions with Luxembourgish authorities and obliged entities, and information provided by the authorities, including statistics, risk assessments and case studies.

Immediate Outcome 5 (Legal Persons and Arrangements)

481. All legal persons incorporated in Luxembourg must be registered with the Luxembourg Trade and Company Register (RCS). This register contains basic information on legal persons. There are two registers maintaining beneficial ownership (BO) information: the RBE on legal persons and the RFT on legal arrangements. The RCS and RBE are managed by the LBR (an economic grouping placed under the authority of the MoJ) and the RFT by the AED.
482. Luxembourg recognises domestic *fiducies*⁶⁰ and foreign trusts (in line with The Hague Convention of 1 July 1985). Trusts created under foreign law can be administered in Luxembourg and anyone can act as trustee. BO for both forms of legal arrangements must be filed with the RFT. Additionally, *fiducies* are required to register with the AED for tax purposes if a tax liability occurs.

⁵⁹ 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.

⁶⁰ Domestic *fiducies* are contractual agreements whereby the settlor (fiduciant) agrees with the fiduciary (fiduciaire) that the latter will become the owner of certain fiduciary assets (patrimoine fiduciaire) under agreed conditions. Luxembourg legislation prescribes which professionals can act as a fiduciary (i.e., credit institution, investment firm, an investment company with variable or fixed share capital (SICAV, SICAF), securitisation company, fiduciary representative acting in the context of a securitisation transaction, management company of common funds (FCP) or of securitisation funds, pension fund, insurance or reinsurance undertaking, national or international public body operating in the financial sector, other professionals covered by the 2004 AML/CFT Law and 2020

Public availability of information on the creation and types of legal persons and arrangements

483. Luxembourg has five main types of legal persons: commercial companies, civil companies, *Associations sans but lucratif* (ASBLs), *Fondations* and other legal persons (e.g., public institutions). Private limited companies (a type of commercial company) are the most common sort of legal person and account for 53.4% of all entities active in the RCS (see Table 1.3 for a complete overview of legal persons in Luxembourg).
484. Information on the creation and types of legal persons in Luxembourg is publicly available in English, French and German through an information portal published and hosted by the government: www.guichet.lu. This website provides user-friendly access explaining the main steps for creating a legal person, including legal forms and guidance documents. For ASBLs, information and guidance on registration is also publicly available in French and German on www.benevolat.public.lu.
485. Investment funds can have two types of structures: (1) non-corporate established by contract (*Fonds commun de placement*, FCP) and (2) corporate. All Luxembourg investment funds, whether non-corporate (FCP) or corporate (e.g., a *Société d'Investissement à Capital Variable* (SICAV) or *Société d'Investissement à Capital Fixe* (SICAF)) must register with the RCS and RBE. Information on the forms of investment vehicles and funds is publicly available on the websites of the CSSF and *Association Luxembourgeoise des Fonds d'Investissement* (ALFI).
486. For legal arrangements, information on the creation and obligations is publicly available in English, French and German through the same website (www.guichet.lu) and several other sources, including the AED website (<https://pfi.public.lu/fr/blanchiment/registre-fiducies-trusts.html>), the 2003 *Fiducies* and Trusts Law and TCSPs providing information directly to their customer interested in setting-up a *fiducie*. Luxembourg has 1 430 legal arrangements, out of which 22 are foreign law trusts (as of 30 September 2022).

Identification, assessment and understanding of ML/TF risks and vulnerabilities of legal entities

487. Luxembourg identified and assessed the ML/TF risks and vulnerabilities of legal persons and legal arrangements through several risk assessments. Luxembourg recognises that its open economy and large financial sector means that Luxembourg's corporate sector is more exposed to foreign threats compared to domestic threats. Competent authorities demonstrated a good understanding of how legal persons can and are misused for ML purposes; however, the level of TF risk understanding is less comprehensive compared to that of ML.

RFT Law). The conditions include instructions for the fiduciary over managing the entrusted assets (*fiduciary mission*) and the obligation to clearly separate entrusted asset of each agreement (*fiduciary estate*) from other property belonging or entrusted to the fiduciary agent. The transfer of ownership requires the agreement of two parties.

488. The 2018 NRA and 2020 NRA (update) concluded *high vulnerability* of specific legal persons and legal arrangements (namely commercial companies and *fiducies*). The dedicated and more granular 2022 LPA VRA confirmed this, while the 2022 TF VRA focused on TF risks and vulnerabilities in the FI, DNFBP, VASP and NPO sectors. The risk assessments involved Luxembourg authorities and the private sector and were based on various sources including from the registers to understand the risks. The CSSF also conducted SSRAs on the collective investment sector (2020; 2022 update) and TCSPs (2020) which reflect the economic activity undertaken through Luxembourg's legal persons and the sector's vulnerability to ML; however, the TF assessment is more limited as it focuses on low-level forms of TF (e.g., low value transactions, short-term requirements, reliance on informal payment channels).
489. Overall, the ML risk assessment and understanding is thorough as demonstrated by the 2022 LPA VRA which, for instance, analysed the extent to which legal persons owned and controlled (director roles in) Luxembourg legal persons. The national-level risk assessments also investigated transnational cases such as those involving the concealment of assets in Luxembourgish and foreign companies through complex corporate operations and multiple trusts. Luxembourg acknowledges that commercial companies, representing 87% of the total registered entities, have the highest probability of misuse due to a high exposure to corporate shareholders and foreign (beneficial) ownership.
490. As regards TF risk, Luxembourg has been developing its TF understanding for which the confidential version of the 2022 TF VRA shows a good understanding of low-level and high-level TF risks. The analysis examined financial and non-financial connections of legal persons with higher risk jurisdictions, and focused on higher risk sectors and NPOs (ASBLs and *Fondations*). However, there has been less scrutiny of the activities and assets of other forms of legal persons and legal arrangements than NPOs to ascertain their TF vulnerabilities. Authorities explained that, due to a high TF exposure, the VRA focused on the NPO sector, while ML and TF risks were considered together for other types of legal entities. While the assessment team acknowledges this approach, it is unclear if Luxembourg sufficiently assessed and considered the TF threats for other forms of legal persons than for ASBLs and *Fondations*.
491. Luxembourg authorities pro-actively took steps to investigate and address events which could involve potential ML/TF misuse of Luxembourg legal persons. For instance, the Panama Papers triggered thematic inspections and review by the CSSF, using external inspectors to augment its on-site supervisory programme, of the use of corporate legal structures by banks, investment firms, IFMs and specialised PFS (see 10.3). Similarly, the Luxembourg tax authorities commenced investigations into Luxembourg companies linked to the Panama Papers (see Box 7.1).

Box 7.1. Case Study: Panama Papers – ACD investigation

In September 2020, the tax authorities of a neighbouring jurisdiction spontaneously transmitted to the ACD a large quantity of documents from the "Panama Papers" with a direct link to Luxembourg, including e-mail traffic, incorporation documents of offshore companies, trust agreements, company resolutions, source of funds, and copies of passports. The ACD's analysis resulted in the identification of various Luxembourgish beneficial owners of offshore companies. The information went to the various tax offices and investigations were launched mid-2022 which were ongoing at the time of the on-site visit for this mutual evaluation.

Mitigating measures to prevent the misuse of legal persons and arrangements

492. Transparency of legal persons and legal arrangements is a key pillar in Luxembourg's AML/CFT efforts. Luxembourg relies on a wide range of measures to prevent misuse of legal persons and legal arrangements for ML/TF purposes, including licensing and tax controls, BO registers, and supervision of obliged entities involved in the creation and maintenance of legal persons and arrangements.

AML/CFT gatekeepers

493. Various obliged entities are involved at the creation and during the life of legal persons and legal arrangements (e.g., banks, TCSPs, statutory auditors, notaries). All these entities perform checks on their clients, including identifying and verifying the beneficial owner and screening names against TFS and PEP lists. These actors are supervised for compliance with their AML/CFT obligations (see IO.3, IO.4).
494. Many companies can only be incorporated through a notarial deed (i.e., SARL, SA, SCA, SAS, SE, SCE, *Fondations*). Once the notarial deed is issued, the legal person must file with the RCS to register. In practice, for the vast majority of companies registered in Luxembourg these filings are undertaken by a notary or a TCSP. Around 77% of the legal persons registered in the RCS were established by notarial deed as of Q3 2022 (see Table 7.1). Any subsequent amendment to the articles of association must also go through the notary and most commercial companies need to have their financial statements audited by an approved statutory auditor. This close involvement of obliged entities in the formation and maintenance of such a large percentage of legal persons helps to prevent the misuse of legal persons and legal arrangements.

Table 7.1. Number of legal persons registered with the RCS as of Q3 2022

| | Number | % total | Notarial deed mandatory | Notarial deed optional |
|---|----------------|-------------|-------------------------|------------------------|
| Commercial companies, incl. | 126 183 | 87.1% | | |
| <i>Société à responsabilité limitée</i> (SARL) | 77 357 | 53.4% | √ | |
| <i>Société anonyme</i> (SA) | 31 532 | 21.8% | √ | |
| <i>Société en commandite spéciale</i> (SCSpé) | 7 735 | 5.3% | | √ |
| <i>Société à responsabilité limitée simplifiée</i> (SARL-S) | 4 701 | 3.2% | | √ |
| <i>Société en commandite par actions</i> (SCA) | 2 200 | 1.5% | √ | |
| <i>Société en commandite simple</i> (SCS) | 1 944 | 1.3% | | √ |
| <i>Société en nom collectif</i> (SENC) | 140 | 0.1% | | √ |
| <i>Société par actions simplifiée</i> (SAS) | 241 | 0.21% | √ | |
| <i>Société cooperative</i> (SC) | 149 | 0.1% | | √ |
| <i>Société coopérative organisée comme une SA</i> (SCSA) | 127 | 0.1% | | √ |
| European companies (SE) | 56 | <1% | √ | |
| <i>Société cooperative européenne</i> (SCE) | 1 | <1% | √ | |
| Civil companies | 6 044 | 4.2% | | √ |
| ASBLs | 8 664 | 6% | | √ |
| <i>Fondations</i> | 193 | 0.1% | √ | |
| Other legal entity types* | 3 768 | 2.6% | | √ |
| <i>Société d'Investissement à Capital Variable</i> (SICAV) | 1 111 | 0.8% | √ | |
| <i>Fonds commun de placement</i> (FCP) | 1.491 | 1.03% | | √ |
| Total registered in RCS | 144 081 | 100% | | |

*Note: See for the full breakdown of this category Chapter 1. Note that FCPs do not have a legal personality but are registered in the RCS.

Supervision

495. Supervisory monitoring of FIs and DNFBPs compliance is an important tool to ensure legal persons and legal arrangements are not misused. During off- and on-site inspections, supervisors check whether obliged entities consistently identify beneficial owners as part of the CDD process (see IO.3, IO.4). Within this framework, supervisors consult the registers and report discrepancies to the registrars. For example, in November 2021 the CSSF conducted an AML/CFT on-site inspection to a bank and, as the bank offered fiduciary services to its clients, it specifically added a control point to the inspection plan. During the inspection, the CSSF verified that the bank complied with its information reporting requirements to the RFT. The insurance sector supervisor (CAA) performs an annual check of the RBE against the information it holds. These supervisory measures help ensure the accuracy of information held in the registers.
496. Another example of supervisory action as a means to prevent the misuse of legal persons, is the work of the CSSF and OAL (SRB of lawyers). Following the Panama Papers, Pandora Papers and OpenLux reports, several supervisors analysed the potential implications of these revelations on their supervised entities. In this context, the CSSF's thematic analysis following the Panama Papers led to two large, specialised PFS decreasing their number of offshore legal persons serviced from 24 and 41 in March 2016 to three and eight in 2020, respectively (see IO.3). The OAL investigated whether their registered lawyers or law firms were implicated in the Pandora Papers and OpenLux reports but found no link with Luxembourgish legal professionals.

License, VAT registration and tax controls

497. Licensing and VAT registration regimes provide further risk mitigation, including when an obliged entity is not yet involved. The MoE and AED require BO information, which they check against the registers. A business permit by the MoE is required for commercial companies to offer commercial, craft or industrial activities⁶¹. *Fondations* are established through a strict licensing process involving the MoJ and the approval by a Grand-Ducal decree.
498. To supply goods or services, an entity must register with the AED for VAT purposes. The AED requires a set of information and documents which it will verify against the registers⁶². The VAT registration is suspended or refused if the required information is not provided: on average 4,1% of the registration requests was refused in the past five years (2017-2021). While civil companies may not necessarily be constituted through a notary deed, they are required to submit an annual tax declaration. Furthermore, over the past years, with the introduction of tax crime as a predicate offence in 2017, the ACD increased investigations and convictions for aggravated tax evasion and/or tax fraud of company directors or employees who misuse legal persons (see Box 7.1).

Registers: RCS, RBE and RFT

499. The Luxembourg registers containing basic and BO information of legal persons and legal arrangements constitute a strong risk mitigating measure. While the RCS existed for many years, prior to the current review period, the RBE and RFT were established in 2019 and 2020 respectively. These registers play a prominent role in Luxembourg's framework to prevent abuse of legal persons and arrangements, and seek to enhance transparency at various levels.

⁶¹ To obtain a business permit, a person needs to fill in the application form, meet the prerequisite conditions (e.g., professional integrity, professional qualification in line with the planned activity, compliance with tax and business obligations (the business manager must not have evaded business and tax obligations in their previous or current business activities), effective and permanent management of the business by the business holder), submit proof of payment of the stamp duty and provide supporting documents (which vary depending on the type of activity to be pursued). For commercial activities, such supporting documents include a copy of the ID and an extract of the criminal record. The final granting of the business permit requires that the articles of association are filed with the RCS. Information on the process and documents required is publicly available at: <https://guichet.public.lu/en/entreprises/creation-developpement/autorisation-etablissement/autorisation-honorabilite/autorisation-etablissement.html>.

⁶² To register for VAT, the taxable person must submit a declaration (which contains the company name, legal form, address of the registered office, date of the constitutional documents, names and address of named partners listed in the constitutional documents and/or business managers/directors of the company), and submit, in the case of legal persons, copies of the constitutional documents and ID of the partners listed in those documents and/or business managers/directors of the company. Further information on the information and documents required is publicly available at: <https://guichet.public.lu/en/entreprises/creation-developpement/declarations-initiales/tva-impots/inscription-tva.html>.

500. All entities are obliged to submit and update their data in the respective registers and are subject to administrative and criminal sanctions if they do not comply with these requirements (see section 7.2.6). A unique identifier (*LuxTrust*) is needed to enter the register, which allows the registrar to trace the person who has submitted the information (see section 7.2.4). The LBR checks the data at submission. The LBR received around 184 000 applications for the RCS and 44 000 for the RBE in the first three quarters of 2022. The LBR regularly refuses to register legal persons in the RCS and RBE on the basis of incomplete information (see Table 7.2). The LBR also carries out ex post controls through its administrative striking off process (see sections 7.2.4 and 7.2.6).

Table 7.2. Percentage of refusals to register in the RCS and RBE, 2019-Q3 2022

| | 2019 | 2020 | 2021 | Q3 2022 |
|----------------------------|------|------|------|---------|
| RCS percentage of refusals | 16% | 14% | 14% | 15% |
| RBE percentage of refusals | 19% | 15% | 14% | 20% |

501. Competent authorities (including supervisors, see above) and obliged entities demonstrated that they make use of the registers and report inconsistencies to the LBR. Between September 2019 and May 2022, the LBR received 206 discrepancy reports from competent authorities and obliged entities. The LBR sent verification requests and 153 files were updated in the RBE with 41 transmitted to the State Prosecutor and 12 files pending.

502. Regarding the RFT, the AED has not yet refused to register a legal arrangement. The AED performs no verification checks as it is not responsible for the content of the registered information provided by obliged entities in their role as fiduciaire (see section 7.2.5). Only some obliged entities, such as banks and investment firms, can act as fiduciaire and they are required to verify the information and documentation as part of their CDD before filing the BO information with the RFT. Competent authorities have direct access, and obliged entities can register for access to the RFT. At the end of the on-site visit, 15 obliged entities had registered. The AED has not yet received any discrepancy reports. These are not considered as a significant concern given the relatively small number of legal arrangements recorded.

Bearer shares and bearer share warrants

503. Bearer shares are permitted and can be issued in Luxembourg. There are strong controls in place including dissuasive fines for non-compliance, resulting in a significant decline in the overall number and issuance of new bearer shares. Companies issuing bearer shares must designate a depository with whom all bearer shares are deposited and who is not a shareholder of the company itself. Only certain FIs and DNFBPs, who are obliged entities, may act as depository: i.e., credit institutions, asset managers, distributors of UCI shares, specialised PFS, lawyers, notaries, statutory auditors and CPAs. The designated depository must keep a register of bearer shares in Luxembourg and have its identity registered in the RCS and published in the official Gazette. There are 3 536 companies who declared having bearer shares, 187 registered depositories in the RCS out of which 135 are legal persons, including two banks in Luxembourg (in 2021). The number of legal persons having issued bearer shares that are deposited with banks, specialised-PFS, investment firms or IFMs has been decreasing over the years: 493 in 2017, 377 in 2018, 364 in 2019 and 318 in 2020. Bearer shares are monitored through regular tax audits, manual review of the RCS by the LBR and supervisory work (e.g., on-site inspections (for example, the CSSF inspected two out of the three investment firms acting as depository of bearer shares), annual off-site supervisory AML/CFT questionnaires and supervisory outreach).
504. Luxembourg does not have explicit restrictions on the issuance of bearer share warrants and there are no measures in place to mitigate the risks poses by these specifically (see R.24). However, in practice this appears to be a minimal risk, as under the Luxembourg 1915 Companies Law, companies cannot issue instruments that could be considered as equivalent to bearer share warrants⁶³.

⁶³ Companies, can, however, issue subscription rights (*droits de souscription*) which give a person a right to acquire a share in a company at a given time and at a given price. These *droits de souscription* are only an option, they provide the possibility to become a shareholder/to acquire a share at the expiration of the offering/subscription phase and do not result in any right which could be attached to a shareholder or beneficial owner before such option is activated by the holder of the *droits de souscription*. Thus, the holding of *droits de souscription* cannot result in such a person being able to control a company, receive dividends, or have voting rights, which are only attached to the share itself. A person having acquired *droits de subscription* cannot therefore exercise any right that would qualify him as a shareholder or beneficial owner of the company. Ownership of shares will only be possible if the holder of such warrant decides to make use of such option. If the option is used, the warrants can be converted into nominative shares and are then registered in the shareholders registers or converted into bearer shares and the bearer share mechanism fully applies to them, i.e., they have to be immobilized at the depository and registered in the bearer shares register. Only then, can the holder be qualified as a shareholder of the company.

Nominees

505. While Luxembourg does not formally recognise the concept of nominee shareholders or nominee directors, proxy arrangements⁶⁴ and directorship services are possible and where they arise, they are mostly provided by TCSPs who are obliged entities. Proxy arrangements and directorship services, which seek to facilitate administrative formalities, neither correspond to the nominee shareholder or nominee director concepts nor enable shareholders to conceal their identity. Proxy arrangements and directorship services have been analysed as part of the 2022 LPA VRA and considered as having a *low* vulnerability. Luxembourg legal persons could have legal persons acting as directors. In these situations, a natural person is required to be identified which mitigates the risk around directorship services. When it comes to proxy arrangements, these are short-term and limited in nature, and the RBE captures beneficial owners. These contracts may be drawn up by a lawyer or may be notarized.

Timely access to adequate, accurate and current basic and beneficial ownership information on legal persons

506. Luxembourg ensures timely access to basic and BO information on legal persons via three sources: (1) the registers, (2) directly from obliged entities, and (3) directly from legal persons themselves. None of the competent authorities interviewed indicated having experienced difficulties obtaining basic or BO information over the review period.

Source #1 – registers of basic and beneficial ownership information

507. The RCS and RBE provide immediate and easy access to information for competent authorities. FIs and DNFBPs can also access the RCS and, until the end of the on-site visit, the RBE allowing them to conduct background checks and due diligence on corporate clients.⁶⁵ In general, LBR statistics show that there were 16.6 million documents researched in the RCS website and 11.1 million page views on the RBE website. The online dedicated search portal allows authorities to search by name of beneficial owners and by entity name. The accuracy of the data contained in the registers is ensured through checks by the LBR upon first entry and through ongoing monitoring (such as *ad-hoc* reviews or following-up on discrepancy reporting). The search functionality and information available to authorities is more comprehensive and detailed than that previously available to the public. The RBE was introduced in 2019, and by the end of that year BO information had been filed for 92% of legal persons.

⁶⁴ Under a proxy arrangement service, the proxy will not only be obliged by law to identify his or her principal but will also disclose the existence of this proxy relationship to any relevant stakeholder. Consequently, (i) the identity of the beneficial owner (the principal) will be known and verified before being registered in the shareholder books and ii) the status of the proxy acting on behalf of the principal will be transparent and disclosed to third parties, thus preventing any misuse of shareholder arrangements which would hide the identity of ultimate beneficial owner.

⁶⁵ On 22 November 2022, the Court of Justice of the European Union issued a decision on the compatibility of the public access to the BO information kept in registers by the EU Member States. This decision does not impact the access of the Luxembourg competent authorities to the information held in the RBE. The assessment of IO.5 only takes into account the effectiveness of the authorities' access to the BO information (and not of the

508. Registration in the RCS is needed for the daily business operation of a legal person and is done through an online process. To submit a request to the RCS the applicant requires a unique identifier (*LuxTrust*). Most registrations are requested by TCSPs or notaries, which are obliged entities and thus are required to conduct CDD on their clients. The information submitted is checked against the national natural persons register (RNPP), the CACLR platform for addresses and whether there is a business licence issued by the MoE. Each entity registered in the RCS, except for traders who are natural persons, must file with the RBE and similar verification controls are put in place. A company not meeting the RBE filing obligations is identified as “certificate of non-registration of beneficial owner(s)”. Since 2020, the LBR sends, every month, to the State Prosecutor a list of new entities registered in the RCS that have not declared with the RBE: in 2020 13% of the new registered entities was referred for not having filed with the RBE; this fell to 6% in 2021 and in 2022 (until end of Q3 2022).
509. After registration, entities are obliged to update information in the RCS and RBE within thirty days following a change in their data. Entities face penalties for non-compliance with their filing obligations, ranging from EUR 1 250 to EUR 5 000 for the RCS and EUR 1 250 and EUR 1 250 000 for the RBE (see section 7.2.6). In 2019, the LBR launched annual exercises to clean the RCS register of inactive entities: legal persons who have not filed updates for more than ten years were contacted and those who did not respond within the set timeframe were struck off from the RCS. These exercises resulted in many companies (about 25 000 between 2020 and 2022) struck off from the RCS. In 2020, the LBR reached out to 1 319 entities who declared BO information with the RBE but had not updated their RCS data for more than ten years. This operation revealed 286 entities with an outdated address and the files were transmitted to the State Prosecutor.
510. LEAs, supervisors, the CRF-FIU and other authorities (e.g., tax) consult the registers as a starting point to corroborate information. Competent authorities and obliged entities report to the LBR discrepancies uncovered between the information they hold and what is registered in the RBE. The RBE compliance rate with the filing of BO information has been improving and is now 93% for commercial companies, 85% for civil companies, 84% for *Fondations*, 94% for ASBLs and 96% for other legal persons⁶⁶.

Source #2 – obliged entities

511. The CRF-FIU and the Office of the Investigative Judge (investigative judge) directly request information from FIs, DNFBPs and VASPs. The CRF-FIU applies a double check approach: when it detects missing BO information in the RBE or inconsistencies between the RBE and the information the CRF-FIU holds, it sends information requests to the obliged entities (see Table 7.3). On average the CRF-FIU receives a reply within six days, which the assessment team considers to be timely.

public’s access). After a temporary suspension of the online access to the RBE for persons other than competent authorities, the LBR issued Circular LBR 22/01 (December 2022) reopening access to the RBE for professionals based on the signature of an agreement by the professional.

⁶⁶ The remainder consists of newly formed legal persons who still have time to file their BO information with the RBE as well as legal persons who did not meet their RBE filing requirements.

Table 7.3. Number of BO information requests sent by the CRF-FIU to obliged entities (2017-Q3 2022)

| Types | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|------------------------|------|------|------|------|------|---------|
| Financial Institutions | 184 | 257 | 373 | 511 | 625 | 409 |
| DNFBPs | 42 | 46 | 89 | 69 | 93 | 46 |
| VASPs | 1 | 4 | 11 | 11 | 14 | 7 |
| Total | 227 | 307 | 473 | 591 | 732 | 462 |

512. Supervisors identified few serious CDD deficiencies and whilst there have been remediation programmes within FIs and DNFBPs, these have not been around identity information but related to changes in regulatory requirements, or remediation brought about by acquisitions.

7

Source #3 – legal persons themselves

513. Authorities (including supervisors) can directly request beneficial ownership information from concerned legal persons, who must respond within three days of the request. The assessment team considers this to be timely. Judicial authorities and the CRF-FIU do not use these powers as to avoid any risk of tipping-off, and rather use the abovementioned sources to investigate potential misuse of corporate structures.

Timely access to adequate, accurate and current beneficial ownership information on legal arrangements

514. Competent authorities obtain beneficial ownership information on legal arrangements directly from the fiduciaries and trustees or the register (RFT).
515. Fiduciaries and trustees are required to obtain and keep adequate, accurate and current BO information of any *fiducie* and trust administered in Luxembourg for which they act as fiduciary or trustee. They are also required to obtain and keep basic information on other professionals and entities governed by foreign law which, if their registered office were located in Luxembourg, would be considered as professionals which provide services to the trust or *fiducie* or which enter into a business relationship with the trust or *fiducie* (see R.25). Competent authorities and SRBs can directly request this information from fiduciaries and trustees. For example, the CRF-FIU sought to obtain BO information from directors of companies mentioned in the OpenLux press articles who acted as trustees. While no specific statistics are kept, experience so far on other similar information requests to obliged entities indicates that responses would be received timely and within timeframes set by the authorities. The CRF-FIU explained it receives responses within four to eight days.

516. Since 2020, BO information of legal arrangements is recorded in the RFT. Competent authorities have immediate and unrestricted access to the register. The RFT⁶⁷ captures three situations of *fiducies* and trusts.⁶⁸ Each *fiducie* and trust registered is assigned a unique registration number⁶⁹ and records the BO information. The AED, as the registrar of the RFT, checks the entries against TFS and PEPs lists but does not undertake verification controls. An obligation to update the information, within thirty days of change, rests on the fiduciaries and trustees. To date, the AED has not received any discrepancy reports.
517. Luxembourg ensures the adequacy and accuracy of the information through supervisory activities. Only a set number of obliged entities can act as fiduciary (e.g., banks, investment firms, asset management companies). When obliged entities enter a business relationship with, or provide an occasional transaction to, a *fiducie* or trust, they are required to investigate corporate structures and record beneficial owners as part of the CDD process. As such supervisors monitor compliance by obliged entities with their reporting and record-keeping requirements. Furthermore, if the corporate settlor or corporate beneficiary is a Luxembourg or EU company, BO information will be available in the RBE or an equivalent register of another EU Member State. Where the legal person is incorporated in a non-EU Member State, the beneficial owner has to be registered with the RFT. Nearly half of all *fiducies* are formed by one bank for short-term cash management of funds held by collective investment schemes. The CRF-FIU generally goes directly to the obliged entity acting as fiduciary or trustee to obtain the information and supporting documents, instead of relying solely on the RFT. International cooperation demonstrates that basic and BO information is exchanged regularly and in an accurate manner (see IO.2).

⁶⁷ The following website specifies what information is declared: <https://pfi.public.lu/content/dam/pfi/pdf/blanchiment/registre-des-fiducies-et-des-trusts/Exemple-demarche-RTF.pdf>.

⁶⁸ Every *fiducie* or trusts of which a fiduciary or trustee is established or resides in Luxembourg must be registered in the RFT. This also goes for fiduciaries and trustees established or resident in a different EU Member State, and those not established either in the Luxembourg or in another EU Member State where the fiduciary or trustee, on behalf of the trust or *fiducie*, enters into a business relationship in Luxembourg with a professional or acquires real estate which is situated in Luxembourg (2020 RFT Law, Art.13).

⁶⁹ The registration specifies the registration number, the name of the *fiducie* or trust, if any, the date on which the *fiducie* or trust was entered into, the BO information and whether the *fiducie* or trust holds or has controlling interest in a company or legal entity (2020 RFT Law, Art.14(1)).

Effectiveness, proportionality and dissuasiveness of sanctions

518. Luxembourg can apply administrative measures, criminal fines and supervisory sanctions for failing to file or provide basic and BO information. Luxembourg implemented effective, proportionate and dissuasive sanctions to some extent. While a variety of sanctions and measures have been issued for non-compliance with basic information record-keeping requirements, only criminal penalties have been imposed to breaches relating to requirements on filing and providing BO information of legal persons. The latter requires the involvement of the State Prosecutor's Office and the District Court, which limits the timely application of sanctions for those kinds of breaches and also raises concerns regarding proportionality. No sanctions have been applied for non-compliance with the legal arrangement information requirements.

7

RCS

519. There are several sanctions available for non-compliance with basic information requirements: (1) administrative striking-off from the RCS, (2) judicial liquidation of the legal person, (3) pecuniary fines.
520. Over the past three years, the LBR conducted an annual administrative exercise to remove from the RCS registered entities that have not made any filing for ten years. More than 25 000 entities were considered inactive in annual exercises undertaken between 2020 and 2022 and were flagged as "struck off" in the RCS.⁷⁰ This administrative measure is considered effective, proportionate and dissuasive to a certain extent. The ten years timeframe is quite broad, but there are proposals to reduce this to five years which would make the measure more effective. Entities not yet struck off but considered inactive are analysed by the LBR and, if necessary, referred to the State Prosecutor for criminal investigations.
521. The Luxembourg District Court, at the referral of the State Prosecutor, may order the dissolution or liquidation of the entity if it did not update its file with the RCS after a change in its deed. In implementing the 2019-2020 national strategy, the State Prosecutor prioritised this line of work and co-operated with the LBR in identifying legal persons not fulfilling their filing obligations. This led to a sharp increase of the number of judicial liquidations since 2019 as shown in Table 7.4:

⁷⁰ Such a note in the register means that no RCS extracts are issued, and a certificate is made available flagging that the entity has been de-listed. Consequently, the entity has no means to prove the identity or composition of its board of managers/directors to open a bank account or sign a contract.

Table 7.4. Number of judicial liquidations of legal persons, 2017-Q3 2022

| 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|------|------|------|------|------|---------|
| 488 | 546 | 568 | 942 | 1046 | 567 |

522. The most frequent cases relate to an absence of a registered office, minimum number of board members not respected and non-publication of balance sheets for at least three years. The State Prosecutor's Office is informed of such inactive or shell companies by the LBR, competent authorities (e.g., AED, ACD, CRF-FIU, PGD) and private sector (e.g., TCSPs). The State Prosecutor's Office can also act on its own motion. For example, in the summer of 2022, on the instruction of the State Prosecutor's Office, the judicial police visited four hundred addresses, including those of NPOs. This exercise showed that most entities were in compliance with their information requirements and only a few cases lead to judicial liquidation proceedings.
523. Criminal fines of EUR 500 to 25 000 are imposed on managers or directors for not updating the list of members of a SARL or civil company in the RCS (see Table 7.5). Knowingly failing to maintain a register of shares, to appoint a custodian or not depositing bearer shares with the custodian, or to acknowledge bearer shares rights beyond what is legally permitted, is punishable by a criminal fine of EUR 5 000 to 125 000 for natural persons and EUR 500 to 25 000 for legal persons. However, these fines are not considered effective as they have been applied in a limited way.

Table 7.5. Average fine and number of fines for not updating list of members, 2017-Q3 2022

| | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|--------------------|------|-------|-------|------|-------|---------|
| Average fine (EUR) | 833 | 1 039 | 1 250 | 813 | 1 450 | 1 167 |
| Number of fines | 6 | 18 | 4 | 8 | 10 | 9 |

RBE

524. Criminal penalties apply for breaches of requirements regarding BO information of legal persons. To initiate sanctions proceedings, the LBR transmits the files to the State Prosecutor's Office who can either request the court to rule by way of penal order (maximum fine of EUR 2 500) or to issue a summons to appear in court to prosecute the offence and access the full range of penalties available (EUR 1 250 - 1 250 000). So far, given the volume of non-compliant entities (in the thousands), the State Prosecutor's Office processed the files *en masse* and sought penal orders against the legal persons which are capped at EUR 2 500 (since the law of 9 December 2021, this has been increased to EUR 15 000) (see Table 7.6). The authorities noted that these cases related to mostly ignorance of filing requirements and non-fraudulent non-filing. This process raises concerns over the effectiveness and proportionality of ensuring compliance with BO information requirements, as no other measures are available and the LBR, as the registrar, does not have any administrative sanctioning powers itself.

Table 7.6. Number and average amount of pecuniary fines pronounced, 2020-June 2022

| | 2020 | 2021 | June 2022 |
|-------------------------|---------|-----------|-----------|
| Issuance of penal order | 421 | 543 | 15 |
| Average fine (EUR) | 1 960 | 2 163 | 3 500 |
| Total amount (EUR) | 825 000 | 1 174 500 | 52 500 |

525. Luxembourg also applies imprisonment or criminal fines for breaches with the rules relating to the domiciliation of companies, as illustrated by the case study below (see Box 7.2).

7

Box 7.2. Case study: Illegal provision of domiciliation services

In October 2015, following a report from the CRF-FIU, the State Prosecutor requested the opening of a judicial investigation against Mr. J, who is the principal of company A, for offences under the Domiciliation Law, and money laundering and offences under the 2004 AML/CFT Law.

The SPJ searched the company's premises in July 2016 based on an order from the investigating judge in charge of the investigation. The search revealed that the premises leased by company A for its activity does not allow the sub-leasing of offices to other companies domiciled there. The company rents on the ground floor of the building a set of premises consisting of a reception area, an individual office occupied by Mr. J and a collective office used by the other employees of the company. The company also rents a storage room and a car park to store the cars entrusted to the company.

The SPJ investigators noted that 24 companies were domiciled at the registered office of company A, including French-incorporated companies. The SPJ investigators also found a leaflet in which company A advertised offering "to set up a civil company to hold property in Luxembourg in order to be able to register your cars" for an annual price of EUR 2 400.

In December 2018, Mr J and company A were each fined for EUR 10 000 and EUR 20 000 respectively. The State Prosecutor's Office monitored the 24 domiciled companies and discovered that five of the companies were not in compliance with their beneficial information filing requirements as no beneficial information was made available: for two a European Investigation Order to France is pending execution and for one a hearing at the Luxembourg courts.

Following the State Prosecutor's Office's finding that some of the previously domiciled companies had set up at the same address, the AED visited the premises and sent a report to the State Prosecutor's Office in February 2020. It appeared from the AED's findings that the companies were now domiciled with a lawyer registered at the Luxembourg Bar (Mr. J' brother), and that it appeared from the checks carried out that the rules on professional obligations in AML/CFT matters were not respected. As a result, the State Prosecutor's Office proceeded in June 2020 to open a judicial investigation which is currently in progress.

526. Aside from criminal penalties, a legal person not complying with the RBE declaration requirements is flagged by the LBR as “certificate of non-registration of beneficial owner(s)”. The entity would continue to exist, but the certificate would be available for anyone consulting the RBE. The legal person is only struck off from the register after the completion of the judicial liquidation but the register will flag that a liquidation process is ongoing.

RFT

527. The AED may impose administrative sanctions and measures, such as warnings and fines. However, with the recent conception of the RFT, no non-compliance has been detected and therefore no sanctions were imposed. Prior to the establishment of the register, obliged entities acting as fiduciaries or trustees have been sanctioned for gaps in BO identification, verification and record-keeping (see IO.4).

Other measures: Supervisory action

528. Supervisors have the power to impose administrative sanctions (i.e., twice the amount of the benefit derived from the breach or EUR 1 250 000 if the benefit cannot be determined) or measures (i.e., warning, reprimand, public statement) when inaccurate or delayed information is provided by fiduciaries or trustees under their supervision. These can be issued to fiduciaries, trustees, members of their management bodies, their effective managers or other persons responsible for such non-compliance. Supervisors also apply sanctions to their supervised entities when they come across deficiencies related to beneficial ownership identification or verification (CDD) of corporate or *fiducie*/trust customers (see IO.3).

Overall conclusion on IO.5

Luxembourg undertakes a multi-pronged approach to obtain accurate, adequate and up to date basic and BO information in a timely manner. This is mainly achieved through the Trade and Company Register (RCS), and the BO information registers established for legal persons in 2019 (RBE) and for legal arrangements in 2020 (RFT)).

Positive weight is given to the LBR’s annual large-scale exercises, which started in 2019 to inspect the RCS and RBE on the availability and accuracy of information. Consequently, many companies were struck off whose information was not updated for over ten years, ensuring that registers are kept accurate.

There are moderate shortcomings in relation to the understanding of how Luxembourg legal persons can be misused for TF and the effective application of sanctions. Sanctioning the violation of legal person BO disclosure obligations require criminal proceedings and the involvement of the State Prosecutor and District Court, which sharply limits timely application, proportionality and effectiveness of sanctions. Also, only limited criminal fines have been imposed for not maintaining or updating lists of members or a register of shares.

Luxembourg is rated as having a Substantial level of effectiveness for IO.5.



Chapter 8. INTERNATIONAL COOPERATION

Key Findings and Recommended Actions

Key Findings

1. International co-operation is vital for Luxembourg, and it factors in all areas of its AML/CFT framework. Over the review period, Luxembourg consistently provided constructive and good quality mutual legal assistance and extradition, as confirmed by the positive feedback received from the FATF Global Network and many case studies shared with the assessment team. Incoming MLA requests not requiring coercive measures are processed within three to four months. However, timeliness is an issue in some cases, as approximately 30% of incoming MLA requests requiring coercive measures are executed in a timeframe longer than eight months.
2. Luxembourg competent authorities proactively seek legal assistance from their foreign counterparts. Over the period reviewed, Luxembourgish authorities sent approximately 4200 MLA requests relating to domestic ML and related predicate offences, aiming at following illicit financial flows through Luxembourg. Requests sent to Luxembourg's main MLA counterparts (France, Germany, Belgium) are drafted in the language of the destination country. However, Luxembourg has a manual procedure to monitor outgoing MLA requests, the effectiveness of which is questionable. This impedes competent authorities' ability to effectively monitor and follow up on pending outgoing requests and maintain comprehensive statistics on outgoing requests.
3. Luxembourg competent authorities employ several highly specialised staff in each competent authority involved in executing MLA requests. Despite the moderate increase of human resources in some of the competent authorities, adequate resourcing remains an issue that affects to some extent the effective delivery of MLA.
4. As demonstrated in case studies, most Luxembourgish competent authorities proactively seek and provide (including spontaneously) other forms of international co-operation to exchange financial intelligence, supervisory, law enforcement, and basic and BO information, in an appropriate and timely manner with their foreign counterparts for AML/CFT purposes.
5. The extent to which supervisory authorities engage in other forms of international co-operation varies. The CSSF and CAA are particularly effective in their engagement with foreign counterparts. The AED is less proactive in providing and seeking international co-operation.

Recommended Actions

1. Luxembourg should take effective steps to reduce the identified delays in the execution of incoming MLA requests on coercive measures.
2. Luxembourg should strengthen resource allocation across all authorities engaged in formal and informal international co-operation with a primary focus on the investigative judge, PAL/PAD, and the Council Chamber. This could include incentives in reducing staff turnover in the Office of the Investigative Judge.
3. Luxembourg should establish a robust case management system to effectively monitor pending outgoing MLA requests, ensuring timely execution, and maintain comprehensive statistics on outgoing MLA requests. Competent authorities should tailor this system to meet their needs and ensure effective output.

529. 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.

Immediate Outcome 2 (International Cooperation)

530. Given Luxembourg's role as a leading international financial centre (IFC), and the world's second largest investment fund centre, international co-operation is critical, and factors in all areas of Luxembourg's AML/CFT framework. Luxembourg's financial sector generates significant cross-border financial activity, correspondingly proportionate ML and, to a lesser extent, TF risks. International co-operation, both provided and received, primarily relates to foreign predicate offences, such as fraud and forgery, tax crimes, corruption and bribery and drug trafficking, and related ML. Luxembourg provides MLA and extradition in accordance with the requirements set out in international treaties and domestic legislation (see R.36-39) and prioritises these accordingly.
531. This assessment was based on comprehensive statistics, case studies, feedback from the FATF Global Network, and interviews with relevant Luxembourgish authorities.

Providing constructive and timely MLA and extradition

532. Luxembourg provides mutual legal assistance (MLA) and extradition in a constructive manner. Incoming MLA requests not requiring coercive measures are processed within three to four months. However, timeliness is an issue in some cases, as approximately 30% of incoming MLA requests requiring coercive measures are executed in a timeframe longer than eight months. Feedback received from the FATF Global Network indicates that the provision of MLA is of good quality and properly prioritised. There are simplified procedures for executing MLA and extradition within the EU (i.e., European arrest warrant (EAW) and European Investigation Order (EIO)), which account for the vast majority of MLA requests received (i.e., France, Germany, Belgium). In addition, there is active cooperation on asset tracing and confiscation.

Mutual Legal Assistance

533. The General State Prosecutor's Office of the Grand Duchy of Luxembourg (PG) is the central authority for the execution of incoming requests. Incoming MLA requests requiring coercive measures and non-coercive measures are prioritised. The Office of the Investigative Judge (investigative judge) sets the former as high priority and executes them. An investigative judge and a state prosecutor are always on-call duty to act immediately upon receipt of the request. The State Prosecutor's Offices of the Luxembourg and Diekirch District Courts (PAL/PAD) executes the latter. Luxembourgish competent authorities have internal guidelines and guidance in place that facilitate the smooth execution of incoming MLA and extradition requests.
534. Luxembourg has established two judicial co-operation regimes for executing MLA and extradition requests, including EAWs, and EIOs. The regime for EU Member States and the regime for non-EU Member States. Both regimes are overseen by the PG. The former is based on the principle of mutual recognition of judicial decisions (EIOs, freezing and confiscation certificates, judicial controls, EAWs and custodial sentences). The latter is based on bilateral or multilateral conventions concluded, in particular, within the framework of the UN, the Council of Europe or the OECD, or based on reciprocity if there is no applicable agreement.
535. Between 2017 and 2022, Luxembourg received approximately 3 600 MLA requests on coercive measures and 6 400 MLA requests on non-coercive measures. Throughout this period there is an increasing trend in the volume of incoming requests. The vast majority of incoming MLA requests concern investigations of white-collar offences linked to the laundering of criminal funds (i.e., fraud and forgery, tax crimes and illicit trafficking in narcotic drugs and psychotropic substances), which is in line with Luxembourg's risk profile. As indicated in the table below (table 8.1), incoming MLA requests on coercive measures have steadily increased since 2017. Luxembourg also received a significant number of MLA requests on non-coercive measures.

Table 8.1. Incoming MLA requests received, 2017–Q3 2022

| Year | MLA requests (coercive measures) | MLA requests (Non-coercive measures) | ML-related MLA requests | TF-related MLA requests |
|---------|----------------------------------|--------------------------------------|-------------------------|-------------------------|
| 2017 | 560 | 1 399 | 110 | 3 |
| 2018 | 550 | 1 194 | 126 | 12 |
| 2019 | 591 | 999 | 126 | 3 |
| 2020 | 624 | 1 036 | 114 | 2 |
| 2021 | 728 | 1 108 | 90 | 0 |
| Q3 2022 | 490 | 618 | 57 | 1 |

Table 8.2. Incoming MLA requests broken down by predicate offences*, 2017-Q3 2022**

| Predicate Offences | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|---|----------|----------|----------|----------|----------|----------|
| Corruption | 22 (16) | 22 (13) | 19 (12) | 16 (11) | 13 (8) | 6 (3) |
| Counterfeiting and piracy of products | 2 (0) | 1 (0) | 3 (1) | 0 (0) | 1 (1) | 0 (0) |
| Counterfeiting currency | 2 (1) | 3 (1) | 2 (0) | 3 (0) | 2 (0) | 1 (0) |
| Cybercrime | 64 (12) | 62 (3) | 55 (9) | 59 (12) | 55 (5) | 41 (6) |
| Environmental crimes | 0 (0) | 0 (0) | 0 (0) | 0 (0) | 1 (0) | 0 (0) |
| Extortion | 17 (1) | 15 (1) | 14 (0) | 1 (1) | 7 (1) | 5 (1) |
| Forgery | 60 (19) | 42 (20) | 26 (14) | 31 (19) | 33 (15) | 21 (8) |
| Fraud | 240 (50) | 214 (50) | 214 (51) | 264 (64) | 337 (48) | 172 (18) |
| Illicit arms trafficking | 8 (1) | 2 (1) | 5 (1) | 2 (2) | 6 (1) | 5 (0) |
| Illicit trafficking in narcotic drugs and psychotropic substances | 30 (9) | 42 (12) | 30 (6) | 29 (5) | 32 (2) | 10 (3) |
| Illicit trafficking in stolen and other goods | 21 (11) | 14 (6) | 4 (3) | 6 (4) | 8 (7) | 1 (0) |
| Insider trading and market manipulation | 4 (0) | 1 (0) | 0 (0) | 2 (2) | 1 (0) | 0 (0) |
| Kidnapping, illegal restraint, and hostage taking | 5 (0) | 7 (0) | 0 (0) | 1 (0) | 0 (0) | 0 (0) |
| Murder, grievous bodily injury | 28 (0) | 26 (1) | 15 (0) | 13 (0) | 14 (0) | 9 (0) |
| Participation in an organized criminal group & racketeering | 56 (29) | 48 (29) | 47 (27) | 58 (38) | 50 (28) | 18 (7) |
| Robbery or theft | 49 (7) | 49 (7) | 30 (4) | 31 (3) | 31 (3) | 27 (0) |
| Sexual exploitation, including sexual exploitation of children | 35 (1) | 28 (3) | 52 (1) | 7 (0) | 12 (0) | 8 (1) |
| Smuggling | 0 (0) | 0 (0) | 1 (0) | 0 (0) | 0 (0) | 0 (0) |
| Tax crimes | 52 (24) | 51 (20) | 53 (28) | 33 (7) | 26 (5) | 11 (1) |
| Trafficking in human beings and migrant smuggling | 4 (0) | 0 (0) | 4 (0) | 3 (2) | 3 (1) | 7 (0) |

*Note: Some MLA requests may be counted more than once as they are linked to multiple predicate offences.

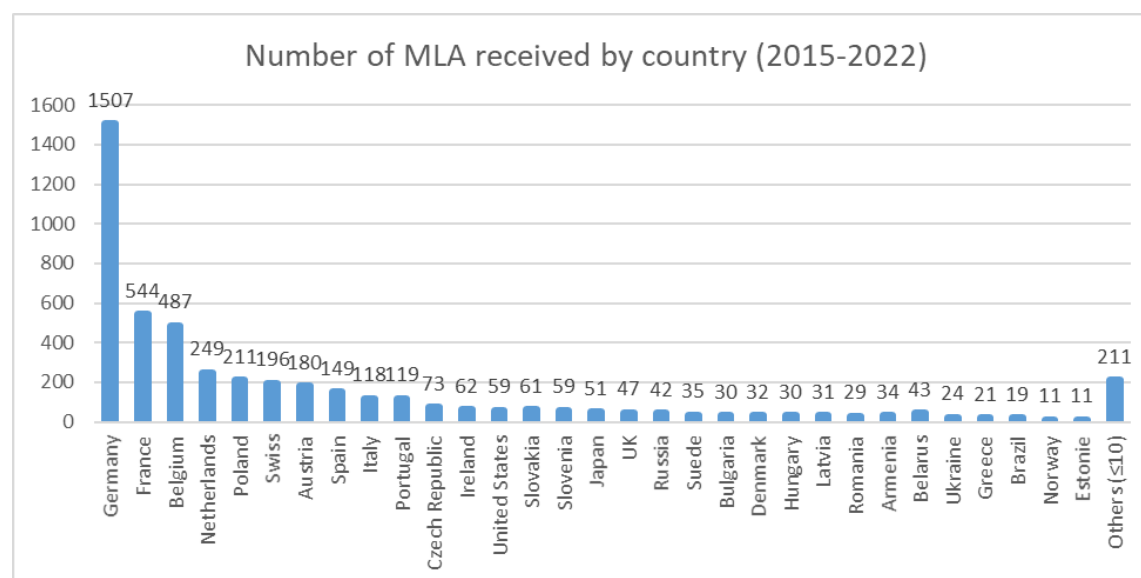
**Note: The numbers in parentheses () indicate requests with an ML component.

536. Luxembourg also received and successfully executed many follow-up MLA requests to initial ones aiming at gathering additional evidence. Such requests are made because of information provided by Luxembourg either during or after the execution of the initial MLA request or following further discoveries made by the requesting foreign counterparts. The execution of an MLA request may lead to increased STRs related to the subject of the request. Information requests to obliged entities stemming from incoming MLA requests, occasionally, triggers STRs as they assist obliged entities to establish suspicion. Such cases, often, led the CRF-FIU to freeze funds on its own initiative. Upon freezing of funds, the CRF-FIU informs concerned countries that the seizing of frozen funds should be requested through an MLA request.

Table 8.3. Number of follow-up incoming MLA requests, 2017-Q3 2022

| Year | Follow-up MLA requests | follow-up MLA requests related to predicate offences | Follow-up ML-related MLA requests | Follow-up TF-related MLA requests |
|---------|------------------------|--|-----------------------------------|-----------------------------------|
| 2017 | 139 | 73 | 66 | 0 |
| 2018 | 139 | 66 | 71 | 2 |
| 2019 | 151 | 88 | 63 | 0 |
| 2020 | 181 | 130 | 51 | 0 |
| 2021 | 260 | 195 | 64 | 1 |
| Q3 2022 | 179 | 133 | 46 | 0 |

537. Regarding incoming MLA requests, 90% of them originate from EU Member States. Luxembourg's most frequent counterparts are Germany, France, Belgium and the Netherlands. Outside of the EU, the most frequent incoming requests originate from Switzerland, the United States, Japan and the UK.

Figure 8.1. Number of MLA requests received by country, 2015-2022

Timeliness

538. Luxembourg maintains clear and comprehensive statistics that demonstrate the timeframe of MLA requests executed. Approximately 70% of incoming MLA requests on coercive measures are executed within seven months, whilst requests on non-coercive measures are executed, on average, more than three months. Long delays in executing MLA requests refer to: (a) very complex cases; (b) limitations in human resources; (c) missing information from the requesting state; (d) additional MLA requests added to the original one⁷¹; and (e) heavy digital data included in requests. All incoming MLA requests on TF, save for one, were executed within seven months.
539. In urgent cases, the transmission from the PG to the investigative judge (and the SPJ) and the PAL/PAD may happen within hours. Given Luxembourg's small size and the high level of co-operation and co-ordination among all domestic competent authorities involved in the execution of incoming MLA requests, competent authorities use informal communication on a regular basis to speed up the execution of urgent MLA requests. The moment when a foreign country files an MLA request with the PG, Luxembourgish competent authorities involved in the execution of the request are informed via telephone to begin preparations for the execution of the request prior to its formal arrival.

Table 8.4. Average time (by date of execution) for processing MLA requests on coercive measures 2017–Q3 2022

| Year | less than 3 months | 4-7 months | 8-10 months | over 10 months | Total |
|---------|--------------------|------------|-------------|----------------|-------|
| 2017 | 193 | 228 | 89 | 69 | 579 |
| 2018 | 166 | 206 | 67 | 95 | 534 |
| 2019 | 215 | 197 | 56 | 79 | 547 |
| 2020 | 144 | 189 | 83 | 102 | 518 |
| 2021 | 250 | 247 | 117 | 125 | 739 |
| Q3 2022 | 225 | 155 | 52 | 72 | 504 |

Table 8.5. Average time (by date of execution) for processing MLA requests on non-coercive measures 2017–Q3 2022

| Year | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|----------------------------|-------|-------|-------|-------|------|---------|
| Duration (Average in days) | 114.0 | 124.4 | 112.1 | 103.1 | 99.0 | 101.1 |

540. According to input from the FATF Global Network on incoming ML/TF related MLAs, quality of responses, including on timeliness, is good. Although Luxembourgish competent authorities do not regularly seek feedback on the quality of their replies, they shared with the assessment team many examples of unsolicited feedback expressing gratitude for the assistance provided.

⁷¹ Luxembourg counts the execution time of an additional/subsequent request on the overall execution time of the corresponding initial MLA requesting.

Box 8.1. Case Study – Execution of incoming MLA request

In June 2022, an international MLA request was sent to Luxembourg to identify different accounts held/linked to individual A, who is on US and European Sanction lists and who holds a lot of assets in different jurisdictions.

The first and second incoming MLA requests in the same case requested for house-searches to be executed at bank A and B established in Luxembourg.

During these house-searches it was also found that the Luxembourgish banks had not, or too late, informed the CRF-FIU about changes to the BO status of the individual A. Therefore, in November 2022, separate reports were addressed by the SPJ-EJIN to the Prosecutor in Luxembourg.⁷²

Based on the investigation findings, Luxembourg's foreign counterparts were not aware of all assets and accounts linked to individual A in Luxembourg. The final report of the first two international requests informed that assets of over EUR 1 billion were in Luxembourg at different banks under different names.

Following the outcome of the MLA requests, Luxembourg received immediately a new request targeting many more bank accounts, including another bank in Luxembourg.

Both banking institutions confirmed that as soon as individual A was put under EU Sanctions (March 2022), all related accounts were blocked. However, Luxembourg has not seized them yet, as it has not received such a request.

During the investigation the CRF-FIU collaborated in identifying further accounts.

The investigation is ongoing.

Refusals

541. In the period between 2017 and 2022, Luxembourg refused only a dozen of MLA requests because domestic law did not provide ground for execution or the underlying basis for the request had no link to Luxembourg. At the same time, Luxembourg did not refuse any TF-related MLA requests.
542. Luxembourg's competent judicial authorities employ all means and investigating technics provided by law when executing MLA requests. Furthermore, they use French, German and English language during the international co-operation procedures, and this is of added value for the timely execution of the international co-operation requests, given that Germany, France and Belgium are its main counterparts.

⁷² In January 2023, the PAL opened a preliminary investigation for ML based on the SPJ reports.

Challenges

543. Luxembourg takes a proactive approach aiming at executing all incoming MLA requests. Judges and prosecutors regularly reach out to their foreign counterparts seeking missing information, either directly through telephone/email or indirectly through diplomatic channels. Despite this approach, every year, a dozen of requests remain unexecuted due to the absence of the following information from the requesting party: (a) the name of the requesting party; (b) the purpose of the requested evidence; (c) the date and place where facts committed, including a summary statement of facts and link between those facts, and the purpose of requesting evidence; (d) as far as possible, the identity and nationality of the person concerned; (e) the name and address of the recipient; (f) the text containing the charges and the related sanctions; (g) a translation of the request for mutual assistance and production documents into French, German or English.
544. In support of its approach to ensure adequate execution of incoming MLA requests, Luxembourg's investigative judges and prosecutors immediately acknowledge receipt of a request, informing simultaneously their foreign counterparts of the individual in charge for the execution of the request. This facilitates ongoing dialogue between requesting competent authorities and Luxembourg. Luxembourg has seen significant benefit in the effective execution of MLA requests from the consistent application of this approach.

Human resources and expertise

545. Luxembourg competent authorities employ several highly specialised staff in each competent authority involved in executing MLA requests (see Table 8.6). Many of these employees are also involved in investigations. This is a concern in Luxembourg's context, given the identified delays in the timely execution of MLA involving coercive measures and the increasing volume of MLA requests. Despite the moderate increase of human resources available in some of the competent authorities, including the establishment of a division dedicated to international co-operation in the SPJ-EJIN, adequate resourcing remains an issue. Resource limitations are also an issue for the Council Chamber, which examines of its own motion the "formal" regularity of the procedure. In many instances, MLA delivered by Luxembourg is achieved at the expense of the high professionalism of the individuals involved in the execution of incoming requests. However, as indicated earlier, limitations in human resources impact the timely execution of incoming MLA requests involving coercive measures. To ensure continuity, it is essential that Luxembourg increases human resources dedicated to international co-operation across the competent authorities involved in the execution of MLA requests, prioritising the investigative judge, and set out incentives in reducing staff turnover in its Office.

Table 8.6. Human resources allocated to the execution of incoming MLA requests

| Agency/Officials | Number of dedicated staff |
|----------------------------------|---|
| PG / Advocate Generals | 6 (plus 3 administrative staff) |
| Judiciary / Investigative Judges | 12 (plus 12 clerks) |
| SPJ-EJIN* | 22 (17 investigators and 3 police trainees seconded by 2 secretariat members) |
| PAL/PAD | 7 (plus 5 administrative assistants) |
| Judiciary / Council Chambers | 9 (plus 5 clerks) |

*Note: The SPJ-EJIN team is exclusively working in supporting the execution of MLA request.

SPJ International Mutual Legal Assistance Section (SPJ-EJIN)

546. The execution of MLAs is regularly assisted by the SPJ-EJIN based on the decision of the PAL/PAD or the investigative judge. The SPJ-EJIN employs 17 experienced investigators, each of which process on average 50 incoming MLA requests per year. Whenever the SPJ-EJIN executes measures relating to MLA requests (e.g., searches and seizures) it pays great attention to the information it gathers and if it discovers that offences have also been committed by the involved professionals in Luxembourg, it reports those to PAL/PAD. Both PAL/PAD and the investigative judge commended the work of the SPJ-ENJIN, the importance of which was demonstrated in various case studies shared with the assessment team.

Asset recovery

547. Luxembourg provides a range of assistance for asset recovery, including identifying, tracing, seizing and confiscating assets. The quality and importance of the assistance that Luxembourg provides to its foreign counterparts is apparent when taking into account the amounts of funds seized. Asset recovery is subject to the same challenges and mitigating measures applied by Luxembourg for all incoming MLA requests, as explained above.

Table 8.7. Amount of funds seized (EUR in million), 2017-Q3 2022

| Type | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|--|-------|-------|------|------|------|---------|
| Account, cash | 12.60 | 85 | 200 | 180 | 125 | 68 |
| Insurance | 2.1 | / | 0.27 | 3.63 | 0.07 | 0.01 |
| Other forms of value (property, value of drugs, other values, value of bitcoins) | 0.03 | 29.00 | 2.50 | 0.04 | 1.48 | / |

548. Luxembourg has also demonstrated sound efforts to deal with asset recovery requests from foreign jurisdictions (see IO.8). Between 2017 and 2022, the ARO received and executed 36 requests for confiscation, with value of approximately EUR 47 million. Luxembourg can share assets with foreign countries (see R.38) and has done so for most of the incoming requests. Asset-sharing with some countries is pending, subject to ongoing discussions for the conclusion of bilateral/multilateral agreements.

AMO

549. In June 2022, Luxembourg established the AMO. Since October 2022, the AMO is the competent authority responsible to manage the sums, including cash and balances on accounts, claims, virtual assets and other assets entrusted to it by the judicial authorities and that have been seized through a domestic case or an MLA request. The AMO is already operational for the management of sums. By the end of the onsite visit, AMO did not engage in asset recovery requests and its exchanges with foreign counterparts were limited to benefit from good practices. AMO does not condition international co-operation to a MoU.

Extradition

550. There are two extradition regimes in operation in Luxembourg: a simplified extradition process for EU Member States under the EAW framework and a standard procedure for non-EU Member States. Luxembourg maintains comprehensive statistics on both regimes (see Tables 8.8 - 8.11). Most incoming requests refer to EAW. Most requests relate to the following ML predicate offences: (a) illicit trafficking in narcotic drugs and psychotropic substances; (b) robbery or theft; and (c) fraud. Between 2017 and 2022, Luxembourg received one TF-related extradition request. Luxembourg executed all EAWs and extradition requests save for those where the individual of concern was not present in its territory. The competent authorities shared with the assessment team two additional examples where EAW/extradition was not executed: (a) related to an individual with cancer who is serving his sentence in Luxembourg; and (b) a request referring to imprisonment for 14 days, despite the requirement of the 2004 EAW Law for a minimum threshold of 4 months of imprisonment for surrender requests.

Table 8.8. Number of EAWs and extradition requests sent to Luxembourg, 2017-Q3 2022

| Year | EAW | Extradition requests | Total |
|---------|-----|----------------------|-------|
| 2017 | 54 | 6 | 60 |
| 2018 | 44 | 6 | 50 |
| 2019 | 50 | 5 | 55 |
| 2020 | 35 | 6 | 41 |
| 2021 | 44 | 8 | 52 |
| Q3 2022 | 49 | 5 | 54 |

Table 8.9. Number of EAW's by predicate offence, 2018-Q3 2022

| Predicate offence* | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|---|------|------|------|------|---------|
| Cybercrime | 1 | 0 | 0 | 0 | 1 |
| Extortion | 4 | 0 | 0 | 0 | 0 |
| Forgery | 2 | 0 | 0 | 4 | 3 |
| Fraud | 5 | 5 | 2 | 7 | 7 |
| Illicit trafficking in narcotic drugs and psychotropic substances | 6 | 14 | 5 | 17 | 9 |

| Predicate offence* | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|--|------|------|------|------|---------|
| Illicit trafficking in stolen and other goods | 0 | 1 | 0 | 0 | 0 |
| Kidnapping, illegal restraint, and hostage taking | 0 | 1 | 0 | 0 | 1 |
| Murder, grievous bodily injury | 9 | 7 | 6 | 6 | 13 |
| Participation in an organized criminal group & racketeering | 3 | 11 | 10 | 10 | 2 |
| Robbery or theft | 19 | 26 | 25 | 13 | 14 |
| Sexual exploitation, including sexual exploitation of children | 0 | 1 | 0 | 0 | 0 |
| Illicit arms trafficking | 0 | 0 | 0 | 0 | 2 |

*Note: Individual EAWs may relate to multiple predicate offences.

Table 8.10. Number of extradition requests by predicate offence, 2017-Q3 2022

| Predicate offence* | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|---|------|------|------|------|---------|
| Fraud | 2 | 1 | 1 | 0 | 0 |
| Forgery | 0 | 0 | 0 | 0 | 1 |
| Illicit trafficking in narcotic drugs and psychotropic substances | 0 | 1 | 1 | 0 | 2 |
| Kidnapping, illegal restraint, and hostage taking | 1 | 0 | 0 | 0 | 0 |
| Murder, grievous bodily injury | 1 | 0 | 0 | 1 | 0 |
| Robbery or theft | 1 | 1 | 1 | 0 | 1 |
| Illicit arms trafficking | 1 | 0 | 0 | 0 | 0 |
| Terrorism and terrorist financing | 0 | 0 | 1 | 0 | 0 |
| Other | 3 | 2 | 2 | 7 | 2 |
| Total | 6 | 5 | 6 | 8 | 6 |

*Note: Individual extradition requests may relate to multiple predicate offences.

Table 8.11. Number of outgoing extradition and surrenders, 2017-Q3 2022

| Year | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|---------------------------------------|------|------|------|------|------|---------|
| Number of extraditions and surrenders | 44 | 42 | 49 | 37 | 51 | 46 |

551. Luxembourg has successfully participated in four joint investigations teams (JITs) since 2017. Examples of such co-operation, including ongoing JITs, and Luxembourg decisive contribution to them were shared with the assessment team when onsite. Luxembourg has never refused its participation in a JIT.

Box 8.2. Case Study: Joint Investigation Case

On 14 February 2022, the European Union Agency for Criminal Justice Cooperation (Eurojust) set up a JIT to investigate five suspects accused of ML. Luxembourg joined the JIT as per “country A” request. According to the facts of the case, between 2002 and 2021, funds of value more than EUR 300 million and EUR 5 million, respectively, were embezzled in “country B”. The competent authorities from the different countries carried out extensive measures to freeze EUR 120 million worth of assets linked to the investigation of a money laundering case in “country B”, of which approximately EUR 11 million were seized across several bank accounts in Luxembourg.

Source: Eurojust Press Release, Action against money laundering freezes EUR 120 million worth of Lebanese assets, seizing bank accounts. Link: www.eurojust.europa.eu/news/action-against-money-laundering-freezes-eur-120-million-worth-lebanese-assets

Seeking timely legal assistance to pursue domestic ML, associated predicate offences and TF cases with transnational elements

552. Luxembourg is a global financial centre and because of its exposure to international financial flows, most ML/TF and related predicate offences have an international component. Luxembourg competent authorities proactively seek legal assistance from their foreign counterparts, including pursuing requests for asset freezing and confiscation.

Mutual Legal Assistance

553. The investigative judge and PAL/PAD are the competent authorities responsible for outgoing MLA requests. Unlike the system for managing/monitoring incoming MLA requests, there is no horizontal case management system for outgoing MLA requests to assist competent authorities to identify the source of delays. The competent authorities indicated that each investigative judge and prosecutor manually monitors pending outgoing requests for which they have responsibility. However, the effectiveness and outcomes of this procedure is questionable. The assessment team considers that this an issue, as, on several occasions, it increases the overall length of investigations given the delays observed in receipt of MLA-related intelligence and/or evidence. The assessment team acknowledges that to some extent delays are caused by the requested party, however case studies (see IO.7) indicate long periods with no follow-up by Luxembourg authorities. All other structures, procedures and instruments used for incoming MLA requests apply equally for outgoing ones. Between 2017 and 2022, Luxembourg sent approximately 4 200 MLA requests to its foreign counterparts. Based on data provided, responses to approximately 30 outgoing MLA requests are pending per year. As with incoming MLA requests, Germany, France and Belgium are Luxembourg's main counterparts for outgoing MLA requests. Outgoing MLA requests are in line with Luxembourg's ML/TF risk profile. Many of these requests concern ML cases, associated predicate offences or both. One of the main reasons for the high number of MLA requests sent abroad is that the investigative judge and PAL/PAD aim at following the money trail transiting through Luxembourg bank accounts, i.e., flows initially credited to accounts in Luxembourg and then transferred to banks in other jurisdictions.

Box 8.3. Case study: Outgoing MLA requests

In the context of the case study “Bad Banker” (please see more in Box 3.7), Luxembourg sent 32 MLA requests to acquire information and develop evidence.

As a result of the first MLA request to Switzerland, Luxembourg received banking documentation proving that an account had been opened with a Swiss bank by the suspect. The information also indicated that the misappropriated amount of EUR 3.5 million had been divided into three parts within seven days and channelled to other accounts in Liechtenstein and Hong Kong, China.

Information received from the MLA request sent to Liechtenstein revealed that a part of the funds was transferred to Latvia.

MLA requests to Latvia, Hong Kong, China, and Liechtenstein revealed that funds were further channelled from Latvia to Hong Kong, China, thereafter to Liechtenstein, and finally returning to Luxembourg.

Hong Kong, China provided information that EUR 1.2 million was transferred to China, before returning to Luxembourg at the bank where the suspect was employed. One of these accounts had been opened by an English company, whose beneficial owner was a professional resident in Luxembourg (suspect B). The money trail revealed that a part of the funds was transferred to Spain, the UK and France. MLA requests to those countries provided information about the ultimate beneficial owners of accounts and the destination of the funds.

Additional MLA requests to Spain, the UK and France helped to establish that the funds ended up in foreign accounts mostly held by shell companies formed under English law serving as a conduit of suspect A.

In addition to the “follow the money” principle, other letters rogatory were aimed at locating the suspect. The suspect was arrested in Switzerland based on an extradition request and placed in pre-trial detention for more than two years.

A third category of letters rogatory was aimed at locating assets, with a view to seizing them.

554. Feedback from Luxembourg’s main counterparts and the FATF Global Network indicates that outgoing MLA requests are of good quality and that Luxembourgish competent authorities take a constructive approach to co-operation. Luxembourg rarely receives requests for additional clarification to its initial MLA requests, particularly from its main foreign counterparts. This speaks of the comprehensiveness of outgoing MLA requests.

Table 8.12. Investigative Judge outgoing MLA requests, 2017-Q3 2022

| Year | EIOs/CRIs sent abroad seeking evidence | EIOs/CRIs sent abroad seeking evidence in ML cases or where ML is mentioned | Freezing certificates/CRIs with requests for asset seizure | Freezing certificates/CRIs with requests for asset seizure where ML is mentioned |
|---------|--|---|--|--|
| 2017 | 315 | 86 | 13 | 7 |
| 2018 | 282 | 121 | 13 | 8 |
| 2019 | 338 | 151 | 18 | 14 |
| 2020 | 365 | 191 | 36 | 25 |
| 2021 | 385 | 188 | 37 | 36 |
| Q3 2022 | 271 | 197 | 30 | 26 |

Table 8.13. PAL/PAD outgoing MLA requests, 2017-Q3 2022

| Year | Outgoing MLA requests |
|---------|-----------------------|
| 2017 | 339 |
| 2018 | 396 |
| 2019 | 370 |
| 2020 | 355 |
| 2021 | 442 |
| Q3 2022 | 308 |

555. All professionals employed by the investigative judge and PAL/PAD are multilingual and draft their MLA requests either in French or German, depending on the destination country. This adds to the timeliness of outgoing MLA requests, given that Luxembourg's main counterparts are French or German speaking countries.
556. Urgent outgoing MLA requests are supported by the solid network of direct contacts with foreign counterparts as established by the investigative judge and PAL/PAD. This also includes the use of Eurojust and the European Judicial Network contact points or diplomatic channels when appropriate. Luxembourg shared with the assessment team, when onsite, several examples where direct contacts were used to address urgent MLA requests.
557. As noted earlier, Luxembourg does not have a central authority, or horizontal case management system for monitoring outgoing MLA requests. Monitoring of requests on a case-by-case basis falls on the investigative judge and PAL/PAD in charge. Monitoring of outgoing requests stretches the human resources available to the said authorities, given the increasing number of outgoing MLA requests. This is also evident, whenever there is need for the investigative judge and PAL/PAD to go the extra mile with non-responsive countries.
558. Luxembourg has also established JITs. Competent authorities shared with the assessment team, when onsite, examples of ongoing JITs established on their own initiative. Between 2017 and 2022, no outgoing request for JIT was refused by Luxembourg's foreign counterparts.

Extradition

559. The investigative judge is the Luxembourgish competent authority responsible for requests for extradition and EAWs. Between 2017 and 2022, the investigative judge sent approximately 700 extradition requests and EAWs. Most requests relate to predicate offences (i.e., robbery/theft, fraud and forgery) and ML. responses to 235 requests/EAWs is pending, because the wanted suspects could not be located by Luxembourg foreign counterparts. Luxembourg informed that only six extradition requests were refused (i.e., countries do not extradite their own nationals). There is only one request linked to TF, which is generally in line with Luxembourg's assessed risk profile.

Table 8.14. Outgoing surrender and extradition requests pertaining to ML and TF, 2017-Q3 2022

| Year | Surrender and extraditions requests | Thereof ML | Thereof TF |
|---------|-------------------------------------|------------|------------|
| 2017 | 130 | 17 | 0 |
| 2018 | 157 | 11 | 0 |
| 2019 | 128 | 12 | 1 |
| 2020 | 89 | 18 | 0 |
| 2021 | 101 | 28 | 0 |
| Q3 2022 | 86 | 21 | 0 |

*Note: Luxembourg counts persons who have been linked to a predicate offence in JUCHA, which allows the comparison between ML and total statistics. Furthermore, only persons are counted in this table and not arrest warrants (mandat).

560. Between 2017 and 2022, 597 individuals were extradited to Luxembourg. It should be noted that the year of extradition does not always coincide with the year of issue of the arrest warrant. Extradition requests can be sent either to a State where the suspect might live or be published through channels such as Interpol if there are no clues as to where the suspect might live.

Table 8.15. Number of surrenders and extraditions to Luxembourg, 2017-Q3 2022

| Year | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|---------------------------------------|------|------|------|------|------|---------|
| Number of surrenders and extraditions | 99 | 102 | 105 | 78 | 100 | 113 |

Asset recovery

561. Luxembourg actively requests assistance in asset recovery cases. Looking specifically at ML cases and predicate offences. Case studies demonstrate that Luxembourg is seeking assistance from foreign countries, to freeze and confiscate assets, but it does not maintain statistics on the number of outgoing asset recovery requests.

Table 8.16. MLA requests sent abroad by Investigative Judges on asset recovery, 2017- Q3 2022

| Year | Total number of freezing certificates/CRI with requests for asset seizure | Freezing certificates/CRI with requests for asset seizure where ML is mentioned | Freezing certificates/CRI with requests for asset seizure where TF is mentioned |
|---------|---|---|---|
| 2017 | 13 | 7 | 0 |
| 2018 | 13 | 8 | 0 |
| 2019 | 18 | 14 | 0 |
| 2020 | 36 | 25 | 0 |
| 2021 | 37 | 36 | 0 |
| Q3 2022 | 30 | 26 | 0 |

Seeking other forms of international co-operation for AML/CFT purposes

562. Luxembourg competent authorities are engaged in a range of international co-operation networks, and actively seek non-legal forms of international co-operation for AML/CFT purposes. Exchanges with Luxembourg's EU counterparts are more frequent compared to non-EU countries, which is in line with Luxembourg's risk and context.

CRF-FIU

563. The CRF-FIU actively seeks input from its foreign counterparts via the Egmont Group and the FIU.net. In the aftermath of the 2018 NRA, the CRF-FIU always seeks input from its foreign counterparts on all cases qualified of medium or high ML risk. As for TF risk, the CRF-FIU will seek input from its foreign counterparts regardless of the risk level. Between 2017 and 2022, the CRF-FIU sent approximately 5 000 information requests. Most requests are linked to fraud, criminal tax offences, corruption, ML and TF, which is in line with Luxembourg's risk and context. The CRF-FIU does not condition the exchange of information with its foreign counterparts to an MoU. However, it does engage in such arrangements if this is a condition for its foreign counterparts.

Table 8.17. CRF-FIU outgoing requests to EU and non-EU counterparts, 2017-Q3 2022

| Information Requests | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|----------------------|------|------|------|-------|-------|---------|
| Number | 424 | 605 | 726 | 1 174 | 1 098 | 900 |

SPJ

564. The SPJ sends requests for police-to-police co-operation on a regular basis through the Europol and Interpol channels. The Directorate of International Relations within the SPJ is responsible for all international co-operation requests. As of 2022, the Directorate employs 42 staff members. Human resources allow the SPJ to maintain its vital role in supporting and conducting investigations. Luxembourg has also bilateral and multilateral agreements that facilitate police-to-police co-operation with all BENELUX countries.

Table 8.18. Outgoing requests through Europol, 2017-Q3 2022

| Information Requests | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|--|------|------|------|------|------|---------|
| Number of messages sent abroad by the Police related to ML | 197 | 221 | 291 | 369 | 465 | 463 |

ARO

565. The ARO is managed by a senior magistrate of the economic and financial section of the PAL, assisted by the SPJ AML unit (SPJ-AB). The ARO is a member of the CARIN network. Information between AROs is mainly exchanged via the Secure Information Exchange Network Application (SIENA). The exchange of information and the response time via the platform is fast, accurate and the information provided regarding the assets held by suspects located in foreign countries is very detailed. Answers are usually provided within 5 days and the information received is immediately forwarded by the ARO to the competent judicial authority for the requested purposes. Between 2017 and 2022, the ARO sent out over 198 information requests to its foreign counterparts. Statistics provided show that, since 2019, the ARO has taken a proactive approach in seeking international co-operation. The Police Exchange of Information Law provided the ARO with extended powers amongst which the exchange of information with European counterparts and freezing powers.

Table 8.19. ARO outgoing requests, 2017-Q3 2022

| | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|--------------------|------|------|------|------|------|---------|
| Outgoing ARO/CARIN | 2 | 1 | 21 | 36 | 53 | 85 |

ACD

566. The ACD actively sought information from its foreign counterparts. To facilitate international co-operation, the ACD established an international co-operation department that employs 36 FTEs. International co-operation is conducted based on internal guidance that also deal with urgent requests.

Table 8.20. ACD outgoing requests, 2017-Q3 2022

| | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|---------------------|-------|-------|-------|-------|-------|---------|
| Outgoing | 6 | 9 | 11 | 20 | 62 | 41 |
| Requests about B.O. | 0 | 0 | 0 | 1 | 1 | 1 |
| in % | 0.00% | 0.00% | 0.00% | 5.00% | 1.61% | 2.44% |

AED

567. Unlike all other Luxembourgish competent authorities, the AED does not engage in international co-operation with a view to its supervisory capacity, as it has never received or requested information from its foreign counterparts. This happens partly because the population of supervised entities are mainly local and domestically oriented, and partly due to the lack of the resources to identify its various international non-EU counterparts for each subcategory of supervision.

CSSF

568. The CSSF proactively seeks input from its international counterparts. It provides AML/CFT co-operation and exchange of information, spontaneously or upon request, in a comprehensive manner (e.g., the CSSF is lead supervisor of 47 AML/CFT dedicated AML/CFT supervisory colleges). Between 2018 and 2022, the Banking department engaged in international co-operation 71 times on AML/CFT matters. During the same period, the OPC department engaged in international co-operation on AML/CFT 159 times, of which the majority of exchanges (64% of the exchanges) were initiated by CSSF.

Table 8.21. Banking and OPC department outgoing requests, 2018–November 2022

| | 2018 | 2019 | 2020 | 2021 | Nov. 2022 | Total |
|--|------|------|------|------|-----------|-------|
| Banking department o/w CSSF-initiated | 10 | 16 | 13 | 22 | 10 | 71 |
| OPC department o/w CSSF-initiated | - | 57 | 27 | 52 | 23 | 159 |

CAA

569. Since 2018, the CAA has intensified its efforts to seek input from its international counterparts as indicated by statistics provided. The CAA generally acted as 'host' authority, as it conducted its risk-based AML/CFT supervision on Luxembourg subsidiaries or branches of international groups. Thus, the CAA exchanged information directly with foreign supervisory authorities, notably at market entry within the context of the fit and proper process or at the occasion of other specific requests. The CAA also exchanged information with foreign competent authorities at the occasion of supervisory colleges. In the review period, the CAA participated in 41 colleges of supervisors (EU and non-EU), in one case as a Group supervisor ('home' supervisor) and 40 times as a 'host' supervisor. Since 2020, the CAA participates in dedicated AML/CFT colleges (e.g., 12 participations in 2021).

Table 8.22. CAA outgoing requests on ML/TF, 2017-November 2022

| Outgoing requests | 2017 | 2018 | 2019 | 2020 | 2021 | Nov. 2022 |
|--|------|------|------|------|------|--------------|
| Number of requests sent abroad by the CAA related to ML/TF | 37 | 124 | 55 | 92 | 80 | 59 |
| Number of requests sent by CAA and executed by foreign authority | 25 | 98 | 29 | 63 | 49 | 42 |
| Number of requests sent and refused by foreign authority | 0 | 0 | 0 | 0 | 0 | 0 |

Providing other forms of international co-operation for AML/CFT purposes

570. Throughout the review period, Luxembourg was committed to increasing and strengthening networks for providing international co-operation for AML/CFT purposes. Different authorities play an active role in initiatives and projects aimed at doing so at the European and international level.

CRF-FIU

571. The CRF-FIU was actively involved in multilateral and international working groups to enhance and improve the international co-operation between FIUs. The CRF-FIU co-chaired the working group IEWG e-Catalogue on VASPs delivering the “first of a kind” e-Catalogue on this topic. The CRF-FIU also participated in working groups on criminal tax offences, the fight against child sexual abuse material, the fight against terrorism, Extreme Right-Wing TF, virtual currencies, asset recovery, the abuse of corporate structures for TBML/SBML purposes and large-scale cross-border ML schemes. The CRF-FIU further co-chaired an informal working group on FIU operational issues.

572. The CRF-FIU considers international co-operation as a key component to its work. To this end, the CRF-FIU engages in international co-operation in every possible legal avenue. This approach taken by the CRF-FIU is greatly appreciated by its foreign counterparts. Feedback from the FATF Global Network is highly positive on the quality and timeliness of assistance provided by the CRF-FIU.

573. Between 2017 and 2022, the CRF-FIU received and responded to approximately 3 300 requests. The average response time provided by the CRF-FIU is seven days, save for 2020, where Covid-19 impacted its operations for a limited period of time.

Table 8.23. CRF-FIU incoming requests, 2017-Q3 2022

| IRI | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|-----------------------------------|-------------|-------------|-------------|-------------|-------------|----------------|
| Received | 395 | 491 | 575 | 567 | 694 | 519 |
| Executed | 395 | 491 | 575 | 567 | 694 | 515 |
| Refused | 0 | 0 | 0 | 0 | 0 | 0 |
| Average number of days to respond | 5 | 9 | 7 | 23 | 9 | 13 |
| Refusal grounds applied | N/A | 0 | 0 | 0 | 0 | 0 |

Freezing measures

574. The CRF-FIU regularly exercises its powers to freeze assets and monitor bank accounts on behalf of foreign FIUs. This is not conditioned to reciprocity. In most cases, the requesting FIU will liaise with the judicial authorities to request the freeze. CRF-FIU information can be used as evidence to courts during penal procedures on request from foreign FIUs.

575. Between 2017 and 2022, the CRF-FIU implemented a total of 647 freezing measures in 423 different cases (domestic and international cases) for a total amount of EUR 0.7 billion. Most cases refer to fraud, corruption and bribery, and ML, which is in line with Luxembourg’s risk profile.

Table 8.24. CRF-FIU Freezing measures, 2017-Q3 2022

| Freezing measures | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|-----------------------|------------|------------|-------------|-------------|------------|-------------|
| N° of freezing orders | 50 | 54 | 91 | 291 | 96 | 65 |
| N° of involved cases | 35 | 41 | 64 | 186 | 58 | 39 |
| Amount frozen (EUR) | 12 563 431 | 87 407 533 | 231 148 557 | 216 701 317 | 38 273 048 | 154 570 652 |

Spontaneous disseminations

576. Between 2017 and 2022, the CRF-FIU sent out 6 877 spontaneous information reports to foreign FIUs. Most disseminations related to criminal tax offences, fraud, ML and TF (given Luxembourg's sensitive reflexes on T and TF elements). The CRF-FIU provided a number of examples where its assistance contributed significantly to cases pursued by its foreign counterparts.

Table 8.25. CRF-FIU spontaneous disseminations per designated offence, 2017-Q3 2022

| Designated Offences | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|---|------|------|------|------|------|---------|
| Breach of professional obligations | 1 | 4 | 5 | 3 | 10 | 9 |
| Corruption | 43 | 40 | 26 | 58 | 33 | 46 |
| Counterfeit money | 2 | 1 | 0 | 0 | 0 | 0 |
| Counterfeiting and product piracy | 2 | 1 | 0 | 5 | 5 | 5 |
| Criminal tax offences | 78 | 205 | 216 | 180 | 354 | 289 |
| Cybercrime | 9 | 15 | 36 | 31 | 16 | 25 |
| Environmental crime | 0 | 0 | 0 | 1 | 0 | 1 |
| Extortion | 0 | 3 | 3 | 1 | 0 | 0 |
| Forgery | 66 | 24 | 19 | 31 | 26 | 19 |
| Fraud | 239 | 209 | 247 | 320 | 445 | 363 |
| Human trafficking and migrant smuggling | 0 | 2 | 4 | 1 | 3 | 2 |
| Illicit arms trafficking | 3 | 3 | 3 | 4 | 3 | 1 |
| Illicit trafficking in narcotic drugs and psychotropic substances | 5 | 18 | 18 | 11 | 13 | 10 |
| kidnapping, illegal restraint and hostage-taking | 0 | 0 | 1 | 2 | 1 | 0 |
| Market abuse | 7 | 24 | 6 | 9 | 16 | 15 |
| Money laundering | 0 | 0 | 0 | 57 | 74 | 115 |
| Murder and grievous bodily harm | 1 | 3 | 3 | 0 | 4 | 1 |
| Others | 124 | 225 | 268 | 170 | 216 | 228 |
| Participation in an organised criminal group and racketeering | 12 | 1 | 6 | 5 | 3 | 4 |
| Sexual exploitation, including child sexual exploitation | 0 | 3 | 6 | 44 | 120 | 69 |
| Smuggling | 0 | 0 | 1 | 1 | 1 | 0 |
| Terrorism and terrorist financing | 215 | 232 | 190 | 243 | 193 | 63 |
| Thefts | 5 | 6 | 4 | 1 | 1 | 4 |

EU cross-border disseminations

577. The CRF-FIU regularly exchanges information, upon request or spontaneously, with other EU FIUs through the secure channel FIU.net. The CRF-FIU disseminates every year through the EU cross-border reporting mechanism between 30 000 and 40 000 reports. All incoming requests are treated in a timely manner. The CRF-FIU developed tailor-made add-ons to interconnect goAML and FIU.net. Ma3tch⁷³ matches are automatically synchronised between the two systems and exports to XBR⁷⁴ and XBD⁷⁵ exchange systems are done automatically. The system entails quality improvement scripts aiming at raising the overall data quality continuously. The CRF-FIU mainly focuses on XBR, as it ensures relevancy and quality of reports.
578. The CRF-FIU is also active in exchanging information with non-counterparts. In this context, it may authorise a foreign FIU to pass the requested information and supporting documents on to other authorities for the purposes for which they were requested or other purposes. Between 2017 and 2022, 1 171 reports were filed by reporting entities based on a request from a foreign authority. All were exchanged with the relevant counterparts together with the supporting documents. In the same period, the CRF-FIU responded to approximately 167 incoming requests from ARO's foreign counterparts.

SPJ

579. The SPJ receives and sends requests for police-to-police co-operation through EUROPOL and INTERPOL. These requests typically involve a check in databases concerning persons under investigation (e.g. identify a person's address, checking whether a person is under investigation, or has real estate or other property in Luxembourg, including exchange information on fingerprints, DNA, etc.). To facilitate international co-operation, the SPJ has a desk officer present in its EUROPOL national desk. The Office is open 24-7 to treat incoming requests. The SPJ-AB unit can respond to any request for international police-police co-operation within one working day and, in most of the cases, within few hours.

Table 8.26. Incoming request through Europol, 2017-Q3 2022

| Europol Messages | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|---|------|------|------|------|-------|---------|
| Foreign messages received by the Police related to ML | 460 | 545 | 651 | 763 | 1 014 | 1 003 |
| Foreign messages executed | 100% | 100% | 100% | 100% | 100% | 100% |

Table 8.27. Incoming messages for information through Interpol, 2017-Q3 2022

| Year | Number of messages processed regarding ML |
|------|---|
| 2017 | 37 |
| 2018 | 34 |
| 2019 | 30 |

⁷³ Ma3tch technology enables virtual information integration to build a 'dynamic networked collective intelligence' without infringing upon security, confidentiality, privacy and/or data protection regulations.

⁷⁴ Cross-border reporting.

⁷⁵ Cross-border dissemination.

| Year | Number of messages processed regarding ML |
|---------|---|
| 2020 | 45 |
| 2021 | 62 |
| Q3 2022 | 59 |

580. The SPJ Anti-Terrorism section (SPJ-SAT) has an additional channel for international police-to-police information exchange, namely the Police Working Group on Terrorism (PWGT) network, where the following messages were sent to Luxembourg for checks in the field of TF.

Table 8.28. Incoming messages for information, PWGT, 2017-Q3 2022

| Year | Number of messages processed regarding TF |
|---------|---|
| 2017 | 7 |
| 2018 | 7 |
| 2019 | 4 |
| 2020 | 6 |
| 2021 | 3 |
| Q3 2022 | 23 |

ARO

581. Between 2017 and 2022, the ARO received 470 international incoming requests for information from its counterparts. The average response time was two days. Given Luxembourg's context and ARO limited resources, this is commendable. The assessment team did not come across any negative information about the quality of ARO's input to its foreign counterparts.

Table 8.29. ARO incoming requests, 2017-Q3 2022

| | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|--------------------|------|------|------|------|------|---------|
| Incoming ARO/CARIN | 55 | 66 | 40 | 52 | 98 | 159 |

ACD

582. Throughout the review period, the ACD received and responded to numerous requests from its foreign counterparts in a comprehensive and timely manner. Requests relate to BO information, bank information, accounting records, and legal ownership. Incoming requests occasionally refer to more than one of the said categories.

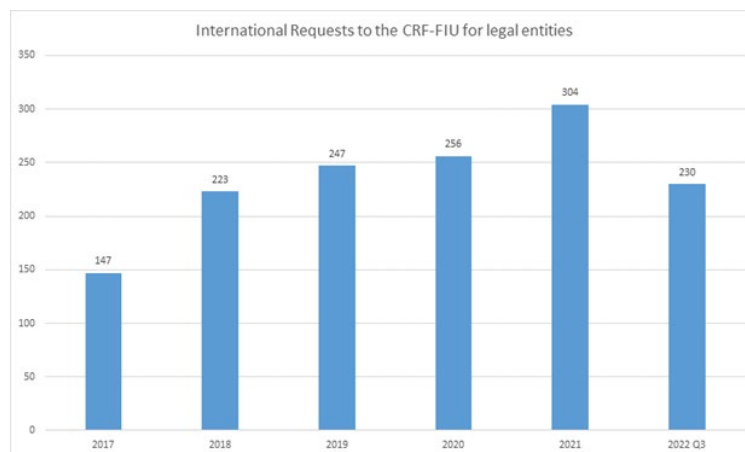
Table 8.30. ACD incoming request, 2017-Q3 2022

| | 2017 | 2018 | 2019 | 2020 | 2021 | Q3 2022 |
|--------------------------|-------|-------|-------|------|-------|---------|
| Incoming | 1 007 | 1 251 | 1 114 | 833 | 1 109 | 793 |
| Requests about BO | 65 | 48 | 24 | 77 | 60 | 35 |

International exchange of basic and beneficial ownership information of legal persons and legal arrangements

583. Luxembourg provides and responds to foreign requests for co-operation in identifying and exchanging basic and BO information of legal persons and legal arrangements in a timely and effective manner. In the review period, basic and BO information on all types of legal persons was publicly available, easily accessible, and free at the RCS (basic information) and at the RBE (BO information). In addition, information on legal arrangements was available through the Register of *Fiducies* and Trusts (RFT). This facilitated international co-operation to a significant degree, as it assisted Luxembourg's foreign counterparts in conducting preliminary research aiming at identifying potential misuse of legal persons (e.g., tax evasion, fraud, or corruption schemes), before contacting Luxembourgish competent authorities. Luxembourg competent authorities (CRF-FIU, CSSF, CAA, ACD) did not receive complaints from their foreign counterparts on the accuracy and currency of information available provided or available in the registries. Luxembourg provided a number of case studies demonstrating that basic and BO information is exchanged regularly and in an accurate and current manner.

Figure 8.2. CRF-FIU incoming requests on legal entities, 2017-Q3 2022



Box 8.4. Case Study: Foreign supervisor request

In August 2018, the CSSF received a request from a foreign supervisory authority to provide information on a customer, including transactions, to assist in an ongoing ML investigation.

According to the foreign supervisory authority, between April 2012 and October 2017, a company may have been engaged, wittingly or unwittingly, in trade with no commercial rationale and could have been used for illegal activities. The foreign supervisory authority also indicated that a Luxembourg bank was the counterparty bank to several trade activities.

The CSSF obtained from the bank and provided to a foreign supervisory authority information on transactions (i.e., initiators, employees who received the orders, details of the orders and execution of transactions) and customers behind these transactions (i.e., ultimate BOs, account information, powers of attorney and KYC/AML documentation).

The CSSF did not request or received feedback on the outcome of investigation conducted by its foreign counterpart.

Overall conclusions on IO.2

Overall, competent authorities demonstrated a very strong commitment to formal and informal international co-operation. On an operational level, competent judicial and investigative authorities, CRF-FIU, SPJ, and most supervisory authorities, effectively provided and sought MLA and other forms of international co-operation. Incoming MLA requests not requiring coercive measures are processed within three to four months. However, timeliness is an issue in some cases, as approximately 30% of incoming MLA requests requiring coercive measures are executed in a timeframe longer than seven months. In addition, the absence of an effective case management system to monitor and follow up outgoing MLA requests, impeded to some extent the ability of competent judicial authorities to swiftly execute outstanding requests. Resource limitations impacted to some extent quality and timelines of international co-operation sought and provided. Moderate improvements to address these issues will be needed.

Luxembourg is rated as having a Substantial level of effectiveness for IO.2.

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.

Where both the FATF requirements and national laws or regulations remain the same, this report refers to analysis conducted as part of the previous Mutual Evaluation in 2010. This report is available <https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Mutualevaluations/Mutualevaluationofluxembourg.html>.

Recommendation 1 – Assessing risks and applying a risk-based approach

This is a new Recommendation, which was not assessed in the 3rd Round MER.

Criterion 1.1 – Luxembourg identifies and assesses the ML/TF risks for the country through a national risk assessment (NRA) process involving all major stakeholders in public and private sectors. Luxembourg completed its first NRA in 2018 and updated it in September 2020 building on the risk assessments and sources identified in the 2019 EU Supranational Risk Assessment (EU SNRA). Luxembourg also completed a TF-focused vertical risk assessment (2022 TF VRA) in May 2022, and vertical risk assessments on VA/VASPs (2021) and legal persons and legal arrangements (2022). Luxembourg's methodological approach to these assessments takes into account, among other, inherent risk and mitigation measures in place, and is largely in line with guidance provided by the FATF. Luxembourg has also developed sub-sectoral risk assessments, including on sectors identified by the 2020 NRA (update) as higher risk.

Criterion 1.2 – A National Prevention Committee (NPC) is designated as the authority to co-ordinate actions to assess risks and is housed under the Ministry of Justice (MoJ) (2009 NPC Reg., Art.1(1)).

Criterion 1.3 – Luxembourg requires the NPC to keep the NRA up-to-date. Luxembourg began in early 2020 to update the 2018 NRA to reflect the risk environment as of end-2019, resulting in the completion of the 2020 NRA (update) (2009 NPC Reg., Art.1(1)).⁷⁶

Criterion 1.4 Luxembourg has mechanisms to provide information on the results of the risk assessments to all relevant competent authorities, and self-regulatory bodies (SRBs), FIs and DNFBPs (2009 NPC Reg., Art.1(2)(d) and 2(1)). In 2020, Luxembourg published a comprehensive version of the NRA update (except certain confidential sections) on numerous government websites⁷⁷ and the Luxembourg Financial Intelligence Unit (CRF-FIU) proactively disseminated it to all obliged entities registered in the STR/SAR tool, goAML. Luxembourg followed the same approach

⁷⁶ Luxembourg is in the process of drafting its third NRA.

⁷⁷ Example: <https://mj.gouvernement.lu/fr/dossiers/2020/lutte-blanchiment.html>

with the 2022 TF VRA. Furthermore, Luxembourg uses newsletters, presentations and participation in conferences to disseminate the results of the ML/TF NRAs and VRAs.

Criterion 1.5 Luxembourg largely applies a sound and reasonable risk-based approach (RBA) to allocating and prioritising resources and implementing measures to prevent or mitigate ML/TF at a high level. Luxembourg developed several national AML/CFT Strategies, including agency-level action plans, based on the results of the 2018 NRA and the 2020 NRA (update). These plans include the allocation of additional resources in line with risks identified, such as extra staffing the CSSF, and the establishment of the Asset Management Office (AMO).

Criterion 1.6 There are no wholesale exemptions from applying the FATF Recommendations for particular sectors. Based on findings of a service-specific risk assessment in 2015, obliged entities providing certain e-money and payment services are permitted to postpone verification as a part of their customer due diligence (CDD), subject to conditions and thresholds (such as transactions under EUR 250 or transactions through accounts with EU-based payment services providers) (2010 AML/CFT Reg., Art.2, 2004 AML/CFT Law, Art.3(2a)).

Criterion 1.7 Obligated entities are required to apply enhanced due diligence (EDD) measures in higher ML/TF risk situations, and to consider all relevant risk factors specified in the laws when conducting risk assessments. The obligation for EDD measures is risk-based and obliged entities are required to incorporate the high-risk information into their risk assessments (2004 AML/CFT Law, Art.2-2(2), 3-2(1), and 3-2(2)).

Criterion 1.8 Obligated entities are allowed to apply simplified due diligence measures when they identify a lower ML/TF risk. They are required to consider a non-exhaustive list of factors in the relevant laws and both national and supranational risk assessments while identifying risks (2004 AML/CFT Law, Art.2-2(2) and 3-1 and Annex III).

Criterion 1.9 Supervisors and SRBs are required to ensure that FIs and DNFBPs are implementing their obligations under R.1 (2004 AML/CFT Law, Art.2-1, 2-2, 8-1, 8-2, 8-2(a)).

Criterion 1.10 Obligated entities are required to take appropriate steps to identify, assess, and understand their ML/TF risks (for customers, countries or geographic areas; and products, services, transactions or delivery channels). This includes being required to **(a)** document their risk assessments; **(b)** consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied; **(c)** keep these assessments up to date; and **(d)** have appropriate mechanisms to provide risk assessment information to competent authorities and SRBs (2004 AML/CFT Law, Art.2-2(1) and 2-2(2)).

Criterion 1.11 Obligated entities are required to **(a)** have policies, controls and procedures, which are approved by senior management, to enable them to manage and mitigate the risks that have been identified (either by the country or by the FI or DNFBP); **(b)** monitor the implementation of those controls and to enhance them if necessary; and **(c)** take enhanced measures to manage and mitigate the risks where higher risks are identified (2004 AML/CFT Law, Art.2-2(2), Art.3-2 and 4(1)).

Criterion 1.12 Luxembourg permits obliged entities to take simplified due diligence measures if lower risks have been identified, and criteria 1.9 to 1.11 are met.

Simplified measures are not permitted when there is a suspicion of ML/TF (2004 AML/CFT Law, Art.3-1).

Weighting and Conclusion

Recommendation 1 is rated compliant.

Recommendation 2 - National Co-operation and Co-ordination

The 3rd Round MER identified effectiveness-related deficiencies, which are not assessed as part of technical compliance under the 2013 Methodology. Luxembourg subsequently formalised co-operation between the FIU and two supervisory bodies in 2011 and 2012.

Criterion 2.1 – Luxembourg develops and implements national AML/CFT policies, including a national strategy, that are based on identified risks and regularly reviewed by the NPC (2009 NPC Reg., Art.1). In October 2022, Luxembourg adopted the national AML/CFT Strategy 2023-2024 that builds on two previous national strategies (2019-2020 and 2020-2022) and groups initiatives across four priorities (further enhancing the prosecution of ML/TF, further developing the ML/TF investigative capabilities, harmonizing the supervision of DNFBPs, and improving TCSP market entry controls).

Criterion 2.2 – The NPC is responsible for developing, coordinating and evaluating national AML/CFT policies and strategies (2009 NPC Reg., Art.1(1)). Since November 2021, the AML/CFT Inter-ministerial Steering Committee (ISC) defines high-level strategic objectives whose operational implementation is monitored by the NPC (Grand-Ducal Decree of 10 Nov. 2021).

Criterion 2.3 – Luxembourg has a range of mechanisms to enable policy makers, CRF-FIU, law enforcement authorities (LEA), supervisors and other relevant competent authorities to co-operate, and where appropriate, co-ordinate and exchange AML/CFT information and knowledge domestically with each other concerning the development of national AML/CFT policies. Such mechanisms (e.g., statutory requirements, Memoranda of Understanding (MoU) signed between AML/CFT competent authorities, regular meetings) apply at both the policymaking level through the NPC, and at the operational level (2009 NPC Reg., Art.1(1); 1980 Judiciary Organisation Law, Art.74-4; 2004 AML/CFT Law, Art.9-1).

Criterion 2.4 – Luxembourg has a co-operation and co-ordination mechanism in place to combat proliferation financing (PF) at policymaking and operational levels. A monitoring committee established for the broader objectives of TFS is responsible for co-operation and co-ordination on TF and PF-related TFS (2022 Monitoring Committee Law, Art.2). The committee also invites participation by relevant national stakeholders to ensure co-operation and, where appropriate, co-ordination at an operational level.

Criterion 2.5 – Luxembourg has data protection laws with specific provisions in relation to data for AML/CFT purposes. It also has co-operation and co-ordination mechanisms to ensure the compatibility of AML/CFT and data protection and privacy requirements, for example through the NPC, as well as on a bilateral basis between the CRF-FIU and the National Data Protection Commission (CNPD), and between the CSSF and the CNPD (2004 AML/CFT Law, Art.9-1; 2018 CNPD Law, Art.8).

Weighting and Conclusion

Recommendation 2 is rated compliant.

Recommendation 3 - Money laundering offence

In its 3rd MER, Luxembourg was rated PC due to effectiveness issues that are no longer assessed as technical compliance under the 4th Round, and three technical deficiencies. These were incomplete criminalisation of terrorism and TF, and identification of predicate offences for ML; incomplete coverage of ML offence as required by the Vienna and Palermo Conventions; and criminal liability for ML did not extend to legal persons.

Criterion 3.1 – ML is criminalised on the basis of Art.3(1)(b)&(c) of the Vienna Convention and Art.(6)1 of the Palermo Convention (Penal Code, Art.506-1(1); 1973 Drug Trafficking Law, Art.8-1, respectively).

Criterion 3.2 – Luxembourg adopts a combined approach that includes a list of predicate offences and a penalty threshold, covering all serious offences with a view to including the widest range of predicate offences (Penal Code, Art.506-1(1)).

Criterion 3.3 – Luxembourg adopts a combined approach that includes a threshold, and predicate offences comprise all offences that are punishable by a minimum of more than six months' imprisonment (Penal Code, Art.506-1(1)).

Criterion 3.4 – Luxembourg's ML offence extends to any type of property, regardless of its value, that directly or indirectly represents the proceeds of crime (Penal Code, Art.31 and 506-1(2)).

Criterion 3.5 – There are no requirements that a person be convicted of a predicate offence to prove that property is the proceeds of crime (Penal Code, Art.506-8; 1973 Drug Trafficking Law, Art.8-1(5)).

Criterion 3.6 – Predicate offences for ML extend to conduct that occurred in another country, which constitutes an offence in that country, and which would have constituted a predicate offence had it occurred domestically (Penal Code, Art.506-3; 1973 Drug Trafficking Law, Art.8-1(4)).

Criterion 3.7 – ML offence applies to persons who commit the predicate offence and covers "self-laundering", unless this is contrary to fundamental principles of domestic law (Penal Code, Art.506-4; 1973 Drug Trafficking Law, Art.8-1(4)).

Criterion 3.8 – Intent and knowledge can be inferred from objective factual circumstances to prove the ML offence. This is demonstrated through domestic case law (Case n°14/17; Case n°173/19 V).

Criterion 3.9 – Natural persons convicted of ML offences are subject to a maximum imprisonment of five years, a maximum fine of EUR 1 250 000, or both. Sentences may also be doubled in the event of recidivism within 5 years and could be raised to an imprisonment of 15 to 20 years if the offence constitutes participation in the activity of an association or organisation. ML offences are also punishable independently of the predicate offence. Considering the risks identified in the 2020 NRA (update) and the range of applicable sanctions, the criminal sanctions are considered proportionate and dissuasive (Penal Code, Art.506-1, 506-5, 506-7, 506-8; 1973 Drug Trafficking Law, Art.8-1).

Criterion 3.10 – Legal persons are subject to criminal liability and sanctions. Parallel criminal, civil or administrative proceedings with respect to legal persons is not precluded in Luxembourg, as demonstrated through case law (Case n°3508/2015). Sanctions (a maximum criminal fine of EUR 12 500 000) are considered proportionate and dissuasive. The criminal liability of legal persons is without prejudice to that of natural persons. (Penal Code, Art.34 38, 506-1; Civil Code, Art.1382-1383).

Criterion 3.11 – Luxembourg provides ancillary offences to the ML offence, including: participation in; association with or conspiracy to commit; attempt; aiding and abetting; facilitating; and counselling the commission (Penal Code, Art.67(2) and 506-1, 506-4, 506-5, 506-6).

Weighting and Conclusion

Recommendation 3 is rated compliant.

Recommendation 4 - Confiscation and provisional measures

Luxembourg was rated PC in the former R.3. Deficiencies were related to the restricted scope of confiscation of property used or intended for use in an offence, and property of corresponding value, and insufficient provisional measures for blocking or freezing assets. Luxembourg addressed most of these deficiencies in the follow-up process.

Criterion 4.1 – Luxembourg has measures (including legislative measures) that enable their competent authorities to confiscate the property referred to in paragraphs (a) – (c) of this criterion. However, regarding confiscation of property of corresponding value (sub-criterion (d)), Luxembourg only has measures in relation to convicted persons, and proceeds of crime held by third parties (Penal Code, Art.31(2)(1-5), 31(3)).

Criterion 4.2 – Luxembourg has measures (including legislative measures) that enable:

(a) competent authorities to identify, trace, and evaluate property that is subject to confiscation through general search and investigative powers (Code of Criminal Procedure (CPP), Art.48-24, 51-1(1), 65, and 66; 1980 Judicial Organisation Law, Art.74-6);

(b) competent authorities to carry out provisional measures, such as freezing or seizing, to prevent any dealing, transfer or disposal of property subject to confiscation and without prior notice (CPP, Art.24-1, 31, 33, 66; 2004 AML/CFT Law, Art.5(3), 8-2(1)(f));

(c) competent authorities to take steps that will prevent or void actions that prejudice the country's ability to freeze or seize or recover property that is subject to confiscation (Penal Code, Art.31(2)(2) and 2004 AML/CFT Law, Art.5(3));

(d) competent authorities to take any appropriate investigative measures, including interrogations, search and seizure, surveillance, undercover operations and access to databases (CPP, Art.22, 30-31, 47, 48, 65-112; 2004 AML/CFT Law, Art.5(1)(a)-(b), 9-1; 1980 Judicial Organisation Law, Art.74-6).

Criterion 4.3 – The rights of *bona fide* third parties are protected (Penal Code, Art.31- 2(2); CPP, Art.68).

Criterion 4.4 – The Asset Management Office (AMO) is empowered to manage and, when necessary, dispose of property frozen, seized or confiscated (2022 Asset Management and Recovery Law, Art. 3-4).

Weighting and Conclusion

Luxembourg’s legal framework for confiscation and provisional measures is generally consistent with the requirements of R.4. However, the lack of measures that enable the confiscation of property of corresponding value to instrumentalities of crime creates a minor gap.

Recommendation 4 is rated largely compliant.

Recommendation 5 - Terrorist financing offence

In its 3rd MER, Luxembourg had numerous gaps regarding the scope of TF offence, including types of conducts and offences covered under international conventions and the former SRII; financing of terrorist organisations and individuals beyond the commission of an act of terrorism; definition of terrorist group; and criminal liability concerning legal persons. Luxembourg had since updated its CFT framework to address these deficiencies.

Criterion 5.1 – Luxembourg’s TF offences are consistent with the terrorist acts described in Article 2 of the International Convention for the Suppression of TF (TF Convention) (Penal Code, Art.135-5; 2021 Beijing Convention Law).

Criterion 5.2 – TF offences in Luxembourg are extended to any person who wilfully provides or collects funds or other assets by any means, directly or indirectly, with the unlawful intention that they should be used, or in the knowledge that they are to be used, in full or in part: (a) to carry out a terrorist act(s); or (b) by a terrorist organisation or by an individual terrorist (even in the absence of a link to a specific terrorist act or acts) (Penal Code, Art.135-5).

Criterion 5.2 bis – TF offences in Luxembourg include financing the travel of individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training (Penal Code, Art.135-5, 135-13, 135-15).

Criterion 5.3 – TF offences in Luxembourg extend to “funds” and “property”, which are interpreted broadly to cover all assets regardless of their source (Penal Code, Art.135-5(4)).

Criterion 5.4 – TF offences in Luxembourg do not require that the funds or other assets: (a) were actually used to carry out or attempt a terrorist act(s); or (b) be linked to a specific terrorist act(s) (Penal Code, Art.134-5(1)).

Criterion 5.5 – Intent and knowledge can be inferred from objective factual circumstances to prove an offence. This is demonstrated through domestic case law (Case n°279/09 of 3 June 2009).

Criterion 5.6 – Under Luxembourg laws, criminal sanctions applicable to natural persons convicted of TF are the same as those of terrorism convictions (i.e., a maximum of 20 years imprisonment, or up to life imprisonment if the act leads to a death). The imprisonment terms ensure that penalties are proportionate and dissuasive whereas the levels of criminal fines are proportionate and dissuasive as

compared to other offences in Luxembourg (from EUR 2 500 to 50 000) (Penal Code, Art.112-1, 135-1-17, 442-1).

Criterion 5.7 – Legal persons are subject to criminal liability and sanctions for TF. Parallel criminal, civil or administrative proceedings with respect to legal persons is not precluded in Luxembourg, as demonstrated through case law (Case n°3508/2015). The sanctions and fines (from EUR 500 to 750 000, or quintuple (i.e., EUR 3 750 000)) applicable to legal persons are proportionate and dissuasive. The criminal liability of legal persons is without prejudice to that of natural persons (Penal Code, Art.35-37; Civil Code, Art.1382-1383).

Criterion 5.8 – The Luxembourgish law covers the offences outlined in paragraphs (a), (b) and (d) of this criterion. Luxembourg relies on general provisions and provisions concerning accomplices to cover an offence to organise or direct others to commit a TF offence or attempted offence, under paragraph (c) (Penal Code, Art.51, 66, 67-69, 135-3, 135-4, 135-14).

Criterion 5.9 – TF offences are designated as ML predicate offences in Luxembourg (Penal Code, Art.506-1).

Criterion 5.10 – TF offences apply regardless of whether the financier is located in the same country or a different country from the one in which the terrorist organisation is located, or the terrorist act occurred/will occur (Penal Code, Art.135-4, CCP Art.7).

Weighting and Conclusion

Recommendation 5 is rated compliant.

Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing

In its 3rd Round MER, Luxembourg was rated PC due to narrow scope of freezing obligations; lack of de-listing, unfreezing, and unblocking procedures; as well as inadequate procedures for FIs and other persons liable to hold terrorist assets. While most of the deficiencies were addressed, those concerning procedures for FIs and other persons to hold terrorist assets, as well as freezing, seizure, and confiscation of terrorist assets other than UNSCRs 1267 and 1373 remained in the follow-up process.

Criterion 6.1 – In relation to UNSCRs 1267/1989 and 1988:

(a) The Ministry of Foreign Affairs (MoFA) is the competent authority for proposing persons or entities to the UNSCR 1267/1989 Committee and the 1988 Committee for designations (2020 Sanctions Implementation Law, Art.7).

(b) Despite Luxembourg having a monitoring committee to handle matters relevant to the implementation of TFS, the committee has no responsibility for identifying targets for designation based on the criteria in the relevant UNSCRs (2010 GDR, Art.3).

(c) As an EU Member State, Luxembourg is bound by decisions of the Court of Justice of the EU regarding the standard of proof, which call for “reasonable grounds” or “reasonable basis” for deciding whether to make a designation. Internal guidelines note that this evidentiary standard of proof applies when making proposals for designation. However, they incorporate by reference confidential EU-level guidance on how to develop sufficient evidence to support a designation, but this is not tailored

to Luxembourg's context. Under the governing designation and de-listing procedure, proposals for designation are not conditional upon the existence of a criminal proceeding.

(d) Luxembourg relies on an internal memo to govern the listing submissions that would need to be made using the UN standard forms (MoFA Internal Vademecum for the process of conveying information for the designation of persons, groups and entities, 13 April 2022).

(e) Submissions prepared by the MoFA should provide as much relevant information as possible on the proposed name and provide a statement of case containing as much detail as possible on the basis for the listing, consistent with UN and EU guidelines (MoFA internal Vademecum and internal Luxembourg Designation Procedures). The Vademecum also incorporates by reference standardized submission forms, which includes a field for specifying whether their status as a designating state may be made known in the case of UNSCR 1267/1989 committees.

Criterion 6.2 – In relation to UNSCR 1373:

(a) At the EU level, the Council of the EU is the competent authority for making EU designations to implement UNSCR 1373. This is prepared by the EU Working Party on the application of specific measures to combat terrorism (COMET), which applies designation criteria consistent with those of UNSCR 1373. At the national level, the MoF is the competent authority responsible for designating persons or entities that meet the UNSCR 1373 designation criteria (2020 Sanctions Implementation Law, Art.6).

(b) At the EU level, COMET has the mechanism for identifying targets for designations in line with UNSCR 1373 (EUCP 2001/931/CFSP, Art.1). At the national level, Luxembourg has no mechanism(s) for identifying targets for designations based on UNSCR 1373 criteria.

(c) At the EU level, requests are received and examined by the COMET. All Council CP working parties consist of representatives of the governments of EU Member States. EU designations are directly effective in all EU Member States and must include sufficient identifying information to exclude those with similar names. At the national level, there is no formal mechanism(s) for making a prompt determination of whether the request is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in UNSCR 1373, though authorities demonstrated that this has occurred as a practical matter.

(d) At the EU level, the COMET Working Party applies a “reasonable basis” evidentiary standard, and the designation is not conditional on the existence of criminal proceedings (EUCP 2001/931/CFSP, Art.1(4)). Under the governing designation and de-listing procedure, proposals for designation are not conditional upon the existence of a criminal proceeding.

(e) The internal Vademecum and internal Luxembourg Designation Procedures provide guidelines regarding provision of information in support of a designation proposal.

Criterion 6.3 –

(a) At the EU level, competent authorities have legal authorities and procedures to collect or solicit information to identify persons and entities that, based on reasonable grounds, or a reasonable basis to suspect or believe, meet the criteria for

designation (EUCP 2001/931/CFSP, Art.4). At the national level, the monitoring committee described in c.6.1(b) serves this role. Competent authorities have the power to collect information to identify persons and entities who meet the criteria for designation (2020 Sanctions Implementation Law, Art.6).

(b) At the EU level, designations take place without prior notice to the person/entity identified (EU Council Reg.881/2002, Art.7(a)(1); EC Council Reg.1286/2009, Preamble para.5). For asset freezing, the Court of Justice of the EU makes an exception to the general rule that notice must be given before the decision is taken to avoid compromising the effect of the first freezing order. The 1979 Grand Ducal Regulation for State administrative procedure authorizes *ex parte* proceedings where “important public interests require secrecy to be kept.”

Criterion 6.4 – Luxembourg, instead of relying on the EU framework, relies on a national legal framework that automatically transposes EU and UN designations for implementing TFS without delay (2020 Sanctions Implementation Law, Art. 4(2)).

Criterion 6.5 – In Luxembourg, EU Regulations and 2020 Sanctions Implementation Law provide the legal authority for implementing and enforcing TFS. MoFA and MoF are the competent authorities for implementing TFS.

(a) At the EU level, for UNSCRs 1267/1989 and 1988, all natural and legal persons are required to freeze all funds, financial assets, or economic resources of all designated persons and entities (irrespective of their nationality) (EU Council Reg.881/2002, Art.2(1); EU Council Reg.1286/2009, Art.1(2); EU Council Reg.753/2011, Art.3; EU Council Reg.754/2011, Art.1). For UNSCR 1373, natural and legal persons are required to freeze the assets of designated persons once the relevant EU Regulation comes into force (EU Reg. 2580/2001, Art.2(1a)). However, the transposition of UN designations into EU Regulations does not occur without delay and can result in de facto prior notice to designated persons.

(b) At the national level, there are obligations requiring natural or legal persons to freeze funds for the purposes of any UN designations, without delay and without prior notice (2020 Sanctions Implementation Law, Art. 1(1) and 3; GDR of 14 November 2022).

(c) At the EU level, for UNSCRs 1267/1989 and 1988, the freezing obligations extend to all funds or other assets that are owned or controlled by the designated person or entity (EU Council Reg. 881/2002, Art.2, EC Council Reg. 753/2011, Art.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, para.34-35).

(d) For UNSCR 1373, the freezing obligations apply to assets belonging to, owned or held by the designated individual or entity. However, this obligation does not apply to funds or assets controlled by, or indirectly owned by, or derived from assets owned by, or owned by a person acting at the direction of a designated person or entity. Like deficiencies identified in UNSCRs 1267/1988, jointly owned funds/assets are not covered under the freezing obligations (EU Council Reg.2580/2001, Art.1(a), 2(1)(a), 2(3)(iii) and (iv)).

(e) At the national level, all elements of funds or other assets mentioned in c.6.5(b) are covered for the purposes of any UN designation. There are no limitations requiring that funds be tied to a particular terrorist act, plot, or threat to be subject to freezing (2020 Sanctions Implementation Law, Arts.1(1), 2(1), 2(2), 2(4)).

(f) At the EU level, all EU nationals and legal persons incorporated or constituted under the laws of EU Member States are prohibited from making funds or other economic resources available to designated persons and entities (EU Council Reg.881/2002, Art.2(2); EU Council Reg.753/2011, Art.3(2); EU Council Reg.2580/2001, Art.2(1)(b)). At the national level, the prohibition from making funds or other assets, economic resources, or financial or other related services applies to Luxembourg nationals, as well as any other natural or legal persons operating in or from the territory of the country (2020 Sanctions Implementation Law, Art.3).

(g) At the EU level, designations are published in the Official Journal of the EU and information on designations is included in the financial sanctions database maintained by the EC.

(h) At the national level, the MoF publishes designations in the Official Gazette and on a website that is accessible to FIs and DNFBPs, and also communicates UN and EU designations via a newsletter, which occurs in under 24 hours. The MoF also provides general guidance on the implementation of UN financial sanctions on its website. Supervisors including CSSF and CAA have published additional guidance to FIs. However, there does not appear to be a mechanism for providing clear guidance to other persons or entities, including DNFBPs, that may be holding targeted funds or other assets on their obligations in taking action under freezing mechanisms (2010 GDR, Art.5; 2020 Sanctions Implementation Law, Art.4).

(i) At the EU level, natural and legal persons (including FIs and DNFBPs) are required to immediately provide any information about accounts and amounts frozen (EU Council Reg.881/2002, Art.5.1; EU Council Reg.2580/2001, Art.4; EU Council Reg. 753/2001, Art.8). At the national level, natural and legal persons (including FIs and DNFBPs) are required to report to MoF the prohibition actions taken (2020 Sanctions Implementation Law, Art.6(1)).

(j) At the EU level, there are measures which protect the rights of bona fide third parties. (EU Council Reg. 881/2002, Art.6; EU Council Reg.753/2011, Art.7) At the national level, the rights of bona fide third parties are also protected (2020 Sanctions Implementation Law, Art.8).

Criterion 6.6 –

(a) At the EU level, there are publicly known procedures to seek de-listing and unfreezing the funds or other assets of persons and entities which do not, or no longer, meet the criteria for designation (EU Council Reg.753/2011, Art.11(4) for designations under UNSCR 1988; EU Council Reg.881/2002, Art.7(a)(b)(1) for UNSCR 1267/1989). At the national level, MoF's website⁷⁸ provides information to direct persons and entities to submit de-listing requests through the UN Focal Point for De-listing under UNSCR 1730 or via the country. MoF has internal guidelines governing the de-listing procedures.

(b) At the EU level, there are publicly known procedures under its “working method”⁷⁹ for de-listing UNSCR 1373 designations. Such de-listing is immediately effective and may occur ad hoc or after mandatory reviews every 6 months (EU

⁷⁸ <https://mfin.gouvernement.lu/dam-assets/dossiers/sanctions-financi%C3%A8res-internationales/documentation/guidesheader2021/Guide-de-bonne-conduite-Sanctions-financi%C3%A8res-Non-TF-EN.pdf>

⁷⁹ www.data.consilium.europa.eu/doc/document/ST-10826-2007-REV-1/en/pdf

Council Reg. 2580/2001). Luxembourg's general administrative procedure law applies to de-listing requests.

(c) Designations pursuant to UNSCR 1373: At the EU level, a listed person or entity can write to the EU Council to have the designation reviewed or can challenge the relevant Council Regulation pursuant to the Treaty on the Functioning of the European Union⁸⁰ (TFEU, Art.263(4)). At the national level, a listed person or entity relies on the general appeal mechanism provided under the 1999 Administrative Procedures Law (Art.15-17) to seek redress to challenge a designation decision.

(d) Designations pursuant to UNSCR 1988: At the EU level, a person or entity is informed of the listing, its reasons and legal consequences, rights of due process and the de-listing procedures (including the UN Office of the Ombudsperson for UNSCR1267/1989 and the UN Focal Point Mechanism for UNSCR 1988). There are EU procedures that provide for delisting names, unfreezing funds, and reviews of designation decisions by the Council of the EU (EU Council Reg.753/2011, Art.11; EU Council Reg.881/2002, Art.7(a), 7(e)). At the national level, Luxembourg provides the relevant information on MoF's website.⁸¹ MoF has internal guidelines governing the de-listing procedures.

(e) Regarding designations on the Al-Qaida Sanctions List, Luxembourg relies on the same EU and national level measures referred to in c.6.6(d).

(f) False positives: At the EU level, there are publicly known procedures for obtaining assistance in verifying whether persons or entities having the same or similar name as designated persons or entities are inadvertently affected by a freezing mechanism (EU Best Practices for the Effective Implementation of Restrictive Measures, Part II).⁸² At the national level, the MoF is the competent authority to address questions and challenges to designations (including false positives). The Guidelines Relating to the Implementation of TF Financial Sanctions, published on the MoF's website, contain general procedures on addressing false positives.

(g) Mechanisms for communicating de-listing and unfreezing to the financial sector and DNFBPs: At the EU level, the Official Journal of the European Union (OJEU) provides the mechanism. At the national level, the MoF publishes de-listings in the Official Gazette and on its website. The MoF also communicates de-listings via its newsletter, and subscription of this newsletter is open to all and free-of-charge, though the newsletter is not directed at FIs and DNFBPs specifically. The website of the MoF and CSSF (supervisor for FIs save for insurance sector) also have general guidance for FIs and other persons or entities on their obligations to respect a de-listing or unfreezing action.

Criterion 6.7 – At the EU level, there are mechanisms for authorising access to frozen funds or other assets which have been determined to be necessary for basic expenses, the payment of certain types of expenses, or for extraordinary expenses. At the national level, the MoF is responsible for authorising such access to frozen funds or other assets (EU Council Reg.881/2002, Art.2a; EU Council Reg.753/2011, Art.5; EU

⁸⁰. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12016ME%2FTXT>

⁸¹. <https://mfin.gouvernement.lu/dam-assets/dossiers/sanctions-financi%C3%A8res-internationales/documentation/guidesheader2021/Guide-de-bonne-conduite-Sanctions-financi%C3%A8res-Non-TF-EN.pdf>

⁸² <https://data.consilium.europa.eu/doc/document/ST-10572-2022-INIT/en/pdf>

Council Reg. 2580/2001, Art.5-6; 2020 Sanctions Implementation Law, art.6 (1), 2010 GDR, Art.1(1), 2(2)).

Weighting and Conclusion

There are minor shortcomings in Luxembourg's TF-TFS framework, particularly in identifying and proposing targets for designation with a view to UNSCRs 1267/1989 and 1373.

Recommendation 6 is rated largely compliant.

Recommendation 7 – Targeted financial sanctions related to proliferation

These requirements were added to the FATF Recommendations when they were last revised in 2012, and therefore were not assessed during Luxembourg's 3rd Round MER.

Criterion 7.1 – UN PF-TFSs are implemented through the EU framework, and a national framework that provides for automatic transposition of EU and UN designations. (2020 Sanctions Implementation Law, Art.4(2)).

Criterion 7.2 – The MoF is the legal authority and competent authority responsible for implementing and enforcing PF-TFS.

(a) The EU framework requires all natural and legal persons within the Member States to freeze, without delay and without prior notice, the funds or other assets of designated persons and entities. However, the obligation is not triggered until publication in the OJEU. This suggests a possibility that freezing may not happen without delay for natural and legal persons that have not yet been designated by the EU. This also raises the question of the UN designated person/entity to receive prior notice before a freezing action can take place (EU Council Reg. 2017/1509, Art.1; EU Council Reg. 267/2012, Art.49). At the national level, there are obligations requiring natural or legal persons to seize funds for the purposes of any UNSC Chapter VII designations, without delay and without prior notice (2020 Sanctions Implementation Law, Art. 1(1) and (2); GDR of 14 November 2022).

(b) The freezing obligations are specified under the EU framework. However, the relevant EU Council Regulations do not expressly require the freezing of those funds or other assets that are jointly owned or controlled by designated persons or entities (EU Council Reg. 2017/1509, Art.34; EU Council Reg. 267/2012, Art.1, 23(1) and 23(2)(a)). At the national level, save for sub-element (iii), all elements of funds or other assets mentioned in c.7.2(b) are covered for the purposes of any UNSC Chapter VII designations. (2020 Sanctions Implementation Law, Arts.1(1), 2(1), 2(2), 2(4)).

(c) The EU framework prohibits funds and other assets from being made available, directly or indirectly, to or for the benefit of designated persons and entities unless otherwise authorised or notified in compliance with the relevant UN resolutions (EU Council Reg. 2017/1509, Art.34; EU Council Reg. 267/2012, Art.23 and 23a). At the national level, the prohibition from making funds or other assets available to, or for the benefit of UNSC Chapter VII designated persons and entities applies to Luxembourg nationals, as well as any other natural or legal persons operating in or from the territory of the country (2020 Sanctions Implementation Law, Art.3).

(d) The MoF publishes national designations in the Official Gazette, newsletter, and on a website that is accessible to FIs and DNFBPs, and also communicates UN and

EU designations via a newsletter, which occurs in under 24 hours. In addition, the MoF, through its website, provides general guidance on the implementation of UN financial sanctions, including DPRK and Iran-related resolutions. Financial supervisors (CSSF and CAA) have published additional guidance to FIs. However, most SRBs (other than the OEC) responsible for supervising DNFbps and other entities have not provided guidance on their obligations in taking action under freezing mechanisms.

(e) At the national level, natural and legal persons (including FIs and DNFbps) are required to report to the MoF the prohibition actions taken (2020 Sanctions Implementation Law, Art.6(1)).

(f) The rights of *bona fide* third parties are protected under the EU framework and national level (EU Council Reg. 2017/1509, Art.54; EU Council Reg. 267/2012, Art.42; 2020 Sanctions Implementation Law, Art.8).

Criterion 7.3 – EU Member States are required to take all necessary measures to ensure that the EU Council Regulations on PF-TFS are implemented, and to determine a sanction system that is effective, proportionate and dissuasive. At the national level, Luxembourg requires its supervisors and SRBs to monitor and ensure compliance by FIs and DNFbps for PF-TFS obligations. Failure to comply with such laws or enforceable means are subject to the same civil, administrative or criminal sanctions as mentioned in R.35 (EU Council Reg. 2017/1509, Art.55; EU Council Reg. 267/2012, Art.47; 2020 Sanctions Implementation Law, Arts. 6, 10).

Criterion 7.4 – Luxembourg communicates the de-listing published in the OJEU on the MoF's website and its newsletter (available on subscription at the national level, the MoF's website provides information to direct persons and entities to submit de listing requests through the UN Focal Point for De listing).

(a) The Council of the EU communicates its designation decisions and the grounds of listing to designated persons and entities, which have the rights of due process. The Council of the EU also enables designated persons and entities to petition for de-listing at the Focal Point for de-listing established pursuant to UNSCR 1730, or informing designated persons or entities to petition the Focal Point directly (EU Council Reg. 2017/1509, Art.47(3)-(5); EU Council Reg. 267/2012, Art.46(4)-(7)).

(b) At the national level, the MoF is the competent authority to address questions and challenges to designations (including false positives). The Guidelines Relating to the Implementation of non-TF Financial Sanctions, published on the MoF's website, contain general procedures on addressing false positives (2020 Sanctions Implementation Law, Art.6 (1)).

(c) The MoF is responsible for granting designated persons or entities access to funds or other assets should the exemption conditions set out in UNSCRs 1718 and 2231 be met, in accordance with the EU framework (EU Council Reg. 2017/1509, Art.35-36; EU Council Reg. 267/2012, Art.24, 26, 27, 28, 28b; 2020 Sanctions Implementation Law Art.6(1)).

(d) The OJEU is the mechanism at the EU level for communicating de-listings and unfreezings. The MoF, through its newsletter, communicates de-listings and unfreezings to its subscribers at the national level, generally in under 24 hours. Subscription of this newsletter is open to all and free-of-charge, though the newsletter is not directed at FIs and DNFbps specifically. Like c.7.2(d), the MoF and supervisors,

including CSSF and CAA, have provided general guidance to FIs on UNSC financial sanctions. However, there is no mechanism for providing clear guidance to DNFBPs, including entities supervised by SRBs on their obligations to respect a de-listing or unfreezing action.

Criterion 7.5 – Regarding contracts, agreements or obligations that arose prior to the date on which accounts became subject to TFS:

(a) The EU framework permits the addition to the accounts frozen pursuant to UNSCRs 1718 or 2231 of interest or other earnings 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 any such interest, other earnings and payment continue to be subject to these provisions and are frozen (EU Council Reg. 2017/1509, Art.34; EU Council Reg. 267/2012, Art.29).

(b) The EU framework permits the making of payments due under a contract entered prior to the date of listing, provided that (i) competent authorities have determined that the contract is not related to any of the prohibitions referred to in UNSCR 2231; (ii) competent authorities have determined that the payment is not directly or indirectly received by a listed person or entity; and (iii) prior notification is made to the UNSC (EU Council Reg. Art.25).

Weighting and Conclusion

Luxembourg relies principally on the EU framework to implement PF-TFS. There are, however, minor shortcomings concerning limited guidance provided to DNFBPs on their obligations in taking action under freezing mechanisms.

Recommendation 7 is rated largely compliant.

Recommendation 8 – Non-profit organisations

Luxembourg was rated PC in its 3rd Round MER due to an absence of (a) outreach for associations and foundations; (b) supervision and oversight; and (c) domestic co-operation and co-ordination mechanism, as well as incomprehensive sanctions.

Criterion 8.1 –

(a) Luxembourg has recently completed a comprehensive review to identify which subset of organisations fall within the FATF definition of NPOs, to identify the features and types of NPOs which by virtue of their activities or characteristics, are likely to be at risk of TF abuse. Luxembourg considers all *associations sans but lucratif* (ASBLs) and *Fondations* that focus on international development projects in developing countries (DNGOs, 91 in total) to fall within the FATF definition, along with 16.4% of *Fondations* (33), and approximately 1.85% of ASBLs without public utility status (based on a statistical sampling of a representative subset of 8 000 registered ASBLs).

(b) Luxembourg is aware of the relevant reports published by the FATF on emerging TF risks (including those posed by NPOs). Luxembourg conducted an assessment as a part of its vertical risk assessment of legal persons and legal arrangements (adopted in February 2022) to identify the nature of threats posed by terrorist entities to the NPOs which Luxembourg deems most likely to be at risk, as well as how terrorist actors abuse those NPOs.

(c) Luxembourg has several laws and circulars related to the registration and transparency of NPOs. In 2020, the MoJ conducted a review of the adequacy of these measures as they may apply to the subset of the NPO sector that may be abused for TF support. The review finds that the strict licensing measures in place for *Fondations* are proportionate and effective. As for a lesser set of requirements in place for the subset of ASBL that fall within the FATF definition, they are also considered appropriately proportionate due to the smaller size of these entities.

(d) Luxembourg makes use of its recently-initiated regular NRA process to assess the sector's potential vulnerabilities to terrorist activities to ensure effective implementation of measures. The first of such review was initiated in 2020 and published in early 2022.

Criterion 8.2 – Luxembourg's policies to promote accountability, integrity, and public confidence in the administration and management of NPOs have manifested in a number of ways, including through public statements describing all of the contractual obligations that DNGOs are subject to (including many of the licensing measures described in 8.1(c)) for approval by the MoFA, public guidance to facilitate *Fondations* and ASBLs' implementation of transparency requirements, and direct outreach by the MoJ to all *Fondations* and ASBLs with public utility status regarding their legal obligations.

(a) Luxembourg undertakes both regular outreach to the NPO sector on general administration and management and has recently undertaken outreach and educational programmes to raise and deepen awareness among NPOs as well as the donor community about the potential vulnerabilities of NPOs to TF abuse and TF risks, and the measures that NPOs can take to protect themselves against such abuse. These have included, among other things, wide dissemination of a paper on the risks to the NPO sector of TF (via publication on websites and direct distribution to all DNGOs and the subset of *Fondations* that fall within the FATF definition), roundtables, webinars, and outreach to the donor community.

(b) Luxembourg has developed best practices to address TF risk and vulnerabilities and protect the NPO sector from TF abuse and engages the sector to promote such best practices through regular contacts, meetings, roundtables and webinars since 2019.

(c) The MoJ encourages NPOs to conduct transactions via regulated financial channels as a best practice in its general guidance to NPOs on transparency and compliance. Luxembourg authorities have promoted the use of regulated financial channels in webinars and roundtables and reminded NPOs of the importance of declaring cash transactions more than EUR 10 000 when using cash in areas where financial channels are disrupted.

Criterion 8.3 – Luxembourg has introduced some supervision/monitoring measures on DNGOs (e.g., reporting obligations and inspection); however, these measures are neither based on risk nor on the findings of the risk assessment. There is no targeted risk-based supervision of the subset of *Fondations* nor of ASBLs without public utility status that fall within the FATF definition.

Criterion 8.4 – (a) The MoFA, supported by an external auditor, has initiated monitoring for some DNGOs for compliance with the requirements of this Recommendation, but this was not performed on a risk-basis. The criteria for selecting five DNGOs, each year for supervision review, are not based on the findings of the risk assessment. The subset of *Fondations* and ASBLs without public utility

status is subject to monitoring on a “case-by-case” basis. However, this determination is not made on a risk-sensitive basis. (b) NPOs are subject to sanctions for failure to abide by the disclosure obligations described above, including liquidation and potentially criminal penalties for both the responsible legal and natural persons. Luxembourg can apply general provisions of its Penal Code against NPOs, as relevant and appropriate. These provisions encompass a wide range of prospective penalties that have never been applied. Sanctions are considered neither proportionate nor dissuasive. Luxembourg did not provide any indication of the provisions of the Penal Code that would apply for violations under sub-criterion 8.4(b), nor the expected range of penalties in this regard.

Criterion 8.5 –

(a) The CRF-FIU has an MoU with the MoFA and MoJ to facilitate co-operation, coordination and information sharing regarding NPOs. For the same purpose, an MoU also exists between the MoJ and the MoFA.

(b) Luxembourg relies on the CRF-FIU to examine those NPOs suspected of either being exploited by, or actively supporting, terrorist activity or terrorist organisations. An expert is dedicated to TF and NPOs within the CRF-FIU.

(c) Information on the administration and management of particular NPOs is available to the CRF-FIU, law enforcement and prosecution authorities during an investigation. NPO regulators (MoFA and MoJ) have full access to information on the administration and management of particular NPOs published at the RCS or RBE. DNGOs are also required to submit relevant information to the MoFA, and the MoFA has the right to demand any relevant information from DNGOs as a condition of funding (2004 AML/CFT Law, Art.5(1)(b); 1980 Judiciary Organisation Law, Art.74-6).

(d) All public officers and civil servants (including those in the MoFA and MoJ), as well as FIs and DNFBPs are required to report suspicions covered under this sub-criterion to the CRF-FIU (CPP, Art.23; 2004 AML/CFT Law, Art.5(2)).

Criterion 8.6 – International requests for information regarding particular NPOs suspected of TF or involvement in other forms of terrorist support are handled in the same way as any other request for information. The central point of contact is the General State Prosecutor (PG). The CRF-FIU can be directly contacted by a foreign FIU and exchange all information and evidence that may be relevant to processing or analysing information on ML, associated predicate offences or TF on the natural or legal person concerned, which include NPOs. International agencies can also directly access publicly available information held at the Trade and Company Register (RCS) and at the BO register (RBE). (2000 MLA Law, Art.2(1), 1980 Judiciary Organisation Law, Art.74-5(1)).

Weighting and Conclusion

Luxembourg has moderate shortcomings in its framework to prevent TF abuse through NPOs: absence of a targeted risk-based supervision or monitoring of NPOs and lack of effective and dissuasive sanctions.

Recommendation 8 is rated partially compliant.

Recommendation 9 – Financial institution secrecy laws

In its 3rd Round MER, Luxembourg was rated partially compliant on financial secrecy. The deficiencies were that FIs can invoke professional secrecy against sharing information with the FIU and that private sector representatives can be prosecuted for reporting information violating professional secrecy.

Criterion 9.1 –

Access to information by competent authorities:

No professional secrecy laws inhibit disclosures by FIs and DNFBPs to supervisors and the CRF-FIU (2004 AML/CFT Law, Art.5(4)). For natural and legal persons, subject to prudential supervision by the CSSF, the European Central Bank or a foreign supervisor, professional secrecy does not exist where the disclosure of information is authorised or required by, or pursuant to, any legislative provision (1993 LFS Law, Art.41(2)(e)).

Sharing of information between competent authorities:

Supervisors and the CRF-FIU are empowered under law to exchange information to fulfil their AML/CFT duties (2004 AML/CFT Law, Art.9-1). The CSSF and CAA can exchange information for combatting ML and TF, both domestically (2004 AML/CFT Law, Art.9-1a), and with foreign competent authorities (2004 AML/CFT law, Art.9-2a). Supervisors also rely on MoUs to enable information sharing with each other (e.g., Co-operation and Exchange of Information Agreements between the CRF-FIU and the CAA and the CRF-FIU and the CSSF, MoU for the purposes of AML/CFT supervision between the CAA and CSSF, MoU between the CSSF and AED, MoU between the CAA and AED).

Sharing of information between FIs:

There are no financial institution secrecy laws that explicitly restrict the sharing of information between FIs where this is required by R.13, 16, and 17. FIs are required to share information notwithstanding any applicable rules on confidentiality or professional secrecy. FIs must be satisfied that respondents are able to provide relevant CDD data and information upon request (2004 AML/CFT Law, Art.3-2(3)(e)). Third party FIs must make relevant information requested immediately available (2004 AML/CFT Law, Art.3-3(3)).

Weighting and Conclusion

Recommendation 9 is rated compliant.

Recommendation 10 – Customer due diligence

In its 3rd MER, Luxembourg was rated partially compliant with these requirements. The deficiencies related to: the narrow scope of FI coverage; fictitious accounts, numbered accounts and passbooks; no or lack of requirements to verify the authorisation of a natural person claiming to act in the name of a legal person or arrangement, or verify if a customer is acting on behalf of another person, or identify the beneficial owner; no requirement to verify if a customer is acting on behalf of another person; insufficient EDD obligations, and wide scope and threshold of CDD exemption; exemption of CDD requirements for FIs in EU/EEA countries and non-residents.

Criterion 10.1 – FIs are prohibited from keeping anonymous/numbered accounts, anonymous/numbered passbooks or anonymous/numbered safe deposit boxes, and accounts in obviously fictitious names (2004 AML/CFT Law, Art.3(4) third para.).

Criterion 10.2 – CDD measures are required when:

- (a) establishing a business relationship (2004 AML/CFT Law, Art.3(1)(a));
- (b) carrying out a transaction above EUR 15 000, whether this transaction is carried out in a single operation or in several operations which appear to be linked (2004 AML/CFT Law, Art.3(1)(b)(i));
- (c) carrying out occasional transactions that are wire transfers in the circumstances covered by R.16 and its Interpretive Note (2004 AML/CFT Law, Art.3(1)(b)(ii));
- (d) when there is a suspicion of ML/TF, regardless of any exemptions or thresholds (2004 AML/CFT Law, Art.3(1)(c)); and
- (e) there are doubts about the veracity or adequacy of the previously obtained customer identification data (2004 AML/CFT Law, Art.3(1)(d)).

Criterion 10.3 – FIs are required to identify the customer (whether permanent or occasional, and whether natural or legal person or legal arrangement) and verify that customer's identity using reliable, independent source documents, data or information (identification data) (2004 AML/CFT Law, Art.3(1), (2)).

Criterion 10.4 – FIs are required to verify any person purporting to act on behalf of or for the customer is so authorised, and to identify and verify the identity of that person (2004 AML/CFT Law, Art.3(2)(d), second para., sub-para.(a)).

Criterion 10.5 – FIs are required to identify and take reasonable measures to verify the identity of beneficial owners using relevant information or data obtained from a reliable and independent source, such that they are satisfied that they know who the beneficial owner is (2004 AML/CFT Law, Art.3(2)(b), 3(2a)).

Criterion 10.6 – FIs are required to understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship (2004 AML/CFT Law, Art.3(2)(c)).

Criterion 10.7 – FIs are required to conduct ongoing due diligence on the business relationship (2004 AML/CFT Law, Art.3(2)(d)), including by:

- (a) scrutinising transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the FIs' knowledge of the customer, their business and risk profile, including where necessary, the source of funds (2004 AML/CFT Law, Art.3(2)(d));
- (b) ensuring that the documents, data or information collected under the CDD process are kept up-to-date and relevant for higher-risk categories of customers (2004 AML/CFT Law, Art.3(2)(d)).

Criterion 10.8 – FIs are required to understand the nature of business, ownership, and control structure of customers that are legal persons or legal arrangements (2004 AML/CFT Law, Art.3(2)(d), second para., sub-para.(b)(i)).

Criterion 10.9 – For customers that are legal persons or legal arrangements, FIs are required to identify the customer and verify its identity through the following information:

- (a) name, legal form, and proof of existence (2004 AML/CFT Law, Art.3(2)(d), second para., sub-para.(b)(ii));
- (b) the powers that regulate and bind the legal person or arrangement, as well as the names of the relevant persons having a senior management position in the legal person or legal arrangement (2004 AML/CFT Law, Art.3(2)(d), second para.(b)(iii)); and
- (c) the address of the head office and, if different, a principal place of business (2004 AML/CFT Law, Art.3(2)(d), second para.(b)(iii)).

Criterion 10.10 – For customers that are legal persons, FIs are required to identify and take reasonable measures to verify the identity of the beneficial owners through the following information:

- (a) the identity of the natural person(s) who ultimately has a controlling interest in a legal person (2004 AML/CFT Law, Art.3(2)(b), second para.(i));
- (b) where, after applying the requirements under (a), there is a doubt as to whether the person(s) with the controlling ownership interest is the beneficial owner(s) or where no natural person exerts control through ownership interests, the identity of the natural person(s), if any, exercising control of the legal person through other means (2004 AML/CFT Law, Art.3(2)(b), second para., sub-para.(ii));
- (c) where no natural person is identified under (a) or (b) above, the identity of the relevant natural person who holds the position of senior managing official (2004 AML/CFT Law, Art.3(2)(b), second para.(iii)).

Criterion 10.11 – For customers that are legal arrangements, FIs are required to identify and take reasonable measures to verify the identity of the beneficial owners through the following information:

- (a) for trusts, the identity of the settlor(s), the trustee(s), the protector(s), if any, the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate control over the trust, including through a chain of ownership or control (2004 AML/CFT Law, Art.1(7)(b), 3(2)(b), fourth para.(i));
- (b) for other types of legal arrangements, the identity of persons in equivalent or similar positions (2004 AML/CFT Law, Art.1(7)(c), 3(2)(b), fourth para.(ii)).

Criterion 10.12 – In addition to the CDD measures required for the customer and the beneficial owner, FIs are required to perform CDD measures on the beneficiary of life insurance and other investment related insurance policies, as soon as the beneficiaries are identified or designated:

- (a) for a beneficiary that is identified as a specifically named person or arrangement, the name of the person (2004 AML/CFT Law, Art.3(2b), first para., sub-para.(a)).
- (b) for a beneficiary that is designated by characteristics or by class or by other means, sufficient information concerning the beneficiary to satisfy the FI that it will be able to establish the identity of the beneficiary at the time of the payout (2004 AML/CFT Law, Art.3(2b), first para.(b)).

(c) for both above cases, the verification of the identity of the beneficiary must occur at the time of payout (2004 AML/CFT Law, Art.3(2b)).

Criterion 10.13 – FIs are required to include the beneficiary of a life insurance policy as a relevant risk factor in applying EDD measures. If the FI determines that a beneficiary who is a legal person or a legal arrangement presents a higher risk, the FI is required to take reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary at the time of payout (2004 AML/CFT Law, Art.3(2b), third para.).

Criterion 10.14 – FIs are required to verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers, provided that (a) this occurs as soon as reasonably practicable; (b) this is essential not to interrupt the normal conduct of business; and (c) the ML/TF risks are effectively managed. (2004 AML/CFT Law, Art.3(4)). While FIs are permitted to verify the identity of the customer and beneficial owner after the opening of certain transferable securities accounts, verification must nevertheless be carried out in line with elements (a) to (c) before any transactions can be made (2004 AML/CFT Law, Art.3(4), third para.).

Criterion 10.15 – FIs are required to adopt risk management procedures concerning the conditions under which a customer may utilise the business relationship prior to verification (2004 AML/CFT Law, Art.3(4), sixth para.).

Criterion 10.16 – FIs are required to apply CDD to existing customers on the basis of materiality and risk, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained (2004 AML/CFT Law, Art.3(5); 2010 AML/CFT GDR, Art.1(4)).

Criterion 10.17 – FIs are required to apply EDD when they identify higher ML/TF risks, either through a list of non-exhaustive risk factors provided in the law or through a risk assessment (2004 AML/CFT Law, Art.3-2(1)).

Criterion 10.18 – FIs may apply simplified CDD when lower ML/TF risks are identified through an analysis of risks by the FI. When assessing risk, FIs are required to take into account, among other things, risks identified in the supranational and national risk assessments (2004 AML/CFT Law, Art.2-2(2), 3-1(1), (2)). FIs must be able to demonstrate that the simplified measures are commensurate with the ML/TF risks identified (2004 AML/CFT Law, Art.3(2a)). FIs cannot apply simplified CDD when there is suspicion of ML/TF or specific higher risk scenarios apply (2004 AML/CFT Law, Art.3-1(5)).

Criterion 10.19 – Where an FI is unable to comply with relevant CDD measures, it is required:

- (a) not to establish a business relationship or perform the transaction, and to terminate the business relationship; and
- (b) to consider making an STR (2004 AML/CFT Law, Art.3(4), fourth para.).

Criterion 10.20 – In cases where FIs form a suspicion of ML/TF, and they reasonably believe that performing the CDD process will tip-off the customer, they are permitted to not pursue the CDD process if they file an STR (2004 AML/CFT Law, Art.3(4), sixth para.)

Weighting and Conclusion

Recommendation 10 is rated compliant.

Recommendation 11 – Record-keeping

Luxembourg was rated largely compliant in the 3rd Round MER. Deficiencies related to the coverage for FIs and no requirements to extend the record keeping requirement beyond 5 years at the request of a competent authority or to keep documents that permit reconstruction of transactions.

Criterion 11.1 – FIs are required to retain all necessary records on transactions, both domestic and international, for at least five years following completion of the transactions (2004 AML/CFT Law, Art.3(6)(b)).

Criterion 11.2 – FIs are required to keep a copy of the documents, data and information necessary to comply with CDD requirements, account files and business correspondence, and results of any analysis undertaken for five years after the end of the business relationship or occasional transaction (2004 AML/CFT Law, Art.3(6)(a); 2010 AML/CFT GDR, Art.1(4); 2020 CSSF Reg., Art.27).

Criterion 11.3 – FIs are required to keep transaction records sufficient to permit reconstruction of individual transactions to provide, if necessary, evidence for prosecution of criminal activity (2004 AML/CFT Law, Art.3(6)(b)).

Criterion 11.4 – FIs are required to maintain personal data to ensure that all CDD information and transaction records are available promptly to the domestic competent authorities to properly fulfil their tasks and facilitate investigation and detection of ML/TF (2004 AML/CFT Law, Art.3(6), (6a) fourth para. 5(1)).

Weighting and Conclusion

Recommendation 11 is rated compliant.

Recommendation 12 – Politically exposed persons

Luxembourg was rated partially compliant with obligations regarding domestic PEPs in the 3rd Round MER. Deficiencies included restrictive definition of PEP; and no obligations for EDD on PEPs residing in Luxembourg, having a risk management system to determine whether the beneficial owner is a PEP or obtaining senior management approval before opening an account or continuing a business relationship with a customer who has become a PEP.

Criterion 12.1 – In relation to foreign PEPs, in addition to performing CDD required under R.10, FIs are required to:

- (a)** put in place risk management systems to determine whether a customer or a beneficial owner is a PEP (2004 AML/CFT Law, Art.3-2(4)(a));
- (b)** obtain senior management approval before establishing (or continuing, for existing customers) such business relationships (2004 AML/CFT Law, Art.3-2(4)(b));
- (c)** take reasonable measures to establish the source of wealth and source of funds (2004 AML/CFT Law, Art.3-2(4)(c), 2010 AML/CFT GDR, Art. 3(4) subparagraph 5);
- (d)** conduct enhanced ongoing monitoring of the business relationship (2004 AML/CFT Law, Art.3-2(4)(d)).

Criterion 12.2 – Luxembourg makes no distinction between foreign and domestic PEPs. The measures described in c.12.1 apply equally to domestic PEPs.

Criterion 12.3 – FIs are required to apply relevant requirements of c.12.1 and c.12.2 to family members or persons known to be close associates of all types of PEPs (2004 AML/CFT Law, Art.1(9-12)).

Criterion 12.4 – In relation to life insurance policies, FIs are required to take reasonable measures to determine whether the beneficiaries and/ or, where required, the BO of the beneficiary are PEPs. Those measures shall be taken no later than at the time of the payout or at the time of the assignment (2004 AML/CFT Law, Art.3-2 (4), third para.). In cases of higher risk, FIs are required to inform senior management before payout, conduct enhanced scrutiny of the entire relationship with the policyholder and consider filing an STR (2004 AML/CFT Law, Art.3-2 (4), third para.).

Weighting and Conclusion

Recommendation 12 is rated compliant.

Recommendation 13 – Correspondent banking

In its 3rd Round MER, Luxembourg was rated non-compliant due to major shortcomings concerning: the narrow scope of FI coverage and FIs located in the EU/EEA; no requirements regarding FIs located in equivalent non-EU countries; no requirements for FIs to verify whether the respondent institution was subjected to an ML/FT investigation or regulatory action; and no requirement to obtain senior management approval to establish a correspondent banking relationship.

Criterion 13.1 – In the case of cross-border correspondent banking or other similar relationships (including intermediary relationships in collective investment schemes), FIs are required to:

- (a) gather sufficient information about a respondent institution to understand fully the nature of the respondent’s business, and to determine from publicly available information the reputation of the institution and the quality of supervision including whether it has been subject to a ML/TF investigation or regulatory action (2004 AML/CFT Law, Art.3-2(3)(a), 2012 CSSF Reg., Art.3);
- (b) assess the respondent institution’s AML/CFT controls (2004 AML/CFT Law, Art.3-2(3)(b), 2012 CSSF Reg., Art.3);
- (c) obtain approval from senior management before establishing new correspondent relationships (2004 AML/CFT Law, Art.3-2(3)(c), 2012 CSSF Reg., Art.3);
- (d) clearly understand and document the respective AML/CFT responsibilities of each institution (2004 AML/CFT Law, Art.3-2(3)(d), 2012 CSSF Reg., Art.3).

The above measures apply to cross-border respondent institutions within and outside the EEA.

Criterion 13.2 – FIs providing payable-through accounts to respondent institutions must satisfy themselves that the respondent bank:

- (a) has performed CDD obligations on the customers having direct access to the accounts of the correspondent bank (2004 AML/CFT Law, Art.3-2(3)(e));

(b) can provide relevant CDD information to the correspondent bank upon request (2004 AML/CFT Law, Art.3-2(3)(e)).

Criterion 13.3 – FIs are prohibited from entering into or continuing a correspondent banking relationship with a shell bank or with a credit institution or FI that is known to allow its accounts to be used by a shell bank. FIs should also satisfy themselves that respondent FIs do not permit their accounts to be used by shell banks (2004 AML/CFT Law, Art.3-2(3)).

Weighting and Conclusion

Recommendation 13 is rated compliant.

Recommendation 14 – Money or value transfer services

Luxembourg was rated partially compliant in the 3rd Round MER due to gaps of preventive measures in relation to MVTS and no mechanism for detecting MVTS operating without a licence. The FATF has since introduced new requirements concerning the identification of MVTS providers who are not authorised or registered.

Criterion 14.1 – MVTS are carried out by payment services providers, e-money institutions and post office banks who are required to obtain a written authorisation from the CSSF (2009 PSL Law, Art.4, 4-1, 6, 24-2; Law on Postal Financial Services, Art.1). MVTS may also be provided by credit institutions, the European Central Bank and national central banks (when not acting in their capacity as monetary authority or other public authorities), EU countries and their regional or local authorities (when not acting in their capacity as public authorities). FIs already licensed in Luxembourg or other EU Member States can provide MVTS and do not need a separate licence. Payment institutions offering domestic services with total annual transactions below EUR 3 million and e-money institutions offering domestic services with the total business activities generating an average outstanding e-money not exceeding EUR 5 million, and for which none of the persons responsible for the management or operation of the business is convicted of ML, TF or other financial crimes, are only required to be registered with the CSSF rather than obtaining written authorisation (2009 PSL Law, Art.48, 48-1).

Criterion 14.2 – To identify natural or legal persons that carry out MVTS without a licence or registration, the MVTS supervisor (i.e., CSSF) relies on information obtained from other competent authorities responsible for detecting illegal financial activity (e.g., AED), information in registries, as well as via a system for receiving whistleblowing reports. Criminal sanctions apply to natural and legal persons engaging in unlicensed activities with punishment up to five years imprisonment and/or a fine of EUR 5 000 to EUR 125 000 for natural persons and up to EUR 250 000 for legal persons (2009 PSL, Art.47; Penal Code, Art.36). The sanctions are proportionate and dissuasive.

Criterion 14.3 – The CSSF monitors AML/CFT compliance by MVTS providers (2004 AML/CFT Law, Art.2-1(1); 2009 PSL Law, Art.48 and 48-1).

Criterion 14.4 – Agents acting for a payment institution or an e-money institution, including those of payment institutions operating under the licensing exemption under articles 48/48-1 (as outlined in c.14.1), are required to be registered with the CSSF. A payment institution intending to provide services through an agent must provide CSSF with the name and address of the agent (2009 PSL, Art.18(1)(a), 24-7(6)). The agents' details are registered in a public register held by the CSSF, which is

published on the CSSF website and the Official Gazette of Luxembourg (2009 PSL Law, Art.36(1)). The institution is required to update the CSSF without delay of any changes.

Criterion 14.5 – Agents of payment and e-money institutions are required to be included in AML/CFT programmes or monitored for compliance (2004 AML/CFT Law, Art.2(1)).

Weighting and Conclusion

Recommendation 14 is rated compliant.

Recommendation 15 – New technologies

Luxembourg was rated partially compliant with these requirements in the 3rd Round MER due to a narrow scope of FI coverage; no law requiring FIs to adopt policies or have measures to prevent the misuse of new technologies; CDD requirement regarding non-face-to-face relationship restricted the application of risk mitigation measures; no provision covering non-face-to-face transactions. Since then, R.15 has been amended significantly to include new requirements relating to virtual assets (VA) and virtual asset service providers (VASP).

Criterion 15.1 – The 2020 NRA (update) includes a brief segment on ML/TF risks related to new technologies, including new payment methods (such as prepaid cards, electronic wallets, online and mobile payments not directly linked to a bank account, etc.), the use of new or developing technologies for both new and pre-existing products as well as emerging threats emanating from cybercrime and online extortion, especially in the context of the COVID-19 pandemic (2020 NRA, Ch.8). The CSSF also has an overarching policy for all ML/TF risk assessments across the CSSF, which provides guidance to supervisors on risk assessments (CSSF 19/477) and a market entry controls policy that also requires the CSSF to assess and understand ML/TF risks in general (CSSF 19/507). However, the 2020 NRA (update) and CSSF policies are general and do not include a comprehensive assessment of ML/TF risks related to new technologies.

FIs are required to identify and assess ML/TF risks which may arise in relation to the development of new products and business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products (2004 AML/CFT Law, Art.2-2(3) and Circular 12-552 paragraphs 180-185).

Criterion 15.2 – FIs are required to (a) assess ML/TF risks prior to the launch or use of new products, practices, and technologies, and (b) take appropriate measures to manage and mitigate such risks (2004 AML/CFT Law, Art.2-2 (3)(a) and (b)).

Virtual assets and virtual asset service providers

Criterion 15.3 –

(a) The 2020 NRA (update) identifies and assesses ML/TF risks (including emerging risks) posed by VAs and the activities of VASPs, including by VASPs established in other jurisdictions but providing services in Luxembourg. In addition to the NRA, the 2020 ML/TF vertical risk assessment on VAs and VASPs (2020 VRA VA/VASPs) provides a more detailed assessment of ML/TF risks emerging from VA

and VASP activities, further details on different aspects of threat and vulnerabilities, with some illustrated case studies, and presents red flag indicators.

(b) Luxembourg has measures in place to prevent or mitigate ML/TF risks arising from VAs and VASPs, which are based on the 2020 VA/VASP VRA.

(c) Luxembourg requires VASPs to take appropriate steps to identify and assess ML/TF risks as required by c.1.10, as well as manage and mitigate such risks as required by c.1.11 (2004 AML/CFT Law, Art.2-2(1), (2), 3-2, 4(1)).

Criterion 15.4 –

(a) Luxembourg requires VASPs, as both legal and natural persons, that are created or provide services in Luxembourg to be registered with the CSSF (2004 AML/CFT Law, Art.1(20c), 7-1(2)).

(b) Beneficial owners of, and persons performing a management function within VASPs must provide the CSSF with the necessary information to justify their professional standing (i.e., “fit- and proper”). The CSSF assesses good professional standing based on criminal records and of any evidence demonstrating that the persons are of good repute (2004 AML/CFT Law, Art.7-1(3)). Other VASPs which are licensed as payment service providers (e.g., credit, payment, electronic money institutions, etc.) are subject to fit and proper requirements described under c.26.3.

Criterion 15.5 – - To identify natural or legal persons that carry out VASP activities without the requisite registration, the CSSF carries out newspaper and Internet searches as well as searches in the Luxembourg Trade and Company Register (RCS). It also holds meetings with other competent authorities (e.g., quarterly meetings with the CRF-FIU and awareness raising meetings with other authorities) and has established a whistle-blower procedure on VASP activities. The CSSF also remains in contact with the Luxembourg House of Financial Technology to identify VASPs that have not filed for VASP registration at the CSSF. The CSSF has the power to impose appropriate administrative sanctions to VASPs operating without the required registration (2004 AML/CFT Law, Art.8-4(1), (2), 7(2). See also c.15.8).

Criterion 15.6 –

(a) VASPs are subject to risk-based supervision by the CSSF (2004 AML/CFT Law, Art.2-1(1), 8-1(4); see also R.26).

(b) The CSSF has adequate powers to monitor and ensure compliance by VASPs with AML/CFT requirements (2004 AML/CFT Law, Art.8-2; see also R.27).

Criterion 15.7 – The CSSF (supervisor) and the CRF-FIU have established guidelines and provided feedback to assist VASPs in applying national AML/CFT measures and detecting and reporting suspicious transactions. These include the CSSF guidance on virtual assets of 29 November 2021, communiqués, FAQs, a dedicated section on the CSSF website, the CRF-FIU annual report, regular consultation meetings with and presentations for the industry (such as an AML/CFT Conference for payment institutions, e-money institutions and VASPs in March 2022).

Criterion 15.8 –

(a) The CSSF can impose administrative sanctions on VASPs including warning, reprimand, public statement, withdrawal or suspension of the licence/registration, temporary ban for a period not exceeding five years, fine up to EUR 1 million (2004 AML/CFT, Art.8-4(1), (2)). Criminal sanctions can be imposed, including a fine on

legal or natural persons of between EUR 12 500 and EUR 5 million for any person who knowingly contravenes the listed provisions of the 2004 AML/CFT Law (Art.9). These penalties are proportionate and dissuasive.

(b) Sanctions can also be imposed on the members of the executive bodies, managers, directors or employees responsible for the VASP's non-compliance (2004 AML/CFT Law, Art.8-4(1)). Moreover, the CSSF can impose a temporary ban for a period not exceeding five years to exercise a professional activity in the financial sector or to exercise managerial functions within a covered VASP. The criminal sanctions described under sub-criterion 15.8(a) also apply directors and senior management.

Criterion 15.9 – VASPs are generally subject to the requirements set out in R.10 to 21 in the same manner as for FIs and DNFBPs (2004 AML/CFT Law, Art.2(1)(16)).

(a) R.10 – CDD must be conducted, where the occasional transaction or occasional operation exceeds the threshold of EUR 1 000 (2004 AML/CFT Law, Art.3(1)(b)(ii); 2010 AML/CFT GDR, Art.1(7));

(b) R.16 – For VA transfers, not all beneficiary and originator information accompanies VASP transactions, in relation to transfers within the EU, in the time period required (2004 AML/CFT Law Art.3(1)(b)(ii); EU Reg. 2015/847, Art.5(2)(a), 6).

Criterion 15.10 – The deficiencies cited in in criteria 6.5(d) are also applicable to VASPs.

Criterion 15.11 – There are no limitations specific to VAs or VASPs on the power of competent authorities to provide MLA, extradition, or international co-operation.

Weighting and Conclusion

Luxembourg has met most of the requirements concerning new technologies and virtual assets, but minor shortcomings exist in its legal framework. There are gaps in the assessment of risks by Luxembourg, wire transfer requirements, and application of targeted financial sanctions.

Recommendation 15 is rated largely compliant.

Recommendation 16 – Wire transfers

In its 3rd Round MER Luxembourg was rated partially compliant with these requirements due to an absence of data submission requirements for intra-European Community transfers.

Ordering financial institutions

Criterion 16.1 – FIs in Luxembourg must ensure that all cross-border wire transfers of EUR 1 000 or more are always accompanied by accurate originator and beneficiary information. The information shall include the items listed in c.16.1 (a) and (b) (2004 AML/CFT Law, Art.3(1)(b)(ii); EU Reg. 2015/847, Art.4(1)-(3)).⁸³

⁸³ Wire transfers taking place entirely within the borders of the EU are covered under c.16.5 pursuant to footnote 41 in the 2013 FATF Methodology.

Criterion 16.2 – The requirements regarding batch files are consistent with the FATF requirements regarding originator and beneficiary information (EU Reg. 2015/847, Art.6(1)).

Criterion 16.3 – FIs are required to ensure that cross-border transfers below EUR 1 000 are always accompanied by the originator and beneficiary information referred to in c.16.3(a) and (b) (EU Reg. 2015/847, Art.6(2)(a), (b)).

Criterion 16.4 – Originator information provided for transactions of less than EUR 1 000 need not be verified, unless there are reasonable grounds for suspecting ML/TF or the funds were received in cash or anonymous e-money (EU Reg. 2015/847, Art.6(2) second para. (b)).

Criteria 16.5 and 16.6 – For domestic wire transfers (which in this case also includes intra-EU wire transfers), ordering FIs need to provide only the payment account numbers (or unique transaction identifiers) with the transfer. If requested by the beneficiary FI, the ordering FI must be able to provide complete information on the originator and the beneficiary within three working days which is consistent with the second part of c.16.5 and c.16.6 (EU Reg. 2015/847, Art.5). FIs are required to respond fully and without delay to requests from law enforcement authorities on originator and beneficiary information (EU Reg. 2015/847, Art.14).

Criterion 16.7 – The ordering FI is required to maintain all collected information on the originator and the beneficiary for five years in line with R.11 (EU Reg. 2015/847, Art.16).

Criterion 16.8 – The ordering FI is not allowed to execute the wire transfer if it does not comply with the requirements set out in c.16.1-16.7 (EU Reg. 2015/847, Art.4(6)).

Intermediary financial institutions

Criterion 16.9 – Intermediary FIs must retain all the information on the originator and the beneficiary that accompanies a cross-border wire transfer (EU Reg. 2015/847, Art.10).

Criterion 16.10 – (Not applicable) Technical limitations cannot be used to justify non-compliance with c.16.9. Accordingly, this criterion is not applicable to Luxembourg.

Criterion 16.11 and 16.12 – Intermediary FIs are required to take reasonable measures, that are consistent with straight-through processing, to identify cross-border wire transfers that lack originator or beneficiary information and to have risk-based procedures for determining: (a) when to execute, reject, or suspend such wire transfers, and (b) the appropriate follow-up action (EU Reg. 2015/847, Art.11, 12).

Beneficiary financial institutions

Criterion 16.13 – Beneficiary FIs are required to implement effective procedures, including, where appropriate, ex-post monitoring or real-time monitoring, to detect cross-border wire transfers that lack required originator or beneficiary information (EU Reg. 2015/847, Art.7(1), 7(2)).

Criterion 16.14 – The beneficiary FI is required to verify the identity of the beneficiary of cross-border wire transfers of over EUR 1 000 and maintain this information for five years in line with R.11 (EU Reg. 2015/847, Art.7(3), 16).

Criterion 16.15 – Beneficiary FIs are required to have risk-based policies and procedures for determining: (a) when to execute, reject or suspend a wire transfer lacking originator or required beneficiary information; and (b) the appropriate follow-up action (which could include reporting to authorities in cases of routine failure to provide information) (EU Reg. 2015/847, Art.8).

Money or value transfer service operators

Criterion 16.16 – The obligations listed above also apply to MVTS providers and their agents (EU Reg. 2015/847, Art.2(1), 3(5)).

Criterion 16.17 – When an MVTS provider controls both the ordering and the beneficiary side of a wire transfer:

(a) the MVTS provider is required to consider information from both sides as a factor when assessing whether an STR has to be filed. (EU Reg. 2015/847, Art.9, 13).

(b) While there is no explicit requirement for the MVTS provider to file an STR in any country affected by the transaction, considering c.16.17(a) and the permissions for intra-group sharing of STR data (see c.18.2(b)), MVTS providers are obliged to report in the countries of the ordering and beneficiary sides of the transaction. In addition, EU Directive 2015/849 requires compliance officers to file an STR with the FIU of the EU Member State in whose territory the MVTS provider is established, i.e., the MVTS provider's headquarters (EU Directive 2015/849, Art.33; 2004 AML/CFT Law, Art.5(1), (1a)).

Implementation of Targeted Financial Sanctions

Criterion 16.18 – FIs are subject to the requirements of the EU regulations and national law which give effect to UNSCR 1267, 1373 and their successor resolutions (2012 CSSF Reg., Art.33; see R.6).

Weighting and Conclusion

Recommendation 16 is rated compliant.

Recommendation 17 – Reliance on third parties

Luxembourg was rated partially compliant in the 3rd Round MER due to a narrow scope of FI coverage; narrow scope on reliance; no obligation for FIs to immediately obtain all necessary CDD information from the third party.

Criterion 17.1 – FIs are permitted to rely on third-party FIs and DNFBPs to conduct CDD (2004 AML/CFT Law, Art.3-3(1) and (2)). The ultimate responsibility remains with the FI who are required to:

(a) obtain immediately, upon request, the necessary information relating to the elements (a)-(c) of the CDD measures in R.10 (2004 AML/CFT Law, Art.3-3(2), second para.).

(b) ensure the third party immediately provides, upon request and without delay, copies of identification and verification data and other relevant documentation, including any available data related to digital identification, relating to CDD requirements (2004 AML/CFT Law, Art.3-3(2), second para.).

(c) ensure that the third party is regulated and supervised and has measures in place for compliance with the CDD and record-keeping requirements in line with R.10 and R.11 (2004 AML/CFT Law, Art.3-3(2), third para.).

Criterion 17.2 – When determining in which countries the third party can be based, FIs have regard to information available on the level of country risk and consider (a) the geographical risk factors listed in the 2004 AML/CFT law; and (b) the list of higher risk countries identified by the FATF and the EU pursuant to EU Directive 2015/849 (2004 AML/CFT Law, Art.1(30), 3-3(1), Annex IV Art.3; 2010 GDR, Art.1).

Criterion 17.3 – For FIs that rely on a third party of the same financial group, supervisors may consider the conditions relating to the third party to be fulfilled if:

- (a) the group applies CDD and record-keeping measures and ML/TF programmes in accordance with EU and Luxembourg’s legislation on CDD and record keeping measures (2004 AML/CFT Law, Art.3-3(4)(b));
- (b) the implementation of the referred CDD and record keeping requirements and AML/CFT programmes is supervised at group level by a supervisory authority (2004 AML/CFT Law, Art.3-3(4)(c)); and
- (c) any higher country risk is adequately mitigated by the group AML/CFT policies (2004 AML/CFT Law, Art.3-3(4)(d)).

Weighting and Conclusion

Recommendation 17 is rated compliant.

Recommendation 18 – Internal controls and foreign branches and subsidiaries

Luxembourg was rated partially compliant with these requirements in the 3rd Round MER due to a narrow scope of coverage for FIs and group-wide AML/CFT programmes, a lack of enforceable compliance and screening requirements, and a lack of specific obligations to FIs to monitor branches and subsidiaries in high-risk countries.

Criterion 18.1 – FIs are required to implement programmes against ML/TF that have regard to ML/TF risks identified at the international, European, national, sectoral and institutional levels and are proportionate to the size of the business (2004 AML/CFT Law, Art.4(1)). These programmes include the following internal policies, procedures and controls:

- (a) Nominate an officer responsible for managing the FI’s internal policies for AML/CFT compliance with a direct report line to the board or authorised management (2004 AML/CFT Law, Art.4(1)(a); 2012 CSSF Reg., Art.40; 2020 CAA AML/CFT Reg., Art.38 (1)-(4));
- (b) Screen and perform identity checks on employees prior to hiring, particularly on the AML/CFT compliance officers and persons responsible for compliance (2004 AML/CFT Law, Art.4(1), para. 4; 2012 CSSF Reg., Art.45; 2020 CAA Reg., Art.43);
- (c) Education and training of management and employees to prevent ML/TF (2004 AML/CFT Law, Art.4(2); 2012 CSSF Reg., Art.38(2), 42(3); 2020 CAA Reg., Art.36(2), 40(4)); and

(d) An independent audit function to test the system (2004 AML/CFT Law, Art.4(1)(b); 2012 CSSF Reg., Art.49; 2020 CAA Reg. Art.47; 2016 RAIF Law, Art.4; 2013 AIFM Law, Art.1; CSSF Reg. 10-4, Art.12).⁸⁴

Criterion 18.2 – FIs are required to implement group-wide AML/CFT programmes that are applicable to all branches and majority-owned subsidiaries of the financial group (2004 AML/CFT Law, Art.4-1(1)). These include the measures in c18.1 and:

(a) Policies and procedures for sharing information within the group for AML/CFT purposes (including for purposes of CDD and ML/TF risk management) (2004 AML/CFT Law, Art.4-1(1));

(b) Provision of customer, account and transaction information from branches and subsidiaries when necessary for AML/CFT purposes to group level compliance, audit and AML/CFT functions (2004 AML/CFT Law, Art.4-1(1)(b)). Transaction information refers to data and analysis of transactions or activities which appear unusual, if such analysis was done (2004 AML/CFT Law, Art.4-1(1)(b)). Similarly, branches and subsidiaries receive such information from these group-level compliance functions when relevant and appropriate for risk management (2004 AML/CFT Law, Art.4-1(1)(b)); and

(c) Adequate safeguards on the confidentiality and use of the information exchanged, including safeguards to prevent tipping-off (2004 AML/CFT Law, Art.4-1(1)(c), 5(5)). The information must be shared as appropriate between the members of the group, as long as all group members have group policies and information sharing procedures in place equivalent to Luxembourg law or EU Directive 2015/849 (2004 AML/CFT Law, Art.5(5)).

Criterion 18.3 – FIs are required to ensure that their foreign branches and majority-owned subsidiaries have in place AML/CFT measures that are comparable to those required in Luxembourg to the extent permitted by the host country. Where minimum AML/CFT standards in the country of a branch or subsidiary differ from those applicable in Luxembourg, branches and subsidiaries must impose the higher standard (2004 AML/CFT Law, Art.4-1(3)). If the host country does not permit the implementation of AML/CFT measures consistent with the home country requirements, FIs must require their branches and majority-owned subsidiaries to apply additional measures to effectively handle ML/TF risks and inform supervisors and SRBs (2004 AML/CFT Law, Art.4-1 (4)).

Weighting and Conclusion

Recommendation 18 is rated compliant.

Recommendation 19 – Higher risk countries

In its 3rd Round MER Luxembourg was rated not compliant due to a narrow scope of FIs; no obligations for FIs to monitor business relationships and transactions with residents of countries that did not or insufficiently applied the FATF Recommendations; no obligations to examine operations covered by this requirement; and insufficient counter-measures.

⁸⁴ The CAA does not require a statutory audit of AML/CFT controls from broker firms as they do not handle the funds from premia or benefit payments. The Assessment Team considers this to be risk-based.

Criterion 19.1 – FIs are required to apply EDD, on a risk-sensitive basis, to business relationships or transactions involving high-risk countries, when such countries are identified by the FATF (2004 AML/CFT Law, Arts. 1(30), 3-2(1), (2), (3), (4)).

Criterion 19.2 – Supervisory authorities and SRBs can apply countermeasures proportionate to the risks when called for by the FATF and independently thereof (2004 AML/CFT Law Art.1(3), 3-2(2a and 2b), 8-1(1a)).

Criterion 19.3 – Supervisory authorities have mechanisms in place to inform FIs, under their supervision, of the countries that are included in the FATF public statements, either through circulars or supervisory letters.

Weighting and Conclusion

Recommendation 19 is rated compliant.

Recommendation 20 – Reporting of suspicious transactions

Luxembourg was rated partially compliant with these requirements in the 3rd Round MER. Deficiencies included scoping issues in the coverage of FIs and in the TF offence; gaps in protection for required disclosures; and no explicit STR obligation on tax offences.

Criterion 20.1 – FIs are required to inform the CRF-FIU promptly when they suspect or have reasonable grounds to suspect that ML, an associated predicate offence or TF is being committed or has been committed or attempted (2004 AML/CFT Law, Art.5(1)(a)).

Criterion 20.2 – FIs are required to report all suspicious transactions, including attempted suspicious transactions, regardless of the amount of the transaction (2004 AML/CFT Law, Art.5(1)(a)).

Weighting and Conclusion

Recommendation 20 is rated compliant.

Recommendation 21 – Tipping-off and confidentiality

Luxembourg was rated partially compliant with these requirements in the 3rd Round MER due to a limited scope of and numerous exceptions to the tipping off prohibition.

Criterion 21.1 – FIs and their directors and employees (including authorised management and officers) are protected against any kind of liability when reporting their suspicions in good faith to the CRF-FIU. This applies even in cases where the individual was not precisely aware of the associated predicate offence and regardless of whether illegal activity actually occurred (2004 AML/CFT Law, Art.5(4)).

Criterion 21.2 – FIs and their directors and employees (including authorised management and officers) are prohibited from disclosing the fact that an STR or related information is being or will be reported to the CRF-FIU (2004 AML/CFT Law, Art.5(5)). This prohibition does not apply to sharing this information within a financial group or to a disclosure to relevant supervisory authority or SRBs (2004 AML/CFT Law, Art.5(5), second through fifth paragraphs).

Weighting and Conclusion

Recommendation 21 is rated compliant.

Recommendation 22 – DNFBPs: Customer due diligence

Luxembourg was rated non-compliant in the 3rd Round MER due to coverage of AML/CFT regime concerning TCSPs various gaps on CDD and preventive measures for DNFBPs; and no obligation to require casinos to identify or to take reasonable steps to verify the identity of the beneficial owner.

Criterion 22.1 – DNFBPs are required to comply with the CDD requirements set out in R.10 in the following situations:

- (a) Casinos - when customers engage in transactions amounting to EUR 2 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked (2004 AML/CFT Law, Art.1(23), 3(1)(bb));
- (b) Real estate agents - when they are involved in transactions for a client concerning the buying and selling of real estate and when involved in transactions for a client concerning letting real estate for monthly rent of EUR 10 000 or more. Real estate developers are also obliged to comply with CDD requirements when involved as an intermediary in the buying and selling of real estate (2004 AML/CFT law, Art.2(1)(10), (10a), 3(1)(b)(i), 3(2)(d)).
- (c) DPMS - when they engage in any cash transaction with a customer equal to or above EUR 10 000 (2004 AML/CFT Law, Art.2(1)(15), 3(1)(ba)).
- (d) Lawyers, notaries and accountants - when they prepare for, or carry out, transactions for their client concerning all the activities listed in c.22.1(d) (2004 AML/CFT Law, Art.2(1)(9), (9a), (11), (12), 3(1)).
- (e) TCSPs - when they prepare for or carry out transactions for a client concerning all the activities listed in c.22.1(e) (2004 AML/CFT Law, Art.1(8), 2(1)(13a), 3(1)).

Criterion 22.2 – DNFBPs are required to comply with the same record-keeping requirements as FIs as described in R.11 (2004 AML/CFT Law, Art.2(1), 3(6)).

Criterion 22.3 – DNFBPs are required to comply with similar PEP requirements as FIs in R.12 (2004 AML/CFT Law, Art.2(1) and 3-2(4)(c)).

Criterion 22.4 – DNFBPs are required to comply with the same requirements regarding new technology as FIs as described in R.15 (2004 AML/CFT Law, Art.2(1)).

Criterion 22.5 – DNFBPs are required to comply with the same third-party reliance requirements as FIs in R.17 (2004 AML/CFT Law, Art.2(1)).

Weighting and Conclusion

Recommendation 22 is rated compliant.

Recommendation 23 – DNFBPs: Other measures

Luxembourg was rated non-compliant in the 3rd Round MER due to major deficiencies including coverage of TCSP activities and various gaps in obligations on STR, tipping-off and confidentiality, internal controls and application to foreign branches and subsidiaries, and higher risk countries.

Criterion 23.1 – DNFBPs are subject to the same STR requirements as FIs (see analysis of R.20) and subject to the following:

(a) Lawyers, notaries, other independent legal professionals and accountants when, on behalf of, or for, a client, they engage in a financial transaction in relation to the activities described in c.22.1(d) (2004 AML/CFT Law, Art.2(1), 5(1)(a)). If there is a risk of tipping off the client, lawyers are allowed to transmit an STR to their SRB (Ordre des avocats) who is then required to submit the STR to the CRF-FIU (2004 AML/CFT Law, Art.7 (2), (3)).

(b) DPMS, when they engage in an occasional cash transaction with a customer equal to or above EUR 10 000 (2004 AML/CFT Law, Art.2(1), 5(1)(a)).

(c) TCSPs when, on behalf or for a client, they engage in a transaction in relation to the activities described in c.22.1(e) (2004 AML/CFT Law, Art.2(1), 5(1)(a)).

Criterion 23.2 – DNFBPs are required to comply with the same internal control requirements and group-wide measures as FIs (2004 AML/CFT Law, Art.2(1), 4, 4-1).

Criterion 23.3 – DNFBPs are required to comply with the same higher-risk countries requirements as FIs and supervisors proactively advise DNFBPs of concerns about weaknesses in the AML/CFT systems of other countries (2004 AML/CFT Law, Art.2(1), 8-1(1a)).

Criterion 23.4 – DNFBPs are required to comply with the tipping-off and confidentiality requirements as required by R.21 (2004 AML/CFT Law, Art.2(1), 5(4), (5)).

Weighting and Conclusion

Recommendation 23 is rated compliant.

Recommendation 24 – Transparency and beneficial ownership of legal persons

Luxembourg was rated partially compliant with these requirements in its 3rd Round MER based on the following deficiencies: gaps in the mechanism allowing identification of the beneficial owner of legal persons; no mechanism to ensure that information contained in the company registry is accurate and up-to-date; no measure to ensure transparency of the shareholders of public companies and limited partnerships that have issued bearer shares.

Criterion 24.1 – All legal persons (including ABSLs and *Fondations*) must be registered in the Luxembourg Trade and Company Register (RCS). Luxembourg has mechanisms that identify and describe: (a) the different types, forms, and basic features of legal persons in the country; and (b) the processes for the creation of those legal persons, and for obtaining and recording basic and beneficial ownership information. This information is publicly available on the websites of the RCS and Luxembourg Business Register (LBR).

Criterion 24.2 – Luxembourg assessed the ML and TF risks associated with all types of legal persons created in Luxembourg (2020 NRA (update); 2022 ML/TF Vertical Risk Assessment on Legal Persons and Legal Arrangements).

Basic Information

Criterion 24.3 – All legal persons created in Luxembourg must be registered with the RCS (2002 RCS Law, Art.1(2)). The RCS records the company name, date of incorporation, legal form, registered office address, identity of and list of regulating

powers of the legal person's directors (2002 RCS Law, Art.6, 8). When this information is registered with the RCS by means of requisition forms, documents constituting proof of the registered information (1915 Company Law, Arts. 100-7, 100-8, 100-10, 100-13) also need to be attached and filed (2003 RCS Regulation, Art. 4(2), 6(1)). For ASBLs and *Fondations* the name, purpose, duration for which it is established, the precise address of the registered office, the identity and address of persons authorised to manage, administer and sign for the ASBL or *Fondation* (2002 RCS Law, Art.9). The LBR verifies that the information submitted matches the information laid out in the documentation (2002 RCS Law, Art. 21). This information is publicly available on the RCS's website (2003 RCS Regulation, Art.20; 2018 RCS Regulation).

Criterion 24.4 – Legal persons are required to maintain the information set out in c.24.3, and to maintain at their registered office a register of their shareholders or members containing the number of shares held by each shareholder (1915 Companies Law, Art.310-1(5), 320-1(6), 430-3, 430-6, 710-8, 811-7, 812-1, 813-7). However, there is no requirement to include information in the share register on the nature of voting rights associated with the categories of shares.

Criterion 24.5 – Legal persons must file with the register notification of changes to information referred to in c.24.3 and c.24.4 within 30 days, which is considered sufficiently timely (2002 RCS Law, Art.1(3), 15). Managers of the legal person are liable for failing to ensure that changes are filed on time and are accurate (1915 Companies Law, Art.441-9) and are liable to a fine for failing to maintain the register of shareholders (1915 Companies Law, Art.1500-11).

Beneficial Ownership Information

Criterion 24.6 – Luxembourg utilises all three mechanisms referred to in c.24.6 to ensure that legal persons obtain information on the beneficial ownership of a legal person and that such information is available at a specified location in Luxembourg or can otherwise be determined in a timely manner by a competent authority.

(a) All legal persons must provide the Register of Beneficial Owners (RBE) with information on their beneficial owner(s) including name, nationalities, date of birth, place of birth, country of residence, private or professional address, identification number, type and extent of beneficial ownership (2019 RBE Law, Art.3(1)). Legal persons must also update this information within 30 days of when they are aware of any changes, or when they should become aware of any changes (2019 RBE, Art.4(1), (2), (3)). Companies listed on certain regulated stock exchanges are exempt from these requirements, as such information can be obtained directly there.

(b) Legal persons are required to obtain relevant information on the natural persons who are their beneficial owners (2019 RBE Law, Art.17(1)). The legal person is also required to obtain and store at its registered office, the information on beneficial ownership, along with relevant supporting documents (2019 RBE Law, Art.17(2)). The legal person must keep the beneficial ownership information up to date and request updating within 30 days of a change in a beneficial owner's status (2019 RBE Law, Art.4(1)17(3)).

(c) The CRF-FIU can use existing information, including: (i) information obtained by FIs and DNFBPs, in accordance with R.10 and R.22; (ii) information held by other competent authorities on the legal and beneficial ownership of companies (2004 AML/CFT Law, Art.5(1)(b)); (iii) information held by the company as required in

c.24.3 above (2019 RBE Law, Art.18); and (iv) information held by the stock exchange (2004 AML/CFT Law, Art.5(1)(b)).

Criterion 24.7 – Luxembourg requires legal persons to inform the RBE within 30 days of changes in beneficial ownership information (2019 RBE, Art.3, 4). In addition, the RBE can refuse to register or modify information which does not match supporting information or which is incomplete (2019 RBE Law, Art.7). All persons with access to the register (including obliged entities and registered legal persons) must inform the register of any errors encountered in the information within 30 days (2019 RBE Law, Art.8). See also c.10.7 where FIs are required to conduct ongoing due diligence and keep client information up to date.

Criterion 24.8 – Luxembourg takes a multi-pronged approach to ensure that legal persons to co-operate with competent authorities to the fullest extent possible in determining the beneficial owner, including the following:

(a) Beneficial ownership registry: Legal persons must provide beneficial ownership information to the national authorities within three days, when requested (2019 RBE Law, Art.18). Legal persons are liable to a fine of between EUR 1 250 and EUR 1 250 000 for failing to declare their beneficial owner to the RBE or for (knowingly) providing inaccurate or out-of-date beneficial ownership information (2019 RBE Law, Art.20, 21(2)).

(b) Information gathering powers: The CRF-FIU and the Office of Investigative Judges can require FIs and DNFBPs to provide beneficial ownership information on their corporate customers (2004 AML/CFT Law, Art.5(1)(b)).

(c) TCSPs and notaries are accountable to competent authorities for providing all basic and available beneficial ownership information. The Luxembourg authorities explained that many Luxembourg legal persons engage the services of TCSP but there are no legal requirements for legal persons to have a relationship with an FI or DNFBP (including TCSPs). As such, it cannot be guaranteed that information would always be available via these entities; however, information is available from other sources, as noted above.

Criterion 24.9 – Legal persons must designate where beneficial ownership information will be held for five years following its removal from the register (2019 RBE Law, Art.17(4)). This information is published in Luxembourg's National Gazette. The register is also required to maintain documentation on beneficial owners for five years following a legal person's deregistration (2019 RBE Law, Art. 10(1)). Records and information filed with the RCS are kept for 20 years from the date on which the legal person is struck off from the RCS (2003 RCS Regulation, Art.23). FIs and DNFBPs are required to hold relevant beneficial ownership information on a customer for a period of five years after the end of the business relationship with the customer or after the date of an occasional transaction (2004 AML/CFT Law, Art.3(6)).

Other Requirements

Criterion 24.10 – Throughout the review period, basic and beneficial ownership information was publicly available online, via the RCS and RBE, ensuring timely access for competent authorities⁸⁵. Additionally, competent authorities (including

⁸⁵ On 22 November 2022, the Court of Justice of the European Union issued a decision on the compatibility of the public access to the BO information kept in registers by the EU Member States. This decision does not impact the access of the Luxembourg competent

prosecutors, judges, CRF-FIU and law enforcement) can request beneficial ownership information directly from the legal person, who must provide it within three days (2019 RBE Law, Art.18). The CRF-FIU also has broad powers under the 2004 AML/CFT Law to request information from FIs and DNFBPs (Art.5(1)(b)).

Criterion 24.11 – Luxembourg requires that bearer shares be immobilised and deposited with FIs or DNFBPs who must keep a register of the shares (2014 Shares Register Law, Art.430-6). The depositary FI or DNFBP is required to maintain the register of bearer shares in Luxembourg and the register must contain: the precise designation of each shareholder and the number of shares or fractional shares, the deposit date, transfers and the dates thereof or the conversion of shares into registered shares. The ownership of the bearer share must be registered. Although there are no provisions in the 1915 Companies Law for the issue of bearer share warrants, their issue is not expressly prohibited or regulated. No mechanisms apply to bearer share warrants.

Criterion 24.12 – Only TCSPs may carry out the activities of nominee shareholders or directors in Luxembourg in relation to foreign legal persons (2004 AML/CFT Law, Art. 1(8)(b), (e)). Luxembourg does not recognise the concept of nominees in relation to domestic legal persons. There is no express prohibition in law on nominee directors and shareholders but fines apply to persons who participate in the company or in any vote in a general meeting with shares that do not belong to them (1915 Company Law, Art.1500-1). A legal entity may be director in a Luxembourg company; however, it must designate a natural person as a permanent representative and this information must be filed with the RCS (2002 RCS Law, Art.6, point 8).

Criterion 24.13 – Failure to provide beneficial ownership information can lead to the legal person not being registered (2019 RBE Law, Art.7(1)). Penalties for failing to timely submit beneficial ownership information to the register, or for failing to keep accurate and up to date information, range from EUR 1 250 to EUR 1 250 000 (2019 RBE Law, Art.20(1), 21(1)). The same range of penalties applies to legal persons who knowingly submit an inaccurate application for registration to the RBE or otherwise provide inaccurate information (2019 RBE Law, Art.20 and Art.21). Directors are liable for fines of between EUR 5 000 and EUR 125 000 if they fail to maintain either a share register or a bearer share register (1915 Companies Law, Art.1500-11 and Art.1500-12). These penalties are considered proportionate and dissuasive. The directors or members of the management company are liable for ensuring that basic information on the register is updated (1915 Company Law, Arts.441-9 (for SA and SE), 710-15 (for SARL), 500-6 (for SAS), 600-5 (for SCA), 833-19 (for SEC)). Penalties ranging from EUR 251 to EUR 5 000 apply for failing to update basic information at RCS (2002 RCS Law, Art.21(4)). For certain other types of companies (SNC, SCS, SCSpé and SC), board members would only be liable based on general civil liability rules under the civil code, which are not dissuasive.

Criterion 24.14 – Luxembourg has mechanisms to rapidly provide international co-operation in relation to basic and beneficial ownership information, on the basis set out in Recommendations 37 and 40. This includes:

authorities to the information held in the RBE. After a temporary suspension of the online access to the RBE for persons other than competent authorities, the LBR issued Circular LBR 22/01 (December 2022) reopening access to the RBE for professionals based on the signature of an agreement by the professional.

(a) Luxembourg facilitates access by foreign competent authorities to basic information held by company registries. Basic information is publicly available and accessible on the websites of the Luxembourg business registers. The CRF-FIU can provide guidance to the foreign counterpart on how to access information if requested by a foreign counterpart. It also has full access to the RCS and RBE enabling it to provide basic ownership information.

(b) Information on shareholders may be exchanged by the CRF-FIU with a foreign FIU, spontaneously or upon request. This power covers personal data and all other information and supporting documents which the CRF-FIU has access to as well as those which it is empowered to obtain spontaneously and upon request (2004 AML/CFT Law, Art.5 (1) (b); 2018 FIU Law, Art. 74-2(4)).

(c) Throughout the review period, beneficial ownership information from the RBE was publicly available on the LBR website. In addition, the CRF-FIU has direct access to all the beneficial ownership information contained in the RBE and may use its full range of investigative powers to respond to a foreign counterparty's request (2019 RBE Law, Art.11; 2004 AML/CFT Law, Art.5(1)(b)).

Criterion 24.15 – Luxembourg monitors the quality of assistance it receives from other countries in response to requests for basic or beneficial ownership information or requests for assistance locating beneficial owners residing abroad. The analyst in charge of the case will compare the information received with the information requested. If the answer is not clear or if a requested information is missing, an additional request may be launched to clarify or complement the first answer provided (2018 FIU Law, Art.74-5(1)). Luxembourg relies on the goAML site to maintain records on co-operation with foreign counterparts and uses these records as a basis for follow up with foreign counterparts.

Weighting and Conclusion

Minor deficiencies exist in relation to the inclusion of information on the nature of voting rights associated with the categories of shares, mechanisms covering bearer share warrants, ML/TF risks of nominees have not been sufficiently mitigated, and sanctions for board members of certain types of companies are not dissuasive.

Recommendation 24 is rated largely compliant.

Recommendation 25 – Transparency and beneficial ownership of legal arrangements

Luxembourg was rated non-compliant with these requirements in its 3rd Round MER based on the following deficiencies: no supervision obligation on all relevant TCSPs; and beneficial ownership information was accessible only during criminal proceedings.

Criterion 25.1 – Luxembourg recognises two types of legal arrangements: (a) domestic *fiducies*, which are domestic legal arrangements⁸⁶, and (b) foreign law trusts

⁸⁶ A “*fiducie*” is a legal arrangement formed by a contract between the fiduciant (settlor) and the fiduciary (fiduciaire) by which the fiduciary becomes the owner of certain fiduciary assets (patrimoine fiduciaire) under agreed conditions. These conditions include instructions for the fiduciary over managing the entrusted assets (fiduciary mission) and the obligations to clearly separate entrusted asset of each agreement

(2003 *Fiducies* and Trusts Law). “Express trust” is defined in line with the FATF definition (2020 RFT Law, Art.1(12)). No trusts are governed under Luxembourg law, but trusts created under foreign law can be administered in Luxembourg by either professional or non-professional trustees. The following administrative conditions apply to both:

(a) Trustees and fiduciaries shall obtain and keep adequate, accurate, and current information on the beneficial owners of any express trust administered in Luxembourg and of any *fiducie* for which they act as trustee or fiduciaire (2020 RFT Law, Art.2(1)). This information includes the identity of the settlor(s), the trustees (or fiduciaries(s), the protector(s) if any, the beneficiaries or class of beneficiaries and any other natural person exercising effective control over the trust or *fiducie*.

(b) Trustees of express trusts administered in Luxembourg and fiduciaries must obtain and keep basic information on other FIs, DNFBPs and VASPs (including foreign FIs, DNFBPs and VASPs) which provide services to the trust or *fiducie* or which enter into a business relationship with the trust or *fiducie* (2020 RFT Law, Art.3(1)). Although not specifically referenced, this includes investment advisers/managers, accountants and tax advisers.

(c) Trustees and fiduciaires are required to retain the information referred to in (a) and (b) for five years after ceasing to be involved in the trust or *fiducie* (2020 RFT Law, Art.4). Luxembourg law applies to professional and non-professional trustees and fiduciaries.

Criterion 25.2 – Luxembourg requires that information held pursuant to this Recommendation must be adequate, accurate and up-to-date. It shall be updated within one month after any change (2020 RFT Law, Art.2(2), 3(1)).

Criterion 25.3 – Trustees and fiduciaries are required to disclose their status to FIs, DNFBPs and VASPs if they enter into a business relationship or carry out an occasional transaction (2020 RFT Law, Art.6(1)).

Criterion 25.4 – Trustees and fiduciaries are not prevented by law or enforceable means from providing Luxembourg competent authorities and relevant SRBs relevant information on a trust in response to domestic requests (2020 RFT Law, Art.5(1), (2)), as well as requests made by foreign counterparts (2020 RFT Law, Art. 32 - for supervisory authorities; 1980 Judiciary Organisation Law, Art.74 5(1), (3) -for the CRF-FIU). Trustees and fiduciaries can also provide FIs and DNFBPs with beneficial ownership information, the unique registration number or certificate of registration, and information on the assets held or managed in the context of the business relationship (2020 RFT Law, Art.6(1), (2)).

Criterion 25.5 – Competent authorities have direct access to the register of *Fiducies* and Trusts (RFT), which contains information about beneficial owners (2020 RFT Law, Art.25, 14). Competent authorities and SRBs are also empowered to request, and trustees and fiduciaries are required to provide, in a timely manner, any information they hold on any *fiducie* or trust for which they serve as trustees or fiduciaries (2020 RFT Law, Art.5(1), (2), 8(5)). FIs and DNFBPs must also provide certain national authorities (including PG, State Prosecutors, members of the State Prosecution

(fiduciary estate) from other property belonging to the fiduciary agent or other fiduciary estates entrusted to him (2020 RFT Law).

Offices, investigative judges, the CRF-FIU) and supervisors with any information they hold on any *fiducie* or any trust which includes (a) to (c) (2020 RFT Law, Art.8(6)).

Criterion 25.6 – Luxembourg is able to provide rapid international co-operation relating to information on trusts and other legal:

(a) Competent authorities can facilitate access by foreign competent authorities to basic and beneficial ownership information held by registries. The AED maintains the RFT through which the national authorities and supervisors have access to basic and beneficial ownership information (2020 RFT Law, Art.25 and 26). In addition, supervisors can request information from trustees and fiduciaries directly (2020 RFT Law, Art.5 (1), 8(5)).

(b) Supervisory authorities, the CRF-FIU and SRBs are required to co-operate closely and to share all information obtained pursuant to their activities (2020 RFT Law, Art.32(1),(2); 2004 AML/CFT Law, Art. 9-2(a)).

(c) As noted in (a) and (b), supervisors and the CRF-FIU can use their full powers to obtain and respond to requests. Furthermore, state prosecutors, investigative judges and judicial police (SPJ) officers acting on their request can use the full range of their domestic investigative powers to provide MLA to obtain from trustees any information relating to the trust (See c.25.5, as well as R.37).

Criterion 25.7 – Supervisors can impose administrative and monetary sanctions on trustees and fiduciaries for failure to comply with their obligations under the RFT Law (2020 RFT Law, Art.9(1)). Trustees supervised by SRBs are obliged entities under the AML/CFT Law. SRBs have powers to impose a wide range of penalties that are proportionate and dissuasive (2020 RFT Law, Art.11; 2004 AML/CFT Law, Art.8-10). The AED can also impose administrative sanctions upon trustees and fiduciaires who fail to comply with obligations to the RFT and provide relevant basic and beneficial ownership information (2020 RFT Law, Art.22). These penalties include (for both AED and supervisors): a warning, reprimand, public statement, fine up to twice the amount of benefit capped at EUR 1 250 000, and fines of EUR 250 to EUR 250 000 who obstruct provision of information to the authorities (2020 RFT Law, Art.9(3)-(4),22(2)). Similar provisions exist for trustees and fiduciaries subject to an SRB. These sanctions are considered proportionate and dissuasive.

Criterion 25.8 – Supervisors can impose administrative penalties and fines of EUR 250 to EUR 250 000 on natural and legal persons for failure to provide timely information to the authorities concerning the trust (2020 RFT Law, Art.9(3)). In the context of Luxembourg, where the registries established under the 2020 RFT Law are the primary means of accessing beneficial ownership information on legal arrangements, the AED has additional powers to sanction trustees and fiduciaire or members of their management body for failure to enter accurate and timely information in the relevant register concerning a trust or *fiducie* under their management (2020 RFT Law, Art.22(2)). Furthermore, any entity failing to comply with information requests from the CRF-FIU is liable for criminal sanctions ranging from EUR 12 500 to EUR 5 000 000 (2004 AML/CFT Law, Art. 9). These sanctions are considered proportionate and dissuasive.

Weighting and Conclusion

Recommendation 25 is rated compliant.

Recommendation 26 – Regulation and supervision of financial institutions

In its 3rd Round MER Luxembourg was rated partially compliant due to a narrow coverage of FIs, no market entry obligations to prevent criminals' associates from holding or being the beneficial owner of a significant or controlling interest in an FI, and no obligation on risk-based approach to supervision and monitoring.

Criterion 26.1 – Luxembourg has designated two supervisors with the responsibility for supervising FIs' compliance with AML/CFT requirements. The CSSF is responsible for the AML/CFT supervision of credit institutions, investment firms, investment managers, payment and e-money institutions, pension funds, specialised professional financial services, and foreign institutions for occupational retirement schemes (2004 AML/CFT Law, Art.2-1). The CAA is responsible for the AML/CFT supervision of life insurance undertakings, pension funds, intermediaries, insurance and reinsurance undertakings, and intermediaries performing credit and surety operations (2004 AML/CFT Law, Art.2-1(2)).

Criterion 26.2 – All Core Principles FIs must be licensed by one of the following competent authorities: the European Central Bank (ECB), CSSF or CAA (Reg. 1024/2013, Art.4(1)(a) for ECB; 1998 CSSF Law, Art.3 for MoF). While an exemption allows certain MVTs with lower transaction thresholds to forego licensing requirements, such MVTs are required to register with the CSSF (PSL Law, Art.48).

Authorisation for credit institutions is conditional on the production of evidence of the existence in Luxembourg of the central administration and registered office of the applicant institution (1993 LFS Law, Art.5). The CSSF has clarified in a guidance that "central administration" encompasses decision making, internal governance and management applied on an ongoing basis through offsite and onsite supervision. Luxembourg does not approve the establishment, or continued operation of, shell banks.

Criterion 26.3 – Luxembourg takes regulatory measures to prevent criminals or their associates with ties to organised crime from becoming beneficial owner or holding a significant or controlling interest or holding a management function in an FI supervised by the CSSF and CAA (1998 CSSF Law, Art.2(4); 2015 Insurance Law, Art.2(1)(f)). Luxembourg requires "fit and proper" tests on management bodies (1993 LFS Law, Art.6(9), 7(1), 19; 2009 PSL Law, Art.13, 24-9; 2010 OPC Law, Ch. 15 Art.102(1), 125-1(2), Ch. 19, Art.129(5); 2013 AIFM Law, Art.7(1); 2004 SICAR Law, Art.7(1); 2007 SIF Law, Art.42(3); 2005 Pension Funds Law, Art.53(5); 2004 Securitisation Law, Art.20(2); 2018 Law on Markets in Financial Instruments, Art.4(1), (2); 2015 Insurance Law, Art.32(1) point 15, 274, 283-1, 283-2). These checks are conducted at market entry and when there are changes.

Criterion 26.4 –

(a) Core Principles FIs are subject to regulation by the CSSF and CAA in accordance with legal and regulatory requirements set by EU directives which align to the relevant Core Principles.

(b) Payment services institutions and agents of payment institutions established in Luxembourg are subject to risk-based supervision for AML/CFT compliance (1998 CSSF Law, Art.2(4); 2004 AML/CFT Law, Art.8-1(4)).

Criterion 26.5 – Supervisors are required to apply a risk-based approach to supervision (2004 AML/CFT Law, Art.8-1(4)). Supervisors are required to base the frequency and intensity of on-site and off-site supervision on:

- (a) the ML/TF risks and the policies, internal controls and procedures associated with the institution or group, as identified by the supervisor’s assessment of the institution’s or group’s risk profile (2004 AML/CFT Law, Art.8-1(4)(c)(i)). This is considered annually;
- (b) the ML/TF risks in Luxembourg (2004 AML/CFT Law, Art.8-1(4)(c)(iii)). The supervisors use the results from the NRAs and EU SNRAs in prioritising the sectors or sub-sectors for supervision;
- (c) the characteristics of the FIs and their financial group, in particular the diversity and number of FIs and the degree of discretion allowed to them under the risk-based approach (2004 AML/CFT Law, Art.8-1(4)(c)(ii)).

Criterion 26.6 – Supervisors are required to review the ML and TF risk profile of a FI or group, including the risk of non-compliance, periodically and when there are major events or development in the management and operation of the FI or group (2004 AML/CFT Law, Art.8-1(5)).

Weighting and Conclusion

Recommendation 26 is rated compliant.

Recommendation 27 – Powers of supervisors

Luxembourg was rated largely compliant in the 3rd Round MER based on the following deficiencies: lack of explicit powers of AML/CFT supervisors; narrow range of sanctions available to supervisors; the amounts of disciplinary and administrative fines were low and dissuasive.

Criterion 27.1 – Supervisors (CSSF, CAA)– are empowered to supervise, monitor, and ensure compliance by FIs with AML/CFT requirements (2004 AML/CFT Law, Art.8-2(1)).

Criterion 27.2 – Supervisors have the authority to conduct inspections of FIs (2004 AML/CFT Law, Art.8-2(1)(c)) and can do so without providing advanced notice.

Criterion 27.3 – Supervisors have the right to access any documents or information relevant to their supervision and can compel production without needing to obtain a court order (2004 AML/CFT Law, Art.8-2(1)(a), (b), (d), 8-2(4)). Administrative fines can be applied to natural and legal persons ranging from EUR 250 to EUR 250 000 for obstructing access (2004 AML/CFT Law, Art. 8-4).

Criterion 27.4 – Supervisors have a range of administrative sanctions available, under the 2004 AML/CFT law and other sectoral laws, including: warning, reprimand, public statement, withdrawal or suspension of registration or authorisation, a temporary ban of up to five years and maximum administrative fines of twice the amount of benefit derived from the breach or EUR 1 000 000 maximum. For legal person FIs, the maximum fine is EUR 5 000 000 or 10% of turnover and for a natural person EUR 5 000 000 (2004 AML/CFT Law, Art.8-4, 8-5, 8-6). LEAs can also apply criminal sanctions to FIs in case of non-compliance with AML/CFT requirements (2004 AML/CFT Law, Art.9).

Weighting and Conclusion

Recommendation 27 is rated compliant.

Recommendation 28 – Regulation and supervision of DNFBPs

Luxembourg was rated non-compliant in the 3rd Round MER based on the following deficiencies: no explicit obligation regarding the scope of securitisation firms when performing TCSP activities; no supervision obligation for all relevant activities performed by real estate agents, dealers in high-value goods and TCSP providers; limited enforcement powers and no penalty provisions for lawyers, notaries, accountants and auditors.

Casinos

Criterion 28.1 – Casinos are subject to AML/CFT regulation and supervision in Luxembourg:

- (a) Luxembourg requires casinos to be licensed (1977 Gambling Law, Art.7, 14).
- (b) The Luxembourg Government Council, in collaboration with the MoF and MoJ, as the competent authorities, take legal measures to prevent criminals or their associates from engaging in gambling activities in Luxembourg, including holding a management function or being an operator of a casino (1977 Gambling Law, Art.7, 8, 11). This approval includes conducting criminal records checks on the directors, shareholders and beneficial owners of the casino at market entry and ongoing.
- (c) Casinos are supervised for compliance with AML/CFT requirements by the AED (2004 AML/CFT Law, Art.2-1(8)).

DNFBPs other than casinos

Criteria 28.2 & 28.3 – All DNFBPs in Luxembourg are subject to AML/CFT compliance monitoring:

- Real estate agents and developers and DPMS by the AED (2004 AML/CFT Law, Art.2(1) Points 10, 10a, 15).
- Lawyers and other independent legal professionals by the *Ordre des avocats* (OAs: OAL and OAD) (2004 AML/CFT Law, Art.2(1) Point 12, Art.2-1(6)).
- Notaries by the *Chambre des Notaires* (CdN) (2004 AML/CFT Law, Art.2(1) Point 11, 2-1(5)).
- Accountants by the AED (accounting professionals) and OEC (chartered professional accountants) (2004 AML/CFT Law, Art.2(1) Points 8, 9 & 9(a)), 2-1(3), 2-1(4), 2-1(8)).
- TCSPs by the AED, CAA, CSSF, OEC, IRE and OAs (2004 AML/CFT Law, Art.2(1) Point 13a), 2-1(1-4, 6, 8)).

Criterion 28.4 –

- (a) Competent authorities and SRBs have adequate powers to perform their functions, including powers to monitor compliance (2004 AML/CFT Law, Art.8-2(1) and Art.8-2a).
- (b) The following market entry measures are available to competent authorities or SRBs:

- *For real estate agents, DPMS, accounting professionals and chartered professional accountants:* the authorisation delivered by the Ministry of Economy (MoE) is subject to the circumstance that the conditions of establishment, good repute and qualification provided for are met (2011 Business Licenses Law, Art.2 to 27). The 1999 CPA Law also provides additional registration requirements for chartered accountants (Art.10).
- *For lawyers:* To be admitted to the Luxembourg or Diekirch Bar as a lawyer, the candidate must provide the necessary guarantee of being a fit and proper person (1991 Lawyers Law, Art.6a, 34, 34-3). Members of the management bodies of law firms need to be registered at the Luxembourg Bar or an EU bar. Non-EU bars may be recognized as equivalent (for the purpose of admitting foreign registered lawyers as partners) under the condition that lawyers at such non-EU bars have conditions for registration, exercise of their profession and of partnership equivalent to those applicable in Luxembourg (1991 Lawyers Law, Art.34(2)). To date, only solicitors registered at the Law Society of England and Wales and subject to the Solicitors Regulation Authority have been recognized as equivalent.
- *For notaries:* notaries are subject to procedures similar to those of lawyers, with the General Prosecutor issuing a statement of good character. The Disciplinary Council of the CdH exercises disciplinary authority over all notaries for facts contrary to delicacy and professional dignity as well as honour and probity (1976 Notaries Law, Art.86(3)). In addition, it may impose sanctions including fines, suspension and dismissal (1976 Notaries Law, Art.87(6)).
- For TCSPs:
 - *supervised by the AED* (i) for business centres, the authorisation delivered by the Ministry of Economy (MoE) is subject to the circumstance that the conditions of establishment, good repute and qualification provided for are met (2011 Business Licenses Law, Art.4 to 27); (ii) for professionals providing directorship services, registration by the AED is required, which verifies their professional repute (2004 AML/CFT Law, Art.7-2).
 - *supervised by the CSSF:* the legal framework as described in c.26.3 is applicable here.
 - *supervised by the CAA:* natural persons applying for a licence must demonstrate good reputation as part of their application (2015 Insurance Law, Art.261). Legal persons must identify all direct or indirect shareholders of at least 10% of share capital or voting rights. The CAA also has measures to verify that natural or legal persons known to have, direct or indirect, ties with organised crime, do not take control of such TCSPs (2015 Insurance Law, Art.2(1)(f)).
 - *supervised by the IRE (approved statutory auditors and audit firms):* natural persons are required to provide proof of good repute and professional qualifications and register as a member of the IRE (2016 Audit Profession Law, Art.3(2)(b)). Legal persons have similar obligations (2016 Audit Profession Law, Art.5(3)(d)). The CSSF has the

powers to withdraw the approval of statutory auditor or audit firm (2016 Audit Profession Law, Art.7).

(c) DNFBP supervisors and SRBs have the same range of administrative sanctions as financial supervisors (2004 AML/CFT Law, Art.8-4 to 8-6, 8-10 to 8-12). Criminal sanctions are also applicable in case of non-compliance of AML/CFT requirements by DNFBPs (2004 AML/CFT Law, Art.9).

Criterion 28.5 – Supervision of DNFBPs is required to be undertaken on a risk-sensitive basis, including:

(a) determining the frequency and intensity of on-site and off-site supervision on the basis of their understanding of ML/TF risks (2004 AML/CFT Law, Art.8-1(4)).

(b) when assessing the adequacy of internal AML/CFT policies, controls and procedures, taking into account the ML/TF risk profile of DNFBPs, and the degree of discretion allowed to them under the risk-based approach (2004 AML/CFT Law, Art.8-1(4), 8-1(6)).

Weighting and Conclusion

Recommendation 28 is rated compliant.

Recommendation 29 – Financial intelligence units

Luxembourg was rated LC in the 3rd Round MER and had only minor shortcomings in terms of effectiveness, which is not assessed as part of technical compliance under the 2013 Methodology. The FATF Standards have been significantly strengthened in this area since the last evaluation.

Criterion 29.1 – The CRF-FIU is the national authority tasked with receiving and analysing STRs and other information that could involve ML, associated predicate offences and of TF; and for the dissemination of the results of that analysis (1980 Judiciary Organisation Law, Art.74-2).

Criterion 29.2 – The CRF-FIU is the national authority for the receipt of disclosures filed by reporting entities, including STRs (1980 Judiciary Organisation Law, Art.74-2(1) and (4)). Luxembourg does not require the reporting of cash transactions, or wire transfers, save for cross-border cash declarations that is collected directly by the Customs and Excise Administration (ADA) (see R.32). The ADA is required to forward such information to the CRF-FIU as soon as possible (EU Reg. 2018/1672, Art.9; 2021 Cash Control Law, Art.9; CRF-FIU Service Note on Cash Control version 4, 11 March 2020 and CRF-FIU Vademecum version 4.1 of 16 November 2021).

Criterion 29.3 – The CRF-FIU:

(a) is able to obtain and use any additional information from reporting entities, as needed to perform its analysis properly, including documents on which reports are based (2004 AML/CFT Law, Art.5(1)(b)); and

(b) has access to financial and administrative information that it requires to properly undertake its functions, and indirect access to law enforcement and MLA information contained in the case management system of state prosecutors (JU-CHA) (1980 Judiciary Organisation Law, Art.74-6 and CPP, Art.48-24).

Criterion 29.4 –

(a) The CRF-FIU conducts operational analysis, which uses available and obtainable information to identify specific targets, to follow the trail of particular activities or transactions, and to determine links between those targets and possible proceeds of crime, ML, predicate offences and TF (1980 Judiciary Organisation Law, Art.74-2(5)(1)).

(b) The CRF-FIU uses available and obtainable information, including data provided by other competent authorities, to conduct strategic analysis of ML/TF trends and patterns, and publish such information in CRF-FIU annual reports (1980 Judiciary Organisation Law, Art.74-2(5)(2), CRF-FIU Vademecum version 4.1 16 November 2021, 3.3).

Criterion 29.5 – The CRF-FIU disseminates, spontaneously and on request, information and the results of its analysis to relevant competent authorities and law enforcement agencies (1980 Judiciary Organisation Law, Art.74-2(2) and 74-4(1)). All CRF-FIU users are required to use dedicated, secure and protected channels for communication. (CRF-FIU Vademecum version 4.1 of 16 November 2021, 4-5)

Criterion 29.6 – The CRF-FIU protects its information in the following ways:

(a) Has rules in place governing the security and confidentiality of information, including procedures for handling, storage, dissemination, and protection of, and access to, information (2018 Criminal Data Protection Law, Art.28; CRF-FIU internal rules governing the security and confidentiality of information). The CRF-FIU may decline a request for information when the requesting FIU is not able to protect the information (1980 Judiciary Organisation Law, Art.74-5(5), CRF-FIU Vademecum version 4.1 of 16 November 2021, 4-8).

(b) Ensures that its staff members have the necessary security clearance levels and understanding of their responsibilities in handling and disseminating sensitive and confidential information (1979 Civil Servants Law, Art.11; 2004 Security Clearance Law, Art.14-17; CRF-FIU guidelines on work ethics, including professional secrecy, conflicts of interest, interviews and publication of research). Disclosing confidential information is punishable under the Penal Code (Art.458).

(c) The CRF-FIU facilities are part of the “cité judiciaire”, which is controlled 24/7 by security staff. Access to the CRF-FIU premises is limited to CRF-FIU staff and persons named on a list maintained by the CRF-FIU, who identify themselves with a personal digital badge. CRF-FIU IT systems are monitored 24/7 by qualified IT specialists dedicated to the CRF-FIU and government data security specialists (GOVECERT)(CRF-FIU Vademecum version 4.1 of 16 November 2021, 2.3-2.4).

Criterion 29.7 –

(a) The CRF-FIU has express authority and capacity to carry out its functions freely, including the autonomous decision to analyse, request and share specific AML/CFT information with the relevant authorities (1980 Judiciary Organisation Law, Art.74-1 (4)).

(b) The CRF-FIU can independently exchange information with other domestic authorities as well as with foreign FIUs (2004 AML/CFT Law, Art.9-1; 1980 Judiciary Organisation Law, Art.74-5(11); MOUs with the CSSF, CAA, ACD, AED and ADA;

(c) While the CRF-FIU is under the administrative supervision of the PG, it has distinct and separate core functions as set out in law (1980 Judiciary Organisation Law, Art.74-1; Art.74-2 to 74-7).

(d) The Director of the CRF-FIU makes independent budget requests to the PG's Office, who integrates them into the budget of the judicial administration.

Criterion 29.8 – The CRF-FIU became a full member of the Egmont Group in December 1995.

Weighting and Conclusion

Recommendation 29 is rated compliant.

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

Luxembourg was rated PC in the 3rd Round MER, mainly due to deficiencies concerning effectiveness, which are not assessed as part of technical compliance under the 2013 Methodology.

Criterion 30.1 – Luxembourg has designated LEAs with responsibility for investigating ML, TF, and predicate offences and there is a sub working group on investigation set up under the NPC, which is the authority co-ordinating national AML/CFT policies in the country. The State Prosecutors, investigative judges, and SPJ have responsibility for undertaking criminal investigations into ML, TF, and predicate offences; and the SPJ has the responsibility for investigating TF and major or complicated ML cases (CPP, Art.9, 23-24, 26, 49-52).

Criterion 30.2 – Law enforcement investigators of predicate offences are authorised to pursue the investigation of any related ML/TF offences during a parallel financial investigation and are able to refer the case to another agency to follow up regardless of whether the predicate offence occurred, through the State prosecutor (CPP, Art.23(2)).

Criterion 30.3 – State prosecutors, investigative judges and SPJ officers acting on their request are designated to identify, trace, and initiate freezing and seizing of property that is, or may become, subject to confiscation, or is suspected of being proceeds of crime. In practice, competent authorities usually act expeditiously to do so. However, there is no explicit requirement for the authorities to act expeditiously (except in the context of international co-operation) and some more coercive means of asset identification are only applicable if the criminal prosecution carries a maximum criminal sentence or correctional sentence of at least two years of imprisonment (CPP, Art.24-1, 31, 33, 34, 40, 47, 63, 66-67).

Criterion 30.4 – Recommendation 30 applies to the ADA, the only non-LEA competent authority that has the responsibility for pursuing financial investigations of drug-related offences (1973 Drug Trafficking Law, Art.2).

Criterion 30.5 – (Not applicable) There are no specific anti-corruption enforcement authorities in Luxembourg.

Weighting and Conclusion

Luxembourg has met most of the requirements of this Recommendation. However, there is a minor gap in powers to identify assets and to act expeditiously in domestic cases.

Recommendation 30 is rated largely compliant.

Recommendation 31 - Powers of law enforcement and investigative authorities

Luxembourg was rated LC in the 3rd Round MER due to minor shortcomings in prosecutors' powers and other effectiveness issues which are not assessed as part of technical compliance under the 2013 Methodology.

Criterion 31.1 – Competent authorities investigating ML, TF, and predicate offences are able to obtain access to necessary documents and information. Competent authorities are empowered under Luxembourg laws to:

- (a) request the production of records held by FIs, DNFBPs and other natural or legal persons. Failure to comply with information request may constitute criminal and administrative fines, and administrative sanctions (2004 AML/CFT Law, Art.5(1), 8-2, 8-2(a) and 9);
- (b) search persons and premises with a warrant or without a warrant either upon arrest or in certain urgent circumstances (CPP, Art.24-1, 33, 39(7), 48-10, 52-1, 65);
- (c) take witness statements by summons (CPP, Art.24-1, 38, 48, 69);
- (d) seize and obtain evidence with a warrant or without a warrant upon arrest (CPP, Art.24-1, 31(3), 33, 34, and 36).

Criterion 31.2 – Different competent investigative authorities can use a wide range of investigative techniques for the investigation of ML, associated predicate offences, and TF, including:

- (a) undercover operations by SPJ in cases where offences involve at least two years' imprisonment (though the minimum threshold for predicate offences is six months' imprisonment), where traditional investigative techniques are found unsuccessful, and with the authorisation by the state prosecutor or investigative judge (CPP, Art.48-17(1-3), 48-18);
- (b) intercepting communications including (i) electronic interception of wire, oral communications, and electronic media, as well as (ii) the use of tracking devices are used by the Luxembourg LEAs, under certain conditions (CPP, Art.67-1, 88-1);
- (c) accessing computer systems by SPJ and investigative judges, and monitoring of data in such systems in serious offences (CPP, Art.24-1, 31(3), 66, 88-1, 88-2);
- (d) controlled delivery, subject to the same qualifications as for undercover operations (CPP, Art.48-19; 2018 EIO Law, Art.38(1)).

Criterion 31.3 –

- (a) Luxembourg has an electronic data retrieval system, managed by the CSSF, that allows users to identify, in a timely manner, whether any natural or legal person holds or controls accounts (2020 RBASD Law, Art.7). The CRF-FIU has direct access

to this system. Other national authorities, including LEAs and investigative authorities, can designate a limited number of persons to request and receive this data from the CSSF without delay (2020 RBASD Law, Art. 8). Investigative judges can order banks to disclose whether a person being investigated holds, controls or has power of attorney over accounts of any kind, or has held, controlled or had power of attorney in the past (CPP, Art. 66-2).

(b) Competent investigative authorities are empowered to identify assets without prior notification to the owner. Judicial authorities (including PG, State Prosecutors and other prosecution authorities, and investigative judges), CRF-FIU and criminal investigation police have direct access to a number of systems (e.g. legal persons and tax registers) to identify assets without notification to the owners (2020 RBASD Law, Art.8(2) for safe deposit boxes, CPP, Art. 48-24, 51-1 (for road vehicles), 66-2, 66-3, 66-4 and 66-5 for banking information).

Criterion 31.4 – State prosecutors, investigative judges, and SPJ officers, AML/CFT supervisors, tax authorities and SRBs are able to ask for relevant information held by the CRF-FIU under Luxembourg laws and MoU signed between CRF-FIU and respective competent authorities (1980 Judiciary Organisation Law, Art.74-4(1)).

Weighting and Conclusion

Recommendation 31 is rated compliant.

Recommendation 32 – Cash Couriers

Luxembourg was rated NC in the 3rd Round MER owing to major shortcomings. These include: (1) the system is limited to movements beyond the EU and does not cover shipments by freight, mail, or legal persons; (2) absence of powers to stop or restrain by the ADA; (3) inadequate domestic co-ordination and international co-operation; (4) lack of dissuasive, effective, and proportionate sanctions.

Criterion 32.1 – Luxembourg has a declaration system for incoming and outgoing cash and bearer negotiable instruments (BNI) that applies to all accompanied cross-border movement, including between the Grand Duchy and other EU Member States or non-EU countries (EU Reg. 2018/1672, Art.4; 2021 Cash Control Law, Art.1, 3). A disclosure declaration system applies to unaccompanied cash and BNI of EUR 10 000 or more that enters or leaves Luxembourg (or the EU via Luxembourg) by mail, cargo, courier express (EU Reg. 2018/1672, Art.4; 2021 Cash Control Law, Art.1, 4).

Criterion 32.2 – All persons entering or leaving Luxembourg or the EU via Luxembourg making a physical cross-border transportation of currency or BNIs, which are of a value of EUR 10 000 are required to submit a truthful declaration to the ADA (the designated authority for R.32). (EU Reg. 2018/1672, Art. 2 - 4; 2021 Cash Control Law, Art.3).

Criterion 32.3 – The sender or receiver (or their representative) of unaccompanied cash or BNI is required to make a truthful disclosure declaration in writing within 30 days of the cash or BNI entering or leaving Luxembourg (or the EU through Luxembourg) (2021 Cash Control Law, Art.4).

Criterion 32.4 – Upon discovery of a false declaration/disclosure of cash or BNI, the ADA is empowered to request and obtain further information to establish the origin or destination of the cash, from the carrier, the sender, the recipient or the representative thereof, including the intended use of the cash or BNI and to inspect

persons, their luggage and means of transport and any consignment, container or means of transport that may contain unaccompanied cash (EU Reg. 2018/1672, Art. 5; 2021 Cash Control Law, Art.3, 4 and 5)).

Criterion 32.5 – Persons who make a false declaration are subject to a fine of between EUR 251 and EUR 25 000. In the event of a repeated infringement within five years of the previous conviction, the fine may be doubled. Upon conviction, partial confiscation of the seized cash is permitted (2021 Cash Control Law, Art.13). These sanctions are not proportionate and dissuasive.

Criterion 32.6 – Information obtained through the declaration/disclosure system is available to the CRF-FIU directly through the ADA electronic cash control database (EU Reg. 2018/1672, Art. 9; 2021 Cash Control Law, Art.9).

Criterion 32.7 – Luxembourg relies on the ADA electronic cash control database and information system (DOCASH) and the EU database CIS + for ADA and CRF-FIU co-operation regarding the implementation of R.32. Co-operation and exchange of information on cash controls between the ADA and the CRF-FIU is also provided under the MoU concluded on 21 March 2022. Co-operation between the ADA and the Police is enabled under the MoU concluded on 19 May 2016 for the purpose of preventing illegal immigration and protection against general crime and the threat of terrorism. The ADA and the immigration authorities are members of an inter-ministerial steering Committee of the National Integrated Border Management Strategy, which covers co-ordination for the purpose of R.32.

Criterion 32.8 – The ADA can stop or restrain currency or BNIs for a period of 30 days to ascertain whether evidence of ML/TF may be found in cases (a) where there is a suspicion of unlawful activities such as ML/TF; or (b) where there is a false declaration or false disclosure (Cash Control Law, Art.7(1)). The detention period can be extended to 90 days upon decision of the Director of ADA based on necessity and proportionality (2021 Cash Control Law, Art.7(3)).

Criterion 32.9 – EU Competent authorities can exchange information on declarations and disclosures with non-EU countries (EU Reg. 2018/1672, Art. 10 and 11) and the CRF-FIU can exchange information with foreign FIUs. The ADA retains information in the DOCASH and CIS+ information system for requirements referred to in paragraphs (a) - (c) of this criterion. (1980 Judiciary Organisation Law, Art.74(2-6) 2021 Cash Control Law, Art.9).

Criterion 32.10 – The use of data and information collected through Luxembourg's declaration system is governed by the 2018 Criminal Data Protection Law, which ensures proper use of information. The ADA is also bound by a general obligation of secrecy (EU Reg. 2018/1672, Art. 12). There are no express provisions restricting either (i) trade payments between countries for goods and services; and (ii) the freedom of capital movements (2018 Criminal Data Protection Law, Art.28; 2021 Cash Control Law, Art.11).

Criterion 32.11 – Persons who are carrying out a physical cross-border transportation of currency or BNIs that are related to ML, TF or predicate offences are subject to:

(a) penalties that apply to ML and TF offences (see R.3 and R.5) imprisonment from one to five years and fines from EUR 250 to EUR 1 250 000 in addition to the sanctions mentioned in c.32.5. These sanctions are considered proportionate and dissuasive;

(b) ADA may seize cash or equivalent means of payment when there is suspicion of ML or TF and ultimately confiscate the cash if a criminal conviction is achieved (see R.4). However, deficiencies identified in R.4 relating to property of corresponding value are relevant here (Penal Code, Art.31, 2021 Cash Control Law, Art.13).

Weighting and Conclusion

Luxembourg has a domestic declaration/disclosure system to complement the EU regulation on transportation of cash and BNI and make it applicable at the domestic borders. However, there are some minor shortcomings in relation to the proportionality and dissuasiveness of available sanctions and ability to confiscate all cash or BNI in line with R.4.

Recommendation 32 is rated largely compliant.

Recommendation 33 – Statistics

In the 3rd Round MER, Luxembourg was rated PC. The deficiencies include, amongst others, limited statistics on prosecution of predicate offences; no statistics on confiscations or on frozen terrorist assets; and no statistics on information sharing between supervisors and certain inspection data.

Criterion 33.1 – Luxembourg keeps statistics on:

- (a)** STRs received and disseminated by the CRF-FIU. The data can be broken down by reporting activity type and the information is available through an annual report (1980 Judiciary Organisation Law, Art.74-3(2));
- (b)** ML/TF investigations, prosecutions, and convictions by PAL/PAD, as a part of the MoJ Annual Report and made publicly available on the MoJ website (1980 Judiciary Organisation Law, Art.28);
- (c)** property frozen, as a part of the CRF-FIU Annual Report, and seized and confiscated assets, as a part of the annual compendium “Justice in Figures” and MoJ Annual Report (1980 Judiciary Organisation Law, Art.28 and 74-3(2); 2022 Asset Management and Recovery Law, Art.9; AMO Annual Report); and
- (d)** mutual legal assistance or other international requests for co-operation made and received by the CRF-FIU, as a part of the CRF-FIU Annual Report and the MoJ Annual Report (1980 Judiciary Organisation Law, Art.28 and 74-3(2)). However, there are no requirements for the AED to keep statistics regarding international requests for co-operation made or received.

Weighting and Conclusion

Luxembourg maintains statistics in all required fields; however, there are no requirements for the AED to keep statistics regarding international co-operation.

Recommendation 33 is rated largely compliant.

Recommendation 34 – Guidance and feedback

In the 3rd Round MER, Luxembourg was rated PC. Gaps include restricted content and quality of guidelines on STRs, guidelines provided to various financial sectors, limited feedback on received STRs, absence of up-to-date guidelines for DNFBPs and non-binding guidance provided to DNFBPs.

Criterion 34.1 – Competent authorities, supervisors, and SRBs have established guidelines and feedback procedures that assist FIs and DNFBPs in applying national AML/CFT measures, particularly in detecting and reporting suspicious transactions.

FIU: The CRF-FIU is required to provide feedback on STRs it receives through the publication of annual STR Annual Report. This Annual Report includes figures of number of STRs received and follow-up action undertaken, and survey of types and trends of ML/TF activities. The CRF-FIU has also provided general guidelines on how to report suspicious transactions on its website, and arranged awareness raising sessions for FIs and DNFBPs since 2016 (1980 Judiciary Organisation Law, Art.74-3).

Supervisors and SRBs: Supervisory authorities and SRBs have devised different sectoral-specific guidelines and feedback procedures on national AML/CFT measures for FIs and DNFBPs and on detecting and reporting suspicious transactions.

Other competent authorities: The MoF has guidelines to help its supervised entities to comply with financial sanctions, including TF-TFS obligations. SPJ also provides input to the CRF-FIU typologies that are shared with FIs and DNFBPs.

Weighting and Conclusion

Recommendation 34 is rated compliant.

Recommendation 35 – Sanctions

Luxembourg was rated NC in the 3rd Round MER due to major shortcomings such as the limited coverage of FIs, low fine thresholds, no administrative sanctions applicable to legal persons, and limited range of sanctions. There are also gaps concerning effectiveness, which are not assessed as part of technical compliance under the 2013 Methodology.

Criterion 35.1 –

(a) Targeted financial Sanctions (R.6): Non-compliance with TFS obligations are subject to imprisonment (from a minimum of eight days to a maximum of five years) and/or fine (between EUR 12 500 and 5 000 000 or fourfold the amount of the violation if significant). This applies to natural and legal persons and where the person is a FI or DNFBP, supervisors and SRBs can apply their sanction powers (2020 Sanctions Implementation Law, Art.10 and Art.6(4)).

(b) NPO (R.8): NPOs are subject to a range of sanctions. It is unclear whether they can be considered proportionate or dissuasive (see c. 8.4).

(c) Preventive measures (R.9-23): Supervisory authorities and SRBs are empowered to use a range of proportionate and dissuasive criminal, civil or administrative sanctions to deal with failure by natural and legal persons (including ECB authorised FIs) to comply with AML/CFT requirements of Rs.9-12, 17-18 and 20. They include criminal fines (a maximum of EUR 5 million), administrative fines (a maximum of EUR 250 000 for natural person and EUR 5 million or 10% of turnover for a legal person for legal person that is an FI), warning, reprimand, public statement, withdrawal or suspension of authorisation or registration for the FI and prohibition (up to five years) for an individual. Criminal sanctions are sought when there is intent. However, only administrative sanctions are available for breaching certain requirements of R.14 and 16 ((fine ranging from EUR 250 and 250 000 (2004 AML/CFT Law, Art.8-4, 8-5, 8-10, 8-11, 9)), which is a minor shortcoming.

Criterion 35.2 – Criminal and administrative sanctions are applicable not only to FIs and DNFBPs, but also to their directors and senior management (2004 AML/CFT Law, Art.8-4, 8-10, 9).

Weighting and Conclusion

Luxembourg has a range of criminal and administrative sanctions. There are minor shortcomings on sanctions available for NPOs and breaching certain requirements of R.14 and 16.

Recommendation 35 is rated largely compliant.

Recommendation 36 – International instruments

Luxembourg was rated partially compliant with these requirements in its last evaluation. The main technical deficiencies were gaps in the criminalisation of ML, terrorist acts and TF; limited confiscation and freezing measures; inadequate provisional measures and powers, and no criminal liability for legal persons. Implementation of the Merida Convention was not assessed under the 3rd Round.

Criterion 36.1 – Luxembourg is a party to the Vienna Convention (ratified in March 1992), the Palermo Convention (ratified in May 2008), the Merida Convention (ratified in November 2007) and the TF Convention (ratified in November 2003).

Criterion 36.2 – Luxembourg largely implements the Vienna, Palermo, Merida and TF Conventions. However, elements of the relevant articles of the Merida Convention are not covered (elements of Arts. 26, 30, & 46 (13 & 14)).

Weighting and Conclusion

Luxembourg implements the relevant international instruments. However, gaps exist with respect to the Merida Convention which, given Luxembourg's context, are minor.

Recommendation 36 is rated largely compliant.

Recommendation 37 - Mutual legal assistance

The 3rd Round MER rated Luxembourg partially compliant with requirements related to MLA based on the following deficiencies: limitations imposed by the dual criminality requirements and gaps in the ML and TF offences; professional secrecy and notification requirements; and limitations on co-operation related to fiscal matters.

Criterion 37.1 – Luxembourg has a legal basis that allows it to rapidly provide a wide range of MLA in relation to ML, associated predicate offences and TF investigations, prosecutions and related proceedings (2000 MLA Law, Art.5, 8). The PG can provide any non-coercive assistance, including: obtaining objects, documents, funds and property of any kind seized in the Grand Duchy of Luxembourg.

Criterion 37.2 – The PG is the central authority for the transmission and execution of requests (2000 MLA Law, Art.2(1), (2)). The MoJ has clear processes for the timely prioritisation and execution of requests. In case of an urgent request, the relevant competent authority may carry out the requested investigative duties and informs the PG (2000 MLA Law, Art.2(3),(5)). MLA cases are treated as a priority and are monitored through a central case management system called *JU-CHA*.

Criterion 37.3 – MLA is not prohibited or made subject to unreasonable or unduly restrictive conditions (2000 MLA, Art.3, 4).

Criterion 37.4 – (a) Exchanges on all types of tax crimes are permissible (2017 Tax Reform Law); (b) Requests cannot be refused based on professional secrecy (1993 LFS, Art.41).

Criterion 37.5 – Luxembourg maintains the confidentiality of MLA requests received and the information therein (CPP, Art.8, 458; 2000 MLA Law, Art.7). Parties concerned by an MLA request would only have access if they are questioned during the judicial phase of the proceedings (CPP, Art.46).

Criterion 37.6 – MLA requests not involving coercive measures are considered ancillary requests and dual criminality is not required to provide assistance. There are no grounds for refusing an ancillary request.

Criterion 37.7 – Where dual criminality is required for MLA that requirement is satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence (2000 MLA Law, Art.5).

Criterion 37.8 – Powers and investigative techniques available domestically are available for use in response to MLA requests. Specifically, Luxembourg can use:

- (a) powers mentioned under R.31 relating to production, search and seizure of information, documents or evidence, including financial records, and the taking of witness statements for the purpose of coercive MLA cases; and
- (b) a broad range of other powers and investigative techniques (see c.31.2).

Weighting and Conclusion

Recommendation 37 is rated compliant.

Recommendation 38 – Mutual legal assistance: freezing and confiscation

Luxembourg was rated LC in the 3rd Round MER based on the following deficiencies: the dual criminality requirement and gaps in ML/TF offences limit Luxembourg's ability to freeze, seize and confiscate; no mechanism for sharing seized assets; overly restrictive limitations on funding the asset forfeiture fund.

Criterion 38.1 – Luxembourg has the authority to take expeditious action in response to requests by foreign countries to meet all requirements referred to in paragraphs (a) – (e) of this criterion (CPP, Art.48-24, 51-1(1), 66, Art. 704; 1980 Judicial Organisation Law, Art.74-6, Art.74-7 & 8; 2004 AML/CFT Law, Art.5(3); 2000 MLA Law, Art. 8).

Criterion 38.2 – Luxembourg can provide assistance to requests for co-operation made on the basis of non-conviction based confiscation proceedings in the case of acquittal, exemption from punishment, where the prescription period has lapsed or expired or when the perpetrator is unavailable by reason of death, absence, flight or the perpetrator is unknown (Penal Code, Art.31(3); 2000 MLA Law, Art.5, point 4; CPP, Art.66, 34, and 666.).

Criterion 38.3 –

(a) Luxembourg can coordinate seizure actions either directly through the requesting or executing authorities, or through the Asset Recovery Office (ARO), which is part of the CARIN network or, for EU Member States, through Europol or Eurojust (Council decision 2007/845/JHA of 6 December 2007; EU Reg. 2018/1727 and 2016/794).

(b) Luxembourg has a mechanism in place to manage, and when it is necessary, dispose of seized and confiscated property. The Asset Management Office (AMO) is responsible to ensure the management of all seized assets for criminal proceedings and, when necessary, disposing of such assets (2022 Asset Management and Recovery Law, Art. 3-4).

Criterion 38.4 – Luxembourg law generally provides for the possibility of sharing agreements in relation to confiscated property in the context of the judgment ordering enforcement of the foreign confiscation order (CPP, Art.668).

Weighting and Conclusion

Recommendation 38 is rated compliant.

Recommendation 39 – Extradition

Luxembourg was rated largely compliant with these requirements in the 3rd Round MER due to refusal to extradite its own nationals (and no guarantee of domestic prosecution) and given the limitations imposed by the dual criminality requirement and gaps in ML/TF offences.

Criterion 39.1 – Luxembourg can execute extradition requests in relation to ML/TF based on 1) the 2001 Extradition Law, 2) the 2004 EAW Law (EU Member States' requests), or 3) a bilateral treaty. In cases under the EAW law, the requests are executed without undue delay. In particular:

(a) ML and TF are extraditable offences (2001 Extradition Law, Art.3(1)).

(b) Judicial authorities maintain an electronic case management system (JU-CHA) to keep track of EAWs. Certain timelines exist under the 2004 EAW Law requiring prioritisation, such as a 10-day period within which the country should turn over the arrested person, after making the decision (Art.14(2)). For other extradition requests, the MoJ maintains a paper case management system. This system is sufficient considering the relatively low number of incoming extradition requests issued by non-EU countries (37 in total over the period 2015–2021).

(c) Luxembourg does not place unreasonable or unduly restrictive conditions on the execution of requests.

Criterion 39.2 –

(a) Luxembourg cannot extradite its own nationals to non-EU countries (2001 Extradition Law, Art.7(1)).

(b) Where Luxembourg refuses extradition, it is required to submit the case for prosecution, in accordance with the stipulated rules of the Luxembourg Penal Code (2001 Extradition Law, Art.14-1.) Such a case will be submitted to the State Prosecutor without delay (2001 Extradition Law, art. 14-1, CPP, art.23). Where

surrender under an EAW is refused, Luxembourg authorities should execute the sentence or detention order domestically (2004 EAW Law, Art.5).

Criterion 39.3 – Where dual criminality is required for extradition that requirement is satisfied regardless of whether both countries place the offence within the same category of offence or denominate the offence by the same terminology provided that both countries criminalise the conduct underlying the offence (2001 Extradition Law, Art.3(4), Art.3(1)).

Criterion 39.4 – Luxembourg has simplified extradition measures in place in cases where the subject consents to the extradition (2001 Extradition Law, Art.23; 2004 EAW Law, Art.3(3)).

Weighting and Conclusion

Recommendation 39 is rated compliant.

Recommendation 40 – Other forms of international co-operation

Luxembourg was rated largely compliant with these requirements in the 3rd Round MER with the deficiency that FIU co-operation may not focus on ML/TF.

Criterion 40.1 – All competent authorities in Luxembourg can rapidly provide a wide range of international co-operation, both spontaneously and upon request (1980 Judiciary Organisation Law, Art.74-5, Art.74-8; 2018 Police Exchange of Information Law, Art.1-13; 2004 AML/CFT Law, Art.9-2a, 9-2b, 9-2c).

Criterion 40.2 –

(a) All competent authorities have a lawful basis for providing international co-operation (see c.40.1).

(b) Competent authorities are authorised to share information by the most efficient means. Supervisors and the CRF-FIU can co-operate directly.

(c) Competent authorities have clear and secure gateways, mechanisms or channels to facilitate and allow for the transmission and execution of requests. Co-operation occurs largely through: EU mechanisms (e.g. EUROPOL's SIENA Platform, CARIN, FIU.Net, and Common Communication Network (CCN)); and international mechanisms: Interpol, the Common Transmission System (CTS), the International Data Exchange Service (IDES), the Eurojust agency and the Egmont Secure Web. Supervisors are required to exchange information in a secure way through reliable channels or mechanisms (2004 AML Law, Art.9-2a(7)).

(d) Competent authorities have processes in place to prioritise requests and ensure timely assistance provided. All requests received by the CRF-FIU receive an initial response within 24 hours. ARO treats all requests as urgent requests (1980 Judiciary Organisation Law, Art.74-8(3)). PGD is obliged to transmit personal data for urgent requests within a maximum of eight hours and for non-urgent requests within one week or within 14 days. ACD has a series of internal circulars and other guidance materials to ensure that requests are executed in a timely manner. CSSF and CAA have policies for prioritising requests (internal note de service 20/535; CAA Policy on national and international co-operation). However, the AED do not yet have such a policy.

(e) Competent authorities have processes for safeguarding information received (2018 Police Exchange of Information Law, Art. 6; 2018 Criminal Data Protection Law, Art.3; 2004 AML/CFT Law, Art.9-2a (7); 1998 CSSF Law, Art.16; 2015 Insurance Law, Art.7).

Criterion 40.3 – When bilateral or multilateral agreements are required, most competent authorities can establish them in a timely way and with a wide range of foreign counterparts. The CRF-FIU has access to the Egmont Group and the FIU.net, and has concluded 26 MOUs for information exchange. The AMO is a member of the CARIN network and is linked to five regional networks (ARINs) across the globe. The PGD exchanges information through international/multilateral agreements or European legislation and bilateral agreements with neighbouring countries. The ACD's network for exchange of information on request covers more than 130 jurisdictions. The CSSF and CAA can establish bilateral or multilateral agreements in a timely manner⁸⁷ and has concluded bilateral agreements with a wide range of counterparts (CSSF: 58 MOUs; CAA: 5 MOUs). The AED, under its supervisory capacity, does not have similar agreements or arrangements with foreign counterparts, although there are no obstacles preventing it from entering into such agreements. It is unclear though, whether this can be concluded in a timely way. AED can exchange information indirectly under its MoU with the CSSF. The AED, as tax authority, has negotiated and signed agreements with foreign counterparts.

Criterion 40.4 – The CRF-FIU provides feedback to foreign FIUs upon request (1980 Judiciary Organisation Law, Art.74-5(10)). In some major cases, feedback is provided spontaneously via FIU.net or ESW. The PGD provides feedback on a case-by-case basis. The ACD also provides feedback in the shortest possible time if the sending jurisdictions requests it. Supervisors, including the AED, are required to provide feedback on the usefulness of the information obtained upon request by a foreign counterpart (2004 AML/CFT Law, Art.9-2a(5)). However, despite similarities in the legal framework for international co-operation by the CRF-FIU and the ARO, the ARO is not subject to a similar requirement to provide feedback on request (1980 Judiciary Organisation Law, Art.74-8).

Criterion 40.5 – Competent authorities do not prohibit, or place unreasonable or unduly restrictive conditions on, the provision of exchange of information or assistance. They do not refuse a request for assistance on the grounds set out in paragraphs (a) to (d) (2004 AML/CFT Law, Art.9-2b; 1980 Judiciary Organisation Law, Art.74-5).

Criterion 40.6 – Competent authorities are required to maintain appropriate confidentiality consistent with domestic requirements on privacy and data protection (1980 Judiciary Organisation Law, Art.74-4(2), par.2; Art.74-5(8) and (9), 74-8(5); 2018 Police Exchange of Information Law, Art.6; 2004 AML/CFT Law, Art.9-2a(6)).

Criterion 40.7 – Competent authorities (CRF-FIU, PG Office, State Prosecutors Offices, PGD, all supervisors) maintain appropriate confidentiality for any request for co-operation and the information exchanged, consistent with both parties' obligations concerning privacy and data protection (1980 Judiciary Organisation Law, Art.74-6, Art.74-5(5)(5), Art.74-5(9) (par.2), Art.74-8(4); CCP, Art.8 and 48-24; Penal Code, Art.458; 2018 Criminal Data Protection Law, Art.28; 2004 AML/CFT Law, Art.9-2a(4), Art.9-2a(7), 9-2c(8)). However, the ARO does not have the express power to refuse to

⁸⁷ CSSF: EBA; CAA: IAIS Multilateral Memorandum on Co-operation and Information Exchange, ECB.

provide information if the foreign authority cannot protect the information effectively.

Criterion 40.8 – Competent authorities are able to conduct inquiries on behalf of foreign counterparts and exchange with them information that would be obtainable by them if such inquiries were being carried out domestically (1980 Judiciary Organisation Law, Art.74-5(1) (3), 74-8 (3)); 2018 Police Exchange of Information Law, Art.7; 2014 EOIR Law, Art.3; 2004 AML/CFT Law, Art.9-2a(2)).

Exchange of Information between FIUs

Criterion 40.9 – The CRF-FIU has an adequate legal basis for providing co-operation on ML, associated predicate offences and TF (1980 Judiciary Organisation Law, Art.74-5(1)).

Criterion 40.10 – The CRF-FIU provides feedback to foreign counterparts on request. This includes feedback on the use of the information and the outcome of the analysis conducted based on the information provided (1980 Judiciary Organisation Law, Art.74-5(10)).

Criterion 40.11 – The CRF-FIU can exchange:

- (a) all information required to be accessible or obtainable directly or indirectly by the FIU, under R.29, and
- (b) any other information which it can obtain or access, directly or indirectly (1980 Judiciary Organisation Law, Art.74-5(3)), including through the central electronic data retrieval system (2020 RBASD Law, Art.8(1)).

Exchange of information between financial supervisors

Criterion 40.12 – Supervisors have a legal basis to co-operate with foreign counterpart authorities, regardless of their respective nature or status, consistent with international standards for supervision, by exchanging information, including supervisory information, and co-operating in investigations related to or relevant for AML/CFT purposes (2004 AML/CFT Law, Art.9-2c(1), 9-2a(2)).

Criterion 40.13 – Supervisors are required to use all powers available to them domestically to collect information in response to requests from foreign counterparts (2004 AML Law, Art.9-2a(2) third para). Upon receipt of a request by a foreign power, the CSSF and CAA are required to use their full legal powers to obtain the relevant information on behalf of the foreign counterpart (2004 AML/CFT Law, Art.9-2c(2)).

Criterion 40.14 – Supervisors can communicate any information relevant to AML/CFT purposes (2004 AML/CFT Law, Art.9-2a, 9-2c(1)). Specifically, they can exchange:

- (a) regulatory information, such as information on the domestic regulatory system, and general information on the financial sectors;
- (b) prudential information, in particular for supervisors applying “Core Principles for Effective Banking Supervision”, including information on the credit institutions’ and FIs’ business activities, beneficial ownership, management and professional

(c) AML/CFT information, such as internal AML/CFT procedures and policies of credit institutions and FIs, CDD information, customer files, samples of accounts and transaction information (2004 AML/CFT Law, Art.9-2c(9)).

Criterion 40.15 – Supervisors can conduct inquiries on behalf of foreign counterparts and may authorise foreign counterparts to participate in a domestic investigation or on-site inspection. (2004 AML/CFT Law, Art. 9-2a(9)).

Criterion 40.16 – Where supervisors receive confidential information, any dissemination of this information to other authorities or third parties, or any use of this information for other purposes or for purposes beyond those originally approved, must first be authorised by the authority which communicated it (2004 AML/CFT Law, Art.9-2a(6), second para. for all supervisory authorities; Art. Art.9-2c(6), second para. specific to CSSF and CAA).

Exchange of information between law enforcement authorities

Criterion 40.17 – The PGD, including the SPJ, and ADA can exchange domestically available information for both intelligence and investigative purposes with police services (both within and outside the EU), bodies of the European Union, Interpol and customs services to the extent that they are involved in law enforcement. (2018 Police Exchange of Information Law, Art.5(1)). The ARO is specifically empowered to exchange information for the identification and tracing the proceeds and instrumentalities of crime (1980 Judiciary Organisation Law, Art.74-8(1)). 7

Criterion 40.18 – The PGD, including the SPJ, and ADA can use all investigative techniques available under domestic law to obtain information on behalf of foreign counterparts ((2018 Police Exchange of Information Law, Art.5(1)). The ARO may instruct the SPJ to use all investigative techniques available under domestic law to trace and identify proceeds and instrumentalities of crime that may be in Luxembourg (1980 Judiciary Organisation Law, Art.74-8(3)).

Criterion 40.19 – LEAs are able to form joint investigative teams involving LEAs from EU countries (2006 Joint Investigation Law, Art.1) and non-EU countries that are member of the 1959 Strasbourg Convention and its Second Additional Protocol (2021 MLA Strasbourg Protocol Law, Art. 4 to 6) LEAs can establish joint investigative teams with non-EU countries based on the international conventions including the Vienna, Palermo and Merida Conventions, and multilateral/bilateral agreements (see c.40.3).

Exchange of information between non-counterparts

Criterion 40.20 – All authorities in Luxembourg (CRF-FIU, LEAs, supervisors and tax authorities) can exchange information indirectly with non-counterparts either on their own or via the CRF-FIU. All incoming requests must indicate the purpose and entity for which the request is made (1998 CSSF Law, Art.16(4); 1980 Judiciary Organisation Law, Art. 74-5(3), 74-5(9), 74-8(6); 2008 Tax Authorities Cooperation Law, Art.16; 2018 Police Exchange of Information Law, Art.5; 2019 multilateral agreement among the ECB, CSSF and CAA; 2004 AML/CFT Law, Art. 9-1; MOU between CRF-FIU and CSSF, Art.2.5).

Weighting and Conclusion

Luxembourg meets most of the requirements of this Recommendation. However, deficiencies exist relating to prioritisation policies for the AED, and ARO's express

power to refuse to provide information if the foreign authority cannot protect the information effectively.

Recommendation 40 is rated largely compliant.



Summary of Technical Compliance – Key Deficiencies

Compliance with FATF Recommendations

| Recommendations | Rating | Factor(s) underlying the rating |
|---|--------|--|
| 1. Assessing risks & applying a risk-based approach | C | All criteria are met. |
| 2. National cooperation and coordination | C | All criteria are met. |
| 3. Money laundering offences | C | All criteria are met. |
| 4. Confiscation and provisional measures | LC | There are no measures to enable confiscation of property of corresponding value in the absence of conviction or held by third parties. |
| 5. Terrorist financing offence | C | All criteria are met. |
| 6. Targeted financial sanctions related to terrorism & TF | LC | <p>Internal guidelines incorporate by reference confidential EU-level guidance on how to develop sufficient evidence to support a designation, but this is not tailored to Luxembourg's context.</p> <p>At the national level, Luxembourg has no mechanism(s) for identifying targets for designations based on UNSCR 1373 criteria.</p> <p>At the national level, there is no formal mechanism(s) for making a prompt determination of whether the request is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in UNSCR 1373, though authorities demonstrated that this has occurred as a practical matter.</p> <p>At the EU level, the definition of assets does not explicitly cover jointly-owned assets or funds or assets controlled by, indirectly owned by, derived from assets owned by, or owned by a person acting at the direction of a designated person or entity.</p> <p>For UNSCR 1373, the obligation to freeze does not apply to funds or assets controlled by, or indirectly owned by, or derived from assets owned by, or owned by a person acting at the direction of a designated person or entity.</p> <p>Like deficiencies identified in UNSCRs 1267/1988, jointly owned funds/assets are not covered under the freezing obligations (EU Council Reg.2580/2001, Art.1(a), 2(1)(a), 2(3)(iii) and (iv)).</p> <p>There does not appear to be a mechanism for providing clear guidance to other persons or entities, including DNFBPs, that may be holding targeted funds or other assets on their obligations in taking action under freezing mechanisms (2010 GDR, Art.5; 2020 Sanctions Implementation Law, Art.4).</p> |
| 7. Targeted financial sanctions related to proliferation | LC | AT EU level, freezing may not happen without delay for natural and legal persons that have not yet been designated by the EU. This also raises the question of the UN designated |

| Recommendations | Rating | Factor(s) underlying the rating |
|---|--------|--|
| | | <p>person/entity to receive prior notice before a freezing action can take place (EU Council Reg. 2017/1509, Art.1; EU Council Reg. 267/2012, Art.49).</p> <p>The relevant EU Council Regulations do not expressly require the freezing of those funds or other assets that are jointly owned or controlled by designated persons or entities (EU Council Reg. 2017/1509, Art.34; EU Council Reg. 267/2012, Art.1, 23(1) and 23(2)(a)).</p> <p>At the national level, save for sub-element (iii), all elements of funds or other assets mentioned in c.7.2(b) are covered.</p> <p>Most SRBs (other than OEC) responsible for supervising DNFBPs and other entities have not provided guidance on their obligations in taking action under freezing mechanisms.</p> <p>There is no mechanism for providing clear guidance to DNFBPs, including entities supervised by SRBs on their obligations to respect a de listing or unfreezing action.</p> |
| 8. Non-profit organisations | PC | <p>There is no targeted risk-based supervision or monitoring of NPOs</p> <p>Sanctions are considered neither proportionate nor dissuasive. Luxembourg did not provide any indication of the provisions of the criminal code that would apply for violations under sub-criterion 8.4(b), nor the expected range of penalties in this regard.</p> |
| 9. Financial institution secrecy laws | C | All criteria are met. |
| 10. Customer due diligence | C | All criteria are met. |
| 11. Record keeping | C | All criteria are met. |
| 12. Politically exposed persons | C | All criteria are met. |
| 13. Correspondent banking | C | All criteria are met. |
| 14. Money or value transfer services | C | All criteria are met. |
| 15. New technologies | LC | <p>Luxembourg does not comprehensively assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.</p> <p>For VA transfers, not all beneficiary and originator information accompanies VASP transactions in relation to transfers within the EU in the time period required.</p> <p>The deficiencies in R.6 apply here.</p> |
| 16. Wire transfers | C | All criteria are met. |
| 17. Reliance on third parties | C | All criteria are met. |
| 18. Internal controls and foreign branches and subsidiaries | C | All criteria are met. |
| 19. Higher-risk countries | C | All criteria are met. |
| 20. Reporting of suspicious transaction | C | All criteria are met. |

| Recommendations | Rating | Factor(s) underlying the rating |
|---|--------|---|
| 21. Tipping-off and confidentiality | C | All criteria are met. |
| 22. DNFBPs: Customer due diligence | C | All criteria are met. |
| 23. DNFBPs: Other measures | C | All criteria are met. |
| 24. Transparency and beneficial ownership of legal persons | LC | <p>There is no requirement to include information in the share register on the nature of the associated voting rights.</p> <p>The ML/TF risks of bearer share warrants have not been mitigated.</p> <p>The ML/TF risks of nominee directors and shareholders have not been sufficiently mitigated.</p> <p>The sanctions for board members of certain types of companies are not dissuasive.</p> |
| 25. Transparency and beneficial ownership of legal arrangements | C | All criteria are met. |
| 26. Regulation and supervision of financial institutions | C | All criteria are met. |
| 27. Powers of supervisors | C | All criteria are met. |
| 28. Regulation and supervision of DNFBPs | C | All criteria are met. |
| 29. Financial intelligence units | C | All criteria are met. |
| 30. Responsibilities of law enforcement and investigative authorities | LC | <p>There is no explicit requirement for authorities, in domestic cases, to expeditiously identify, trace and initiate freezing and seizing of property that is, or may become, subject to confiscation, or is suspected of being proceeds of crime.</p> <p>Some more coercive means of asset identification are only applicable if the criminal prosecution carries a maximum criminal sentence or correctional sentence of at least two years of imprisonment.</p> |
| 31. Powers of law enforcement and investigative authorities | C | All criteria are met. |
| 32. Cash couriers | LC | <p>The sanctions available for submitting a false declaration or disclosure are not sufficiently proportionate or dissuasive.</p> <p>The deficiencies in R.4 apply here.</p> |
| 33. Statistics | LC | There are no requirements for the AED to keep statistics regarding international co-operation. |
| 34. Guidance and feedback | C | All criteria are met. |
| 35. Sanctions | LC | <p>It is unclear whether penalties for NPOs are proportionate or dissuasive.</p> <p>There are only administrative sanctions available for breaches of certain requirements under R.14 and R.16</p> |
| 36. International instruments | LC | Luxembourg does not fully implement the Merida Convention. |
| 37. Mutual legal assistance | C | All criteria are met. |
| 38. Mutual legal assistance: freezing and confiscation | C | All criteria are met. |

| Recommendations | Rating | Factor(s) underlying the rating |
|---|--------|--|
| 39. Extradition | C | All criteria are met. |
| 40. Other forms of international co-operation | LC | <p>The AED does not have a policy for prioritisation and timely execution of requests.</p> <p>The ARO is not subject to provide feedback in a timely manner to competent authorities from which it received assistance, on the use and usefulness of the information obtained.</p> <p>The ARO does not have the express power to refuse to provide information if the requesting competent authority cannot protect the information effectively.</p> |

Glossary of Acronyms ⁸⁸

| | DEFINITION |
|---------------------|---|
| ACA | Luxembourg Insurance and Reinsurance Association |
| ACD | Tax Authority - Luxembourg Inland Revenue Authority |
| AED | Tax Authority - Registration Duties, Estates and VAT Authority |
| ADA | Customs and Excise Administration |
| ALFI | Professional association for the Luxembourg asset management and investment fund sector |
| AML/CFT | Anti-Money Laundering and Combating the Financing of Terrorism |
| AMO | Asset Management Office |
| APCAL | Luxembourg Insurance Brokers Business Association |
| ARO | Asset Recovery Office |
| ASBL | <i>Association sans but lucratif</i> |
| BNI | Bearer-Negotiable Instrument |
| BO | Beneficial Ownership |
| CAA | Insurance Supervisory Authority |
| CDD | Customer due diligence |
| CdN | Chamber of Notaries |
| CNPD | Luxembourg's data protection commission |
| CPA | Chartered Professional Accountant |
| CRF-FIU | Luxembourg's Financial Intelligence Unit |
| CSSF | <i>Commission de Surveillance du Secteur Financier</i> |
| DNFBPs | Designated Non-Financial Businesses and Professions |
| DNGOs | Non-Governmental Organisations that engage in development and humanitarian projects abroad |
| DPMS | Dealers in Precious Metals and Stones |
| EAW | European Arrest Warrant |
| EIO | European Investigation Order |
| EMI | Electronic Money Institution |
| EU | European Union |
| EU SNRA | Supranational Report of the European Commission on the assessment of the risk of money laundering and terrorist financing |
| Eurojust | The European Union Agency for Criminal Justice Cooperation |
| FCP | <i>Fonds commun de placement</i> |
| FDI | Foreign Direct Investment |
| FI | Financial institution |
| GDP | Gross Domestic Product |
| IFC | International Financial Centre |
| Investigative Judge | Office of the Investigative Judge of the Luxembourg District Court and Office of the Investigative Judge of the Diekirch District Court |
| IEF | SPJ Economic and Financial Crimes Unit |
| IO | Immediate Outcome |
| IRE | Institute of Statutory Auditors |
| ISC | AML/CFT Inter-ministerial Steering Committee |

⁸⁸ Acronyms already defined in the FATF 40 Recommendations are not included into this Glossary.

| | |
|-----------------|--|
| JIT | Joint Investigation Team |
| JU-CHA | Judicial authorities' database and case management system |
| LBR | Luxembourg Business Registers |
| LEAs | Law Enforcement Agencies |
| MLA | Mutual Legal Assistance |
| MoE | Ministry of Economy |
| MoFA | Ministry of Foreign and European Affairs |
| MoF | Ministry of Finance |
| MoJ | Ministry of Justice |
| NRA | National Risk Assessment |
| NPC | National Prevention Committee |
| OAs | Luxembourg and Diekirch Bar Associations (OAL and OAD) |
| OAD | Diekirch Bar Association |
| OAL | Luxembourg Bar Association |
| OEC | Order of Chartered Professional Accountants |
| PG | General State Prosecutor's Office |
| PGD | Grand Ducal Police |
| PAL | State Prosecutor of the Luxembourg District Court |
| PAD | State Prosecutor's Office of the Diekirch District Court |
| PI | Payment Institution |
| PSA | Professional of the insurance sector |
| PWGT | Police Working Group on Terrorism |
| RBE | Register of Beneficial Owners |
| RCS | Trade and Company Register |
| REA | Real Estate Agent |
| RFT | Register of Fiducies and Trusts |
| RIRA/RIRT | Suspicious Operations Report Codes |
| SAR | Suspicious Activity Report |
| Specialised PFS | Specialised Professionals of the Financial Sector providing Corporate Services |
| SPJ | Judicial Police Service |
| SPJ-AB | SPJ Anti-money Laundering Unit |
| SPJ-EJIN | SPJ International Mutual Legal Assistance Section |
| SPJ-SAT | SPJ Service Anti-Terrorism Section |
| SRB | Self-Regulatory Body |
| SRE | State Intelligence Service |
| SSRA | Sub-sectoral Risk Assessment |
| STR | Suspicious Transaction Report |
| TCSP | Trust and Company Service Provider |
| TFAR | TF Activity Report |
| TFTR | TF Transactions Report |
| VA | Virtual Asset |
| VASP | Virtual Asset Service Provider |
| VRA | Vertical Risk Assessment |
| WIKI-ECOFIN | SPJ Internal Tailored Encyclopedia |



© FATF

www.fatf-gafi.org

September 2023

Anti-money laundering and counter-terrorist financing measures - Luxembourg

Fourth Round Mutual Evaluation Report

In this report: a summary of the anti-money laundering (AML) / counter-terrorist financing (CTF) measures in place in Luxembourg as at the time of the on-site visit from 2-18 November 2022.

The report analyses the level of effectiveness of Luxembourg's AML/CTF system, the level of compliance with the FATF 40 Recommendations and provides recommendations on how their AML/CFT system could be strengthened.