2026 NATIONAL RISK ASSESSMENT OF TERRORIST FINANCING

Observation period: 2021 – 2024

THE GOVERNMENT
OF THE GRAND DUCHY OF LUXEMBOURG
Ministry of Justice

Contents

1. Executive summary 1
   1.1. Scope, purpose and methodology 1
   1.2. Terrorist financing threat – main conclusions 1
      1.2.1. Dominant threat profile: small-scale actors 1
      1.2.2. Large international organisations: theoretical exposure 2
      1.2.3. Regional and global context 2
   1.3. Vulnerability assessment – key findings 2
      1.3.1. CSSF supervised sectors 2
      1.3.2. Other financial and non-financial sectors 3
      1.3.3. Non-profit organisations 3
      1.3.4. Cross-sector and emerging vulnerabilities 3
   1.4. Mitigating factors – key findings 4
   1.5. Residual terrorist financing risk – summary by sector 5
   1.6. Emerging risks and strategic priorities 7
   1.7. Overall conclusion 8
2. Luxembourg context 9
   2.1. Luxembourg's demographic structure 9
   2.2. Luxembourg's economy 10
3. Approach and methodology 14
   3.1. Assessment process and involvement of stakeholders 14
   3.2. Inputs used 16
   3.3. Methodology 17
      3.3.1. Threats assessment 18
      3.3.2. Vulnerabilities assessment 18
      3.3.3. Mitigating factors assessment and residual risk 19
4. Introduction to terrorist financing stages and threats 22
   4.1. Terrorist financing stages 22
   4.2. Terrorist actors and their financing needs 23
      4.2.1. Decentralised networks, small terrorist cells and lone actors 23
      4.2.2. Foreign terrorist fighters 23

4.2.3. International terrorist organisations, linked and affiliated structures 25
4.2.4. Other terrorist actors 25
4.3. Ideologies and terrorist financing needs 25
4.3.1. Jihadism 26
4.3.2. Extreme-right wing terrorism 27
4.3.3. Left wing and anarchist terrorism 28
4.3.4. Ethno-nationalist and separatist terrorism 29
4.3.5. Trends 29
5. Terrorism threat context 32
5.1. Sub-Saharan Africa 32
5.2. Middle East and Northern Africa region 32
5.3. European Union 33
5.4. Luxembourg 36
6. Analysis of terrorist financing reports received by the CRF 38
7. Luxembourg terrorist financing threats related to decentralised networks, FTFs, lone actors and small cells 43
8. Luxembourg terrorist financing threats related to international organisations, affiliated and linked structures and other terrorist actors 45
8.1. Analysis of financial flows with jurisdictions targeted for analysis 46
8.2. Analysis of non-financial flows with jurisdictions targeted for analysis 49
8.2.1. Legal persons and legal arrangements: links to jurisdictions targeted for analysis 49
8.2.2. NPOs and links to jurisdictions targeted for analysis 51
8.2.3. Imports and exports from and to jurisdictions targeted for analysis 52
8.3. Analysis of economic and bilaterial relations with jurisdictions targeted for analysis – conclusion 52
9. Luxembourg terrorist financing threat context – conclusion 53
10. Inherent terrorist financing risk – vulnerabilities assessment 55
10.1. CSSF supervised sectors 55
10.1.1. Banks 55
10.1.2. Investment sector 65
10.1.3. Money value and transfer services 69
10.1.4. Virtual asset service providers 73
10.1.5. Specialised PFS 76
10.1.6. Support PFS and other Specialised PFS 78
10.1.7. Market operators 78

10.2. CAA supervised sectors 79
10.2.1. Life insurance 80
10.2.2. Non-life insurance 81
10.2.3. Reinsurance 82
10.2.4. Intermediaries 83
10.2.5. Professionals of the insurance sector 84
10.2.6. CAA-supervised pension funds 85
10.3. AED supervised sectors 86
10.3.1. Real estate agents and developers 86
10.3.2. Freeport operators 88
10.3.3. Dealers in goods 89
10.3.4. Gambling service providers 91
10.3.5. Legal and accounting professionals supervised by the AED 93
10.4. Legal and accounting professions supervised by SRBs 95
10.4.1. Lawyers 95
10.4.2. Notaries 98
10.4.3. Court bailiffs 99
10.4.4. Audit profession 100
10.4.5. Chartered professional accountants 101
10.5. Legal persons and legal arrangements 103
10.5.1. Legal persons 104
10.5.2. Legal arrangements 108
10.6. Non-profit organisations 110
10.6.1. FATF NPO subset and legal form 112
10.6.2. Geographical activities analysis 113
11. Cross sector vulnerabilities 115
11.1. Cash 115
11.2. Crypto-assets 115
11.3. Crowdfunding 116
11.4. Underground banking and HOSSP 116
12. Emerging risks 118
13. Mitigating factors analysis 120
13.1. National strategy and coordination 120
13.2. Prevention and supervision 121

13.2.1. CSSF 121
13.2.2. Other supervisory authorities and SRBs 126
13.2.3. Oversight of NPOs 127
13.3. Detection by the CRF 128
13.3.1. Analysis of suspicion reports 129
13.3.2. International cooperation 130
13.3.3. Outreach and training 131
13.4. Investigations triggered by information taken from mutual legal assistant requests 132
13.5. Prosecution, investigation and asset recovery 133
13.5.1. State prosecutor 133
13.5.2. Investigative judge 134
13.5.3. Judicial Police Service 134
13.5.4. Prosecutions and convictions 135
13.5.5. National CFT cooperation and coordination 135
14. Residual terrorist financing risk 137
Appendix A Methodology 140
A.1. Threat assessment: selection of jurisdictions targeted for analysis and tier classification 140
A.1.1. Terrorism approach: leveraging the Global Terrorist Index 140
A.1.2. Terrorist financing approach: leveraging the results of the FATF mutual evaluations 141
A.1.3. Jurisdictions targeted for analysis: categorisation into tier groups 142
A.2. Vulnerabilities assessment 144
A.3. Mitigating factors and residual risk 146
Appendix B List of tables, figures, case studies and insight boxes 148
B.1. List of tables 148
B.2. List of figures 148
B.3. List of case studies 149
B.4. List of insight boxes 149
Appendix C Glossary 150

1. Executive summary

1.1. Scope, purpose and methodology

1. This National Risk Assessment (NRA) on Terrorist Financing (TF) provides a comprehensive evaluation of Luxembourg's exposure to TF risks across the 2021–2024 observation period. Following the FATF TF Risk Assessment Guidance (2019)[1], the assessment applies a three-stage framework (threat, vulnerability and mitigating factors) to derive subsector-level inherent and residual TF risk scores. The process engaged, amongst others, supervisory authorities (CSSF, CAA, AED), self-regulatory bodies (SRBs), ministries, judicial authorities, the Luxembourg Financial Intelligence Unit (CRF), and private-sector representatives. Findings were validated through bilateral meetings, data requests and iterative review cycles.

2. Luxembourg presents a specific risk profile: no completed terrorist attack has occurred on its soil, no established terrorist group operates domestically, and the domestic terrorism threat level has been maintained at Level 2 ("Medium") since 2015. However, as an international financial centre ranked 19th globally and first in Europe for investment funds, Luxembourg's deep cross-border exposure necessitates a rigorous, independent assessment of TF vulnerabilities regardless of the domestic terrorist threat context, in line with FATF guidance for jurisdictions with financial centres and low domestic terrorism risk[2].

1.2. Terrorist financing threat – main conclusions

1.2.1. Dominant threat profile: small-scale actors

3. Based on the analysis performed in this report, the prevailing TF threat to Luxembourg emanates from lone actors, small cells and foreign terrorist fighters (FTFs) with low and granular financial needs. These actors, predominantly linked to jihadist ideology, followed by extreme-right wing and ethno-nationalist movements, rely on basic and largely available financial products offered by retail banks, payment institutions (PIs), e-money institutions (EMIs) and, increasingly, virtual asset service providers (VASPs). Funds are mainly of legitimate origin (salaries, social benefits, small loans), making detection challenging. The dominant typologies identified by the CRF include small-amount donations to foreign non-profit associations (NPOs) suspected of links to extremist organisations; peer-to-peer (P2P) online transfers for alleged humanitarian purposes; sale and purchase of items linked to extremist ideologies; and suspicious money-remittance behaviour associated with high-risk jurisdictions.

4. Luxembourg's structural exposure stems from two reinforcing factors: (i) several pan-European Union (EU) PIs and EMIs operate their European headquarters in Luxembourg, extending the geographic reach of the risk surface to the entire EU Single Market; and (ii) the country's geographical situation, high internet penetration and near-universal smartphone adoption among youth amplify

[1] FATF, *Terrorist Financing Risk Assessment Guidance,* 2019, link.
[2] FATF, *Terrorist Financing Risk Assessment Guidance,* 2019, see in particular paragraphs 16 and 34 to 41, link.

exposure to multilingual online radicalisation and fundraising campaigns. The assessed inherent TF threat from this category is "Medium".

1.2.2. Large international organisations: theoretical exposure

5. The threat scenario involving large international terrorist organisations, such as Islamic State (IS), Al-Qaeda (AQ) and affiliated structures, using Luxembourg's financial centre to raise or move substantial TF funds has been assessed and found to remain largely theoretical. Analysis of financial flows with 56 targeted jurisdictions (TJs) classified by terrorism impact and strategic CFT-framework deficiencies reveals that exposure of TJs represents only 2–3% of total Luxembourg financial flows. Importantly, the most exposed TJs present credible and context-specific explanations for financial linkages rooted in legitimate fund structuring, wealth management, Islamic finance and commercial trade. No evidence of materialised TF risk through these channels has been found. The assessed inherent TF threat from this category is "Low".

6. Luxembourg acknowledges its theoretical vulnerability to be misused by large terrorist financiers through corporate vehicles, NPO abuse, correspondent banking and trade finance channels, particularly given the high volume of cross-border fund structures. However, strong AML/CFT controls, the absence of any identified case and the predominance of intra-EU, small-amount TF typologies substantiate the low-threat assessment for this category.

1.2.3. Regional and global context

7. Sub-Saharan Africa, particularly the Sahel, accounts for 51% of global terrorism deaths in 2024 and remains the primary epicentre of international jihadist activity (JNIM, IS-Sahel). The Middle East North Africa (MENA) region remains volatile following the fall of the Assad regime and ongoing Israeli-Gaza conflict. Within the EU, Luxembourg's neighbouring countries, France, Germany and Belgium, experienced over half of all EU terrorist attacks during the observation period, with jihadist lone-actor attacks predominating. These dynamics are directly relevant to sectors offering basic and widely available financial services.

1.3. Vulnerability assessment – key findings

8. The vulnerability assessment, structured along six scorecard dimensions (size and structure, ownership/legal structure, products and activities, geographical exposure, clients and channels), covers all sub-sectors within the scope of the 2004 AML/CFT Law. Key findings by sector cluster are summarised below.

1.3.1. CSSF supervised sectors

9. Retail and business banks, as well as entities operating online, present the highest inherent TF risk profile within the banking sector, driven by vulnerabilities linked to high transaction volumes, widespread card and online-banking products, and exposure to cross-border clientele (with most of the clientele residing within the EU). PIs and EMIs operating all cross-border under EU passport, display "High" inherent TF risk, resulting from elevated vulnerabilities stemming from high-velocity and low-denomination transaction profiles, their use of agents and e-money distributors, and limited face-to-face client interaction. VASPs exhibit "High" inherent TF risk, given the high vulnerabilities in terms of

traceability, speed of transaction and global reach. Wholesale, corporate and investment banking, private banking, custodians, investment funds and pension funds present generally lower inherent TF risk due to sophisticated product complexity, high entry thresholds, discretionary mandates and predominantly institutional client bases.

1.3.2. Other financial and non-financial sectors

10. Life insurance, particularly unit-linked and savings products, presents a “Medium” inherent TF risk due to its cross-border distribution and investment features. Insurance intermediaries, non-life and reinsurance sectors display lower exposure. Among professionals from the non-financial sector, car dealers present high inherent risk due to their size, volume of transactions handled and potential cash transactions. Legal and accounting professions face “Medium” to “High” inherent TF risk stemming from their roles in corporate structuring and real-estate transactions. Legal persons and legal arrangements present a “Medium” to “High” inherent TF risk, reflecting inherent vulnerabilities associated with beneficial ownership transparency.

1.3.3. Non-profit organisations

11. Luxembourg's FATF NPO subset comprises approximately 1 000 ASBLs and *Fondations*, less than 11% of all registered non-profit entities. Of these, approximately 400 conduct primarily international activities, with significant presence in Sub-Saharan Africa (Cameroon, Senegal, DRC, Burkina Faso). The principal TF vulnerability for Luxembourg NPOs is not at the ownership level, beneficial owner links to targeted jurisdictions are minimal, but at the operational/geographical level: NPOs operating in countries with high terrorism impact and weak CFT frameworks face heightened risk of fund diversion at the point of distribution. The main abuse scenarios identified include: diversion of legitimate donations; sham organisations posing as genuine charities; broad exploitation of charitable mandates to channel funds to terrorist-linked individuals; and inter-NPO transfers. The FATF NPO subset's highest-risk sub-group consists of internationally active ASBLs without recognised public-utility (*“utilité publique”*) or development non-governmental organisations (DNGO) accreditation, as these do not benefit from the additional oversight and co-financing monitoring associated with those statuses.

1.3.4. Cross-sector and emerging vulnerabilities

12. Globally, cash remains a prevalent TF instrument, used for deposits, cross-border couriering and prepaid card loading. Transactions carried out *via* underground banking systems or hawala and other similar service providers (HOSSP) constitute an increasing challenge, due to the lack of traceability of these money flows. Crypto-assets, particularly stablecoins (USDT) and self-hosted wallets, are increasingly used for fundraising and fund movement, though overall volumes remain limited. Unregulated donation-based crowdfunding platforms present elevated risk pending AMLR application in July 2027. Virtual IBANs (vIBANs) and instant payments create new monitoring challenges by fragmenting financial chains and compressing response windows. Artificial intelligence (AI)-enabled forged documents, used to access regulated sectors, represent an emerging threat. The growing involvement of minors (30% of EU terrorism-related arrestees in 2024 were aged 12–20) adds a detection dimension that current CFT frameworks are not fully calibrated to address.

1.4. Mitigating factors – key findings

13. Luxembourg's AML/CFT framework rests on five pillars: i) national strategy and coordination; ii) prevention and supervision; iii) detection; iv) prosecution, investigation and asset recovery; and v) international cooperation. The 2025–2026 multi-annual AML/CFT strategy was elaborated by the Interministerial Steering Committee for the Fight against Money Laundering and Terrorist Financing (ISC) and adopted by the Government Council in February 2025. It sets four strategic priorities: enhanced ML/TF risk understanding and public-private information sharing; supervisory architecture reform through a new public authority; improved investigative and prosecutorial effectiveness; and strengthened EU and international cooperation.

14. These high-level strategic objectives of the AML/CFT strategy are translated into operational measures prioritised and implemented by operational actors through the framework of the National prevention Committee (NPC), which is chaired by the national AML/CFT coordinator and composed of representatives of the supervisory authorities (CSSF, CAA and AED), SRBs (OAL, OAD, CdN, CdH, IRE and OEC), the CRF, the investigation and prosecution authorities and the private sector. These operational members carry out the strategy in different working groups, in accordance with their respective competences and areas of expertise. Through this structured approach, successive strategic cycles contribute to further strengthen the effectiveness of the AML/CFT framework and result in operational measures that materially constrain residual TF risk across most sectors.

15. With the financial sector being most exposed to TF vulnerabilities, the CSSF maintains a robust and multi-pronged approach to supervision towards all AML/CFT-obliged financial entities, including a dedicated internal Counter-Terrorism Financing Task Force, sector-specific TF awareness campaigns, questionnaires and targeted reviews.

16. Across the non-CSSF-supervised sectors, AML/CFT mitigation rests on layered licensing and fit-and-proper regimes, annual or biennial AML/CFT questionnaires driving risk-based supervision, mandatory continuing training and active outreach, maturing private-sector controls, credible onsite/offsite inspection programmes backed by disciplinary referrals and material administrative fines, and goAML reporting underpinned by close cooperation between authorities.

17. The CRF operates the goAML platform; the extended professional TF vertical risk assessment (VRA) was disseminated in May 2024 across all sectors and its results presented in conferences, webinars, etc. Prosecution authorities apply a low-threshold preventive investigative policy, and Luxembourg recorded its first terrorism conviction in 2021 and further convictions in 2025. International cooperation through the Egmont Group and bilateral financial intelligence unit (FIU) channels is assessed as effective, with the balance of outgoing/incoming FIU requests consistent with Luxembourg's financial-centre profile.

1.5. Residual terrorist financing risk – summary by sector

18. Table 1 presents the inherent and residual TF risk levels by sub-sector following the application of mitigating measures. Residual risk levels identify priority areas for continued supervisory attention and strategic action.

Table 1: Residual TF risk, summary by (sub-)sector

Sector	Sub-sector	2026 NRA: Inherent TF risk	2026 NRA: Residual TF risk
Banks	Retail and business banks	High	Medium
	Entities operating online	High	Medium
	Wholesale, corporate and investment banks	Medium	Low
	Private banking	Medium	Low
	Custodians and sub-custodians (incl. Central Securities Depositories)	Medium	Low
Investment sector	Investment firms authorized to carry out the services of investment advice and portfolio management[3]	Medium	Low
	Investment firms authorized to carry out the services of reception and transmission of orders in relation to one or more financial instruments and of execution of orders on behalf of clients[4]	Medium	Low
	Investment firms authorized to carry out activities of dealing on own account, of underwriting of financial instruments and/or placing of financial instruments on a firm commitment basis and of placing financial instruments without a firm commitment basis[5]	Low	Very low
	Collective investments	Medium	Low
	CSSF-supervised pension funds	Very Low	Very low
Money value or transfer services (MVTS)	Payment institutions (PIs)	High	Medium
	E-money institutions (EMIs)	High	Medium
	Agents and e-money distributors acting on behalf of PIs/EMIs established in other European Member States	Medium	Medium
VASPs		High	Medium
Specialised professionals of the financial sector (PFSs)	Specialised PFSs providing corporate services	Medium	Low
	Professional depositaries	Low	Very low
	Support PFSs	Very low	Very low

[3] In the 2020 NRA: "Wealth and asset managers".
[4] In the 2020 NRA: "Brokers and broker-dealers (non-banks)".
[5] In the 2020 NRA: "Traders / market-makers".

Sector	Sub-sector	2026 NRA: Inherent TF risk	2026 NRA: Residual TF risk
Support PFSs and other specialised PFSs[6]	Other specialised PFSs		
Market operators		Low	Low
Insurance	Life insurance	Medium	Low
	Non-life insurance	Low	Low
	Reinsurance	Low	Low
	Intermediaries	Low	Very low
	Professionals of the insurance sector (PSAs)	Very low	Very low
	CAA-supervised pension funds	Very low	Very low
Real estate agents and developers	Real estate agents *(agents immobiliers)*	Medium	Medium
	Real estate developers *(promoteurs immobiliers)*	Medium	Medium
Freeport operators		Medium	Low
Dealers in goods	Precious metals/jewellers/clocks	Medium	Low
	Car dealers	High	Medium
	Art/Antiques	Medium	Medium
	Luxury goods (e.g. *"maroquinerie")*	Medium	Medium
Gambling service providers	Casino	Low	Very low
	National lottery	Low	Very low
Legal and accounting professions supervised by the AED	Accountants	High	Medium
	Professional directors and business centres	High	Medium
Legal and accounting professions supervised by SRBs	Lawyers	Medium	Low
	Notaries	High	Medium
	Court bailiffs *(huissiers de justice)*	Low	Low
	Audit profession[7]	Medium	Low
	Chartered professional accountants *(experts-comptables)*	High	Medium
Legal persons and legal arrangements	*Sociétés commerciales*	High	Medium
	Sociétés civiles	Medium	Low
	Other legal persons	Medium	Medium

[6] Analysis covered in NRA vulnerability section; Support PFSs & other specialised PFSs assessed on aggregate due to very low risk.

[7] In this document, the term "audit profession" covers statutory auditors (*réviseurs d'entreprises*), approved statutory auditors (*"réviseurs d'entreprises agréés"*), audit firms (*"cabinets de revision"*) and approved audit firms (*"cabinets de révision agréés"*).

Sector	Sub-sector	2026 NRA: Inherent TF risk	2026 NRA: Residual TF risk
	Domestic *Fiducies*	High	High
	Foreign trusts	High	High
NPOs (as per FATF definition) carrying out primarily international activities – ASBLs and *Fondations*	ASBLs without UP status or without the DNGO accreditation carrying out international activities	High	High
	ASBLs and *Fondations* with the DNGO accreditation carrying out international activities	High	Medium
NPOs (as per FATF definition) carrying out international and local activities – ASBLs and *Fondations*	International and local activities: ASBLs without UP status or without the DNGO accreditation carrying out international and local activities	Medium	Medium
	International and local activities: ASBLs with the UP status and *Fondations* carrying out international and local activities	Medium	Medium
NPOs (as per FATF definition) carrying out local activities – ASBLs and *Fondations*	ASBLs without the UP status	Low	Low
	ASBLs with the UP status and *Fondations*	Low	Low

1.6. Emerging risks and strategic priorities

19. The following emerging risk vectors warrant heightened attention:

- Digital platforms and encrypted messaging: growing use for TF fundraising and propaganda, including by minors; close coordination with relevant national actors responsible for online safety and youth awareness, as well as with law enforcement, is essential.
- Crypto-assets including stablecoins: rising adoption for TF purposes; enhanced supervisory focus on VASPs, self-hosted wallets, mixer usage and stablecoin flows is required.
- Unregulated crowdfunding: donation-based platforms outside the current supervisory perimeter until AMLR applies in July 2027 represent a material gap.
- Virtual IBANs and instant payments: monitoring complexity and reduced reaction time require sector-wide awareness and updated typologies for obliged entities.
- AI-enabled document fraud: increasing risk of forged identity documents used to access remote-onboarding financial services.
- NPO sector maturity: The non-financial sector and NPOs display lower CFT awareness relative to financial institutions (Fis); targeted outreach and a more coordinated cross-sectoral approach are recommended.
- Alternative payment systems: indications of unregistered money-transfer operations in Luxembourg linked to high-risk third countries, including via encrypted messaging groups, require continued monitoring and enforcement.

1.7. Overall conclusion

20. Luxembourg's overall TF risk profile is shaped by its position as a major international financial centre. The principal TF exposure is moderate in character, linked to the misuse of basic financial products for small-amount, cross-border transactions by individuals connected to jihadist and extreme-right wing networks operating predominantly within the EU. The threat from large international terrorist organisations using Luxembourg's financial centre to move significant TF flows remains theoretical, with no evidence of materialisation. Luxembourg's AML/CFT framework, anchored by effective and multi-pronged supervision, the CRF's operational capacity and a mature detection, investigation and prosecution infrastructure, provides meaningful mitigation, resulting in residual risk levels that are generally low to medium across most sectors.

21. Priority sectors requiring continued supervisory focus are: retail and business banks and entities operating online; PIs and EMIs; VASPs; internationally-active NPOs; and professionals providing trust and company service provider (TCSP) services and/or involved in real estate transactions. Emerging vectors, crypto-assets, digital platforms, unregulated crowdfunding, vIBANs and AI-enabled fraud, demand proactive adaptation of the Luxembourg CFT framework in advance of forthcoming EU regulatory milestones, including the application of the AML Regulation in July 2027.

2. Luxembourg context

22. The Grand-Duchy of Luxembourg (or "Luxembourg") is a small, landlocked country in Western Europe bordered by Belgium, France and Germany. With an area of 2 586 km2, it is one of the smallest sovereign states in Europe.

23. Luxembourg has been a sovereign and independent state since the adoption of the Treaty of London on 19 April 1839. The Grand-Duchy is also a founding member of the European Union (EU), OECD, United Nations, NATO, UNESCO, the World Trade Organisation, and Benelux Union reflecting its political consensus in favour of economic, political, and military integration. Luxembourg has always been committed to multilateral and international cooperation and considers itself to be a defender of international agreements and treaties.

24. Luxembourg is home to many European institutions, including the Secretariat of the European Parliament, the Court of Justice of the EU, the European Investment Bank, the European Public Prosecution Office (EPPO), the European Court of Auditors and some Directorate Generals of the European Commission. Luxembourg-City is one of the three "capitals" of the EU along with Brussels and Strasbourg.

2.1. Luxembourg's demographic structure

25. As of 1 January 2025, Luxembourg counts 681 973 inhabitants. Although among the least populous countries in the EU, the number of habitants has increased by around 18% compared to 2015.

26. In the beginning of 2025, people from EU Member States (other than Luxembourg) account for 36% of the resident population and 76% of the foreign population living in the Grand-Duchy. The Portuguese nationality is the first foreign nationality in the country with around 90 000 persons (13% of the total population) followed by the French (7%), Italian (4%) and Belgian (3%) nationalities[8]. The most recent population census in 2021 notes that almost three quarters (73,7%) of Luxembourg's population has a migratory background (i.e., with at least one parent born abroad)[9]. Luxembourg is also member of the Schengen area.

27. Similar to the situation described in the 2025 NRA ML, the unemployment rate remains low (around 6%)[10] and a considerable share of Luxembourg's workforce are non-residents living in France, Germany or Belgium and commuting to Luxembourg for work. Luxembourgish, French and German are the three official languages. English is used in certain professional environments, notably in banking and finance.

[8] LUStat Population by sex and nationality on 1st January (x 1 000), link retrieved on 30 September 2025.
[9] STATEC, link. Note that data refers to the most recent population census in 2021.
[10] Adem, *Indicateurs du marché de l'emploi,* link retrieved on 30 September 2025.

2.2. Luxembourg's economy

28. Luxembourg's economy is open, dynamic and fast growing with a gross domestic product (GDP) at market prices of EUR 86,180 billion in 2024, thus contributing to 0,05% of the total EU GDP in 2024[11].

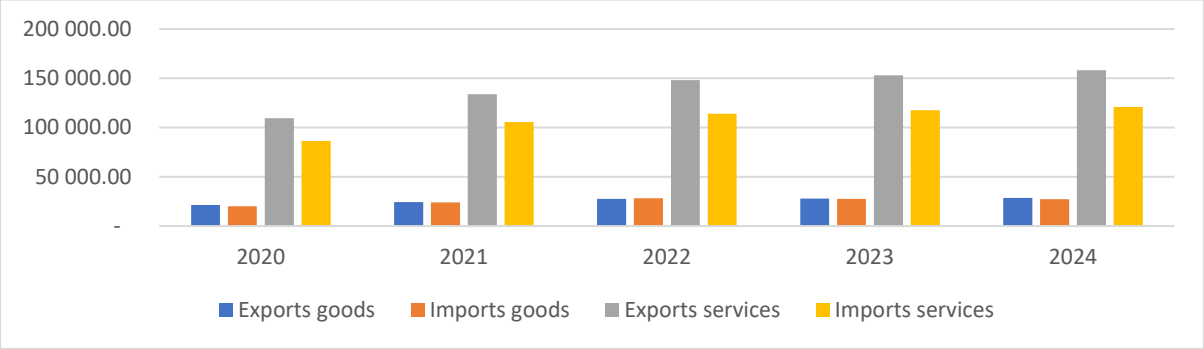
Table 2: EU27 vs. Luxembourg real GDP growth, 2020–2024[12]

	2020	2021	2022	2023	2024	2020 – 2024
EU27	-5,6	6,3	3,5	0,4	0,9	1,1
Luxembourg	-0,5	6,9	-1,1	0,1	0,4	1,16

29. In 2024, Luxembourg continued to have the highest real GDP per capita among the EU Member States, with approximately EUR 127 030, more than three times above the EU average (EUR 39 870)[13]. This is mainly due to the considerable number of non-residents being employed in the country. The latter contribute to its GDP while not being part of Luxembourg's resident population.

30. Luxembourg's current account is heavily influenced by the importation and exportation of services (especially services related to financial and insurance activities). As illustrated in figure below, Luxembourg is essentially an export country of services.

Figure 1: Annual current account of Luxembourg (in millions of euros; BPM6 methodology)[14]



31. Taking a closer look at Luxembourg's key activities, the financial and insurance sector accounts for the biggest share of Luxembourg's economy with 27% of the national GDP being generated by the said sector. Indeed, Luxembourg is an important financial centre in the EU, ranked 19th in the Global Financial Centres Index[15] and 9th worldwide as a green financial centre[16]. The financial centre is diversified with a core focus on banking, investment funds (primarily asset servicing), payment services, insurance (life, non-life and reinsurance) as well as capital markets (notably listing and post-

[11] Eurostat, Gross domestic product at market prices, link retrieved on 30 September 2025.
[12] Eurostat, Real GDP Growth Rate – volume, link retrieved on 30 September 2025.
[13] Eurostat, Gross domestic product at market prices, link retrieved on 30 September 2025.
[14] LUStat, Annual current account of Luxembourg (in millions of euros; BPM6 methodology), link retrieved on 30 September 2025.
[15] The Global Financial Centres Index 38, 2025, link.
[16] Global Green Finance Index 15, 2025, link.

trade services). Luxembourg acts as an EU hub and competence centre for international financial institutions (FIs) in these areas[17,18].

- **Banking activity:** As of December 2024, Luxembourg counts over 110 banks employing over 26 000 employees. Wholesale, corporate and investment banking, depositary and sub-custody bank as well as private banking (including wealth management) are core activities for Luxembourg banks.
- **Asset management:** Luxembourg has been a first mover in the internationalisation of the investment fund industry that has occurred over the last 40 years. Today, fund initiators from 67 countries world-wide make use of Luxembourg undertaking for collective investment in transferable securities (UCITS) funds to distribute in 80 countries globally[19].
- **Payment services:** Leading international players in the payments sector have chosen Luxembourg as their hub to offer payment related services, often in connection to the development of e-commerce platforms[20].
- **Insurance:** Luxembourg's stability and asset management ecosystem are significant draws for insurance firms, whose business is the management of risk. While Luxembourg's insurance ecosystem traditionally focused on life insurance and reinsurance, post-Brexit the Grand-Duchy has increasingly taken on an important role as a major European hub for non-life insurance.
- **Capital markets:** Luxembourg is home to the Luxembourg Stock Exchange (LuxSE) and the Luxembourg Green Exchange (LGX). Luxembourg is also a centre for all aspects of collateral managements including clearing, settlement, custody and asset servicing, with the presence of one the largest International Central Securities Depositary. The Grand-Duchy is also a centre for securitization and structured finance vehicles.

32. The activities of the financial centre are also diversifying into the field of crypto-assets, FinTech, sustainable finance and Islamic Finance. Luxembourg for Finance is the country's agency for the development and promotion of the financial centre.

33. TF vulnerabilities of the financial and insurance sectors are analysed under sections 10.1 and 10.2.

International business: partner countries

34. Considering the limited size of the country and its geographical position, international trade and business is a key component of Luxembourg's economic landscape. Taking a closer look at the foreign direct investment (FDI) stocks, Luxembourg was a net foreign direct investor at the end of 2021, 2022, 2023 and 2024. Together with the Netherlands, Luxembourg accounted for the most important shares of the total inward and outward investment positions of the EU countries. However, for those two countries Special Purpose Entities play a significant role[21], which underlines the importance of Luxembourg as a key hub for structuring cross-border investments and financial services. Nonetheless,

[17] Luxembourg for Finance, *Luxembourg: helping finance go global,* 2023, link.
[18] Luxembourg for Finance, Homepage, link retrieved on 30 September 2025.
[19] Luxembourg for Finance, *Luxembourg: helping finance go global,* 2023, link.
[20] Luxembourg for Finance, *Fintech,* 2022, link.
[21] Eurostat, Foreign direct investment – stocks, link.

it should be noted that the usage of those Special Purpose Entities in Luxembourg has gradually declined over the past few years[22].

Table 3: Net year-ending FDI position of Luxembourg by partner (in millions of EUR), 2021-2024[23]

Year	Outward FDI	Inward FDI	Net FDI
2021	3 948 849	3 136 112	812 737
2022	3 877 393	2 918 822	958 571
2023	3 589 103	2 583 535	1 005 568
2024	3 787 819	2 695 814	1 092 005

35. Both Luxembourg's outward and inward FDI stocks were somewhat concentrated and top-ten countries accounted for about 78% of total stocks between 2021 and 2024.

36. The following table lists top-ten inward FDI countries.

Table 4: FDI position (inward stock) by top-ten partner (in millions of EUR), 2021-2024[23]

Partner country	2021	2022	2023	2024	2021 – 2024 share
United States	813 958	809 475	547 926	618 409	24,7%
United Kingdom	395 985	248 029	274 761	238 434	10,2%
Ireland	230 770	185 610	178 854	313 951	8,0%
Netherlands	248 380	237 760	192 958	206 309	7,8%
Cayman Islands	169 053	185 705	209 989	187 536	6,7%
Canada	136 675	148 512	143 329	126 927	4,9%
Germany	133 700	121 013	142 204	145 566	4,8%
Belgium	130 023	125 762	122 958	118 630	4,4%
Bermuda	131 659	136 294	63 292	54 470	3,4%
British Virgin Islands	87 111	89 900	92 615	114 327	3,4%

37. All European countries (including the United Kingdom) accounted for almost 40% of Luxembourg's inward investments. In addition, the United States alone represented about 25% of the inward investment stock in the same period.

38. The following table lists top-ten outward FDI countries.

Table 5: FDI position (outward stock) by top-ten partner (in millions of EUR), 2021-2024[23]

Partner country	2021	2022	2023	2024	2021 – 2024 share
United States	610 602	646 724	591 929	701 892	16,8%
United Kingdom	666 939	479 029	473 493	499 030	14,0%
Netherlands	511 994	449 690	421 005	425 859	11,9%
Switzerland	329 240	325 503	268 346	259 984	7,8%
Germany	246 308	213 328	232 826	223 691	6,1%

[22] Eurostat, EU direct investment positions by country, ultimate and immediate counterpart and economic activity (BPM6), link retrieved on 3 October 2025.

[23] LuStat, Net year-ending foreign direct investment position of Luxembourg by partner according to the extended directional principle (in millions of euros; 4th OECD benchmark definition), link retrieved 26 January 2026.

Partner country	2021	2022	2023	2024	2021 – 2024 share
Ireland	280 700	259 395	127 881	129 619	5,3%
France	146 822	178 752	190 537	209 961	4,8%
Belgium	121 704	141 266	135 455	132 300	3,5%
Spain	92 755	119 676	119 753	121 921	3,0%
Italy	94 104	99 205	96 193	114 946	2,7%

39. As shown in the table above, Luxembourg's outward FDI was concentrated towards European countries (including the United Kingdom). The United States accounted for another 17% of the stock.

40. To obtain a more in-depth understanding of the general risk and context of Luxembourg's key partner countries in terms of FDI, the FATF mutual evaluation reports of the United States, the United Kingdom, Ireland and the Netherlands, representing together approximately half of Luxembourg's inward and outward stocks for the 2021-2024 period, were studied.

41. All four studied key partner countries have been assessed by the FATF to have effective AML/CFT regimes in place and to provide good international cooperation. TF related to small-amounts, often self-funded and/or raised through NPOs are key typologies cited. This is of particular importance when assessing the overall Luxembourg TF threat context in section 9.

3. Approach and methodology

42. To conduct the assessment, the approach outlined in the FATF TF risk Assessment Guidance (2019) for assessing TF risks in jurisdictions with financial centres and low domestic terrorism risk, which is suitable for Luxembourg's particular situation, was followed[24]. Furthermore, this report leverages on guidance and reports issued by the FATF[25] and other international bodies[26]. The observation period of this analysis covers the years 2021 to 2024, included.

43. Public and private sector stakeholders were engaged for this analysis in order to come to a comprehensive national understanding of Luxembourg's TF threat context, resulting vulnerabilities and mitigating measures.

44. Following the national risk assessment methodology, inherent risk is a factor of threats and vulnerabilities, and the impact of mitigating measures results in a level of residual risk. Consequently, this report is the result of the assessment of the TF threat, the vulnerabilities to TF and the effectiveness to combat TF.

45. First, the threat assessment presents the types of terrorist and extremist actors, their ideologies, their larger or smaller financial TF needs and operation in the three stages of TF (rising, moving, using) and place them in the global, European and Luxembourgish contexts. Then, the threat assessment analyses how Luxembourg may be exposed to these actors by analysing Luxembourg financial and non-financial links to a selection of jurisdictions that may present a TF threat.

46. Second, the vulnerability assessment covers all sub-sectors in the scope of the 2004 AML/CFT Law and follows a scorecard approach similar to the one used in the 2025 NRA ML and the previous NRA of ML/TF (2018, 2020), taking into account the specificities of TF for the six vulnerability dimensions under review (structure, ownership/legal structure, products and activities, geographical exposure, clients/transactions and channels).

47. Lastly, the report analyses the impact of existing mitigating factors in order to determine the residual TF risk level of the different sub-sectors follows a scorecard approach similar to the one used in the 2025 NRA ML taking into account the specificities of TF for the six dimensions under review: market entry controls; understanding of TF risks and AML/CFT obligations; prevention/private sector controls; supervision and enforcement; and detection, prosecution and asset recovery). Considering Luxembourg's commitment to continuously enhance its AML/CFT framework, the findings of the inherent risks and the impact of mitigating factors as well as the outcomes in residual risks constitute a key element to develop the national multi-annual AML/CFT strategy.

3.1. Assessment process and involvement of stakeholders

48. The NRA exercise involves defining the scope, granularity and approach up front, collating relevant national and international data and information, reviewing and refining hypotheses

[24] FATF, *Terrorist Financing Risk Assessment Guidance,* 2019, see in particular paragraphs 16 and 34 to 41, link.
[25] E.g. FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025, link.
[26] E.g. Institute for Economics & Peace, Global terrorist Index, 2025, link or Europol, *European Union Terrorism Situation and Trend Report*, 2025, link.

developed using expert opinion, iterating intermediate outputs with the relevant experts, and agreeing final outputs and improvement measures resulting from the assessment.

49. Throughout the steps of the NRA, multiple public and private stakeholders are involved:

- Supervisory authorities:
  - Commission de Surveillance du Secteur Financier (CSSF)
  - Commissariat aux Assurances (CAA)
  - Administration de l'enregistrement, des domaines et de la TVA (AED)
- Self-regulatory bodies (SRBs)
  - Ordre des Experts-Comptables (OEC)
  - Institut des Réviseurs d'Entreprises (IRE)
  - Chambre des Notaires (CdN)
  - Ordre des Avocats de Luxembourg (OAL)
  - Ordre des Avocats de Diekirch (OAD)
  - Chambre des Huissiers de Justice (CdH)
- Ministries and administrations:
  - Ministry of Justice (MoJ)
  - Ministry of Finance (MoF)
  - Ministry of Economy (MoE)
  - Ministry of Foreign and European Affairs, Defence, Development Cooperation and Foreign Trade (MoFA)
  - Administration des contributions directes (ACD)
  - Administration de l'enregistrement, des domaines et de la TVA (AED)
  - Administration des douanes et accises (ADA)
- Cellule de renseignement financier (CRF)
- Investigative authorities
  - Offices of the investigative judge of the Luxembourg District Court
  - Judicial Police Service (SPJ)[27]
- Prosecution authorities:
  - General State Prosecutor's Office
  - State Prosecutor's Office of the Luxembourg District Court
- Asset management and asset recovery authorities:
  - Asset Management Office (AMO)
  - Asset Recovery Office (ARO)
- Professional associations:
  - The Luxembourg's Banker's Association (ABBL)
  - Luxembourg Insurance and Reinsurance Association (ACA)
  - Association of the Luxembourg Fund Industry (ALFI)
- Private sector representatives
- NPO sector representatives
- Others:
  - Luxembourg Business Registers (LBR)
  - Luxembourg Central Bank (BCL)

[27] The SPJ is the department within the Grand-Ducal Police (PGD) in charge of executing most orders from the State Prosecutors and the investigative judges.

50. Different stakeholders were engaged throughout the risk assessment process. For the threat assessment, the analyses were performed together with the prosecution authorities, the CRF, and with additional inputs from other agencies. The vulnerability assessment primarily involved supervisors and SRBs as stakeholders, with additional information from other agencies, such as the LBR or the BCL. To understand the impact of mitigating factors on inherent risks, and similar to the inherent risk assessments, data requests were sent to supervisors, SRBs and prosecution authorities. Representatives of the private sector, notably professional associations from the private sector (such as ABBL, ALFI and ACA), as well as a panel of the private sector representatives selected specifically for this NRA on the basis of sub-sector materiality and risk, provided further contextual and expert information to complement the risk assessment process.

51. Data requests were sent to the supervisors, SRBs and prosecution authorities to collect relevant data. Bilateral meetings and workshops were held with stakeholders to collect expert insights on the threat and vulnerability status in Luxembourg, identify additional data points to be collected and validate hypothesis on the levels of inherent risk. Following the data and input collection, findings were summarized in an NRA text narrative and scorecards. These were reviewed by the stakeholders via written communication and additional bilateral meetings. This process allowed for increasingly granular analysis, with follow-up communications typically focusing on higher TF related risk areas.

3.2. Inputs used

52. The sources of data and information used to conduct the said assessment can be broadly categorised into five groups: quantitative data from stakeholders, publicly available information, documents describing mitigating factors, expert inputs and judgement from stakeholders, case studies and typologies.

53. Quantitative data from stakeholders was collected through standardised data requests and through follow-up requests for specific data points. Standardised data requests were sent to supervisors to collect data on vulnerabilities and mitigating factors and to prosecution authorities to collect data on threats and mitigating factors. Each data point in the data request could be mapped against a scorecard criterion for threats, vulnerabilities or mitigating factors. In some cases, additional data was requested, for example, to further develop the understanding of particular higher TF related risk factors.

54. Publicly available quantitative data included both international and domestically available data sets. For example, international data sets from various sources were used, such as Europol, the FATF (such as country lists and the results of the 4th round of mutual evaluations) and academia (such as the Global Terrorism Index). Domestic data sources were used to complete international data sets (e.g. data provided by judicial authorities including the CRF, the BCL or the LBR).

55. On top of quantitative data reflecting the efficiency of mitigating factors (such as resources at the supervisor and supervised entity level, sanctions, etc.), documents describing mitigating factors were provided by stakeholders for the mitigating factors section in the NRA. Agencies also provided information on published circulars, guidance, FAQs, and other published materials.

56. Expert inputs and judgements were used to enhance the analyses of threats, vulnerabilities and mitigating factors. For the threats assessments, interviews and dedicated workshops were used to

receive expert inputs on the threat context, understand recent developments and to identify areas where additional data is needed. Similarly, for the vulnerability assessments, interviews were used to receive inputs on high-risk dimensions of different sub-sectors, understand the sub-sectoral developments over the past four years and identify additional data points to be collected. For the mitigating factors, interviews were used to collect additional information on mitigating factors in place, identify key changes in the mitigating factors over the past four years and key future development areas.

57. Case studies and typologies were collected from different agencies and public sources to enhance the vulnerability assessment of sub-sectors further. Typologies from public sources (e.g. FATF) were used to illustrate the TF drivers of sub-sectors observed globally; and Luxembourg stakeholders provided anonymised case studies on previously observed suspicious behaviour. It should be noted that any person mentioned in the case studies of this report are presumed innocent until a final judicial decision is rendered.

58. From the data limitations perspective, note that for cases where information was missing, the assessed level of risk has been increased, in line with a conservative approach recommended by the FATF.

3.3. Methodology

59. The following table defines key concepts used throughout this assessment:

Table 6: Methodology – key definitions[28]

Term	Definition
Threat	A "TF threat" is a person or group of people (natural or legal persons) with the potential to cause harm by raising, moving, storing, or using funds or other assets (whether from legitimate or illegitimate sources) for terrorist purposes. TF threats may include domestic or international terrorist organisations and their facilitators, their funds, as well as past, present and future TF activities, and individuals and populations sympathetic to terrorist organisations.
Vulnerability	The concept of "vulnerability" comprises those things that can be exploited by the threat or that may support or facilitate its activities. In the context of TF, vulnerabilities may include features of a particular sector, a financial product or type or service that makes them attractive for TF. There may be some overlap in the vulnerabilities exploited for both ML and TF.
Consequence	The concept of "consequence" refers to the impact or harm that TF threat may cause if eventuated. This includes the effect of the underlying terrorist activity on domestic or institutional financial systems and institutions, as well as the economy and society more generally. Notably, consequences of TF are likely to be more severe than for ML or other types of financial crime (e.g., tax fraud), which impacts how countries respond to identified threats. Consequences of TF are also likely to differ between countries and between TF channels or sources, and may relate to specific communities or populations, the business environment or national interests.

[28] Definition of "TF Risk", and its factors (threat, vulnerability and consequence) are sourced from FATF, *Terrorist Financing Risk Assessment Guidance,* 2019, paragraph 15, link.

Term	Definition
Risk	A TF risk is a function of three factors: threat, vulnerability, and consequence.
Inherent risk	Inherent risk is defined as the risk of TF *before* mitigating actions are applied.
Mitigating factor	All elements in place in terms of legal, judicial, supervisory and institutional framework that contributes to combat TF (in one or various sub-sectors).
Residual risk	Residual risk is defined as the level of TF risk *after* mitigating measures are applied.

3.3.1. Threats assessment

60. The threat assessment begins with a presentation of the TF stages, the different types of terrorist ideologies and terrorist actors, and categorises them according to their varying financial needs. The aim of this section is to obtain an in-depth understanding of their operational structure, modus operandi and financial activity. With regard to the different stages of TF, this section sheds light on how these actors raise, move and use funds for terrorist purposes. Then, the threat assessment analyses the terrorist threat context in relevant world regions particularly impacted by terrorism, the EU and in Luxembourg. This allows to allocate each type of actor previously identified to a geographical area of operation.

61. Then, Luxembourg's TF threats are analysed with regard to actors needing lower TF funds on the one hand and with regard to actors needing larger TF funds on the other. Whereas the former leverages on CRF's observations and analysis on the field, the later focuses on the analysis of financial and non-financial flows with jurisdictions that may present a potential TF risk either because they are particularly impacted by terrorism within their territory and/or because they present strategic deficiencies in their AML/CFT framework[29]. The methodology followed to elaborate the list of these jurisdictions selected for analysis is detailed in Appendix A.

3.3.2. Vulnerabilities assessment

62. For the vulnerabilities assessment, a three-step approach is used:

1. Definition of the assessment criteria;
2. Data and expert input are gathered for each criterion and information is translated into a vulnerability ranking; and
3. Ratings are aggregated into a sub-sector rating and findings are summarised in the NRA text narrative.

63. The vulnerabilities assessment involves sectors not mapped based on activity but on supervisory set-up[30]. This approach is similar to the one used in the 2025 NRA ML and the previous NRAs of ML/TF (2018, 2020), taking into account the specific adjustments for TF. The scorecard dimensions used to assess vulnerabilities were adjusted from the NRA scorecards to account for TF-specific drivers. The scorecard dimensions used in this risk assessment consist of six criteria:

- Size and structure: Extent to which the scale, fragmentation and complexity of the sector offer opportunities for TF. This dimension considers factors such as the relevance of the sector

[29] Pursuant to their results of the 4th round of mutual evaluations performed by the FATF (or other FATF-style regional body), especially with regard to Immediate Outcome 9.
[30] This is based on the legal framework of the supervisory set-up with authorities.

based on observed domestic and international typologies and the relevance of the sector in the national economy.

- Ownership/legal structure: Describes the ownership structure of professionals operating in Luxembourg.
- Products and activities: Extent to which products or activities are susceptible to TF. This dimension considers factors such as suitability and availability of products and/or activities for TF, and their prevalence in the sector.
- Geographical exposure: Extent to which funds are being moved to and from international jurisdictions.
- Clients: Extent to which clients have a higher exposure to TF. It includes a consideration of factors, such as the number of clients being politically exposed persons (PEPs) residing in countries particularly impacted by terrorism or clients involved in activities with a higher exposure to TF.
- Channels: Extent to which distribution methods are attractive to carrying out TF. It includes factors such as the nature of client interaction (e.g. via intermediaries, online) and transparency and traceability features to move funds.

64. As explained earlier, quantitative and qualitative data are gathered from national data sources (some public, some confidential) along the dimension of the assessment criteria. The data and information collected are then translated into an informed vulnerability rating on a scale of 1 to 5 against each criterion (5 representing highest impact of vulnerability to TF). When valuable, expert opinion is used to enrich the analysis.

65. The aggregate inherent risk score for each sub-sector is calculated by averaging the scores against each criterion. Equal weighting is given to each criterion. The aggregate inherent risk score is then mapped to one of the five outcome levels, ranging from "Very low" to "Very high". The risk level outcomes are specified in Appendix A. A separate vulnerability inherent risk outcome is assigned to each sub-sector following the scorecard approach described above. The resulting assessment is described in the vulnerabilities assessment section of this NRA.

66. The scorecards, together with the dimensions for inherent and residual risk, are provided in Appendix A.

67. In addition, cross-sector vulnerabilities are described separately, without assigning them an inherent risk level.

3.3.3. Mitigating factors assessment and residual risk

68. Following the inherent risk assessment, the impact of mitigating factor are assessed, resulting in a residual risk score. An effective system is one that "properly identifies, assesses and understands is money laundering and terrorist financing risks. […] A country also co-operates and co-ordinates domestically to develop AML/CFT policies"[31]. The aim of this part of the NRA is to establish an accurate and factual picture of the results and effectiveness of the current AML/CFT framework in mitigating inherent TF risk, and to identify improvement measures that can be implemented within the current

[31] FATF, *Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT/CPF Systems,* 2022, link.

framework or taken forward in subsequent national AML/CFT strategic cycles, thereby contributing to the continuous strengthening of the framework's risk mitigation capacity.

69. A three-step approach is followed to assess the impact of mitigating factors:

1. Definition of assessment criteria;
2. Collection of data and information for each criterion and translation into a rating against each criterion; and
3. Aggregation of ratings into a sub-sector rating and translation of findings in NRA text narrative.

70. To assess the impact of mitigating factors, discussions with concerned stakeholders are held to obtain relevant insights with respect to the full lifecycle of supervision, detection and enforcement. The results/effectiveness dimensions are then used to inform the scorecard criteria, which include five different dimensions and nine sub-dimensions or criteria:

- Market entry controls (including authorisation and breaches);
- Understanding of TF risks and AML/CFT obligations (including understanding of TF risks and AML/CFT obligations and regulation & information);
- Prevention/private sector controls (including TF controls in place and internal supporting structures);
- Supervision and enforcement (including level of supervision and enforcement); and
- Detection, prosecution and asset recovery.

71. Considering that ML and TF share a common legal framework, the scorecard approach used for the assessment of the impact of the mitigating measures is similar to the one applied in the 2025 NRA ML. Note that particular attention has been granted to specific CFT actions carried out by relevant stakeholders (for instance, supervisory measures including TF specific awareness actions, webinars, questionnaires).

72. As with the inherent risk assessment, a combination of research, data, expert judgement and bilaterial discussions with concerned stakeholders is used to assess the impact of mitigating factors in place along each of the criteria in the scorecard, on a scale from 1 (least level of impact) to 5 (highest level of impact in reducing inherent risk). Luxembourg-specific data is collected from a wide range of sources, such as annual reports (e.g. CRF, CSSF, CAA, AED), statistics (e.g. STATEC) and non-publicly available data (e.g. data sourced from AML/CFT questionnaires compiled by supervisory authorities and SRBs). The assessment is also based on expert judgement which is formed through agency interactions.

73. An overall score on the mitigating factors in place is obtained by averaging the scores across the criteria and "bucketing" these in five possible outcomes: "Limited or no mitigating factors", "Some mitigating factors", "Significant mitigating factors", "High mitigating factors", and "Very high mitigating factors". The aggregated outcomes for mitigating factors correspond to a reduction in inherent risk of 0, -0,5, -1, -1,5 and -2 respectively.

74. Finally, the residual sub-sector risk score and corresponding level is obtained by taking the inherent risk score outcome (1 to 5) and subtracting the mitigating factors outcome (i.e. reducing the score by 0, 0,5, 1, 1,5 or 2 points). An illustration of the residual risk calculation, together with an illustrative example, is provided in Appendix A. The residual risk assessment considers the remaining

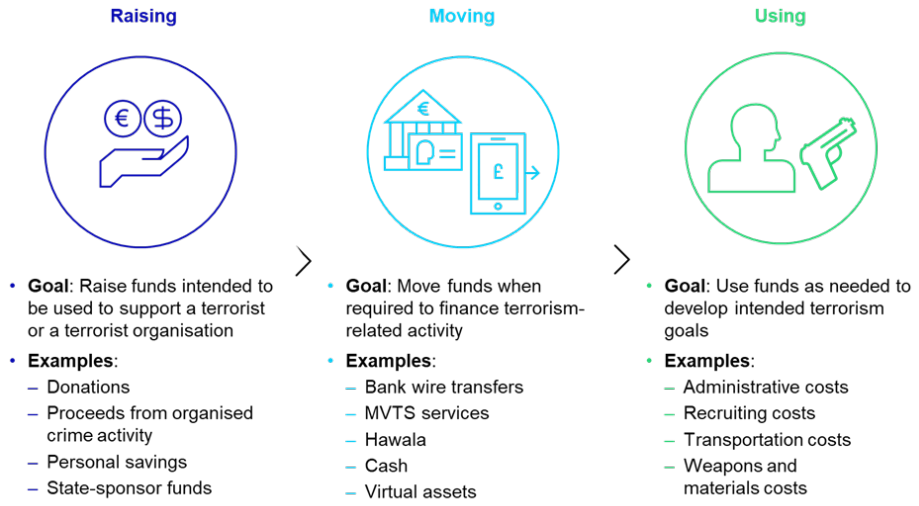
level of TF risk after the implementation of mitigating measures. It identifies areas where Luxembourg remains most exposed and provides a basis for developing and prioritising actions, either within the current framework or in subsequent strategic cycles, to further enhance the effectiveness of the national AML/CFT regime. Similar to the assessment of the sectorial inherent risk, the resulting residual risk level is agreed in conjunction with the concerned authorities and SRBs.

4. Introduction to terrorist financing stages and threats

4.1. Terrorist financing stages

75. This report covers the three stages of TF (raising, moving and using funds) to meet the operational needs of a terrorist actor or organisation. The figure below illustrates these stages.

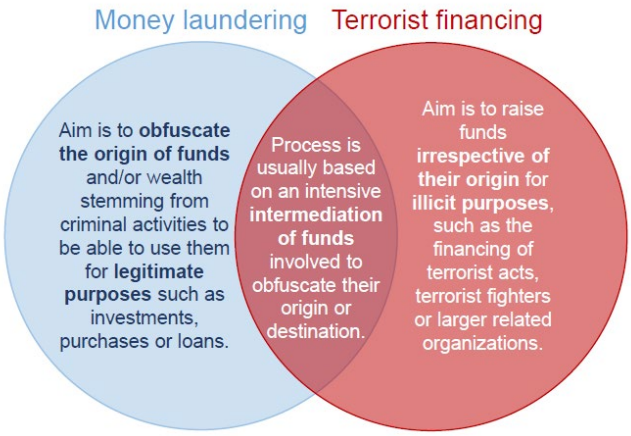
Figure 2: Terrorist financing stages



76. International financial centres such as Luxembourg may be vulnerable to misuse for the movement, management or storage of terrorist-linked assets, given the high volume and cross-border nature of the assets they handle[32].

77. TF risks are nonetheless distinct from ML. ML obfuscates the criminal origin of funds in order to reintroduce them as legitimate; TF aims to fund terrorist activity regardless of whether the source is legitimate or illicit. Overlaps occur where intensive intermediation is used to conceal origin or destination[33].

Figure 3: TF vs. ML



[32] FATF, *Terrorist Financing Risk Assessment Guidance,* 2019, paragraph 39, link.
[33] FATF, *Terrorist Financing Risk Assessment Guidance,* 2019, paragraphs 17 and 18, link.

78. Unlike ML, where the source of funds and source of wealth are central, the destination of funds is primordial in CFT.

79. CFT operates on two complementary tracks: targeted financial sanctions, which require the immediate freezing of assets of designated persons or entities; and detection of TF, which identifies persons and entities financially linked to known terrorism but not yet designated[34].

4.2. Terrorist actors and their financing needs

80. Terrorist actors differ in organisation, motivation and operations and accordingly use different means to raise, move and use funds. The actors below are considered in the analysis.

4.2.1. Decentralised networks, small terrorist cells and lone actors

81. These actors have low financial requirements given the low-scale nature of their attacks and the basic procurement involved (vehicles, bladed weapons, online services). Funds typically blend legitimate sources, salaries, social aid, small loans, with proceeds from petty crime such as drug trafficking. Expenses are low or nil and rarely diverge from normal transactions, leaving few or no red flags. Detection therefore relies heavily on ideological indicators (e.g. propaganda activity) and weak signals derived from financial information. For instance, all completed Jihadist terrorist attacks in 2024 were perpetrated by lone attackers using unsophisticated and easily accessible weapons (e.g. knives)[35], as mentioned above.

82. Extreme-right and ethno-nationalist movements are often international in nature and operate as decentralised networks. Where these movements are not designated, proscribed or recognised as terrorist, their fundraising activities are not unlawful unless directly linked to a violent attack and may take place openly through rallies or online campaigns. Other recurring income streams are membership fees and online sales of music, literature and merchandise.

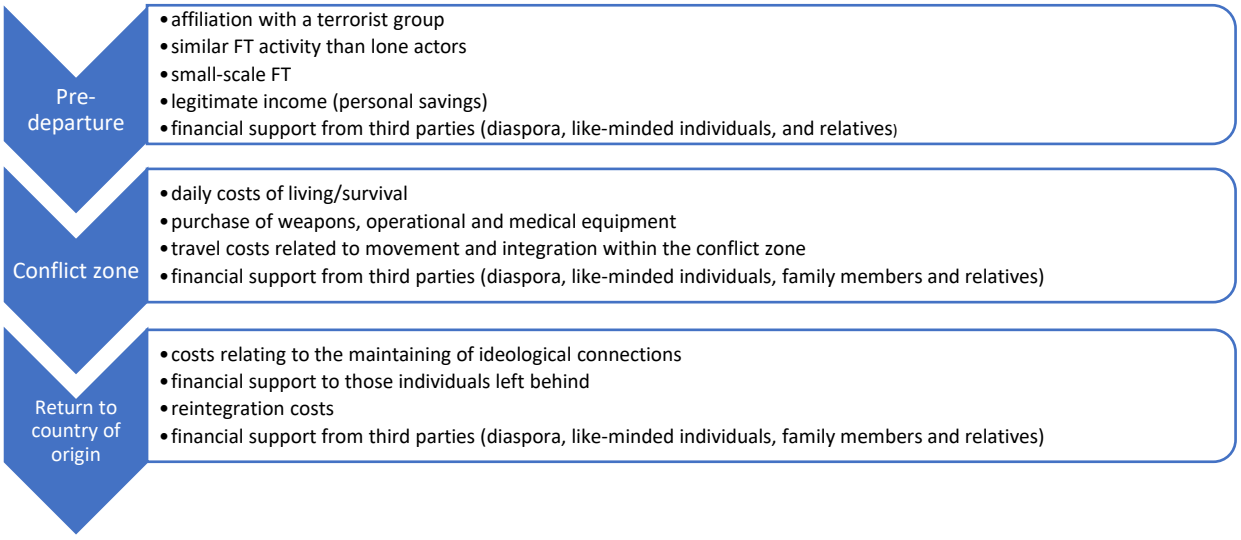
4.2.2. Foreign terrorist fighters

83. The United Nations Security Council resolution (UNSCR) 2178 defines foreign terrorist fighters (FTFs) as "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, including in connection with armed conflict"[36].

84. Financial activity of FTFs varies with the stage of preparation and deployment, as illustrated in Figure 4.

[34] Countering Terrorist Financing, EBA, link.
[35] EU TE-SAT 2025, link.
[36] United Nations Security Council, Resolution 2178 (2014), 2014, link

Figure 4: FT activity of FTFs according to their location



85. Pre-departure: FTFs typically affiliate with a target organisation. Financing resembles that of non-traveling lone actors, salaries, social aid, loans, savings, occasionally complemented by donations (cash, crypto-assets, encrypted platforms) from like-minded individuals, relatives or diaspora.

86. In conflict zones: spending covers travel and living costs plus operational equipment (weapons, medical supplies), inter-zone movements, and payments to local officials or community leaders for protection and information.

87. Pre-return and on arrival: larger sums to traffickers and smugglers have been observed pre-return; on arrival, integration costs (legal, living), funding to maintain ideological networks, and ongoing support to those left in the conflict zone are typical.

88. Historically, FTF trails were straightforward; small cash amounts physically transported, complemented by informal banking systems and HOSSPs, with ATM withdrawals and card payments near final destinations in border regions (the principal transit hubs). More recently, trails have diversified: false-identity bank cards, third-country cards linked to e-wallets, crypto-assets, prepaid cards, encrypted messaging and complicit businesses in conflict zones. The geographical scope has widened from Iraq/Syria to parts of Africa and Afghanistan[37]. Europol notes that, given the situation in Syria, captive militants may be released, and EU nationals may seek to return[38].

Case study 1: Luxembourg suspect using layering techniques to collect and move funds for an FTF in Syria[39]

A person in Luxembourg is suspected to have used layering techniques and multiple transfer steps to collect and move funds for an FTF in Syria. The person is suspected to have collected funds via bank transfers in Luxembourg. Money mules, fake online accounts, foreign bank accounts, as well as electronic wallets and cryptocurrencies were suspected to be involved in this illicit financial network.

[37] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025, link , CTED Trends Tracker – Evolving Trends in the Financing of Foreign Terrorist Fighters' Activity: 2014 – 2024, 2024, link.
[38] EU TE-SAT 2025, link.
[39] Case study taken from EU TE-SAT 2024, link.

4.2.3. International terrorist organisations, linked and affiliated structures

89. International terrorist organisations vary in size, structure, reach, motivation and capability. Financial requirements track centralisation: more centralised structures must cover recruitment, fighter remuneration, support for families of dead or imprisoned members, weapons procurement and training.

90. Funding combines criminal activities (extortion, smuggling, human trafficking), abuse of legitimate businesses and NPOs, digital fundraising and crowdfunding, crypto-assets and social-media campaigns (see section 4.3.5.3). Worldwide propaganda is itself a significant expenditure that sustains recruitment and donor flows; merchandise (flags, t-shirts) is a further income line.

91. Territorial control materially shapes financing. Where governance is weak, organisations levy taxes or fees in exchange for security, tax trade routes, and, where natural resources are present, exploit and traffic them. Controlled territory in turn generates expenditure obligations (services, infrastructure); loss of territory is therefore a key risk variable.

92. A recent trend is the rise of decentralised regional hubs affiliated or linked to core organisations: more agile, locally adapted, and diversifying the core group's funding base geographically and by channel, with lower operational footprint and lower financing needs. Overall, these organisations finance themselves through natural-resource exploitation, criminal activities, donations channelled through social media, cash couriers, mules, HOSSPs and crypto-assets[40].

4.2.4. Other terrorist actors

93. The US Secretary of State defines as State sponsors of terrorism, those that have "repeatedly provided support for acts of international terrorism"[41]. Terrorist safe havens include "ungoverned, under-governed or ill-governed physical areas where terrorists can organise, plan, raise funds, communicate, recruit, train, transit, and operate in relative security because of inadequate governance capacity, political will, or both" [42].

94. "Corporate" terrorist groups sit at the intersection of terrorism and organised crime: ideologically motivated but operationally similar to organised criminal groups, with advanced financing capabilities including fraud, kidnap-for-ransom, robbery and theft.

4.3. Ideologies and terrorist financing needs

95. Following the Europol TE-SAT reports, this analysis distinguishes between the following types of terrorism, based on ideological preferences:

- Jihadist terrorism;
- Right-wing terrorism;
- Left-wing and anarchist terrorism; and
- Ethno-nationalist and separatist terrorism.

[40] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025, link.
[41] US State Department, State Sponsors of Terrorism, retrieved 4 August 2025, link.
[42] US State Department, *Country Reports on Terrorism,* 2023, link.

96. Some actors might operate off a mixture of different ideologies, although one usually dominates. Nonetheless, it should be noted that the analysed ideologies are not mutually exclusive. The categorisation of the different types of terrorist ideologies and their respective definitions serve the needs of this analysis and do not have any formal or legal value.

4.3.1. Jihadism

TE-SAT 2025 definition

Jihadism is defined as a violent sub-set of Salafism, a revivalist Sunni Muslim movement that rejects democracy and elected parliaments, arguing that human legislation is at odds with God's status as the sole lawgiver. Jihadists aim to create an Islamic state governed exclusively by Islamic law (shari'a), as they interpret it. Unlike other Salafist currents, jihadists legitimise the use of violence by referring to the classical Islamic doctrines on jihad, a term that literally means "striving" or "exertion", but which jihadists treat as religiously sanctioned warfare. All those who oppose jihadist interpretations of Islamic law are considered as "enemies of Islam" and therefore considered legitimate targets. Some jihadists include Shi'a, Sufis and other Muslims in their spectrum of perceived enemies.

97. Globally, the four major terrorist organisations of the Islamic State (IS) and its affiliates were responsible for most terrorist deaths in 2024. These terrorist groups are namely, Islamic State (IS), Jamaat Nusrat Al-Islam wal Muslimeen (JNIM), Tehrik-e-Taliban Pakistan (TTP), and alShabaab[43].

98. Jihadist organisations, such as, IS, Al-Qaeda (AQ) and JNIM historically operated as large, networked organisations across multiple jurisdictions. Decentralisation is now the dominant trend, with regional affiliates increasingly autonomous in management and funding. The model, territorial control, ideological influence, opportunistic attacks and locally-tailored strategy, is harder to contain. The MENA region (notably Syria) and Sub-Saharan Africa (notably the Sahel) bear the brunt of IS-attributed activity[44].

99. The EU jihadist milieu is dominated by self-radicalised individuals and small, loose groups embedded in wider terrorist networks. Lone-actor attacks remain the most acute threat: typically perpetrated by sympathisers of jihadi-Salafist ideology acting without operational instructions, weapons or funding. Many are anchored in online communities promoting violence and increasingly display ideological flexibility, reposting AQ- and IS-linked content without clear allegiance, particularly visible among young adults and minors. Radicalisation in prisons and the release of former terrorist convicts remain major Member State concerns.

100. Outbound travel from the EU for terrorist purposes (including military training) to the Middle East and Africa remained low in 2024 but continues to be discussed in radicalised circles. Regional instability may open new destinations. FTFs and returnees from Middle Eastern conflict zones have been detected entering the EU under false pretences using fraudulent documents or international protection claims, sometimes via migrant smugglers.

[43] Institute for Economics & Peace, Global terrorist Index, 2025, Link.
[44] Institute for Economics & Peace, Global terrorist Index, 2025, Link.

101. According to Europol, voluntary donations from supporters and charitable collections account for a significant share of jihadist TF, with small-amount transfers raised through legitimate banking, online donations and crypto-asset transfers. High-risk regions bordering conflict zones, including Türkiye, are repeatedly used as transit points[45].

102. CRF observations align: typologies include small direct donations to foreign humanitarian NPOs or NPOs linked to extremist groups; P2P transfers via online payment service providers (PSPs) supporting widows, prisoners, orphans and families of fighters killed in conflict; and transactions with foreign individuals known as terrorist financiers. Typologies span both large, networked organisations and individual actors (FTFs, small cells)[46].

103. Around 70% of TF-related reports filed with the CRF in the observation period were Islamism-related. The dominance reflects (i) the global reach of the ideology, particularly relevant for an international financial centre, and (ii) the comparative ease of identifying linked persons and entities through open-source information. The European Commission's 2024 New Trends in Jihadism Research Review attributes the movement's resilience to global propaganda production, convergence with other forms of extremism, and targeted online radicalisation (gamification, Telegram bots)[47].

4.3.2. Extreme-right wing terrorism

TE-SAT 2025 definition

Violent right-wing actors (groups or individuals) seek to use violence to transform the entire political, social and economic system into an authoritarian model, rejecting democratic order and values and fundamental rights. Violent right-wing ideologies use narratives centred on exclusionary nationalism, racism, xenophobia and/or related intolerance. A core concept of right-wing violent extremism is supremacism or the idea that as a group of people sharing a common element (nation, race, culture, etc.), they are superior to all others and consider it to be their natural right to dominate the rest of the population. In addition, right-wing violent extremist ideologies feed on a variety of hateful sub-cultures, that often oppose diversity in society and equal rights of minorities, such as misogyny and hostility towards LGBTQ+ communities and anti-immigration attitudes.

104. ERW actors blend transnational online networks, lone actors and a small number of structured online groups[48]. Given the global rise of violent extremist rhetoric, these forms of terrorism and extremism are likely to grow[49].

105. Long-standing ERW organisations often comprise multiple affiliated groups internationally networked, with cells operating inside and outside the EU; splinter groups regularly emerge under new names. Travel typically revolves around music concerts, sports events and training, commemoration

[45] TE-SAT 2025, link.
[46] Considering that the CRF receives filings where there a potential, but reasonable grounds to suspect TF, this paragraph includes typologies observed part of the broader Islamist ideology (including jihadism, but also other non-jihadi movements or ideologies part of the broader Islamist ideology). TFARs/TFTRs received linked to Islamism do not necessarily always involved jihadism.
[47] Vicente A., Driessen M., García-Calvo C., *New trends in jihadism – quarterly research review,* 2024, link.
[48] TE-SAT 2025, link.
[49] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025, link.

marches and demonstration. These events double as networking, recruitment and ideological-reinforcement opportunities, underlining the movement's transnational character.

106. ERW funding blends legal and illegal sources for resilience: cultural events generating revenue from tickets, merchandise and donations; membership fees; online sales of propaganda items, books, clothing and branded products; cryptocurrencies; and, for some groups, links to drug trafficking or extortion[50].

107. Around 10% of CRF TF reports were associated with this ideology: around 50% triggered by the sale or purchase of weapons or suspicious goods (clothing, flags, books, CDs) tied to extremist content; around 35% by open-source information (adverse media, convictions, sanctions hits); and approximately 15% by donations or fundraising for foreign activists or convicted individuals.

4.3.3. Left wing and anarchist terrorism

TE SAT 2025 definition

Left-wing terrorist groups seek to trigger a violent revolution against the political, social and economic system of a state, in order to establish socialism and ultimately a communist and classless society. Their ideology is often Marxist-Leninist. Anarchist terrorism is a term used to describe acts of violence committed by groups or individuals who promote the absence of authority as a societal model. Anarchists pursue a revolutionary, anti-capitalist and anti-authoritarian agenda.

108. Per the TE-SAT 2025, the overall threat from this ideology remains relatively low, with concentrated activity along the Italy–Greece–Spain–Chile–Argentina axis[51].

109. While there is a great deal of diversity, in some cases the structure of the groups active in the terrorist and violent extremist left-wing and anarchist scenes differs. Anarchist groups organise horizontally without a clear chain of command, relying on decentralised clusters connected by ideological affinity. Violent left-wing groups more often follow organisational lines and a chain of command. Lone attackers may act in support of, or under the umbrella of, wider organisations[52].

110. Most 2024 attacks were low-cost and could plausibly be self-financed or covered by broader-network fundraising: membership fees, personal income, donations, solidarity events (concerts, dinners, book fairs), sale of literature and merchandise, and crowdfunding (sometimes in crypto-assets) for legal expenses and support to imprisoned or fugitive members. International transfers are kept small and cash is preferred; funds also cover court costs, prison maintenance and fines[53].

111. Around 2% of CRF TF reports were linked to this ideology, with triggers split evenly between donations/P2P transactions/fundraising and open-source information (notably terrorism-related adverse media).

[50] TE-SAT 2025, link.
[51] TE-SAT 2024, link and 2025, link.
[52] TE-SAT 2024, link.
[53] TE-SAT 2025, link.

4.3.4. *Ethno-nationalist and separatist terrorism*

TE SAT 2025 definition

Ethno-nationalist and separatist terrorist groups are motivated by nationalism, ethnicity and/or religion. Separatist groups seek to carve out a state for themselves from a larger country or annex territory from one country to that of another. Left-wing or right-wing ideological elements are not uncommon in ethno-nationalist and separatist terrorist groups.

112. Per the definition above, this ideology blends elements of left- and right-wing extremism, and CRF-identified TF triggers combine elements analysed in sections 4.3.2 and 4.3.3. Six TF reports could be linked to ethno-nationalist and separatist terrorism during the observation period.

113. CRF analysis (2023–2024) identifies typologies dominated by NPO donations, P2P transactions and fundraising campaigns (18%), followed by sale or purchase of weapons or suspicious goods (13%) and items linked to extremist or hateful ideologies, such as flags, and clothing (9%). Open-source information remains the principal trigger (>55%), with terrorism-related adverse media especially relevant.

4.3.5. *Trends*

4.3.5.1. *Use of digital platforms*

114. Globally, social media, livestreaming and encrypted messaging platforms are increasingly used for propaganda dissemination and fundraising from sympathisers. Well-organised campaigns can attract thousands of donors and meaningful sums; algorithmic exposure of at-risk users to reinforcing content also serves donor identification. Encrypted messaging is used to communicate and to share payment instructions privately.

115. These campaigns are generally linked to bank accounts, mobile payments or digital wallets that can operate with crypto-assets. In case these accounts are blocked, new accounts are set up to bypass these restrictions and new information with regard to payment details and channels can be communicated quickly. Considering this, these platforms are a convenient tool to generate significative revenue in limited time and traceability[54].

116. The CRF observed an increase in social media posts and activities linked to TFARs/TFTRs received. Typically, this would involve social media posts, comments and live streaming contents on platforms such as TikTok, Instagram, and X.

117. In 2024, 94% of Luxembourg residents reported daily internet use (EU 88%); 67% participate in social networks (EU 65%); and approximatively 74% use instant-messaging applications (EU 79%). The country's linguistic diversity allows multilingual content consumption and creation, which, combined with daily exposure, elevates the likelihood of being targeted by at-risk content and fundraising campaigns as shown in Insight Box 1.

[54] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025, link.

Insight Box 1: Editing and reposting material from media outlets of terrorist groups[55]

In Luxembourg, a new generation of suspected jihadi affiliates are alleged to have produced their own nasheeds which contain ideas about fighting the 'kuffar', jihad in the name of Allah, glorification of famous ideologues such as Bin Laden, and in some cases pledges of allegiance to terrorist groups. Their multilingual skills enable them to reach German-, French-, and English-speaking likeminded youngsters.

118. The BEE SECURE Stopline allows users to report potentially illegal online content. In 2023/2024, 136 alerts (vs. 34 in 2022/2023) related to terrorist content were recorded; 96 were assessed as potentially illegal and forwarded to the SPJ (vs. 19 the prior year)[56]. It should be reminded that any person investigated in this context is presumed innocent until a final judicial decision is rendered.

Case study 2: SPJ investigation into a Non-Profit Association

The Public Prosecutor's Office has assigned the SPJ an investigation into a Non-Profit Association based on a reporting (from a whistle-blower) indicating that the association is using private Telegram groups to facilitate illegal money transfers between a High-risk Third Country (HRTC) and Luxembourg, thus bypassing legal frameworks and sanctions.

According to the report, this association, registered under the guise of cultural and student activities, allegedly manages – directly or indirectly – several private Telegram groups in a foreign language, reserved for selected members and subject to prior validation. One of these groups, as well as a specific subgroup dedicated to financial exchanges, is allegedly used to organize, facilitate and oversee currency exchange and money transfer operations between the aforementioned HRTC and Luxembourg, as well as between Luxembourg and said HRTC, outside of any legal framework, hence circumventing banking systems, compliance obligations (AML/CFT) and current international sanctions.

It should be reminded that any person mentioned in this case study is presumed innocent until a final judicial decision is rendered.

4.3.5.2. Minors involved in terrorist and violent extremist activities

119. The growing involvement of minors in terrorist and violent extremist activity is a global concern: per Europol, almost 30% of suspects arrested for terrorism-related offences in 2024 were aged 12–20, predominantly linked to jihadism and to a lesser extent right-wing terrorism.

120. Terrorist organisations adapt communications to younger audiences across popular social-media and gaming platforms, targeting recruits and supporters. Young people experiencing isolation, mental-health difficulties or loneliness are particularly susceptible to the sense of belonging and community these groups offer[57].

[55] Case study taken from TE SAT 2024, link.
[56] Bee Secure, Bee Secure Radar 2025, link.
[57] TE-SAT 2025, link.

121. From a CFT perspective, this trend brings additional challenges, as minors typically depend on others' financial resources and tend to be more proficient with digital tools and innovations.

122. In Luxembourg, smartphone ownership among 12–16-year-olds is near-universal: WhatsApp (88%), YouTube (87%) and Snapchat (82%) lead usage; among 17–30-year-olds, WhatsApp (95%), Instagram (94%) and YouTube (87%) lead. 77% of 12–16-year-olds spend at least one hour per day on social media on weekdays (89% of 17–30-year-olds), with around a quarter in both groups spending 4–6 hours daily; messaging usage is near-universal in both age groups[58].

4.3.5.3. Nexus between terrorist financing and other types of crime.

123. FATF and Europol cite the growing nexus between TF and other crime—drug trafficking, fraud and forgery in particular—as a global trend. Generated proceeds finance terrorist activity or facilitate movement of operatives, and grant access to restricted goods such as weapons and forged documents. The nexus is most often associated with extreme-right wing groups (see 4.3.2). Terrorist groups may engage directly in such crimes or contract organised-crime actors for services such as weapons procurement, ML or smuggling.

4.3.5.4. Gender-based approach

124. The profile of suspects for terrorism-related activity is overwhelmingly male. On the assumption of lower scrutiny, terrorist groups have used women's identities, and active female members, for financial transactions and to support FTFs, including cross-border cash couriering. Some NPOs falsely claim to fundraise for women and children while channelling funds to (male or female) terrorist fighters.

125. While CFT measures are gender-neutral in principle, they may produce discriminatory effects in practice, including a disproportionate impact on women's-rights organisations' access to funding and reluctance among donors and financial-service providers to support assistance programmes[59].

4.3.5.5. Technology

126. TF-related risks from emerging technologies follow general societal uptake (see 2025 NRA ML[60]). AI tools may be misused to create more sophisticated forged documents to access regulated sectors, exposing regulated entities relying in remote onboarding such as VASPs and MVTS providers.

127. Digital methods (e-wallets, prepaid mobile cards, crypto-assets) are expected to expand. Despite progress in tracing crypto-asset transactions, obfuscation techniques (shared wallets, mixers, chain-hopping) have advanced in step, with a shift toward alternative crypto-assets being observed. In line with ongoing decentralisation and fragmentation, terrorist actors increasingly blend offline (cash couriers, HOSSPs) and online channels (crypto-asset fundraising) to sustain operations[61].

---

[58] Bee Secure, Bee Secure Radar 2025, link.
[59] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025, link.
[60] MoJ, *National risk assessment of money laundering,* 2025, link
[61] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025, link.

5. Terrorism threat context

128. To assess TF risk, the terrorist threat outside and within the EU and in Luxembourg is examined, recognising that intense terrorist activity in one region drives demand for TF. Particular attention is paid to actors and ideologies and their respective TF needs.

129. The MENA region recorded the highest number of terrorism deaths from 2007 to the mid-2010s; from 2016 to 2020 the region saw a sustained drop, with the epicentre of terrorism shifting to Sub-Saharan Africa[62].

5.1. Sub-Saharan Africa

130. Sub-Saharan Africa, particularly the Sahel, is the current epicentre of global terrorism, accounting for 51% of global terrorism deaths in 2024. Five of the ten most-affected countries (Burkina Faso, Mali, Niger, Nigeria, Cameroon) are in the region[63].

131. Weak governance, ethnic tensions, environmental stress, disputes over natural-resource extraction and external-actor involvement continue to drive the crisis. The Alliance of Sahelian States (Mali, Burkina Faso, Niger) has strengthened ties with Russia and China and withdrawn from the Economic Community of West African States, creating space for groups such as JNIM to expand into coastal West Africa. The UN Panel of Experts on Mali reported in August 2023 that IS-Sahel had doubled the territory it controlled.

132. Across Africa, terrorist groups exploit large informal economies and porous borders, raising and moving significant resources. Territorial control is central: in the Sahel, JNIM and similar groups generate income by levying taxes, providing security in exchange for payment, and integrating into communities to entrench influence[64,65].

133. Other revenue streams sustaining terrorist activity in the Sahel include cattle rustling and taxation of herders along controlled trade routes; protection and taxation of drug-trafficking operations transiting controlled territory (one of the most lucrative illicit revenue lines); kidnapping for ransom, central to JNIM's economy and used for political leverage and intelligence; and control of artisanal gold-mining areas, where groups typically tax miners rather than extracting or trading directly. These illicit economies long pre-date current terrorist activity in weakly-governed areas, with state and non-state actors both benefiting from them[66].

5.2. Middle East and Northern Africa region

134. The Arab Spring and the rise of Islamic State (IS) from 2011–2013 triggered a surge in terrorism across the Middle East, particularly in Syria and Iraq. The instability following the fall of the Assad

[62] Institute for Economics & Peace, Global terrorist Index, 2025, link; 2024, link; 2023, link; 2022, link.
[63] Institute for Economics & Peace, Global terrorist Index, 2025, link.
[64] Institute for Economics & Peace, Global terrorist Index, 2025, link.
[65] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025, link.
[66] Institute for Economics & Peace, Global terrorist Index, 2025, link.

regime in December 2024 provides fertile ground for terrorist groups to regroup, with IS leveraging the shifting landscape. Syria recorded the highest level of IS attacks and deaths in 2023 and 2024[67].

135. At its territorial peak (2013–2014), IS generated most revenue from gas and oil in parts of Syria and Iraq. After losing territorial control in 2019, IS continued to extort oil networks in eastern Syria as late as 2021 and, facing scarcity, has been reported to excavate buried cash reserves and smuggle funds out of Iraq and Syria.

136. At its culminating point of its territorial control between 2013 and 2014, IS generated most of its revenue through the exploitation of natural resources, especially gas and oil in parts of Syria and Iraq. Despite of IS loss of control over territories in these two countries in 2019, IS has been reported to generate funds through extortion of oil networks in eastern Syria as late as 2021. It has also been reported that some of IS's physical cash reserves were buried in the ground in Iraq and Syria. Due to the relative scarcity of resources currently faced by the group, IS has excavated these cash reserves and smuggled funds out[68].

137. The attack by Hamas-led militants in Israel on 7 October 2023 was by far the largest single terrorist attack since 9/11, with 1 200 people being killed. The consequences of this attack have been immense and are still unfolding, with over 55 000 Palestinians reported dead[69].

138. Consequently, terrorism in Israel is expected to remain a significant challenge due to ongoing regional instability, evolving militant tactics, and unresolved political conflicts. Groups such as Hamas, Hezbollah, and the Houthis may increasingly target critical infrastructure through drones, missiles, and cyberattacks. Tensions in the occupied West Bank and the broader Israeli-Palestinian conflict could also fuel localised or lone wolf attack[70]. The conflict in Gaza has heightened the possibility of terror attacks in the MENA region, and in states perceived as supportive of Israel or with large Jewish populations[71].

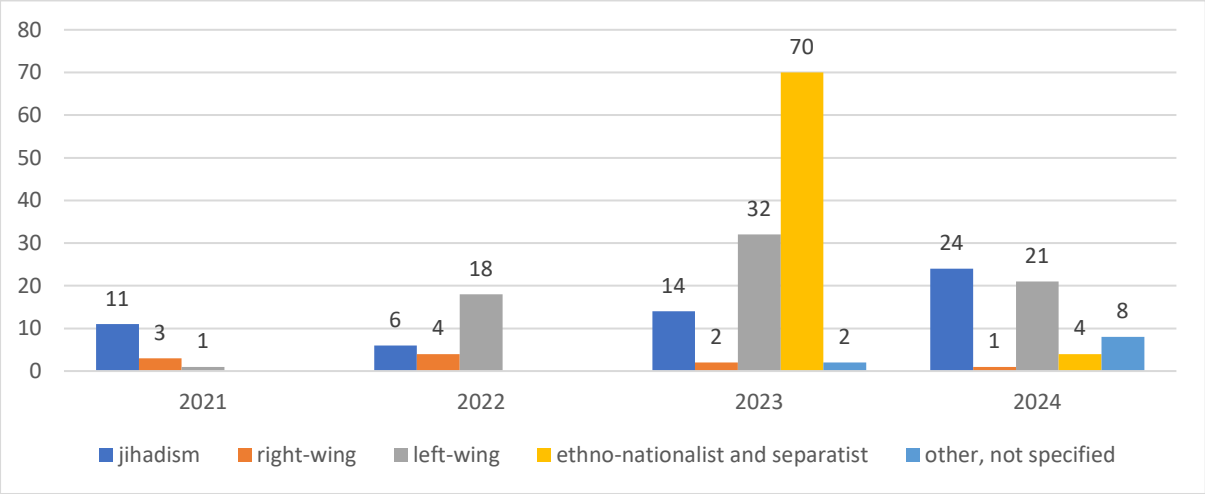
5.3. European Union

139. Terrorism and extremism remain serious public-security threats in the EU. Countries near or neighbouring Luxembourg have been significantly impacted in recent years[72].

140. The EU TF threat profile is dominated by lone actors and small cells with low TF needs. Across the observation period the ideological landscape remained fragmented across left-wing, right-wing, ethno-nationalist and separatist, anarchist and jihadist movements, as shown in Figure 5.

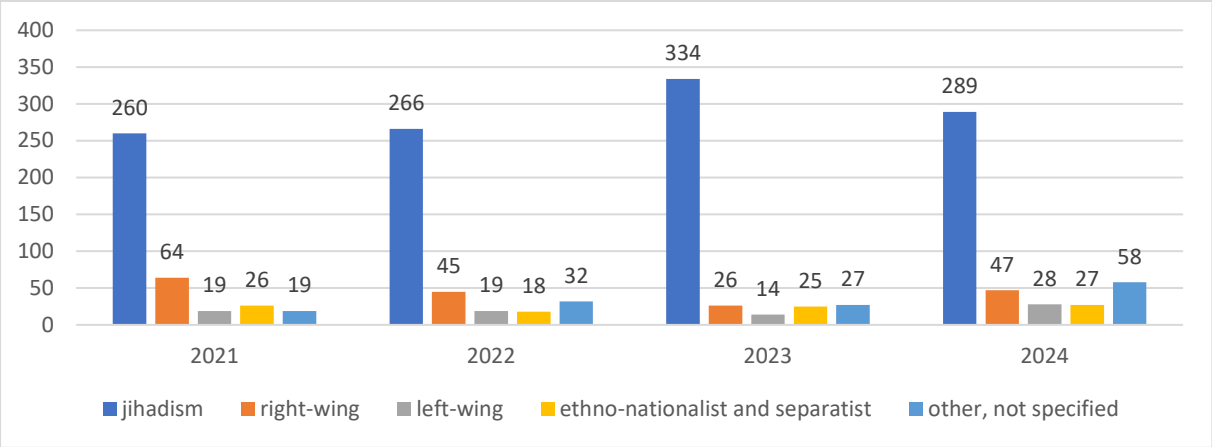
[67] Institute for Economics & Peace, Global terrorist Index, 2025, link.
[68] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025, link.
[69] Institute for Economics & Peace, Global terrorist Index, 2025, link.
[70] Institute for Economics & Peace, Global terrorist Index, 2025, link.
[71] Institute for Economics & Peace, Global terrorist Index, 2024, link.
[72] Unless specified otherwise, all data on terrorism in the EU in this section is sourced from Europol, *European Union Terrorism Situation and Trend Report*, 2021 link, 2022 link, 2023, link, 2024, link and 2025, link.

Figure 5: Number of terrorist attacks in the EU by ideology, 2021–2024



In terms of arrests, however, a prevalence of arrests related to jihadism may be observed[73].

Figure 6: Number of arrests in the EU by ideology, 2021–2024



141. In 2024, the most recurrent offences linked to the arrests was membership to a terrorist organisation (110), planning or preparing an attack (107), and creation and/or dissemination of terrorist propaganda (90). The arrested suspects were predominantly male (405), while 43 were female[74]. The youngest arrestee, charged with planning or preparing an attack, was 12 years old and was ascribed to right-wing ideology.

Jihadist terrorism

142. Across the observation period, 55 jihadist attacks were executed in 10 Member States, France (28) and Germany (11) leading, all by lone actors using easily accessible weapons such as knives and remaining the most lethal category of attack. Jihadism accounts for around 70% of EU terrorism-related arrests (1 643), with at least one such arrest in 23 of 27 Member States. France led with 309

[73] 70 separatist attacks have been committed in the EU in 2023, all in Corsica, France. 34 of the attacks were executed during the night of 8-9 October.
[74] The gender has been specified for 448 out of 449 arrestees.

arrests, followed by Spain (241), Belgium (132) and Germany (130). Jihadism also accounted for 75% (363 out of 485) of total terrorism convictions in 2024.

Extreme-right wing terrorism

143. Extreme-right wing attacks affected 8 Member States; the trend is downward (4 attacks in 2022, 1 in 2024). Across 2021–2024 there were 182 arrests in 17 Member States (47 in 2024, 26 in 2023, 45 in 2022, 64 in 2021), with France (57) and Italy (43) leading. Right-wing actors typically use easily accessible, unsophisticated weapons (more popular here than in other ideologies), bladed weapons, homemade explosives including pipe bombs, and to a lesser extent incendiaries and pyrotechnics. The geographic spread is wider than other ideologies, affecting most Member States.

Ethno-nationalist and separatist terrorism

144. Ethno-nationalist and separatist attacks are concentrated in France (73) and Italy (1); the 70 attacks in Corsica in 2023 (35 in a single night, 8–9 October) skew the totals. Across 2021–2024 there were 96 arrests in 8 Member States (<6% of EU total). Although some groups (e.g. PKK) operate transnationally, the threat is largely localised to countries with separatist movements (France, Ireland, Spain).

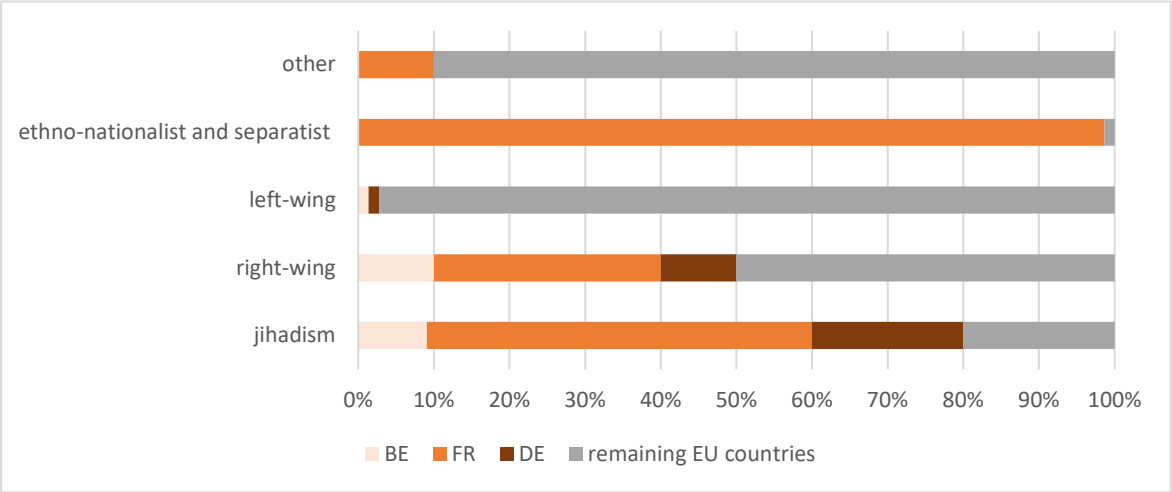
Left-wing and anarchist terrorism

145. Left-wing and anarchist attacks totalled 72 across the period—60 in Italy, 8 in Germany, 2 in Spain, 1 each in France and Belgium. 80 arrests were performed in 6 Member States, with Italy (34) and Greece (26) leading. Per Europol, the overall threat from this ideology remains relatively low despite localised violence.

Insight Box 2: Terrorist situation in Luxembourg's neighbouring countries

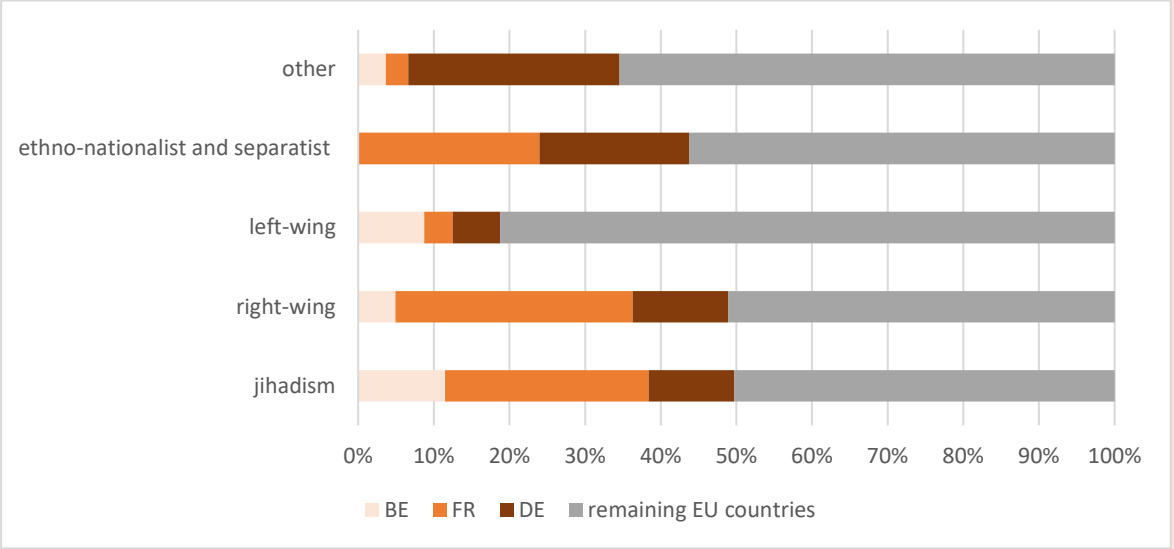
Throughout 2021–2024, Luxembourg's neighbouring countries accounted for 57% of reported EU terrorist attacks, with France alone representing 48%. Nearly all ethno-nationalist and separatist attacks occurred in France, including the 73 attacks in 2023. 44 of 55 jihadist attacks were carried out in a country bordering Luxembourg, as were half (5) of right-wing attacks. Left-wing terrorism was less prevalent, with one attack each in Germany and Belgium during the observation period.

Figure 7: Share of terrorist attacks in Luxembourg's neighbouring countries, split by ideology



Neighbouring countries also accounted for 47% of EU terrorism-related arrests during the period—France 24% and Germany 13%.

Figure 8: Share of arrests in Luxembourg's neighbouring countries, split by ideology



5.4. Luxembourg[75]

146. Luxembourg has not experienced a completed terrorist attack, and no established terrorist group operates on its soil; one right-wing attack was foiled in 2023.

147. Luxembourg's first prosecution and conviction for terrorism took place in 2021: a couple resident in Luxembourg was sentenced to a combined total of more than five years' imprisonment for spreading IS propaganda. Luxembourg applies a low-threshold investigative policy—any indication of terrorism or TF is investigated at an early stage with a preventive aim. A further conviction in 2025 (outside the observation period) related to the planning of an attack inspired by extreme-right ideology, and a Luxembourg resident travelling to Syria was convicted in 2025.

Insight Box 3: Luxembourg: the fight against terrorism and violent extremism[76]

In 2024, early detection of individuals radicalised by jihadist propaganda remained a priority for SRE. Over the past few years western intelligence services have observed a significant evolution in the operating model of jihadist-inspired terrorist groups, who have reoriented towards lone actors—often younger—with rudimentary tactics. The dynamics of radicalisation, recruitment and incitement of extremist movements have evolved significantly, largely relying on digital spaces.

Detecting increasingly younger individuals, radicalised through the internet and social media, likely to engage in violent action, remains a major challenge for SRE.

[75] This section includes the input provided by the State Intelligence Service in accordance with its legal missions set out in article 3 of the law dated 5 July 2016 on the reorganization of the State Intelligence Service.
[76] Translation of section B.5.2. of the Ministry of State's Activity Report 2024, link

Western countries also face a diversification of violent ideologies. These ideologies may be focused on, among others, the opposition to authority and state institutions, conspiracy theories or xenophobia. Perpetrators of violent acts frequently adhere to multiple ideologies simultaneously or shift from one ideology to the other. The decentralisation of terrorist structures has further complicated early detection of individuals likely to engage in violent action.

In 2024 the SRE intensified its prevention work in the fields of terrorism and violent extremism. In this respect, the SRE has worked in close coordination with its national and international partners. The intelligence collected by SRE in the framework of its legal mission consisting of countering the terrorist threat has led to referrals to the Public Prosecutor's Office of the District Court of Luxembourg.

148. The Counter-Terrorism Coordination Group (GCT) continuously assesses the threat to the national territory in light of national and international developments. Based on this assessment, a proposed alert level is submitted to the Government, which determines the applicable level on a 1 ("Low") to 4 ("Very serious") scale[77].

149. Following the 2015 Paris attacks, Luxembourg raised the level to 2 ("Medium"), maintained throughout the observation period of this NRA. Level 2 applies when the analysed threat is real but abstract, meaning that the potential threat is not supported by a concrete piece of evidence for concluding that an attack would be imminent[78].

[77] Infocrise, *Plan gouvernemental de vigilance nationale "Vigilnat"*, link
[78] Infocrise, *Plan gouvernemental de vigilance nationale "Vigilnat"*, link

6. Analysis of terrorist financing reports received by the CRF

AT A GLANCE

The CRF receives TFTRs and TFARs from obliged entities regarding domestic, inward and outward financial flows. During the 2021–2024 observation period, TF-related reports remained relatively stable at between 200 and 300 per year. Approximately 70% of reports for 2023–2024 were linked to Islamism[79], followed by extreme right-wing (10%), separatism (6%) and left-wing terrorism (2%).

Most reports emanate from the financial sector reflecting Luxembourg's role as a cross-border payment and banking hub, and a large share involves non-resident EU individuals.

International cooperation requests, predominantly with neighbouring EU countries, are broadly balanced with the financial centre profile. Key typologies identified include donations directed to NPOs, P2P online transfers for alleged humanitarian purposes, extremist merchandise sales, weapons transactions, and suspicious money remittance behaviour associated with high-risk jurisdictions.

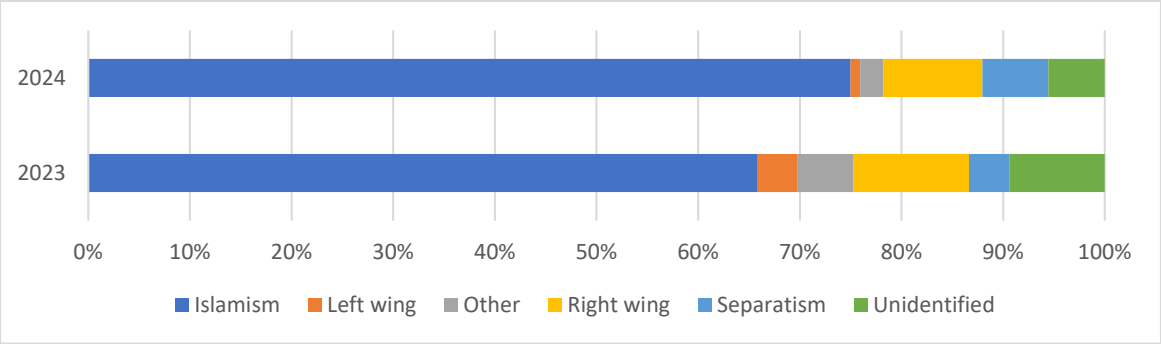
150. As reporting entities file Terrorism Financing Transaction Report (TFTR) and Terrorism Financing Activity Report (TFAR) to the CRF with regard to domestic, inward and outward financial flows, relevant insights may be drawn from Luxembourg's TF context which is influenced simultaneously by Luxembourg's position as a financial centre and its geographic position. The CRF's insights may be of particular use considering their key role in the AML/CFT ecosystem by collecting, analysing and disseminating financial information. Note that data and information in this section is based on the reports submitted with the CRF.

151. During the observation period, the total number of TF-related reports filed with the CRF has remained relatively stable (2021: 321; 2022: 220; 2023: 223; 2024: 230).

152. Most of these reports related to Islamism[79] (around 70% for reports regarding years 2023 and 2024, followed by extreme right wing (10%), separatism (6%) and to a lesser extent extreme left-wing terrorism (2%)).

[79] Considering that the CRF receives filings where there a potential, but reasonable grounds to suspect TF, reference is made to reports received that fall within the broader Islamist ideology (including jihadism, but also other non-jihadi movements or ideologies part of the broader Islamist ideology). TFARs/TFTRs received linked to Islamism do not necessarily always involved jihadism.

Figure 9: Main ideologies observed per year from filed TFARs/TFTRs (2023–2024), in %



153. Reports related to suspected terrorist financing can mainly be attributed to the international exposure of the financial centre and the presence of large online payment and electronic money institutions operating in Luxembourg, which serve an international clientele. A large share of TFAR/TFTR received in both 2023 and 2024 involved natural persons residing in neighbouring countries, and in the EU more generally. 7% of TF-reports filed in 2024 with the CRF concerned Luxembourg residents (6% in 2023).

154. The difference between outgoing and incoming requests is not unexpected in the Luxembourg context. The financial centre operates within a highly internationalised ecosystem, where the only connection to Luxembourg is often the business relationship between a Luxembourg professional and a customer residing in another European or third country. It reflects the nature of the business conducted in Luxembourg, which is characterised by significant international exposure. Consequently, most reports concern non-resident customers, and fewer information requests relate to Luxembourg-based targets. Overall, it appears that the majority of requests, both incoming and outgoing, emanate from EU countries, and more precisely from Luxembourg neighbouring countries.

Table 7: International cooperation CRF, 2021–2024 data

Incoming requests of information		Outgoing requests of information	
Spontaneous: 18 Requests for information: 523	**EU countries (88%)** - France (62%) - Germany (13%) **Non-EU countries (12%)** - Israel (7%)[80]	Spontaneous: 622 Requests for information: 468	**EU countries (75%)** - Germany (33%) - France (16%) **Non-EU countries (25%)** - UK (15%)

155. Based on the analysis of TF-related reports filed between 2017 and 2023, the CRF identified the following main typologies:

- Donations to NPOs and online fundraising campaigns: these donations amount usually to less than EUR 100 and are directed to foreign NPOs that are suspected of being linked to extremist organizations. The use of social media and online fundraising/crowdfunding campaigns launched on behalf NPOs plays also an important role;

[80] With a peak of reports noted in 2023 and 2024 following Hamas attacks on Israel on 7 October 2023.

- Peer-to-peer (P2P) online transactions, especially with regard to unrelated individuals. Again, social media together with informal online fundraising campaigns act as a catalyst to collect funds for alleged humanitarian purposes (support to orphans, widows, prisoners and families of killed);
- Sale and purchase of items relating to extremist ideologies, such as clothes, music, books. Often, involved individuals are known for online hate speech or links with extremist movements;
- Sale and purchase of weapons or other suspicious goods mostly by lone actors or foreign separatists;
- Suspicious behaviour and money remittance which most often show through a broader shift in consumer behaviour. Unusual living and/or expenses made in jurisdictions presenting higher TF risks, money remittance to unrelated individuals located in jurisdictions with higher TF risks or successive purchases of numerous flight tickets to jurisdictions with higher TF risks may illustrate such behaviour.

156. Pursuant to the CRF, open-source information is fuelling an ever-larger share of filed TFAR/TFTR (especially for non-residents subject to T/TF-related asset seizing orders and sanctions). Almost one third of TF-related reports filed in 2023 and 2024 were based upon open-source information, including terrorism-related adverse media or sanctions, usually generated from name screening alerts. While TFARs/TFTRs submitted on the basis of open-source information and name screening performed might be useful to the CRF, the analysis by reporting entities of the potential link between the business relationship / funds involved and the TF-related information is not systematic and varies among reporting entities. Suspicious media posts and related contents are playing a relatively growing role in TF suspicions from reporting entities.

Insight Box 4: TF indicators[81]

There are several indicators that may allow to identify potential suspicious TF activity from a customer's profile, behaviour and transactions.

It should be noted that indicators mentioned below are neither exhaustive nor specific to one TF stage and can therefore be found in different stages.

<u>Customer/KYC indicators</u>

- The customer is mentioned in adverse media articles (open source), or referenced in customer due diligence (CDD) tools;
- the customer is linked to entities or individuals mentioned on sanctions lists, or mentioned in adverse media articles (open source), or referenced in CDD tools;
- the entity has only recently been incorporated and has no financial trading history;
- IP addresses that do not correspond to a customer's reported location data or that are in areas of conflict;
- Customer using an IP address associated with a darknet or other similar software that allows anonymous communication, including encrypted emails and VPNs;
- A new user attempts to trade the entire balance of crypto-assets or withdraws the crypto-assets and attempts to send the entire balance off the platform.

[81] CRF.

Transactional/know your transaction (KYT) indicators

- An entity which begins to receive donations from donors, which have previously donated to terrorist organizations, entities linked to those organizations or an entity whose activity was frozen;
- Crypto addresses, bank accounts, digital payment means, etc. published on the terrorist organisations affiliated social media platforms or having links to such platforms;
- Use of phrases and numbers in the transfer or funds, where there is an indication that they are related to terrorism in general or in the context of current events. For instance, money transfers to organizations whose names indicate a link to terrorism such as the name of a famous martyr or a word such as "jihad" or stated purpose to assist the fighting in the conflict zones;
- Transacting with crypto-assets' addresses or bankcards that are connected to known sanctioned addresses, terrorist organizations clusters, entities or individuals linked to such clusters or illegal fundraising campaigns;
- Activity appearing on an account that is consistent with a previous pattern of activity on an account controlled by a relative or other party which has since been blocked;
- Multiple cash deposits and withdrawals with suspicious references;
- Unexplained third-party payments being received regularly;
- Unexplained periods of account dormancy;
- Deposits were structured below the reporting requirements to avoid detection;
- Multiple cash deposits in small amounts in an account followed by a large wire transfer to another country;
- Frequent electronic money transfers followed by the depletion of funds through transfers to third parties;
- Depositing crypto-assets at an exchange and then withdrawing the crypto-assets without any additional exchange activity;
- Crypto-assets' related transactions making use of mixing and tumbling services;
- Change in customer's transaction behaviour;
- Transaction activity on personal account is indicative of operating an unregistered NPO with a large number of cash or wire donations funding onward transfers to family members or other related accounts;
- Opening an account immediately after engaging in extensive financial activity for humanitarian purposes;
- Funds are generated by a business owned by persons of the same origin or by business, which involves persons of the same origin from high-risk countries.

Fundraising indicators

- A fundraising campaign that mimics and uses an existing charity/initiative as a front to raise funds for TF;
- A non-transparent fundraising campaign with unclear recipient of the donations, fundraising through natural person accounts linked to high-risk jurisdictions;
- Activity on an account consistent with charitable fundraising but the recipient has not registered as a charity in the jurisdiction of operation, or its registration has been suspended or cancelled;

- Recent date of incorporation of the NPO;
- Designation and objectives of NPO might be unclear;
- The NPO has little or no staff, which is suspicious considering its stated purpose and expected financial activity;
- An address given by the NPO or its affiliates, which belongs to or is used by organizations suspected of terrorist activity;
- Evidence that NPO donors, partners, suppliers or beneficiaries are involved themselves or are related to entities involved in terrorist activity.

7. Luxembourg terrorist financing threats related to decentralised networks, FTFs, lone actors and small cells

AT A GLANCE

The principal TF threat associated with decentralised networks, FTFs and lone actors in Luxembourg lies in the misuse of basic financial products — retail banking, PIs, EMIs and VASPs — to collect, transfer and disburse small amounts of money. Luxembourg's structural exposure stems from two factors: several pan-EU institutions headquartered in Luxembourg operate cross-border under EU passport, extending geographic reach to the entire Single Market; and Luxembourg's role as a payment services hub extends its surface to lone-actor and small-cell exposure from higher-threat Member States. Financial needs are characteristically low and granular — covering travel, online communications, small operational outlays and modest cross-border donations — through online retail banking, EMI/PI cards, mobile wallets and, increasingly, crypto-asset transfers. CRF reporting and FATF guidance confirm that Luxembourg's risk profile is more suited for transit rather than a source country for this category of TF, with the inherent threat assessed as "Medium", materially constrained by CSSF supervision and the dissemination of the TF VRA.

157. With regard to Luxembourg's financial centre, the principal threat associated with decentralised networks, FTFs, lone actors and small cells lies in the misuse of basic financial products offered by Luxembourg-based entities to collect, transfer and disburse small amounts of money for TF purposes. The exposure concentrates on retail and business banking, payment institutions (PIs), e-money institutions (EMIs) and, increasingly, virtual asset service providers (VASPs), which together cover the cash-equivalent, low-amount, high-velocity payment surface that lone actors and small cells require.

158. Although basic financial products offered by Luxembourg financial institutions (FIs) do not present more inherent risks than those offered elsewhere, Luxembourg is structurally exposed for two reasons. First, several pan-EU institutions have located their European headquarters in Luxembourg and operate cross-border under the EU passport, expanding the geographic and customer scope to the entire Single Market. Second, Luxembourg's role as a payment services hub for PIs and EMIs materially extends its surface to lone-actor and small-cell exposure originating in higher-threat Member States.

159. Analysis of flows with jurisdictions targeted on the basis of the Global Terrorism Index (GTI) or low FATF mutual evaluation ratings, designed to capture exposure to large international terrorist organisations, is not, by itself, suitable for assessing the threat from decentralised networks, lone actors, small cells and FTFs. In practice, this threat is global and cross-border yet predominantly intra-EU and intra-Western: transnational extremist groups overwhelmingly raise, move and use funds in the EU and the US, and individuals linked to extremist propaganda in Luxembourg or the EU typically generate and use funds inside the EU. Consistently, FATF (TF Risk Indicators) and Europol (TE-SAT) note that lone actors finance attacks principally from legitimate income (salaries, social benefits, small loans) and petty crime, with limited reliance on cross-border high-risk-jurisdiction flows.

160. All Luxembourg FIs are fully regulated and supervised for AML/CFT purposes by the CSSF. Awareness of TF prevention in the financial sector is high and has further increased since the dissemination, in May 2024 *via* goAML, of the extended professional version of the TF VRA 2022 across all sectors subject to AML/CFT obligations. The CRF assesses the volume of TFAR and TFTR reporting as consistent with Luxembourg's risk and context and with the requests received from foreign FIUs, i.e. there is no indication of underreporting from Luxembourg obliged entities. At the time of writing, indications and information point to alternative or unofficial payment systems operating in Luxembourg, which are addressed below.

161. Financial needs of FTFs, lone actors and small cells are characteristically low and granular: low-cost transactions covering travel, online communications, small operational outlays, and modest cross-border donations. The dominant channels in Luxembourg are online retail banking and EMI/PI products (cards, mobile wallets, online transfers, P2P platforms), supplemented by occasional cash transactions and, increasingly, crypto-asset transfers via VASPs. The emerging use of HOSSPs is also taken into consideration and cannot be completely discarded. ATM withdrawals near final destinations and prepaid-card use, both well documented FTF patterns in Europol and FATF reporting, remain key red flags for entities operating in the country, particularly when combined with travel near or to high-risk jurisdictions or to neighbouring countries that act as transit hubs (e.g. Türkiye).

162. Luxembourg has a population of approximately 670 000 with one of the highest shares of foreign residents in the EU (approximately 47%), reflecting a long-standing labour-driven immigration profile and the presence of EU institutions. Cross-border workers add over 220 000 daily commuters from France, Germany and Belgium, integrating Luxembourg's payment surface with the surrounding TF-exposed regions identified in section 5.3. Internet penetration and digital-financial-service adoption are among the highest in the EU (cf. section 4.3.5), which increases plausibility that small-amount, online-channel lone-actor financing will route through Luxembourg-based PIs, EMIs and VASPs serving cross-border customers. The country's linguistic plurality (Luxembourgish, French, German, English, Portuguese) facilitates exposure to multilingual extremist content as noted in section 4.3.5.

163. The assessed inherent threat to Luxembourg from decentralised networks, FTFs, lone actors and small cells is moderate and structurally tied to the country's role as a pan-EU retail-banking, PI, EMI and VASP hub rather than to any domestic terrorist presence. The threat is strongly intra-EU and intra-Western in character; routes via online channels, crypto-assets and cash are observed; and donations and P2P transfers to support widows, prisoners, orphans and families of fighters in conflict zones constitute the most prevalent TF typology associated with this category in CRF reporting. Mitigating factors—notably mature CSSF supervision, high-quality reporting via goAML, and the dissemination of the TF VRA—materially constrain the residual risk, while emerging vectors (multilingual online radicalisation, minors' involvement, alternative or informal payment systems and the widening use of crypto-assets) warrant continued, targeted vigilance, particularly by retail and business banks, PIs, EMIs and VASPs.

8. Luxembourg terrorist financing threats related to international organisations, affiliated and linked structures and other terrorist actors

AT A GLANCE

Although Luxembourg has no active domestic terrorist group, its status as an international financial centre creates theoretical exposure to TF abuse by large international terrorist organisations and their financiers. The key *modi operandi* assessed include: abuse of corporate vehicles and legal arrangements (shell/front companies, trusts, limited partnerships) to obscure beneficial ownership and source/destination of funds; abuse and misuse of NPOs with humanitarian mandates operating near or in conflict zones; use of high-risk jurisdictions as transfer or destination countries; and combination of these traditional channels with crypto-assets, alternative payment systems and underground banking.

164. Active terrorist organisations operating domestically or regionally increases the probability of TF. On the other hand, the contrary is not necessarily the case[82]. Given the cross-border nature of TF, a country with low domestic terrorism risk may nonetheless present significant TF risk: terrorist actors and their facilitators may exploit institutional, geographic and product vulnerabilities to raise or move funds even where no operational presence exists. As an international financial centre with significant cross-border exposure, Luxembourg falls within the category of jurisdictions whose vulnerabilities to TF abuse must be assessed independently of domestic terrorism levels.

165. The *modi operandi* observed by FATF, Europol and the EU Supranational risk assessment (SNRA)[83] in connection with international terrorist organisations, their affiliates and other international financiers fall into a small number of recurrent patterns relevant to Luxembourg. Each is set out below, with focus on those most plausibly capable of misusing Luxembourg-based intermediaries to raise or move large TF flows: the abuse of corporate vehicles and legal arrangements; the abuse and misuse of NPOs (especially those with humanitarian mandates operating in or near conflict zones); the use of high-risk jurisdictions for transit, layering or final placement; and, as noted in section 4.3.5, the increasing combination of these traditional channels with crypto-assets, alternative payment systems and underground banking.

166. Three regulatory anchors structure the analysis. FATF Recommendations 5 (criminalisation of TF), 6 (targeted financial sanctions related to terrorism and TF) and 8 (NPOs) define the substantive perimeter; Recommendations 24 and 25 (transparency of legal persons and legal arrangements) address corporate-vehicle risk; and Recommendation 19 together with the EU list of high-risk third countries set the high-risk-jurisdiction framework. The Luxembourg legal framework, the Law of 12 November 2004 on AML/CFT (as amended), the beneficial ownership registries (the *Registre des*

[82] FATF, Terrorist Financing Risk Assessment Guidance, 2019, link.

[83] European Commission, *Commission Staff Working Document Accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities*, COM (2022) 554 final, link.

bénéficiares effectifs (RBE) for legal persons, and the *Registre des fiducies et des trusts* (RFT) of legal arrangements) and related sectoral laws, operationalises these instruments.

8.1. Analysis of financial flows with jurisdictions targeted for analysis

AT A GLANCE

Luxembourg's financial flows with the 56 TJs classified across six tier groups represent only 2–3% of total flows, with FDI being the outlier at over 10% (largely driven by flows through legitimate fund-structuring arrangements). The top three TJs account for 65–94% of total TJ flows, concentrated in jurisdictions with their own financial centres and larger global economies. While these flows are theoretically capable of concealing TF activity, no evidence of materialised TF risk has been identified through these channels; the analysis consistently supports a picture of low practical TF exposure from large international organisations through Luxembourg's financial centre.

167. In fact, the TF typologies observed do not suggest that large TF funds are raised and moved by large international terrorist organisations and other terrorist financiers. Nevertheless, considering the cross-border nature of Luxembourg's financial centre, and the international character of terrorist organisation's financing activities, the aim of this section is to assess Luxembourg's exposure of being abused for raising and specially moving larger TF funds through its financial centre, even if this exposure remains theorical and not observed in practice.

168. This subsection looks at available data on flows to and from Luxembourg's financial centre with a selection of jurisdictions that were selected for analysis or "target jurisdictions" (TJs), containing countries being significantly impacted by terrorist attacks[84] and/or presenting strategic deficiencies within their CFT framework[85].

169. The detailed approach used to elaborate and categorise the list of these TJs can be found in Annex A.1. Key points of the Methodology are as follows:

Objective:

- Provide a concise, risk-based framework for identifying TJs for TF analysis within the NRA.
- Support proportionate analytical prioritisation, including where TF risks arise through cross-border flows despite the absence of domestic terrorist activity.

Framework and assumptions:

- Link terrorist activity to the three stages of terrorist financing: raising, moving, and using funds.
- Assume jurisdictions heavily affected by terrorism are exposed across all TF stages.
- Assess jurisdictions with weaker counter-terrorist financing (CFT) regimes as more vulnerable to TF raising and movement, with combined exposure indicating higher risk.

[84] On the basis of the Global Terrorist Index 2023. See Appendix A for further detail

[85] Pursuant to their results of the 4th round of mutual evaluations performed by the FATF (or other FATF-style regional body), especially with regard to Immediate Outcome 9. See Appendix A for further detail.

Data sources and selection criteria:

- Global Terrorism Index (GTI) 2023 used as a proxy for scale and intensity of terrorist activity.
- FATF / FSRB Mutual Evaluation Reports (4th round), with emphasis on Immediate Outcome 9 (IO.9).
- Selection where predefined GTI thresholds are exceeded in highly affected regions or where IO.9 effectiveness is rated Low or Moderate for jurisdictions that are subject to FATF calls for increased monitoring (February 2023–October 2024).
- General exclusion of jurisdictions rated Highly Effective on IO.9, reflecting mitigating impact of strong CFT systems.

Outcomes and prioritisation:

- Identification of 56 targeted jurisdictions in total. TJs were classified in tier groups (from tier 1, being exposed both directly to a terrorist threat and presenting weak CFT measures, to tier 6, exposed exclusively by presenting deficiencies in their CFT framework. More specifically,
- T1 and T2: 21 jurisdictions meeting both terrorism impact (GTI 2023) and TF vulnerability (IO.9) criteria. Deemed most vulnerable at being abused for TF purposes and exposed at all TF stages.
- T3 and T4: 19 jurisdictions identified on terrorism impact (GTI 2023) alone; deemed medium priority and exposed to all stages of TF.
- T5 and T6: 16 jurisdictions analysed based on TF vulnerability (IO.9 results) alone and more particularly exposed to raising and movement stages of TF.

170. The following table provides an overview of TJs and their classification into tier groups.

Table 8: Approach used to categorise TJs into tier groups

	Jurisdictions selected following …					
	…both T and TF approach		**…only a T approach**		**… only a TF approach**	
Criteria	GTI score 2023 + result of the 4th round of ME		GTI score 2023		Result of the 4th round of ME (IO9)	
Relevant TF stages	Raising, moving, using		Raising, moving, using		Raising, moving	
Tier groups	T1	T2	T3	T4	T5	T6
Countries identified	→10 TJs	→11 TJs	→9 TJs	→10 TJs	→8 TJs	→8 TJs

171. See Appendix A.1. for a complete description of these criteria and tier groups. The financial flows studied to fulfil this purpose, and the corresponding results are shown in the table below. The information in the table is organised as follows:

- the first column indicates the category of financial flows or position and reports the amount (in value or volume) related to TJs;
- the second column indicates the overall share of TJ flows in comparison to total flows;
- the third column indicates the most relevant TJs in monetary terms or volume;
- the fourth column indicates the percentage channelled by the top three TJs; and
- finally, the fifth column provides a breakdown of the percentage channelled by each of the top three tiers.

172. A detailed table of each financial flow or position can be found in Appendix B.

Table 9: Financial flows to and from TJs, overview: amounts between parenthesis represent million euros as of end 2024 (in the case of balances) or for 2024 (in the case of flows)[86]

	Percentage channelled by TJ (vs total flows LU)	Percentage channelled by top three TJ's	Percentage channelled by top three tiers
Bank deposits by residents in TJs (~25 234)	3,2%	84%	T5: 52% T6: 29% T4: 13%
Loans granted to residents in TJs (13 914)	1,8%	71%	T6: 40% T5: 37% T4: 16%
Corresponding banking, asset side (~8 351)	1,9%	79%	T6: 46% T5: 43% T4: 10%
Corresponding banking, liability side (~6 794)	2,4%	80%	T6: 67% T4: 18% T5: 13%
Investments in Luxembourg banks by residents in TJs (~500 878)	3,5%	65%	T5: 36% T4: 31% T6: 24%
Investments issued by residents in TJs held by Luxembourg residents (~332 317)	3,4%	76%	T5: 62% T4: 17% T6: 12%
Foreign direct investments from Luxembourg to TJs (~59 889[87])	12%	60%[88]	T5: 67% T6: 25% T2: 9%
Foreign direct investments from TJs to Luxembourg (~300 774)	11,2%	94%	T5: 69% T4: 19% T6: 12%

173. From the above positions, and in comparison, to total flows from and to Luxembourg with other countries, it appears that, in general, exposure with TJs is limited and located at around 2% to 3%. FDI stand out, with TJs accounting for more than 10% of total flows (especially due to flows with Cayman Islands).

174. TJs having themselves a financial centre as well as larger global economies account for a considerable share of TJs' flows with Luxembourg. These flows seem to be particularly consolidated and among the 56 countries that were analysed, top three TJs represent overall between 65% and 94% of total flows.

[86] All data provided by the BCL in September and October 2025 (with estimated amounts preceded by the symbol "~") except data on foreign direct investments, retrieved from STATEC website, Link.
[87] Net of a negative EUR 16 550 million position.
[88] 113% in absolute terms.

8.2. Analysis of non-financial flows with jurisdictions targeted for analysis

AT A GLANCE

Non-financial flows with TJs (including beneficial ownership and SMO registrations with the RBE and RFT, NPO activities, and trade flows) are generally limited. Beneficial owners (BOs) resident in TJs represent approximately 4% of total RBE registrations. Legal arrangements (RFT) show slightly higher TJ exposure (4–6%). NPO links to TJs are not at the ownership level but at the geographical/operational level: approximately 400 internationally-active NPOs with around a third operating in or near Sub-Saharan Africa, with significant exposure to T1 and T2 countries. Trade flows with TJs are limited (1,4–2,9% of totals).

8.2.1. Legal persons and legal arrangements: links to jurisdictions targeted for analysis

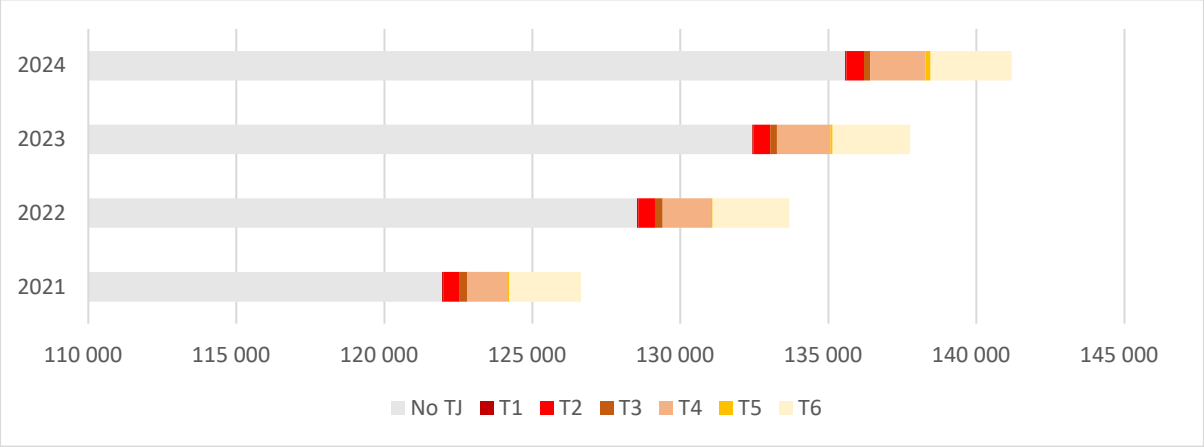
Legal persons

175. The prevalence of beneficial owners and managers residing in TJs has been established by analysing data from the RBE.

Analysis of beneficial owner data

176. Overall, the total number of registered BOs has continuously increased between 2021 and 2024. The number of BOs resident in TJs has followed suit, remained in overall percentage however quite stable (around 4% of total number of BOs).

Figure 10: Number of BO registered with the RBE



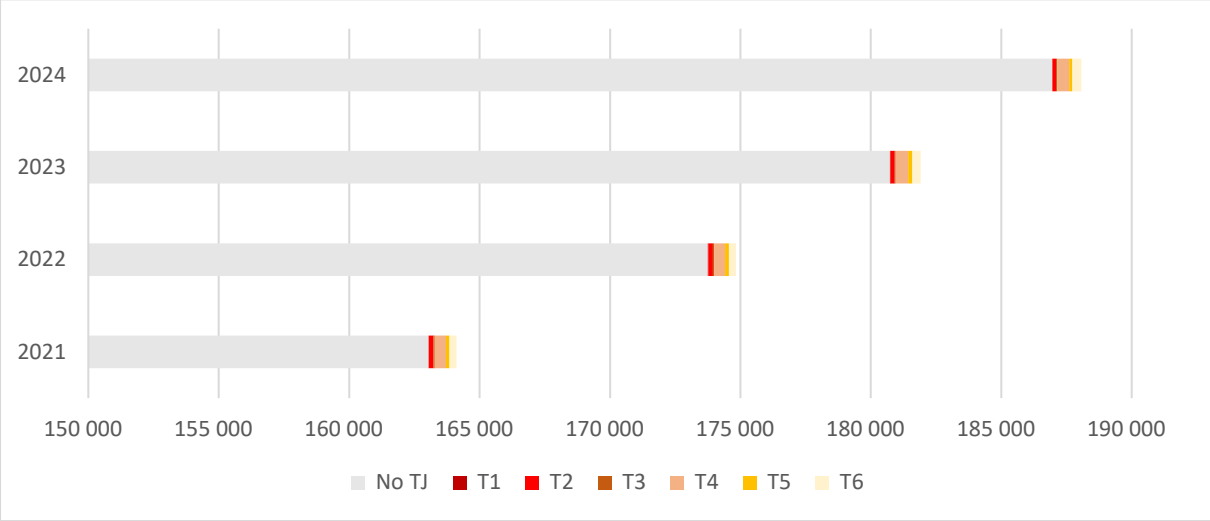
177. The number of BO registered with two countries (T6 and T4) accounts for around 35%, respectively 19% of total TJ registrations. These two countries represent, therefore, alone for more than half (59%) of all TJ registrations.

Analysis of senior management official (SMO) data[89]

[89] SMO as defined under article 1(7), letter (a) point (ii) of the 2004 AML/CFT Law.

178. The total number of SMO registrations has continuously increased between 2021 and 2024. The share of TJ residents has remained stable throughout the observation period and amounted to 0,4%. The proportion of SMOs is, therefore, considerably lower than that of BOs (see above).

Figure 11: Number of SMO registered with the RBE



179. The share of TJ is the highest in T4 and T6 countries, with an average share of 0,25% and 0,17% respectively.

180. Overall, prevalence of BO registrations with the LBR seem to be in line with overall financial flows identified in the previous section. SMO registrations for persons residing in TJ are very limited. These findings will be reflected in the overall risk assessment of legal persons performed in section 10.4.5.

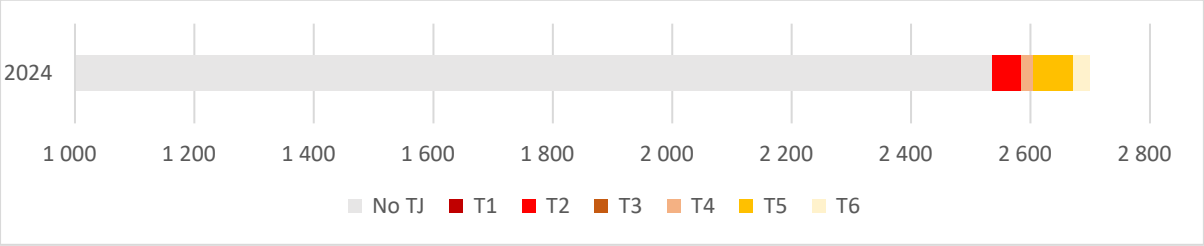
Legal arrangements

181. The prevalence of beneficial owners (all persons having a role in a registered *fiducie* or trust) residents in TJs has been analysed on data from the RFT.

182. Overall, the total number of registered BOs has continuously increased between 2021 (911) and 2024 (2 698). The number of BOs resident in TJs has followed suit, remained in overall percentage however quite stable (from 4% (end 2021) to around 6% (end 2024) of total number of BOs).

183. Looking more into detail at the situation as of end 2024, top 3 TJ country of residence of registered BOs concentrate more than 70% of registrations of all BOs residing in TJs. As shown in the figure below, more than half of BOs residing in TJs reside in T5 and T6 countries, although T2 represents a significant share.

Figure 12: Number of BO registered with the RFT, 2024



184. These findings will be taken into account in the overall vulnerability assessment of legal arrangements in section 10.5.

8.2.2. NPOs and links to jurisdictions targeted for analysis

185. In Luxembourg, legal entities in the non-profit sector may take the legal form of ASBLs and *Fondations*. Section 10.6 outlines in further depth TF vulnerabilities related to Luxembourg NPOs as defined by FATF.

Analysis of SMO data registered with the RBE

186. Considering that ASBL and *Fondations* have neither shareholders, nor partners, their SMO has to be registered with the RBE. Taken all together, the number of SMO of all registered ASBLs residents in a TJ during the observation period is very limited (less than 0,04% of total SMO registrations) and inexistant for *Fondations*. Considering this limited prevalence, further analysis has therefore not been conducted on this matter.

NPOs with an international dimension undertaking activities in jurisdictions targeted for analysis

187. In Luxembourg, the NPO FATF-subset[90] is considered to count around 1 000 ASBLs and *Fondations* as of end 2024 (less than 11% of ASBLs and *Fondations* registered with *the Registre de Commerce et des Sociétés* (RCS))[91]. Out of these FATF NPOs, approximately 400 primarily have an international activity, with around a third specifying the Sub-Sahara Africa region in their in statutory purpose.

NPOs with Development Non-Governmental Organisation (DNGO) status projects in jurisdictions targeted for analysis

188. In 2024, 60 NPOs accredited with the DNGO status from MoFA[92] received funds for carrying out projects abroad for a total amount of approximatively EUR 72 million (in 2023, 69 accredited DNGOs received funds for approximately EUR 82 million)[93].

189. From a geographical point of view Luxembourg's Development Cooperation pursues a policy of targeted action in a limited number of “partner countries”, taking into account the United Nations Development Programme’s human development index as well as considerations relating to the regional approach and situations of fragility. Two of the three partner countries are in sub-Saharan Africa (Cape Verde and Senegal), and the other is located in Asia (Laos). In addition, Luxembourg supports projects in “project countries”, including Costa Rica, El Salvador, Kosovo, Benin, Rwanda, Burkina Faso, Mali, Niger, Mongolia, the Occupied Palestinian Territories and Vietnam[94].

---

[90] NPO FATF-subset refers to those non-profit Luxembourg legal persons that fall under FATF definition of NPO. As explained in the interpretative note to recommendation 8, the FATF has adopted a functional definition of an NPO, which refers “to a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of “good works”.” Pursuant to the FATF’s interpretive note to Recommendation 8, these NPOs are particularly at risk of terrorist financing abuse.

[91] This percentage is presumed to be a high-end estimate.

[92] The number of NPOs accredited as DNGO by the MoFA is roughly 90 every year. Excludes funds provided to Cercle de coopération.

[93] Data received from MoFA on 3 June 2025.

[94] Ministry of Foreign and European Affaires website, accessed 9 July 2024, link.

190. With regards to the countries selected as TJs for the analytical purposes of this NRA, it appears that most of the fund receptors are situated in countries presenting strategic deficiencies in their CFT regimes on top of humanitarian needs and ecological threats (i.e. T1 and T2). Indeed, the very nature and geographical scope of the activities of DNGOs (carrying out development and humanitarian projects in developing countries) make them prone to maintain flows with risky geographies. It is also interesting to point out that Luxembourg has signed Indicative Cooperation Programmes with some of these countries in order to provide development aid.

191. Around 31% of funds from MAEE were allocated to TJs, with 22% alone being allocated to "partner countries" or "project countries".

192. In conclusion, when analysing the link between Luxembourg FATF NPOs and TJs, there is no link with regards to "ownership" (BOs) but a link with regards to "geography/flows with weak CFT geographies", especially with regards to T1 and T2 countries, that will be taken into account in the NPOs vulnerability assessment (section 10.6).

8.2.3. Imports and exports from and to jurisdictions targeted for analysis

193. As noted under section 2, Luxembourg's current account is heavily influenced by the importation and exportation of services (especially services related to financial and insurance services):

- Total imports from TJs amount to around EUR 8 billion during the observation period, representing 1,4% of total Luxembourg imports. Almost 70% of these imports from TJs were services.
- Total exports from TJs amount to around EUR 19 billion during the observation period, representing 2,9% of total Luxembourg exports. Slightly more than 75% of these TJ exports were services.

8.3. Analysis of economic and bilaterial relations with jurisdictions targeted for analysis – conclusion

194. The jurisdictions with which Luxembourg has strongest ties fall into Tiers 3 to 6, meaning that none is directly exposed to a terrorist threat while also presenting a weak CFT framework. To gain further insights on the TF risks encountered by those TJs with whom Luxembourg exchanges significant financial flows, their respective MERs were studied. The analyses of these countries are based not on the level of risk they present, but on the volume of flows between financial markets.

195. Conclusion on key TJ relationships: Four jurisdictions dominate Luxembourg's TJ exposure: a T5 country, linked through complementary investment fund structuring roles that generate large but economically rational FDI flows; a T6 country, linked through private banking, wealth management and Luxembourg life insurance contracts serving high-net-worth individuals; a T4 country, linked through bilateral political/economic relations, Islamic finance structures and sovereign wealth fund investments; and a T6 country, linked through tourism, steel-industry trade and serving as a major FTF transit hub given its geographic situation. ATM withdrawal analysis in border regions showed no evidence linking transactions to TF or FTFs. All four relationships carry theoretical TF relevance, but none shows evidence of materialised risk.

9. Luxembourg terrorist financing threat context – conclusion

AT A GLANCE

Luxembourg's TF threat context is primarily shaped by its role as a pan-EU retail banking, PI, EMI and VASP hub rather than by any domestic terrorist presence. The dominant threat is that of small cells and lone actors with low TF needs abusing basic financial products for small-amount transactions (predominantly intra-EU and jihadism-related) rather than large international terrorist groups or financiers moving substantial sums through sophisticated structures. Luxembourg functions as a transit rather than a source or destination country for TF purposes. The theoretical exposure to large international TF flows exists by virtue of Luxembourg's financial-centre status. But analysed flows, non-financial links and empirical data do not support a conclusion of material risk from this vector. Mechanisms observed in ML schemes, such as corporate structures, NPO misuse, crowdfunding, fraud, AI-enabled forgery, may also feature in TF schemes, particularly for sophisticated actors, warranting continued vigilance.

196. As evidenced by Insight Box 2, Luxembourg's neighbouring countries experienced throughout the observation period of this report over half of the reported terrorist attacks within the EU, with France alone accounting for 48%. In terms of ideologies, arrests and attacks related to jihadism were prevalent. The prevalence of these typologies is also in line with what has been observed by the CRF, where most reports filed concerned Islamism[95]. Most TFTR/TFAR were also reported by some major institutions having their European headquarters in Luxembourg and operating across the EU under European passport. These entities predominantly offer payment services or basic financial services. Most of the time, the only link with Luxembourg is the business relationship between a Luxembourg professional and a client residing in another EU Member State (or in a third country).

197. Luxembourg TF threat context seems therefore to be primarily impacted by financiers wishing to move small amounts through peer-to-peer transactions, cash deposits or withdrawals, or payment transactions. Digital platforms such as social media and gaming platforms, live streaming and encrypted platforms are used for propaganda purposes and to solicitate financing from sympathisers. Algorithms and content are particularly tailored to the attention of a younger audience, especially those experiencing social isolation, mental health problems and loneliness. In addition to that, these individuals often rely on the financial resources of someone else. When financing is not directly linked to a violent attack, and/or when legitimate funds are involved, it poses detection challenges.

198. Luxembourg acknowledges that its financial centre could potentially be misused by large terrorist financiers to invest funds that may at same point be used for terrorist purposes and to this end, Luxembourg has raised awareness on this potential exposure since its TF VRA 2022, but overall, this threat scenario remains rather theoretical. Furthermore, analysed flows and links with

[95] Considering that the CRF receives filings where there are potential, but reasonable grounds to suspect TF, this paragraph includes typologies observed as part of the broader Islamist ideology (including jihadism, but also other non-jihadi movements or ideologies part of the broader Islamist ideology). TFARs/TFTRs received linked to Islamism do not necessarily always involved jihadism.

jurisdictions being particularly impacted by terrorism and/or having weak AML/CFT frameworks do not reveal to pose a material threat in terms of value and volume to the Luxembourg financial centre.

199. In practice, Luxembourg TF threat context does not significantly differ from the broader European context, where the threat is more that of smaller cells and lone actors with small TF needs abusing basic financial products, rather than that of larger international terrorist groups or financiers moving large funds by using more sophisticated products or services. Indeed, reports filed with the CRF suggest that threats stemming from more sophisticated products or services are less prevalent and frequent.

200. For both types of potential TF exposure, Luxembourg is considered a transit rather than a source and destination country for TF purposes. Moreover, mechanisms observed in ML schemes may be found in TF schemes; be it in relation with fraud and forgery to generate falsified documents to access services otherwise not accessible (through artificial intelligence, "crime-as-a-service" operators), to access restricted or illegal goods (i.e. double use items, weapons, chemicals) or to hide the true BO or origin of the funds (through the misuse of corporate schemes, NPOs, crowdfunding activities). The latter are particularly true for threats stemming from these larger international terrorist organizations or wealthy financiers that are required to intermediate and complexify their funds and ownership structures, but as stated below, this TF threat scenario, although it may not be completely discarded, it remains rather theoretical.

201. The table below summarises the results of Luxembourg TF threat assessment with regard to small and high-value financiers:

Table 10: Luxembourg TF threat level

TF requirements	TF relevant actors	Most prevalent geographies	TF Threat level
Small-value financiers	Decentralized networks, small terrorist cells and lone actors; FTFs	European countries, including Luxembourg	Medium
High-value financiers	International terrorist organizations; State sponsors of terrorism; Corporate terrorism	Countries being particularly impacted by terrorism and/or presenting AML/CFT deficiencies	Low

10. Inherent terrorist financing risk – vulnerabilities assessment

202. The sectors falling within the scope of the vulnerabilities assessment are mapped on the basis of supervisory structure rather than on the basis of activity. The vulnerabilities assessment covers all sub-sectors within the scope of the 2004 AML/CFT Law, structured by supervisory architecture rather than activity type. Inherent risk scores reflect sector exposure before the application of mitigating measures, assessed across six dimensions: size/structure, ownership/legal structure, products/activities, geographical exposure, clients and channels. The resulting inherent risk levels do not take into account the effects of existing mitigating measures. In fact, the impact of these mitigating measures in reducing inherent risk for the different sub-sectors is assessed in the section on mitigating measures and reflected in the residual risk levels presented in section 14.

10.1. CSSF supervised sectors

10.1.1. Banks

203. This section includes the analysis of entities with a banking license (chapter 1 of the 1993 LSF) and includes retail and business banks; entities operating online; wholesale, corporate and investment banks; private banking and custodians and sub-custodians (including Central Securities Depositories (CSDs)).

AT A GLANCE

The banking sector, comprising over 110 banks and above EUR 950 billion in managed assets, is assessed across the following sub-sectors: retail and business banks; operating online; wholesale, corporate and investment banks; private banking and custodians and sub-custodians.

Retail and business banks, with over one million client accounts and widespread payment/card products, present the highest inherent TF risk within the banking sector, particularly through deposit-and-withdrawal patterns, consumer credit misuse and cross-border payment services. Entities operating online add exposure through approximately 93 million active client accounts and virtual IBAN issuance and also present high inherent risk. Wholesale/corporate/investment banking and custodian services, characterised by sophisticated, standardised products and high entry thresholds, present medium inherent TF risk. Private banking, while theoretically exposed to TF by state sponsors of terrorism or wealthy financiers, presents medium inherent risk, considering close client relationships, discretionary mandates and high entry thresholds, which have a beneficial impact on the inherent risk score.

Overarching risk factors for the banking sub-sector are the sector's size, volume of clients/transactions handled, as well as the international dimension of the sector's activities. Although products and activities provided by retail and business banks and entities operating online in Luxembourg are not riskier than elsewhere, they contribute to the higher inherent risk of these two sub-sectors relative to the others.

Sector	Sub-sectors	2026 NRA: Inherent risk
Banks	Retail and business banks	High
	Entities operating online	High
	Wholesale, corporate & investment banks	Medium
	Private banking	Medium
	Custodians and sub-custodians	Medium

204. Luxembourg's banking sector is large in terms of size, counting over 110 banks in 2024 from more than 20 different countries. The sector managed assets worth above EUR 950 billion in 2024 and employed over 26 000 people.

10.1.1.1. Retail and business banks, entities operating online

AT A GLANCE

Most relevant TF stage:

☒ Raising ☒ Moving ☒ Using ☐ Non-relevant

Products and activities rather suitable for:

☒ Lone actors, small cells and FTFs with small TF needs
☐ International organisations and other terrorist actors with larger TF needs

At the product level (SNRA)

Products and activities assessed in the 2022 SNRA related to retail and business banks are "retail deposits on accounts (excluding private banking)", "business loans" and "consumer credits and low-value loans". The 2022 SNRA concludes the following TF risks levels regarding the whole EU:

- "retail deposits on accounts" are assessed to bear "High" risk;
- "business loans" are assessed are assessed to bear "Low" risk;
- "consumer credits and low-value loans" are assessed to bear "High" risk;
- "payment services" are assessed to bear "High" risk; and
- "mortgage credit and high-value asset-backed credits" are assessed to bear "Low" risk.

The 2026 NRA assesses associated inherent risk of these products under "products/activities". In the context of Luxembourg retail and business banks and entities operating online, the resulting associated TF risks are considered "High" (in line with the findings of the 2022 SNRA). Products and activities related to entities operating online are mainly e-money activities and payment services. They are in most instances equivalent to products and activities related to retail and business banks notably the offer of payment accounts. However, a bank account is always used for loading the e-money products.

None of the banks of these sub-sectors offer anonymous prepaid cards or products and services linked to anonymous prepaid cards.

At the sub-sector level (NRA)

In Luxembourg, these sub-sectors' TF inherent risk levels are "High", with key risk drivers being:

- The sub-sector's size and volume of clients/transactions followed by products/activities, international business and channels for retail and business banks.
- The sub-sector's, international dimension of business, volume of clients/transactions, and channels followed by products/activities for entities operating online.

Retail and business banks

205. Overall, Luxembourg counted nine retail and business banks managing around EUR 180 billion of assets and generating a total gross income of around EUR 9 billion as of end 2024. The number of employees has decreased less substantially (6%). Indeed, the sub-sector is still the highest employer of the banking-sector, counting around 7 800 employees in 2024. The degree of concentration in the sector is high, with top five banks dominating the sector and accounting on average for almost 95% of the market's assets during the observation period of this report.

206. Retail and business banks offer basic/traditional financial services, such as bank accounts (allowing deposits on accounts and transfers), credit cards, online/mobile banking operations and loans (consumer, low value and mortgage loans). Retail services are oriented towards an individual clientele, (i.e. natural persons), business banks related services towards the needs of businesses, especially small and medium-sized enterprises.

207. In this regard, regulated banking services have globally been observed to be misused in a larger extent in the financial management of small cells and individual terrorists, as well as ethnically or racially motivated terrorist groups (cf. sections 4.2 and 4.3). They have occasionally been involved in larger organizations[96].

- Deposits on (current or savings) accounts are more likely to be used for storage purposes in the context of low-scale threats. Funds from saving accounts are typically withdrawn by self-radicalised individuals and FTFs to be spent in cash[97]. In general, this method requires basic knowledge and planning, which makes it easily accessible, especially when legitimate funds are used. It should also be noted that relatives or the social entourage of financiers could also be used, extending the scope of the intent and capability analysis[98].
- Consumer credits and low-value loans could be used by financiers and terrorist actors to finance travel by FTFs to high-risk non-EU countries. The most commonly used-low value product is consumer credit[99].
- Payment services are likely to be used by financiers to store and move funds and to cover for expenditures. Characteristics like the prevalence of occasional transactions, the large volume and the high-speed of transactions as well as their cross-border nature make these products attractive for TF purposes[100]. In Luxembourg, the level of occasional transactions is relatively

[96] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025, link.
[97] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025, link.
[98] EU Commission, *SNRA,* 2022, link.
[99] EU Commission, *SNRA,* 2022, link.
[100] EU Commission, *SNRA,* 2022, link.

low, and therefore this is not a risk factor particularly applicable to Luxembourg retail and banking banks. According to the latest update on TF risks by the FATF, cards (credit and debit) are globally observed to be used in TF cases. In comparison to wire transfers, they can, in some cases, offer less traceability and transparency on identities of both the initiator and the recipient (for instance when the transaction is disguised as a commercial payment). Cases where such cards were fraudulently obtained through forged documents have also been reported globally[101].

208. Except for the prevalence of occasional transactions already noted, the above-mentioned vulnerabilities apply to Luxembourg retail and business banks. For instance, during the observation period:

- Five retail and business banks operated ATMs;
- Four banks offered credit cards with, on average, around 550 000 cards issued per year;
- On average, one million of cash deposits per year with an average amount of EUR 2 450 per transaction;
- Cash withdrawals at the branches or bank agencies: around 7,6 million transactions per year with an average amount of around EUR 415 per transaction;
- Consumer debt was held by 35% of Luxembourg households, with personal loans accounting alone for 26%. Overall, the average level of personal loans was twice as high in Luxembourg as in the euro area. 70% of households cited the purchase of a vehicle as the main reason for their personal loan, a reason mentioned by only 38% of households in the euro area[102].

209. Although terrorist financiers (FTFs in particular) have been known to use low-limit prepaid cards for TF purposes including to purchase propaganda products[103], it should be noted that no Luxembourg bank offered such cards nor offered products and services linked to anonymous prepaid card during the observation period.

Case study 3: Use of credit cards and e-money accounts and payments to facilitate TF in Luxembourg[104]

The case was detected based on international cooperation between law enforcement authorities regarding a Luxembourgish citizen spreading ISIS-related content on social media. The suspect focused on the pseudo-religious legitimisation of the ISIS ideology and managed to circumvent the measures taken by social media platforms prohibiting such content. The suspect radicalised after the departure of his close friend as a FTF in the Syria/Iraq area.

First results showed that the suspect was holding a bank account and an associated debit card within a bank in Luxembourg, as well as an active account with a payment and e-money institution. Further analyses revealed that the credit card associated to the identified payment and e-money account was also connected to two further payments and e-money accounts held by two unknown individuals. In addition, a total of four payments and e-money accounts seemed to be linked between each other by either the physical address, e-mail addresses or IP addresses. The observed

[101] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025, link

[102] Pulina G., *Consumer debt in Luxembourg and the euro area: evidence from the Household Finance and Consumption Survey*, 2023, link.

[103] FATF, *Comprehensive Update on Terrorist Financing Risks,* 2025 (section 4.2. "Prepaid cards"), link.

[104] Case study from FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025 (Section 4.1 "Banking services"), link.

account movements were mainly purchases of religious clothing for Muslim women, transfers to marriage agencies or donations to religious NPOs. In addition, suspicions were raised that the suspect's wife was involved in the case too. An exhaustive transactional analysis was performed on her payment and e-money accounts and suspicious transfers were identified as to an individual who matched a suspect in the FIU's databases. The individual was suspected in a bordering country to have links to TF.

Red flag indicators included frequent transfers and donations made to religious NPOs with ties to extremist movements, but also to NPOs with the intent of financially supporting widows, families of deceased fighters and prisoners in conflict areas and high-risk jurisdictions in terms of terrorism and TF risks.

210. Products and services offered by retail and business banks in Luxembourg are not riskier than those offered elsewhere in other countries. However, the significant volume and number of client accounts that are by those professionals amplify potential TF exposure. As such, retail and business banks counted over one million client accounts in 2024 with almost 90% of them belonging to natural persons.

211. With regard to risk profiles of retail and business banks' clientele, the share of clients being assessed as high-risk by these banks (entity-level self-assessment) was relatively low and situated around 1% and 2% during the observation period. As noted previously, especially for low-value financiers, the origin of the funds is usually licit, and transactions might occur between unrelated and un-designated individuals, posing additional challenges in terms of detection. The identification of transactional indicators is therefore crucial.

212. Retail and business banks were predominantly involved in face-to-face contact with their clients. Although the Luxembourg branch network was relatively dense (compared to other EU countries), banking transactions have become more and more digital and require less direct client contact. This might increase TF risks.

Case study 4: Use of funds[105]

Client A has a long-standing banking relationship and an unremarkable banking history. Since retiring from the armed services on medical grounds, he has dedicated much of his time to supporting a far-right wing extremist group ("the Group") and regularly raises funds for the Group by way of selling memorabilia and organising training sessions for members in remote locations. Such training includes weapons training and bomb making skills. The Group advocates violent direct action against any organisation that helps to support illegal migrants into the country. In recent times, the Group has focused its attention on community leaders and politicians seeking to intimidate and drive their agenda. Client A uses his bank account to receive third party payments for the sale of the memorabilia and attendance at the weapons training events. Payments are made to hire venues for the training events. He also posts pictures of himself wearing paramilitary clothing and carrying a firearm advertising the next training session. The volume of third-party payments into a personal bank account raises concerns at the bank. When challenged by bank staff, client A claims that the funds received from third parties represent income derived from trading on an online

[105] CRF.

marketplace. Client A is subsequently arrested at a violent demonstration and charged with violent disorder and unlawful association.

Indicators

- Change in banking activity;
- Unexplained third-party payments being received regularly;
- The photographs posted on the website;
- Payments made to secure training venues;
- Client A concealing the true reason for the third-party payments.

Entities operating online

213. The sub-sector serves a considerable number of active client accounts (approximately 93 million in 2024), although it comprises five entities and is dominated by one entity in 2024 in terms of number of clients and volume of transactions.

214. Regarding products and activities, the entities offer mainly payment related services, including in relation to e-money services, transfers of funds, or the settlement of transactions on behalf of other type of regulated financial institutions. It is worth noting that payment services using vIBANs can also be offered.

215. Products and activities provided by entities operating online do not substantially differ to those offered by retail and business banks (especially with regard to payment services and basic financial services). Therefore, the analysis regarding products and activities outlined in the retail and business banking section above also applies to entities operating online providing payment services. Analysis of products regarding e-money services are analysed in section 10.1.3.

216. As for retail and business banks, the clientele is mainly made up of natural persons residing within the EU. Similarly, the share of high-risk clients remains very low. On the contrary, customer communication channels are performed entirely online that may create opportunities for illegitimate users to enhance opacity through fake accounts or opening of accounts using forged documents.

10.1.1.2. Wholesale, corporate & investment banks

AT A GLANCE

Most relevant TF stage:

☐ Raising ☒ Moving ☐ Using ☐ Non-relevant

Products and activities rather suitable for:

☐ Lone actors, small cells and FTFs with small TF needs

☒ International organisations and other terrorist actors with larger TF needs

At the product level (SNRA)

Products and services linked to:

- corporate banking products and activities are assessed to bear "Low" TF risk;
- institutional investment products and services are deemed not relevant with regard to TF risks;
- high value asset-backed credits are assessed to bear "Low" TF risks.

At the sub-sector level (NRA)

In Luxembourg, the sub-sector inherent TF risk is considered to be "Medium".

217. In Luxembourg, there were 38 wholesale, corporate and investment banks in 2024 compared to 44 entities in 2021. The number of employees has more than doubled during that time, counting almost 4 000 employees in 2024. Whereas total assets of the sub-sector have decreased slightly during the observation period reaching EUR 205,5 billion in 2024, total gross income have experienced a fourfold growth, amounting to EUR 18,6 billion in 2024. In terms of market's assets, the sub-sector has become more concentrated since the beginning of the observation period, with top five entities accounting 45,3% of the market's assets in 2021 and 86% in 2024.

218. Services are mostly commoditised and standardised and include lending activities, cash and treasury management, capital market activities as well as custody activities (e.g. custody of securities, and related dividend and interest payment collection and distribution). Some banks also offered trade finance related services. These services generally involve substantial amounts, as well as advanced expertise and knowledge. Consequently, they are not very attractive for TF purposes, which is also confirmed by the SNRA 2022, which specifies that other sectors present more attractive TF features.

219. Nonetheless, it should be noted that, similar to the conclusions drawn in the 2025 NRA ML, the proportion of high-risk and PEP clients in Luxembourg wholesale, corporate and investment banks, along with the significant volumes processed, drives the sub-sector's risk exposure in general.

10.1.1.3. Private banking

AT A GLANCE

Most relevant TF stage:

☐ Raising ☒ Moving ☐ Using ☐ Non-relevant

Products and activities rather suitable for:

☐ Lone actors, small cells and FTFs with small TF needs

☒ International organisations and other terrorist actors with larger TF needs

At the product level (SNRA)

The SNRA continues to assess TF risk in the private banking sector as not relevant. However, it admits the possibility that wealthy terrorism sponsors might use private banking services in the EU to manage on their behalf assets not directly related to, or intended for, the financing of any terrorist activities.

At the sub-sector level (NRA)

The sub-sector inherent TF risk level is assessed to be "Medium".

The 2023 update of the Private Banking Sub-Sector Risk Assessment includes a section dedicated to TF risks. It concludes that there is no strong indication that private banking services are particularly exposed to TF risks, but private banks are well advised to remain cautious.

This report can be consulted on the CSSF's website: link.

220. Luxembourg's private banking sector is large and remained fragmented despite the consolidation process initiated over the past few years. During the observation period, there were 48 entities in 2021 compared to 34 in 2024. Assets under management (AuM) grew substantially, reaching almost EUR 760 billion in 2024. The number of employees varied between 7 300 and 8 300 during the observation period.

221. Whereas the number of clients rose between 2021 and 2023, it fell by almost 20% in 2024. The share of European clients remained, however, stable and high during the observation period (around 88%). On average, the share of natural persons clients slightly exceeds the share of legal persons (58% vs. 42%). The share of high-risk clients is relatively high, with for example 7,5% of clients presenting complex structures[106]. This could pose some risk in case where the BOs and the exact nature and purpose of the relationship for this activity are more difficult to establish.

222. Private banks in Luxembourg do currently not offer high-risk products. The service offered by private banks is mainly portfolio management. Discretionary portfolio management brings the clients' assets under the control of the bank, in line with a signed mandate. Thus, client assets are managed by the bank and investment decisions are made by the bank, not by the client directly. In addition, the funds are usually invested for long term.

223. Thus, the close relationship between the client and the bank, the high entry thresholds, the discretionary mandates and the longer-term view on investments make private banking an unlikely and unsuited tool for the financing of (low value) terrorist support or acts. Indeed, Luxembourg private banks also follow a more traditional operating model, preferring direct contact and face-to-face relationship management over solely online identification and communication methods with clients.

224. Nonetheless, Luxembourg private banks could in theory be exposed to TF risks, where abused by wealthy individuals or organisations acting as terrorism sponsors or supporting terrorist organisations, by investing money not directly linked to, or directed at, the financing of terrorism, via their accounts held with a private bank.

10.1.1.4. Custodians and sub-custodians

AT A GLANCE

Most relevant TF stage:

[106] "Complex" is defined as a legal persons or legal arrangements with several layers, layers having no rationale in the structure, layers being located in countries that do not comply with international tax transparency standards, or layers in countries having no link at first sight with the country of the beneficial owners/shareholders/investors/managers or the investment.

☐ Raising	☒ Moving	☐ Using	☐ Non-relevant

Products and activities rather suitable for:

☐ Lone actors, small cells and FTFs with small TF needs

☒ International organisations and other terrorist actors with larger TF needs

At the product level (SNRA)

The SNRA assesses corporate banking services to bear "Low" TF risks. Furthermore, the report notes that institutional investment products and services are not considered relevant for TF purposes.

At the sub-sector level (NRA)

The sub-sector TF inherent risk level is evaluated to be "Medium".

225. In Luxembourg, the sub-sector encompassed 29 entities resulting in a total gross income of EUR 16,5 billion and assets worth around EUR 282 billion in 2024. In 2024, the sector counted more than 160 000 client accounts, of which 9% were flagged as being high-risk. The majority of the sub-sector's clientele were natural persons, although in a decreasing share since 2021. Among the clients that were legal persons (which constituted on average approximately 34% of the clients), most were Luxembourg investment funds, driven by the requirements applicable for the vast majority of investment funds to appoint a Luxembourg bank for the custody of their investments. During the observation period, the share of PEP clients has almost doubled in relative terms, partly explained by the decrease of the number of client accounts since 2021.

226. Custodian and sub-custodian services are mostly commoditised and standardised (e.g. custody of shares/financial instruments, dividend and interest payment collection and distribution). Central Securities Depositaries provide notary services of securities listed on regulated markets (i.e. maintenance of the register of the issuance program) and operation of the settlement system in accordance with the Central Securities Depositary Regulation. The relationships of the CSD are the participants to the market which are central bank, banks, investment firms, custodian, global custodian (i.e. supervised entities). The CSD plays a pivotal role for post-trade by ensuring that transactions on financial instruments listed (mainly shares/bonds) on a regulated market are settled in due time (T+2 – mitigation of liquidity and counterparty risk). Overall, the SNRA 2022 precises that other sectors present more attractive TF features. Extensive expertise and knowledge are required, as well as a substantial amount of funds in order to access these services, decreasing their risk of TF abuse.

227. Although ongoing client interaction was indirect, client contact for new account services was direct, limiting TF risks to some extent.

10.1.1.5. Cross banking sub-sectors

228. **Innovative financial services** such as the provisions of virtual IBANs (vIBAN) are drawing increased attention in terms of TF risks, as they could provide new opportunities to hide or intermediate the final destination and the economic beneficiary of wire transfer[107]. Indeed, while the transactions are settled through a master payment account identified by an IBAN, vIBANs attached to

[107] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025, link.

this account can be issued to many end-users. There might be a long chain of intermediaries such as a PI or EMI that issue the vIBAN received by the bank to its clients which themselves issued the vIBAN to their clients. The monitoring of the use of vIBAN is challenging and the complexity makes it more difficult and less fast for FIUs to trace the geographical origin and destination of funds, which will require further international cooperation.

229. In addition, due to the speed with which (qualified) instant payments are required to be executed (in 10 seconds, 24/7) by payment service providers (PSPs) pursuant to the Instant Payments Regulation of 13 March 2024 (Regulation (EU) 2024/886)[108], funds are made available instantly to the beneficiary of the euro credit transfer, who can therefore use them immediately. All the schemes detailed above will be used in this context too. It is however worth noting that mitigations are legally foreseen within the Instant Payment Regulation as regards targeted financial restrictive measures, including those linked to TF. Notably PSPs must carry out verifications of their payment service users immediately following the entry into force of a new or amended financial restrictive measure and they are also obliged to screen the client database at least once a day. Transactions cannot be executed as long as potential "hits" have not been cleared.

230. **Trade finance related services** provided by the banking sub-sector could be misused for TF purposes. The level of risk for such a misuse is assessed to be medium. Indeed, considering the high number of parties involved in trade finance services, the process related to those activities requires heavy and varied documentation, making both customer due diligence and the analysis of transactions much harder and more complex to perform.

231. The commonly identified vulnerabilities of trade finance services are the following:

- Over- or under-invoicing to shift value between parties while keeping the transaction looking legitimate;
- False or forged invoices with a misrepresentation of goods/services quantity or prices;
- Use of shell companies, front companies, nominee or any opaque structure to hide the beneficiary;
- Routing trades through corridors where terrorist groups operate or exert influence.

232. End of 2024, 23 credit institutions offered trade finance related services in Luxembourg out of which 15 were wholesale corporate and investment banks (three as main activity, one as regular activity and 11 as some activity), three retail and business banks (one as regular activity and two as some activity), four private banking (some activity) and one custodian and sub-custodian (some activity). As regards to the three banks from the wholesale corporate and investment sub-sector for which trade finance related services correspond with their main activity, those are servicing approximately 5 000 clients i.e. less than 0,1% of clients serviced by all banks, and around 7% of the clients serviced by the wholesale, corporate and investment bank sub-sector. Consequently, the TF risk exposure of Luxembourg through trade finance is relatively limited.

[108] While this regulation is directly applicable in Luxembourg, certain provisions have been adopted at national level to complete the framework, please see amendments introduced by the implementing Law of 4 April 2025 in the Law of 10 November 2009 on payment services.

10.1.2. *Investment sector*

AT A GLANCE

Most relevant TF stage:

☐ Raising ☒ Moving ☐ Using ☐ Non-relevant

Products and activities rather suitable for:

☐ Lone actors, small cells and FTFs with small TF needs
☒ International organisations and other terrorist actors with larger TF needs

Luxembourg's investment sector encompasses investment firms (authorised for advisory, portfolio management, order transmission and execution), collective investment vehicles (UCITS, AIFs and other fund structures) and CSSF-supervised pension funds. Investment firms present relatively low inherent TF risk given that investment decisions are made by portfolio managers on long-term mandates and flows are exclusively channelled through depositary banks. Collective investment vehicles, particularly those with complex structures and international distribution, present moderate exposure linked to the geographic scope of their investor bases and the use of intermediaries; however, the SNRA 2022 notes that other sectors present more attractive TF features. Pension funds present minimal TF risk given their restricted membership, regulatory oversight and long-term investment horizons.

At the product level (SNRA)

The 2022 SNRA assesses TF risks linked to the retail and institutional investment sector as "non-relevant".

At the sub-sector level (NRA)

TF risk levels for the investment sub-sectors are assessed as follows:

Sector	Sub-sectors	2026 NRA: Inherent risk
Investment sector	Investment firms authorized to carry out the services of investment advice and portfolio management	Medium
	Investment firms authorized to carry out the services of reception and transmission of orders in relation to one or more financial instruments and of execution of orders on behalf of clients	Medium
	Investment firms authorized to carry out activities of dealing on own account, of underwriting of financial instruments and/or placing of financial instruments on a firm commitment basis and of placing financial instruments without a firm commitment basis	Low
	Collective investments	Medium
	CSSF supervised pension funds	Very low

10.1.2.1. Investment firms

233. Between 2021 and 2024, the total number of investment firms decreased by around 10% with 90 entities in 2024 (in comparison to 101 in 2021).

234. Their clientele was mainly made up of natural persons (on average 92% between 2021 and 2024). Although most clients resided outside Luxembourg (on average 97%), nine out of ten clients resided within the EU in 2024. The share of clients being legal persons or legal arrangements is less prevalent, representing 7% and 2% respectively in 2024. This could pose a risk limited to those cases where BO identification and the exact nature and purpose of activity are more difficult to establish.

235. Although 60% of investment firms counted high-risk clients among their client base during the observation period, these clients represented 6% of the total client base in 2024. In a similar vein, less than 40% of investment firms had clients from weak AML/CFT countries as identified by the FATF, although total amounts involved are limited, representing around 0,2% in 2024. Overall, it should be noted that flows are exclusively handled through depositary banks, limiting their overall exposure to TF risk.

236. In 2024, almost 80% of investment firms have acquired new clients, with more than half of them having met them face-to-face.

Investment firms authorized to carry out the services of investment advice and portfolio management

237. This sub-sector encompasses investment firms authorised to carry out the specific activities referred to in article 24-4 and 24-5 of the 1993 LSF.

238. Whereas the sub-sector counted 92 entities in 2021, 82 investment firms provided relevant services in 2024:

- 82 investment firms were authorised to carry out the activity of investment advice, with 25 of them exercising those activities. Top-five firms captured around 75% of the total revenues, and almost 70% of portfolio advised; and
- 72 investment firms were authorised to carry out the activity of private portfolio management, with 62 of them exercising those activities. Top-five firms captured just over half of total revenues and managed about 66% of AuM.

239. On average, the sub-sector was assigned 75 000 mandates per year, with almost all of them stemming from private portfolio management (and the remainder from investment advisers).

240. Products and activities are not suitable to TF as investments are done on a long-term perspective, and investment decisions are made by the portfolio managers. However, this activity could theoretically rely on third-party DNFBPs[109] as intermediaries, which could have been involved in TF typologies. However, at the time of writing, there is no evidence of the use of this type of intermediaries by IFs[110].

[109] DNFBPs are defined in the FATF Glossary (link), and consist of a wide range of professionals, such as lawyers, notaries and other independent legal professionals, accountants and trust and company service providers (TCSPs).
[110] CSSF information.

Investment firms authorised to carry out the services of reception and transmission of orders in relation to one or more financial instruments and of execution of orders on behalf of clients

241. This sub-sector encompasses investment firms authorised to carry out the specific activities referred to in articles 24-1 and 24-2 of the 1993 LSF.

242. In 2024:

- Brokers: 88 investment firms were authorised to carry out the activities of reception and transmission of orders in relation to one or more financial instruments, with 30 of them exercising the activity. They generated transactions worth around EUR 2,5 billion; and
- Broker-dealers (non-bank): 80 investment firms were authorised to carry out the activity of execution of orders on behalf of clients, with 15 exercising this activity. They generated transactions worth almost EUR 280 billion.

243. It should be noted that the sub-sector is characterized by a very high degree of concentration, with top-five entities generating the totality of the market's revenues and volume of transactions.

244. Altogether, the number of assigned mandates within this sub-sector amounted to nearly 75 000 in 2024, slightly above the average of 72 500 observed during the observation period of this NRA.

245. Products offered could be more TF vulnerable as the funds used for stock/securities trading can be retrieved on a short term and withdrawn (i.e. the "moving" step of TF). However, this business model does not seem to be particularly suitable for TF as it is mainly addressed to institutional investors and because the financial flows in the context of investments are received and hence subject to a second layer of transaction monitoring by banks.

Investment firms authorized to carry out activities of dealing on own account, of underwriting of financial instruments and / or placing of financial instruments on a firm commitment basis and of placing of financial instruments without a firm commitment basis

246. This sub-sector encompasses investment firms authorised to carry out the specific activities referred to in articles 24-3, 24-6, and 24-7 of the 1993 LSF.

247. In 2024, firms in the sub-sector traded EUR 5,5 billion of assets. As of end 2024, there were ten investment firms providing relevant services. More precisely:

- five investment firms were authorised to carry out the activity of dealing on own account, with three exercising this activity;
- two investment firms were authorised to carry out the activity of underwriting financial instruments and/or placing of financial instruments on a firm commitment basis, with one of them exercising this activity; and
- six investment firms were authorised to carry out the activity of placing of financial instruments without a firm commitment basis, with two of them exercising this activity.

248. The absolute number of high-risk clients for these investment firms is limited (with less than 50 clients per year on average). In addition to that, they do not have legal arrangements as clients. In combination with the limited number of clients, client risk for these professionals is considered less prevalent than for the other investment firms.

249. In addition, products and services offered by the sub-sector are not suitable for TF purposes, as this activity is intended for institutional clients mostly and based on long term investments (for underwriting).

250. Although all traders/market-makers onboarded new clients during the observation period, client flow is less significant for these investment firms (considering the limited number of clients). Onboarding is either performed face-to-face or in combination with remote communication channels.

10.1.2.2. Collective investments

Insight Box 5: Complementarity of information provided in the 2025 update of the Collective Investment Sub-Sector Risk Assessment

Please note that the 2025 update of the Collective Investment Sub-Sector Risk Assessment on the CSSF's website should be consulted for an in-depth assessment of the collective investment sub-sector's TF risks: link

251. The below analysis covered Undertakings for Collective Investments in Transferable Securities (UCITS), Management Companies (ManCo) and Alternative Investment Fund Managers (AIFMs). The number of authorized and registered ManCos has slightly increased from 1 190 in 2021 to 1 205 in 2024. AuMs of ManCos also increased over the period (except in 2022), rising from EUR 5 234 billion in 2021 to EUR 5 887 billion in 2024[111].

252. During the observation period, 96% of UCI initiators (by net assets) were foreign. More precisely, the origin of the main foreign UCI initiators in Luxembourg by net assets were the US (20%), the UK (17%), Germany (15%) and Switzerland (12%), which are considered lower risk in terms of ML and TF for the origin of the products managed by both UCI Manco and AIFMs in these countries.

253. Overall, products and services offered by the sub-sector do not have attractive features for TF abuse, neither by the type of lone actors nor by the type of international organisations:

- Short-term and transitory cash flow requirements to move cash from one party to another (especially uncommon and unrelated parties) are less compatible with an industry generally focused on individual medium to long-term asset appreciation;
- Relying on transfer methods outside of the regulated banking system (e.g. HOSSPs, cash couriers) is incompatible with the custodian's obligations;
- Low value financing requirements do not match the common higher minimum subscriptions. The CIS's exposure to TF is more relevant for wealthy terrorism sponsors outside the EU than for lone actors or small terrorist cells operating within the EU. This is particularly true for discretionary management mandates which typically cater to high-net-worth individuals; and
- Investment decisions are generally taken on a discretionary basis meaning that investment decisions are taken by the professional and not by the client itself.

254. Most investors in the collective investment sub-sector were foreign and Luxembourg is characterized by global cross-border distribution of funds. In terms of inflows, there is a high degree of intermediation with financial intermediaries located in the EU, acting as a gatekeeper. In terms of outflows, most UCITS invest in listed assets, further reducing the attractiveness for TF purposes. For

[111] Figures CSSF Annual Report.

AIFs, the CSSF did not identify a significant number of investments located in countries with a weak AML/CFT framework during its sample testing.

10.1.2.3. CSSF supervised pension funds

255. The TF risk of pension funds supervised by the CSSF remains limited because of the small sector size, high concentration, limited international exposure and provision of standardised products. As of end 2024, 9 entities registered as pension funds fell under CSSF supervision. Together, they had EUR 1,29 billion AuM with a yearly average of around approximately 15 000 affiliates and, the top-five entities concentrated about 80% of AuM. Ownership by entities from foreign countries decreased during the observation period and represented EUR 0,019 billion in 2024 (in comparison to EUR 0,695 billion in 2021). In addition, they offer standardised products, making them less attractive for TF abuse. Clients are employees of companies (with the majority being Luxembourg companies).

10.1.3. Money value and transfer services

AT A GLANCE

Most relevant TF stage:

☒ Raising ☒ Moving ☒ Using ☐ Non-relevant

Products and activities rather suitable for:

☒ Lone actors, small cells and FTFs with small TF needs
☐ International organisations and other terrorist actors with larger TF needs

PIs and EMIs offer high-velocity, low-denomination payment products to large international client bases, with limited face-to-face interaction and significant cross-border exposure — characteristics that align closely with lone-actor and small-cell TF typologies. Agents and e-money distributors acting on behalf of PI/EMIs established in other EU Member States present medium inherent risk within this cluster.

At the product level (SNRA)

The 2022 SNRA assesses TF risks related to payment services as “High”.

At the sub-sector level (NRA)

With the exception of agents and e-money distributors acting on behalf of PI/EMIs established in other European Member States, TF risk levels for the remaining sub-sectors are assessed as posing “High” inherent risk.

Sector	Sub-sectors	2026 NRA: Inherent risk
MVTS	Payment institutions	High
	E-money institutions	High
	Agents and e-money distributors acting on behalf of PI/EMIs established in other European Member States	Medium

256. First and foremost, it should be noted that the sub-sectors analysed below are those that fall within the formal (i.e. supervised for AML/CFT purposes by the CSSF) MVTS sector. Informal MVTS, such as unlicensed remittances, hawala and other similar service providers (HOSSP) are tackled under section 11.4.

257. As noted by the FATF in their recent comprehensive update on terrorist financing risks[112], MVTS can in some cases remain cheaper than wire-transfer through mainstream banks and is often the preferred option to send low amounts without incurring significant fees. As of 2025, nearly all terrorist groups identified have been reported to rely, at least to some extent, on MVTS to transfer funds across jurisdictions. Reports indicate that terrorist groups also frequently use MVTS to move money internally within the organisation, and to manage payments to FTFs, including for purposes of recruitment, travel or sustaining their stay and operations. In such cases, MVTS can be used through multiple small transactions and by mixing cash methods with formal banking services.

10.1.3.1. Payment institutions

AT A GLANCE

The 2026 NRA assesses the inherent TF risk level as "High". Key risk drivers identified are the products and services offered by the sub-sector, the volume of transactions processed, and distribution channels followed by the sector's size, ownership structure and international business.

258. With 15 entities, the number of PIs in Luxembourg has remained stable during 2023 and 2024. Furthermore, the sub-sector counted three Luxembourg branches and 16 branches of PIs established in another EU Member State. With around 500 employees in 2024, the sub-sector generated around EUR 1 billion of revenues. The sub-sector is concentrated, with top-five entities generating approximately 90% of the market's revenues during the observation period.

259. Ownership structure of the Luxembourg sub-sector has remained more or less stable with regards of Luxembourg ownership, at around 10% between 2022 and 2024, but the share of EU and non-EU membership has fluctuated more due to the arrival of new players.

260. As already noted under the section of retail and business banks and entities operating online (section 10.1.1), payment services are likely to be used by financiers to store and move funds and to cover for expenditures. The FATF recent comprehensive update on TF risks further indicates that the growing offer of payment methods, such as P2P payments, e-commerce, or crowdfunding provide opportunities for financiers to diversify their fund-moving channels. Characteristics like the prevalence of occasional transactions, the large volume and the high-speed of transactions as well as their cross-border nature make these products attractive for TF purposes. Additionally, the 2022 SNRA notes that although payments are generally not anonymous (when they are linked to an identified account), they may interact with very significant volumes of higher risk customers or countries, including cross-border movements of funds. Considering that financiers may, wittingly or unwittingly, transfer low-value amounts to unlisted or undesignated groups (operating under the disguise of a NPO or the purchase of merchandise for example), particular caution should be applied by the professional.

[112] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025, link.

261. In 2024, the Luxembourg sub-sector served approximately 16 million clients, with the predominant majority being natural persons (around 90%) and residing within the EU (around 97%). In a similar vein, around 85% of consolidated flows are with EU countries.

262. Transactions and volumes processed by the sub-sector are significant, with 1,5 billion inflow transactions worth EUR 101 billion and 1 billion outflow transactions worth EUR 104 billion. In comparison to the total number of clients served by the sub-sector, the share of high-risk clients is limited and situated below 1% during the observation period. As noted previously, especially for low-value terrorist financiers, the origin of the funds may be licit, and transactions might occur between unrelated and un-designated individuals, posing additional challenges in terms of detection. The identification of transactional indicators is therefore crucial.

263. In addition to that, Luxembourg PIs mostly onboard and engage with their clients through non-face-to-face channels, potentially creating opportunities for obstacles to transparency on initiators and beneficiaries through the use of pseudonyms or fake accounts.

10.1.3.2. E-money institutions

AT A GLANCE

At the product level (SNRA)

The 2022 SNRA assesses the TF risks related to the e-money sector as "High". The main contributing factors are the availability of these products as well as the ease and speed of e-money transactions.

At the sub-sector level (NRA)

The 2026 NRA assesses the inherent TF risk level as "High". EMIs share the same risk drivers as PIs: products and services offered by the sub-sector, the volume of transactions processed, and distribution channels followed by the sector's size, ownership structure and international business.

264. In Luxembourg, the sub-sector was similar in size and activities to the PIs sub-sector and thus shares similar inherent vulnerabilities to TF risk.

265. During the observation period, two new EMIs have obtained their license in Luxembourg. The sub-sector counted 11 entities in 2024 as well as one Luxembourg branch and five branches of EMIs established in another EU Member State. Ownership of these entities was entirely foreign, with 25% belonging to EU owners. The sub-sector employed around 400 people and generated revenues slightly below EUR 1 billion in 2024. The sub-sector is concentrated, with top-five entities accounting for almost all of the sub-sector's revenues.

266. Luxembourg EMIs offer e-money accounts and wallets. As noted by the FATF in its recent comprehensive update on TF risks, financial innovation and products offered by this sub-sector have experienced significant growth in the past few years. Especially the offer of means to raise, move and store funds. Globally, terrorist financiers have been seen to share financial data (such as wallet addresses) and donations instructions (including coded language) to raise funds. As for PIs, financiers may, wittingly or unwittingly, transfer low-value amounts to wallets controlled by unlisted or undesignated groups (operating under the disguise of a NPO or for example). Therefore, particular caution should be applied by the professional.

267. According to the 2022 SNRA, e-money products that are cash-based (i.e. not linked to a current account) offer anonymity features similar to cash, further increasing TF risks. Nonetheless, it should be specified that no Luxembourg EMI offer prepaid card services. The issuance of cards linked to e-money accounts allowing cash withdrawals is very limited, representing less than 0,1% of total outflows processed by EMI.

268. Overall, TF vulnerability for non-cash-based products (i.e. linked to a current account) are similar to those of other basic banking products and payment methods (cf. section 10.1.1).

269. As for the number of entities, the number of clients served by the sub-sector has continuously increased during the observation period, with around 110 million clients in 2024. During the observation period, 92% of clients were natural persons on average. EU clients accounted, on average, for almost 80% of the total client base. Legal persons accounted for around 8% of the total client base, with 25% of BOs residing in the EU and 75% outside the EU.

270. Overall, the sub-sector handled both a large amount and value of transactions, as shown in the table below:

Table 11: Average number and value of transactions, 2021–2024

Number of inflow transactions	2,4 billion
Value of inflow transactions	EUR 95,2 billion
Number of outflow transactions	0,1 billion
Value of outflow transactions	EUR 68,5 billion

271. On average, around 20% of these consolidated flows were with EU countries, and only an average 0,1% were with TJs.

272. The significant number and value of transactions processed drives TF risks. However, this is partially compensated by the low proportion of high-risk clients in the sub-sector. Indeed, on average, 0,85% of clients were considered as high risk by those entities during the observation period.

273. In addition, Luxembourg EMI onboard and engage with their clients through non-face-to-face channels, potentially increasing opportunities for illegitimate users to enhance opacity on initiators and beneficiaries through the use of pseudonyms or fake accounts.

10.1.3.3. Agents and e-money distributors acting on behalf of PI/EMIs established in other European Member States

AT A GLANCE

At the product level (SNRA)

The 2022 SNRA assesses the TF risks with regard to “money remittance services” as “Very high”.

At the sub-sector level (NRA)

The 2026 NRA assesses the sub-sector’s TF risk as “Medium” considering the limited size of the Luxembourg sub-sector, limited fragmentation and complexity of the market structure and direct client interaction.

274. In 2024, the market size for agents and e-money distributors remained limited, with 21 agents working on behalf of five PIs established in other EU Member States. Fragmentation is limited and complexity is considered to be low as all agents were Luxembourg-based companies/persons with a simple structure acting on behalf of an EU-regulated PI/EMI.

275. Payments through agents are attractive, as cash transactions can be easily made, transfers are quickly processed, and transaction fees being usually lower. Intrinsic to the business model, many transactions are one-off/occasional, preventing the agents from establishing a durable relationship with their customers. Hence, it may be challenging to fully observe and understand customer's behaviour and transactional patterns, increasing TF risks.

276. Luxembourg agents of EU PI offer indeed money remittance services, with more than 80% of consolidated flows being cash based. In line with the above, this amplifies TF risks.

277. In 2021, almost all (99,9%) of their customers were natural persons, with 8% being considered as high-risk (based on entities' internal self-risk assessment). More than 12% of clients were linked to a TJ particularly impacted by terrorism (T2). In comparison to the other sectors under analysis, the share of high-risk clients and flows with third countries were considered to be high.

278. Both agents and distributors typically meet their clients face-to-face. This had a positive impact on the risk scoring allocated to distribution channels.

10.1.4. Virtual asset service providers

AT A GLANCE

Most relevant TF stage:

☒ Raising ☒ Moving ☐ Using ☐ Non-relevant

Products and activities rather suitable for:

☒ Lone actors, small cells and FTFs with small TF needs
☒ International organisations and other terrorist actors with larger TF needs

VASPs present "High" inherent TF risk. Despite progress in on-chain analytics, obfuscation techniques have advanced in step, and the volume of crypto-asset TF use is growing, though remaining limited in absolute terms in Luxembourg.

At the product level (SNRA)

The 2022 SNRA assesses TF risks related to crypto/virtual-assets and virtual currencies as "Very high". Global reach, speed of transactions and opportunities for anonymity are cited on this regard.

At the sub-sector level (NRA 2026)

The 2026 NRA assesses TF risk with regard to VASPs as "High" with key risk drivers being the volume of clients/transactions processed, and distribution channels followed by the sector's size, ownership, products and activities and international business.

Sector	2026 NRA: Inherent risk
VASP	High

279. VASPs were identified and assessed as an emerging risk in the 2020 NRA ML/TF. They were analysed in a dedicated VRA[113], including an assessment of TF inherent risks emerging from virtual/crypto-assets and VASP activities as well as a description of the mitigating factors. Similarly to the works performed in the 2025 NRA ML, this NRA integrated VASPs in the NRA taxonomy, updates and completed the assessment of VASPs following the NRA methodology from a TF perspective.

280. The number of entities registered with the CSSF as VASPs has increased steadily since 2021, although total number remains still relatively low. Whereas the sector counted six entities in 2021, it has more than doubled in the meantime, counting 15 entities in 2024. More precisely:

- Two were already operating under the license of a PI;
- Three were already operating under the license of a bank; and
- Five were exclusively providing virtual assets services in Luxembourg.

281. Although the sector was entirely controlled by foreign entities/persons in the first two years of the observation period (i.e. 2021 and 2022), foreign ownership decreased thereafter and reached 93% in 2024 (with an equal share of EU and non-EU ownership).

282. Similar to retail and business banks and MVTS sector, VASP offer channels to raise and move funds. In this regard, funds are crypto-assets, presenting high vulnerabilities in terms of traceability, speed of transaction and global reach (cf. section 11.2).

283. The exact scale of the misuse of crypto-assets for TF purposes is still difficult to measure. As the use of these crypto-assets becomes more widely available and accessible, the use of crypto-assets by terrorist groups and individual terrorists follows suit, including in combination with other methods. Nonetheless, it is globally acknowledged that the misuse of crypto-assets for TF is likely to remain lower compared to the use of other funding channels, such as cash[114].

284. Overall, it appears that much of TF activity with regard to crypto-assets are related to the solicitation of funds and donations by individuals. As already explained in section 10.1.3, terrorist groups appeal overtly and directly to supporters and use propaganda outlets to circulate crypto assets wallet addresses in some cases. In other cases, they may try to hide the true purpose of the funds and utilise fraudulent charitable appeals or other pretences to avoid detection. In such cases, instructions on how to make donations are communicated through private chats or other obfuscated methods. Indeed, detailed instructions to make payments by registering and replenishing digital wallets are routinely provided to transfer funds by crypto-assets.

285. Among the 15 entities registered:

- 13 offered transfers of crypto-currencies which are deemed high risk from a TF perspective, considering the explanations provided above. Between 2022 and 2024, the number and value

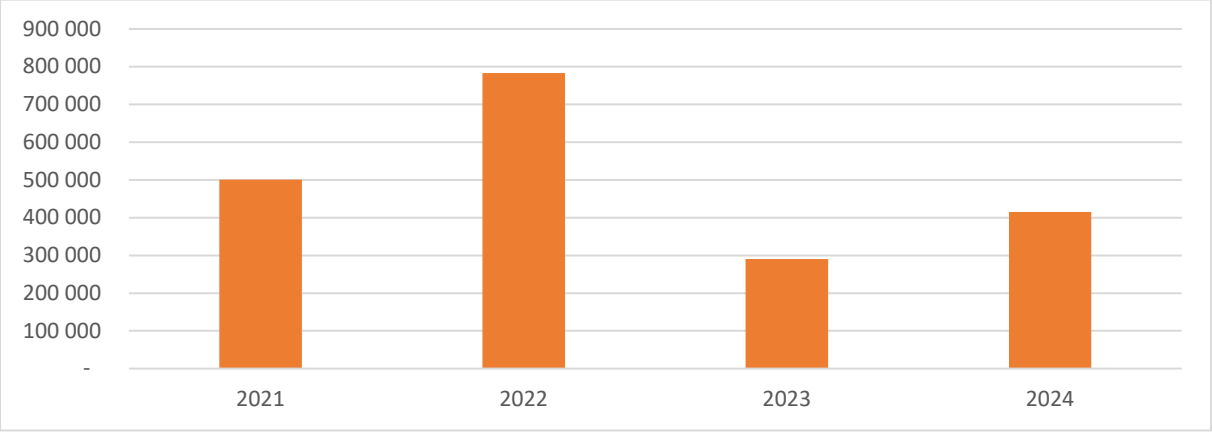
[113] MoJ, *ML/TF Vertical risk assessment: virtual asset service providers*, 2020, link.
[114] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025, link.

of transfers increased, with a peak of the number of transactions in 2023 (around 1,3 million) and in value in 2024 (around 9,3 billion).

- 13 offer safekeeping of crypto-assets and/or administration of instruments enabling control on crypto-assets, which are deemed to bear moderate TF risks. In Luxembourg, these entities held mainly Bitcoin and Ethereum in custody. During the observation period, the value of crypto-assets held in custody has dropped by 40%, reaching EUR 4,3 billion in 2024.
- 10 entities operate an exchange platform, offering exchange crypto-assets to fiat and/or crypto-assets to crypto-assets, considered bearing "high" risks. Indeed, in case crypto-assets are intended to finance goods or services, the conversion into fiat currency is required at some point. In terms of number and value (around 30 million transactions worth almost EUR 50 billion in 2024), this activity has further gained in importance for Luxembourg VASPs with number of transactions having grown by almost 90% and value by almost 200% between 2022 and 2024. Bitcoin and Ethereum were most commonly processed by these entities. It should be noted that these flows are mainly concentrated on one entity which also acts as a PI.

286. The number of clients, which are almost all natural persons, has fluctuated during the observation period, as shown in the graph below:

Figure 13: Number of clients served by Luxembourg VASP, 2021–2024



287. Most clients are concentrated on one VASP, with most of them residing in an EU country (around 90% in 2023 and 2024). In terms of deposits, around 80% were from EU countries in 2024. Most of the deposits from non-EU countries were from Switzerland. A similar picture can be drawn from a transfer's point of view, with around 85% being with EU countries and the remaining predominately from Switzerland.

288. Risks linked to distribution channels are considered significant, as the vast majority of VASPs offered their services online.

Insight Box 6: Looking ahead: transition from VASPs to CASPs under MiCAR and potential implications in TF risk

The regulatory framework around crypto assets has changed with the introduction of Regulation (EU) 2023/1124 on market in crypto assets ("MiCAR"). Under MiCAR, crypto asset services shall not only comply with the AML/CFT requirements laid down in the 2004 AML/CFT Law but also with prudential requirements.

MiCAR is applicable for CASP from 30 December 2024 with a grand-fathering period in Luxembourg until 30 June 2026. Important to note, the definition of crypto assets services has been specified but is still in line with the previous definition of virtual assets services in Luxembourg that was applicable until the application of MiCAR.

Under MiCAR, entities offering crypto assets services shall obtain an authorization in one EU Member States. Once authorized, they can offer services under the freedom of providing services in all EU Member States. Third-countries entities need to have an establishment in one of the EU Member States and obtain an authorization by the competent authorities of this Member State. Some entities which have another type of licence (credit institutions, investment firms, management companies) can, subject to specific conditions, offer crypto asset services upon notification of their competent authorities.

Hence, VASPs registered in Luxembourg shall either obtain a CASP licence in Luxembourg or in one EU Member State, or cease their crypto asset services in the EU.

The inherent TF risk exposure related to crypto asset services of CASPs is similar to the risk exposure of VASPs. Indeed, the services offered are usually the same. Some of the mitigation measures will be stronger notably the market entry controls as CASPs are subject to an authorization process, which is stricter compared to the registration of VASPs. The same applies for prevention as CASPs shall comply with prudential requirements including ICT requirements (e.g. strong cybersecurity measures to mitigate the risk of hacking).

10.1.5. Specialised PFS

AT A GLANCE

Most relevant TF stage:

☐ Raising ☒ Moving ☐ Using ☐ Non relevant

Products and activities rather suitable for:

☐ Lone actors, small cells and FTFs with small TF needs
☒ International organisations and other terrorist actors with larger TF needs

The 2026 NRA assesses inherent TF risk with regard to specialized PFS as follows:

Sector	Sub-sectors	2026 NRA: Inherent risk
Specialised PFS	Specialised PFS providing corporate services	Medium
	Professional depositaries	Low

289. The specialised PFSs sub-sector can include various licenses, each offering different services. These licenses include notably registrar agents, corporate domiciliation agents, professionals providing company incorporation and management services, and family offices, professional depositaries of financial instruments, and professional depositaries of assets other than financial instruments. They can be broadly categorised into two categories: specialised PFSs providing corporate services and professional depositaries.

10.1.5.1. Specialised PFS providing corporate services

Please note that the 2026 update of the ML/FT Sub-Sector Risk Assessment on Specialised Professionals of the Financial Sector providing corporate services (trust and company service provider activities) on the CSSF's website should be consulted for an in-depth assessment of the subsector's TF risks: link.

290. Luxembourg counted 85 specialised PFSs providing corporate services with over 6 500 employees in 2024, with balance sheet assets of over one billion euros and profits reaching EUR 120 million. The sub-sector remained quite fragmentated with top-five entities accounting for 40% of the market's revenues in 2024.

291. Vulnerabilities stemming from foreign ownership are assessed to be moderate, as 58% of specialised PFSs providing corporate services were under Luxembourg ownership, 13% under EU ownership (excluding Luxembourg) and 29% under non-EU ownership in 2024.

292. TCSP activities are globally known to be particularly vulnerable to ML/TF, as professionals delivering these activities might be abused to hide the illegal origin of the funds or the true beneficial owner. In the particular case of TF, TCSP activities might also be abused to hide the illegal destination of the funds. The threat of TF through specialised PFSs providing corporate services in Luxembourg is lower than ML due to several factors. TF typically involves short-term, low-value transactions, which are incompatible with TCSPs' longer-term, higher-value transactions. Additionally, terrorist financiers often prefer informal remittance channels over formal TCSP services. Despite the risk for these services to be abused for TF being lower than that for ML purposes, it cannot be entirely ruled out, especially in case where the abuse or misuse of structures such as corporate and state-sponsored terrorism are involved. Serving almost entirely legal persons the abuse of these services by lone actors, small cells and FTFs for TF purposes seems less relevant.

293. The number of clients served by the sub-sector continuously increased during the observation period, reaching over 32 000 client companies in 2024. As stated above, almost all clients served by the sub-sector were legal persons (99,4% on average through the observation period), with most of their BOs residing outside of the EU, increasing risk exposure to some extent. On average, almost 20% of clients were flagged as high-risk for both ML and TF purposes by the sector. As noted above, this could pose some risk in case where BO and the exact nature and purpose of activity are more difficult to establish. However, the sub-sector counts only a very limited number of clients having NPOs, as defined by the FATF, within their shareholder structures.

294. Being relatively controlled, the distribution channels of this sub-sector pose moderate TF risks. Most players have direct relationships with their clients, whilst any involved intermediaries are either mostly regulated business providers (accountants, ...) or part of the group to which the PFS belongs.

10.1.5.2. Professional depositaries

295. As already noted in the 2025 NRA ML, the main vulnerabilities of the professional depositaries stem from the large size of the professional depositaries sub-sector. Although the number of professional depositaries has remained more or less stable during the observation period, with 16 entities in 2024, AuM has grown by 128%, reaching EUR 486 billion in AuM in 2024.

296. Overall, products and services offered by the sub-sector are neither suitable for smaller nor for larger financiers of terrorism, as professional depositaries are not allowed to open cash accounts in their books to keep cash from their clients. Therefore, there are no cash flows. Risks linked with international business are rather limited as well, as almost all clients are Luxembourg funds. Despite the sharp increase registered during the observation period, the overall number of client funds served by the sub-sector remained limited (2 044 funds served in 2024) further decreasing TF risks.

10.1.6. Support PFS and other Specialised PFS

AT A GLANCE

Most relevant TF stage:

☐ Raising ☐ Moving ☐ Using ☒ Non-relevant

Products and activities rather suitable for:

☐ Lone actors, small cells and FTFs with small TF needs

☐ International organisations and other terrorist actors with larger TF needs

☒ Non-relevant

All the professions included in "Support PFSs and other specialised PFSs" are assessed as very low inherent risk in Luxembourg either due to their activity or very limited number of entities.

Sector	2026 NRA: Inherent risk
Support PFS and other specialised PFS	Very low

297. Some Specialised PFSs, which have been included under this section, are even less exposed to TF risks compared to the wider Specialised PFS sector due to the nature of the services provided. In 2024, five professionals performed lending operations (Article 28-4 of the LSF) and two provided debt-recovery services (Article 28-3 of the LSF). This "other Specialised PFSs" sub-sector also includes professionals performing securities lending (Article 28-5 of the LSF) and mutual savings funds administrators (Article 28-7 of the LSF), none of which are present in Luxembourg and thus cannot be misused for TF purposes in Luxembourg.

10.1.7. Market operators

AT A GLANCE

Most relevant TF stage:

☐ Raising ☐ Moving ☐ Using ☒ Non-relevant

Products and activities rather suitable for:

☐ Lone actors, small cells and FTFs with small TF needs

☐ International organisations and other terrorist actors with larger TF needs

☒ Non-relevant

The 2026 NRA assesses TF risk with regard to market operators as "Low".

Sector	2026 NRA: Inherent risk
Market operators	Low

298. As for ML, exposure to TF risks is driven by size, due to the significant volume of issuance activities (EUR 1 454 billion of debt issued via instruments admitted to trading on the Luxembourg Stock Exchange in 2024), the international nature of the transactions executed and the mostly indirect interaction channels.

299. However, exposure to TF is limited as capital linked to primary issuances does not pass through the accounts of market operators and, moreover, market operators do not intervene in the settlement of secondary market transactions. Exposure is further limited because of the presence of only one market operator, the small number of members to which the only market operator is open, which are all investment firms or banks subject to AML/CFT obligations and the low transactions volume (trading volume of EUR 174,51 million and equity trading volume of EUR 40,8 million in 2024).

10.2. CAA supervised sectors

AT A GLANCE

Life insurance (particularly unit-linked and other savings/investment contracts with investment features) presents a medium inherent TF risk, reflecting cross-border distribution, flexibility of early surrender options and the potential for policy-structure abuse by sophisticated financial actors. Insurance intermediaries present "Low" inherent TF risk, reflecting enhanced concentration and lower exposure to countries analysed in the scope of this report (see section 8). Non-life insurance presents a low inherent TF risk, given the indemnity-based nature of claims and limited utility for fund movement. Reinsurance also presents a low insurance-sector risk, characterised by standardised business-to-business relationships and high knowledge requirements.

At the product level (SNRA)

At the EU level, the SNRA 2022 considers the TF threat related to life insurance moderately significant ("Medium") and of low significance ("Low") for non-life insurance.

For both subsectors, the products are viewed as having limited attractiveness for being abused for TF purposes because, among other factors, they require knowledge and planning expertise. With regard to the levels of vulnerability of the sub-sectors, these are considered of low/moderate significance (medium-low) for life insurance and moderately significant (medium) for non-life insurance.

Finally, the report assessed the TF risk for both life and non-life insurance as moderately significant (medium).

At the sub-sector level (NRA)

At the national level, the 2026 NRA assesses the TF inherent risks related to life insurance as "Medium", with key risk drivers being size, international business, volume and channels.

The remaining insurance sub-sectors are assessed "Low" or "Very low".

Sector	Sub-sectors	2026 NRA: Inherent risk
Insurance	Life insurance	Medium
	Non-life insurance	Low
	Reinsurance	Low
	Intermediaries	Low
	Professionals of the insurance sector (PSAs)	Very low
	CAA-supervised pension funds	Very low

10.2.1. Life insurance

AT A GLANCE

The sub-sector inherent TF risk level is "Medium".

Most relevant TF stage:

☐ Raising ☒ Moving ☐ Using ☐ Non-relevant

Products and activities rather suitable for:

☐ Lone actors, small cells and FTFs with small TF needs

☒ International organisations and other terrorist actors with larger TF needs

Sub-sector size, orientation to international business, volume and channels are key risk drivers for life insurance. Fragmentation/Complexity of the sub-sector as well as the products and services offered were considered less vulnerable to be misused for TF purposes.

300. The life insurance sub-sector remained large between 2021 and 2024. As of end 2024, this sub-sector showed a balance sheet total of EUR 254 billion, EUR 258 billion in technical provisions, EUR 29,5 billion in premiums and 3 103 employees across 34 undertakings falling within the AML/CFT scope[115]. The subsector remains moderately concentrated with slightly more than half of gross written premiums were generated by five entities[116]. No life insurance undertaking is owned by residents in TJs.

301. In its 2023 Opinion[117], the European Banking Authority (EBA) notes that products include features increasing ML/TF risk, such as early termination and flexibility of payment. Nevertheless, the

[115] CAA data 2024. The numbers also include five Luxembourg branches of foreign FIs.
[116] CAA data 2024.
[117] EBA, Opinion of the European Banking Authority on money laundering and terrorist financing risks affecting the EU's financial sector, 2023, link.

SNRA assessed that the products offered by Life insurers have limited attractiveness because of the need of knowledge and planning expertise needed to exploit them for TF purposes. Overall, they are also less accessible than other financial services reducing their TF exposure.

302. In 2024, the Luxembourg life insurance sub-sector continued to be oriented towards foreign residents. The majority (94%) of premiums were linked to foreign countries, although a large majority (86%) from European Economic Area (EEA) countries and the remaining 8% from non-EEA countries were mostly the UK and Switzerland. 3,89% of premiums were paid from countries in the list of TJs and 5,10% of claims were paid to such countries. The share of contracts with PEPs as clients from total was less than 0,28% in 2024. For individual life insurance new contracts in which a PEP is a party and is linked by residence to countries in the TJ list was limited. As for the stock of contracts, the proportion is very limited as it represents 0,012% of the total number of contracts as of end 2024. Moreover, for individual life insurance, the share of contracts in stock in which an NPO, or other type of legal person or legal arrangement is party and is linked by residence to a TJ was close to none as of end 2024.

303. Other TF risk factors included the high volume of transactions and the usage of intermediary distribution channels. In 2024, nearly 266 000 new contracts were underwritten. With regard to distribution channels, 96% (in terms of premiums) were sold through intermediaries[118], which may represent an additional layer potentially reducing transparency and weakening the direct control of the life insurance undertakings.

10.2.2. Non-life insurance

AT A GLANCE

The sub-sector inherent TF risk level is "Low".

Most relevant TF stage:

☐ Raising ☒ Moving ☐ Using ☐ Non-relevant

Products and activities rather suitable for:

☒ Lone actors, small cells and FTFs with small TF needs

☒ International organisations and other terrorist actors with larger TF needs

Ownership/legal structure of the sub-sector size and orientation to international business are key risk drivers for non-life insurance. The products and services offered were considered less vulnerable to be misused for TF purposes.

304. In Luxembourg, the non-life insurance sub-sector is smaller than the life insurance sub-sector. As of 2024, it had EUR 68 billion in total balance sheet, EUR 44 billion in technical provisions, EUR 19 billion in premiums and 9 725 employees across 43 undertakings. With around 66% of gross written premiums generated by five entities, the sector was more concentrated than the life-insurance subsector. Around 92% of premiums were linked to foreign countries among which 66% were linked

[118] CAA data 2024.

to EU countries. Premiums linked to non-EU countries mainly concerned the UK, the USA, Switzerland and Australia[119]. Claims paid by non-life insurers amounted 8,9 billion euros in 2024.

305. Within this sub-sector, classes 14 (credit) and 15 (suretyship) fall within the AML/CFT scope. Out of the total of non-life claims paid, around 5 million (representing 0,056%) are related to credit and suretyship risk paid in countries listed in the TJ list.

306. Only 18 undertakings offered these products and generated EUR 1 332 million of gross written premiums in 2024. Out of those 18 undertakings, 7 were EU owned and the remaining 11 were non-EU owned. None was owned by residents of countries in the TJ list[120].

307. The following features make credit and suretyship products less vulnerable to TF risk:

- the objective of the contract is protection against risk and the amount of premiums correspond to the price of risk;
- the products have no surrender value or investment components. There are no surrender options or other exit options before the contract expiration date; and
- claims paid are compensation for damages sustained. There is no compensation if there are no claims, and it is up to the policyholder to prove the materiality of the claim. Moreover, compensation must correspond strictly to the loss suffered, without allowing for profit or exceeding the actual value of the damage.

Insight Box 7: Non-life insurance TF assessment (cyber, kidnap/ransom and marine)

Beyond the sectors subject to 2004 AML/CFT Law, the CAA has also carried out ML/TF risk assessments of other non-life insurance products, including Cyber insurance, kidnap and ransom insurance, and marine insurance. For each product considered, the CAA has therefore analysed the legal (Insurance Contract Law) and contractual (underwriting/benefit conditions) mechanisms and controls that are likely to mitigate exposure to ML and TF risks.

10.2.3. Reinsurance

AT A GLANCE

The sub-sector inherent TF risk level is “Low”.

Most relevant TF stage:

☐ Raising ☐ Moving ☐ Using ☒ Non-relevant

Products and activities rather suitable for:

☐ Lone actors, small cells and FTFs with small TF needs

☐ International organisations and other terrorist actors with larger TF needs

☒ Non-relevant

[119] CAA data 2024.
[120] CAA data 2024.

Orientation to international business is the key risk driver for reinsurance. Products and services offered were considered less vulnerable to be misused for TF purposes.

308. As of end 2024, the reinsurance sub-sector counted 52 traditional reinsurance undertakings and 144 reinsurance captives (i.e. 196 entities in total), out of which 34 reinsure credit and suretyship risks, and thus are in the scope of the AML/CFT framework. 27 entities were EU-owned, and 7 non-EU owned, with one entity owned by residents from the TJ list (T5). As a whole, the sub-sector remained relatively concentrated with almost 72,6% of written gross premiums generated by five entities[121].

309. The business of the reinsurance sub-sector remained highly international. Around 27% of accepted premiums were written through ceding companies located in the UK, 11% in France, 14% in Germany, nearly 6% in Spain, 9% in other EEA countries and nearly 4% in the USA limiting business with riskier geographies[122].

310. With regards to flows with countries in the TJ list the exposure arises more from accepting than from retroceding premium. In 2024, premium accepted from ceding reached EUR 14,51 billion, out of which slightly over EUR 1 billion (representing 7,43% were related to countries in the TJ list (mainly T6). In contrast, premiums retroceded to reinsurer reached almost EUR 7 billion, out of which almost EUR 39 million (representing 0,56%) were related to countries in the TJ list[123].

311. Offered products have low exposure to TF risk. The business relationship takes place exclusively between institutional players, direct insurers and reinsurers, without any interaction with the final policyholders. Therefore, reinsurers do not collect premiums directly from individual customers or unregulated entities, and financial flows are structured, traceable, and not highly fragmented.

10.2.4. Intermediaries

AT A GLANCE

The sub-sector inherent TF risk level is “Low”.

Most relevant TF stage:

☐ Raising ☐ Moving ☐ Using ☒ Non-relevant

Products and activities rather suitable for:

☐ Lone actors, small cells and FTFs with small TF needs

☐ International organisations and other terrorist actors with larger TF needs

☒ Non-relevant

Orientation to international business is the key risk driver for intermediaries. The products and services offered were considered less vulnerable to be misused for TF purposes.

[121] CAA data 2024.
[122] CAA data 2024.
[123] CAA data 2024.

312. As of end 2024, the intermediaries sub-sector counted 84 brokerage firms, 115 brokers, 454 insurance sub-brokers and 252 insurance agencies. Ownership was mostly from the EU (85%, including 30% of shareholders from Luxembourg) and the remaining 15% ownership were primarily from the UK and from Switzerland. There was no ownership related to residents in the TJ country list[124].

313. New premium flows in 2024 amounted to EUR 2,8 billion for life and EUR 1,1 billion for non-life. The sub sector remains relatively concentrated with around 62% of insurance premiums distributed by five intermediaries for life, and 81% non-life[125].

314. With respect to products, intermediaries distribute life and non-life insurance contracts mainly from Luxembourg insurers. The product related vulnerabilities are therefore the same as for life insurers and non-life insurers, the majority of which were assessed to be inherently low or medium-low TF risk (in 2024, 38% of the contracts distributed by intermediaries were pure protection contracts, assessed low; and 31% of contracts were savings and investment low amounts contracts, assessed low-medium risk[126,127], see sections 10.2.1 and 10.2.2).

315. The TF risk is primarily driven by the high international nature of the business. As such, brokers had mainly international clients (88% of premiums from foreign countries for life and 91% for non-life) mostly focused on the EEA market (non-EEA represents 4% of life and 16% of non-life premiums). However, exposure to countries in the TJ list is limited. Although there was one existing contract with a life insurance undertaking situated in a country listed in the TJ list representing 0,18% of outstandings as of end 2024, no premium was written with a life insurance undertaking situated in a TJ during the observation period 2021–2024[128]. Also, 93% of premiums were written with Luxembourg-based life insurance undertakings. The number of PEPs as clients remain stable and fluctuation from year to year is due to the number of new contracts. In 2024 the share of new contracts with PEPs as clients totalled 0,11%, and none of them were residents in a country included in the TJ list. For the stock as of end 2024, the number of contracts with PEPs residing in a TJ countries is close to zero[129].

10.2.5. Professionals of the insurance sector

AT A GLANCE

The sub-sector inherent TF risk level is "Very low".

Most relevant TF stage:

☐ Raising ☐ Moving ☐ Using ☒ Non-relevant

Products and activities rather suitable for:

☐ Lone actors, small cells and FTFs with small TF needs

☐ International organisations and other terrorist actors with larger TF needs

[124] CAA data 2024.
[125] CAA data 2024.
[126] CAA data 2024.
[127] CAA, *"Analyse des risques BC/FT par catégorie de produits"*, June 2025 (non-public).
[128] CAA data 2021-2024.
[129] CAA data 2024.

☒ Non-relevant

Note that the products and services offered were considered less vulnerable to be misused for TF purposes.

316. Professionals of the insurance sector (PSA) include authorized service providers of corporate governance and management companies for insurance and pension funds. They typically do not manipulate money flows and play an advisory role to the respective insurance undertakings or pension funds and thus have limited exposure to TF risk.

317. There were 27 PSAs in 2024, out of which 14 offering TCSP services. None of them were owned by residents in a country from the TJ list. The sub-sector was relatively concentrated with 85% of market-share being generated by five entities. Moreover, Luxembourg PSAs only served Luxembourg-based clients (insurance and reinsurance undertakings under the supervision of the CAA or companies linked to these undertakings)[130].

10.2.6. CAA-supervised pension funds

AT A GLANCE

The sub-sector inherent TF risk level is "Very low".

Most relevant TF stage:

☐ Raising ☐ Moving ☐ Using ☒ Non-relevant

Products and activities rather suitable for:

☐ Lone actors, small cells and FTFs with small TF needs

☐ International organisations and other terrorist actors with larger TF needs

☒ Non-relevant

Note that the products and services offered were considered less vulnerable to be misused for TF purposes.

318. Luxembourg counted three pension funds supervised by the CAA with EUR 689,6 million in balance sheet total and 10 080 affiliates in 2024. All premiums are collected from EEA countries or Switzerland and there are no flows with high-risk geographies as flows are mostly related to EU and Swiss based corporate sponsors. The TF risk is limited due to the very small sub-sector size, the low fragmentation and the low-risk products offered by these pension funds.

[130] CAA data 2024.

10.3. AED supervised sectors

10.3.1. Real estate agents and developers

AT A GLANCE

Most relevant TF stage:

☐ Raising ☒ Moving ☐ Using ☐ Non-relevant

Products and activities rather suitable for:

☐ Lone actors, small cells and FTFs with small TF needs

☒ International organisations and other terrorist actors with larger TF needs

At the product level (SNRA)

For the 2022 SNRA the threat of TF related to investments in real estate would not be different from the threat relating to organised crime and ML, which is considered as being significant. In a similar manner, the analysis of the vulnerability related to investment in real estate has been considered together with real estate investment-related money laundering schemes to hide the illegal origin of the funds and the SNRA concludes that the TF vulnerability related to investment in real estate is considered as very significant.

The 2022 SNRA notes that with prices being generally stable and likely to appreciate over time, real estate is as attractive to criminals as it is to any investor. Criminals often get back to complex financing techniques and/or corporate structures via professionals when investing in property in order to conceal the proceeds generated by illegal activities, and/or the BO. The 2022 SNRA further notes that investments in the real estate sector are mostly used in combination with other professionals, such as TCSPs or legal advice.

At the sub-sector level (NRA)

The TF inherent risk associated with Luxembourg's real estate agents and developers is assessed as being "Medium" with key vulnerabilities stemming from sub-sector structure in both terms of size and fragmentation, from the products and services offered, and from clients and transactions.

Sector	Sub-sectors	2026 NRA: Inherent risk
Real estate agents and developers	Real estate agents *(agents immobiliers)*	Medium
	Real estate developers *(promoteurs immobiliers)*	Medium

319. In Luxembourg, the real estate and construction sector remains large. Real estate activities accounted for around 8% to Luxembourg's gross value added between 2020 and 2024[131].

320. Generally, Luxembourg's real estate market is focused on residential property attracting mostly a local clientele aiming to acquire real estate not for investment but for residential purposes, as

[131] STATEC, Gross value added by activity (NaceR2)(at current prices) (in millions EUR) 1995 – 2025, code L, link.

illustrated by the fact that the number of notarial deeds of sales and sales in future state of completion including a tax credit clause subject to occupy personally the property for at least two years is six times the number of such deeds including a reselling clause. In a similar vein, the number of natural persons registered with the notarial real estate deeds represent between six and seven times the number of legal persons[132], implying that transactions typically involve mainly natural persons.

321. As indicated above, real estate agents and real estate developers primarily serve a domestic clientele on both sides of real estate transactions. Between 2021 and 2023, more than 91% of buyers and over 82% of sellers were Luxembourg residents. When including residents of neighbouring countries, these proportions rise to 97% and 95% respectively. By contrast, exposure to residents in jurisdictions targeted for analysis during this period was limited, accounting for 0,20% of buyers and 0,21% of sellers[133].

322. As a product, real estate may potentially be misused to either collect funds through a real estate sale or to store and invest funds for later TF use through a purchase. In this later case, the real estate may also offer a functional value for terrorist use. However, misuse of real estate for TF is generally not attractive and tends to be complex, as every transaction typically involves parties such as real estate agents, notaries and banks, required to conduct their own CDD. In more sophisticated schemes, such as transactions involving the sale or purchase of shares or participations in real estate, a lawyer may also be involved, adding an additional layer of complexity for the terrorist financier. Such arrangements would have the characteristics of ML schemes rather than those of straightforward TF.

323. Over the observation period (end 2021 to end 2024), Luxembourg's residential real estate market went through a full cycle: from the final phase of a long price boom to a sharp contraction in both prices and transactions, and finally to early signs of recovery[134]:

- At end 2022 prices were still rising (year-to-year increase of 12% in Q4-2022) but transactions fell sharply (apartments sales fell 30% and sales in future state of completion almost halved), due to higher interest rates and reduced affordability.
- In 2023, the downturn peaked, with prices dropping up to 14,4% year to year in Q4-2023 and transactions hitting historic lows (only 106 sales in future state of completion that quarter and total apartment sales representing roughly one-third of pre-crisis activity), driven by expensive financing and buyer caution.
- In 2024 the market stabilized. Prices stopped falling in Q2-2024 and by Q4-2024 turned positive again (year-to-year increase of 1,4%). Transaction activity rebounded strongly (132% year-to-year increase in apartment sales and 273% year-to-year increase in sales in future state of completion), though still below pre-crisis levels.

10.3.1.1. Real estate agents

324. Luxembourg counted 2 209 real estate agents (REAs) in 2024[135]. Overall, the sub-sector remains fragmented as of end 2024: 56% of REAs generated a turnover less than EUR 120 000, 25%

[132] Chambre des Députés, *Réponse à la question parlementaire n°7781*, 2023, link.
[133] Data source from a survey conducted by the AED in 2024 (observation period: 2021-2023).
[134] See STATEC, LISER, Le logement en chiffres #11 to #17, link.
[135] AED data.

generated a turnover between EUR 120 000 and EUR 620 000, and about 15% generated a turnover exceeding EUR 620 000). Top-five REAs generated 26% of total market turnover in 2024.

325. On the basis of the entity-assessment performed by the AED, most entities were assessed to bear medium risk.

10.3.1.2. Real estate developers

326. The number of real estate developers (REDs) has risen by around 6% during the observation period, from 1 643 as of end 2021 to 1 743 as of end 2024. The sub-sector remained fragmented in 2024: approximately 61% of REDs had a turnover below EUR 120 000, 15% of RED generated between EUR 120 000 and EUR 620 000 and 24% generated a turnover over EUR 620 000. Top-five REDs accounted for 21% of the market's turnover in 2024.

10.3.2. Freeport operators

AT A GLANCE

Most relevant TF stage:

☐ Raising ☒ Moving ☐ Using ☐ Non-relevant

Products and activities rather suitable for:

☐ Lone actors, small cells and FTFs with small TF needs
☒ International organisations and other terrorist actors with larger TF needs

At the product level (SNRA)

The SNRA (2022) notes that: "The TF threat relating to free zones is considered significant [at the EU level]. Free zones operate several restrictions that prevent local authorities from investigating property stored at their premises." However, this is not the particular case of Luxembourg's freeport. Indeed, according to the SNRA, "In most EU free zones and customs warehouses (with the exception of the Luxembourg Freeport), precise information on the ultimate beneficial owners (UBOs) of goods is not available." With respect to the TF vulnerability, the SNRA states that "when used anonymously (which is not the case of Luxembourg's freeport, as explained above), free zones are inherently exposed to TF vulnerability. Awareness in the sector is growing but is still not sufficient. The level of TF vulnerability relating to free zones is therefore considered significant (level 3)".

At the sub-sector level (NRA)

The TF inherent risk associated to the freeport is assessed as "Medium".

Sector	Sub-sectors	2026 NRA: Inherent risk
Freeport operators		Medium

327. The Luxembourg High Security Hub (LHSH; free zone) is located in Luxembourg Findel airport and encompasses 22 000 m² of building structure. It is specifically designed for storage of high value goods (such as artwork, vintage cars and fine wines). Humidity, temperature and other storage

conditions are adapted. It has direct tarmac access to the cargo runway to reduce package manipulations as much as possible. Its fire system is designed to protect artwork (vacuuming oxygen in the rooms). Strong rooms are up to 300 m². Gold and cash storage is allowed, but only for cash stored by local banks.

328. The number of clients remained stable throughout the observation period (between 90 and 100 clients). The share of non-resident clients is stable since 2022: EU resident clients (excluding Luxembourg) represent 30% and non-EU resident clients 33%. Note that the share of clients residents in high-risk jurisdictions based on FATF lists represented 2% through 2021–2024.

329. In 2024, four licensed freeport operators rented space at the LHSH (five operators in previous years), providing services related to art (galleries, a local museum, art intermediaries) and gold storage.

330. The 2023 FATF report ML and TF in the Art and Antiquities Market[136] explains that there are ML/TF vulnerabilities associated with cultural objects and storage facilities, as free trade zones may allow "buyers and sellers conducting transactions anonymously, or property being kept out of reach of law enforcement authorities". This is however not the case of Luxembourg, where customers operators of LHSH operators are subject to the 2004 AML/CFT Law. LHSH operators are required to identify the BOs of the goods that were brought in by their clients. Clients cannot use offshore companies, trusts, lawyers, nominees or galleries to shield their ownership of goods in the Luxembourg freeport. Consequently, these types of clients may prefer using other freeports where information on BO is not required[137]. Hence, the LHSH may be less attractive for criminals, be their purpose to exploit its facilities for ML or for TF purposes.

10.3.3. Dealers in goods

AT A GLANCE

Most relevant TF stage:

☐ Raising ☒ Moving ☐ Using ☐ Non-relevant

Products and activities rather suitable for:

☒ Lone actors, small cells and FTFs with small TF needs
☐ International organisations and other terrorist actors with larger TF needs

At the product level (SNRA)

Although an emerging risk, the 2022 SNRA assesses TF risks related to looted artefacts and antiques and high value assets (precious metals and stones and others) as "High".

At the sub-sector level (NRA)

Car dealers are assessed as having "High" TF inherent risk due to the sub-sector's products and activities followed by the sub-sector's structure (i.e., size and fragmentation), international business and clients/transactions (volume and risk). The level of TF inherent risk related to the other dealers

[136] Link
[137] See for instance, European Parliamentary Research Service, *Money laundering and tax evasion risks in free ports*, October 2018.

in goods (i.e., precious metals/jewellers/clocks, art/antiques and luxury goods) are assessed to be "Medium", with key risk driver stemming from these sub-sectors' products (vulnerability associated to the portability of goods).

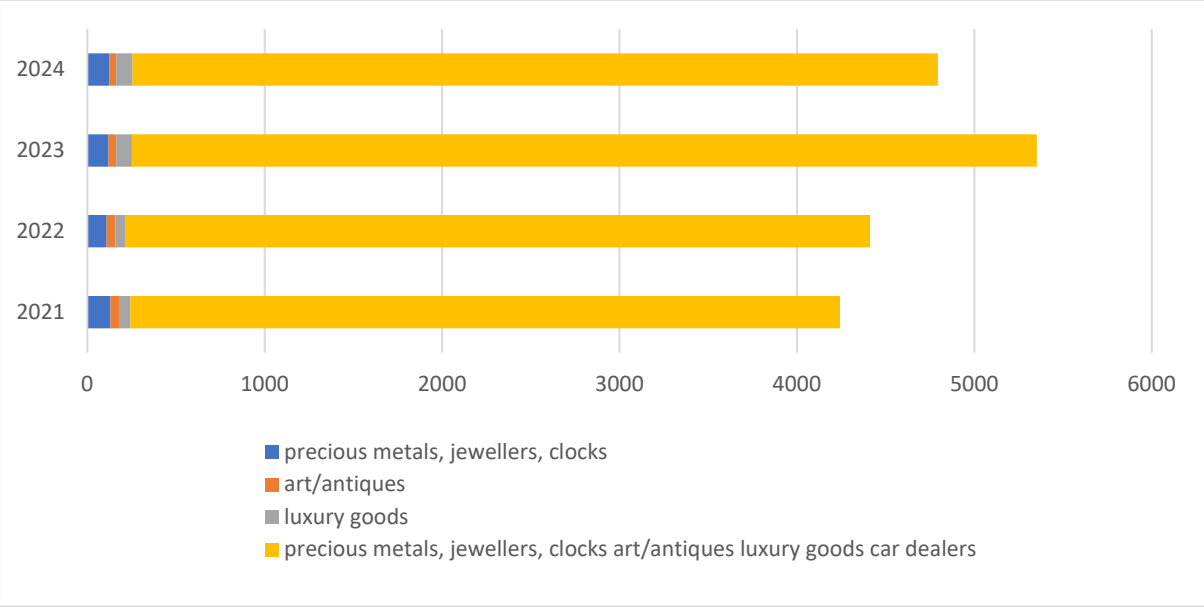
Sector	Sub-sectors	2026 NRA: Inherent risk
Dealers in goods	Precious metals/jewellers/clocks	Medium
	Car dealers	High
	Art/Antiques	Medium
	Luxury goods (e.g. *maroquinerie)*	Medium

331. In Luxembourg, dealers in goods are defined in the 2004 AML/CFT Law as entities dealing with and accepting cash equivalent to EUR 10 000 or more. These include dealers in precious metals, clocks and jewellers, car dealers, art/antiques dealers and luxury goods retailers (e.g. *"maroquinerie"*).

332. Overall, Luxembourg counted 96 dealers in precious metals, jewellers and clocks, 51 art and antiques dealers and 554 car dealers in 2024.

333. As evidenced in the figure below, the overall turnover generated has increased during the observation period and was predominantly (about 95%) generated by car dealers.

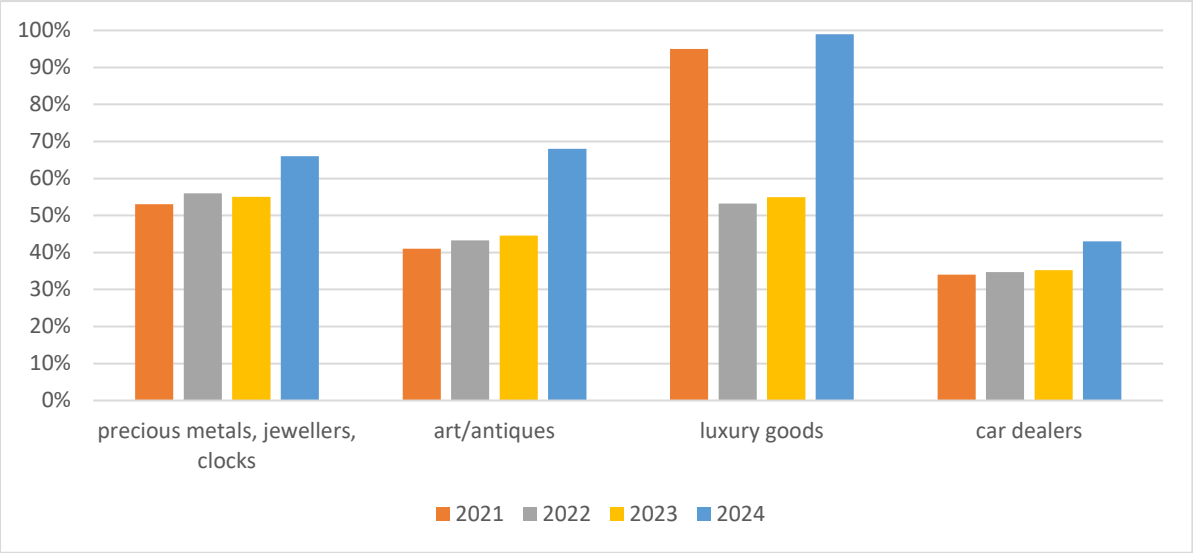
Figure 14: Total turnover generated by dealers in goods[138] (in EUR million), 2021–2024



334. Concentration rate amongst the different dealers in goods sub-sectors varies, as shown in the graph below. Dealers in luxury goods are the most concentrated sub-sector (although the share of turnover generated by top-five entities has plummeted in 2022–2023) followed by dealers in precious metals, jewellers and clocks. In a similar vein, the sub-sector of car dealers presented the least degree of concentration among these sub-sectors.

[138] AED data.

Figure 15: Concentration rates: share of revenues generated by top-five entities (per category), 2021–2024[139]



335. There is no legal limit on cash payments, although professionals must conduct CDD on payments exceeding EUR 10 000. During its interactions with the private sector through their AML/CFT supervisory activity and enforcement measures, the AED has noted that the professionals' risk-appetite with regard to cash transactions has considerably decreased. As such, the share of professionals limiting, or even restricting cash transactions has increased throughout the observation period. This is especially the case for dealers in goods where the AED has conducted systematic controls, such as the dealers in precious metals, jewellers and clocks (113 transactions over EUR 10 000 for a total amount of EUR 3 million in 2020 vs. 54 transactions over EUR 10 000 totalling EUR 1,7 million in 2022)[140] as well as car dealers.

10.3.4. Gambling service providers

336. In Luxembourg, professionals providing gambling services are limited and mostly concentrated around the casino and the National Lottery, which is also the only provider of offline sports/horse betting[141]. The National Lottery launched a sports betting site to contribute to combat illegal online gambling in September 2024. Other than this, no other operator is authorised to provide online gambling or sports betting in Luxembourg.

AT A GLANCE

Most relevant TF stage:

☐ Raising ☐ Moving ☐ Using ☒ Non-relevant

Products and activities rather suitable for:

☐ Lone actors, small cells and FTFs with small TF needs

[139] AED data.
[140] AED study on dealers in precious metals, jewellers and clocks' cash transactions for the years 2020–2022. See Luxembourg NRA of ML (2025), section 6.3.3. for more key finding of this study, link.
[141] PMU for horse betting, Oddset for sports betting.

☐ International organisations and other terrorist actors with larger TF needs

At the product level (SNRA)

In the 2022 SNRA the land-based/offline gambling sector (betting, bingo, casinos and gaming machines outside casinos and poker) is assessed as not relevant for TF. With regards to online gambling, however, the 2022 SNRA explains that when exchangeable tokens are used in video games, these can be assimilated to crypto-assets and are exposed to very high TF risks**.**

At the sub-sector level (NRA)

The 2026 NRA of TF assesses Luxembourg gambling services providers' (the Casino and the National Lottery) as presenting "Low" inherent TF risk.

Sector	Sub-sectors	2026 NRA: Inherent risk
Gambling service providers	Casino	Low
	National lottery	Low

10.3.4.1. Casino

337. Luxembourg counts one privately owned casino with approximately 376 000 visitors in 2024 (around 311 500 visitors per year, on average, during the observation period 2021–2024). Many visitors enter the casino area in order to go to the casino's restaurant or to attend shows. The casino counted 168 employees in 2024 and generated revenues of EUR 61,1 million (of which EUR 56,4 million in gross gaming revenue (GGR)).

338. The casino's client base is mostly regional: 50% of GGR is generated by French residents, nearly 30% by Luxembourg residents, 15% by German residents and 4% by Belgian. The remaining 1% of GGR is generated by clients residents in other countries.

339. With regard to products and activities, slot machines were the most popular gambling activity. It should be noted that activities related to gambling are regulated. Moreover, all transactions regarding gambling activities are registered via personal client cards and require face-to-face interaction with casino staff, further reducing exposure to TF abuse.

10.3.4.2. National Lottery

340. The National Lottery is public owned[142] and operated by the *"Œuvre Nationale de Secours Grande-Duchesse Charlotte",* which is an *"établissement public"* (public entity) under the Law of 22 May 2009[143]. It is run by a dedicated general manager and the management team. Its profits are redistributed to charities in various fields (e.g. healthcare or culture) through the "*Œuvre Nationale de Secours Grande-Duchesse Charlotte"*. The "*Œuvre Nationale"* manages the annual profits generated by the National Lottery.

[142] Note that private lottery operators are possible by Luxembourg law, but none are currently present.
[143] "Loi du 22 mai 2009 relative à l'Œuvre de Secours Grande-Duchesse Charlotte et à la Loterie Nationale", with article 2 stating that *"L'Œuvre a pour missions : […] d'organiser et de gérer la Loterie Nationale."*

341. Total sales, GGR, points of sale and number of employees have increased through the observation period:

- Total sales reached 269,7 million in 2024, compared to 126,9 million in 2021;
- The GGR amounted to EUR 91 million in 2024, compared to EUR 54,7 million in 2021. Around 96% of GGR stemmed from lottery type games (e.g. instant games such as scratch cards) and the remaining 4% from sports/horse betting;
- In 2024, the National Lottery counted 529 points of sale (e.g. supermarkets, kiosks, petrol stations) and one point of online sale (the National Lottery's website). Through the observation period, around 90% of revenues were generated from tickets sold via those intermediaries (points of sales) and 10% were generated via the National Lottery's website[144];
- Number of employees increased from 47 as of end 2021 to 58 as of end 2024.

342. The player base in point of sales has stayed constant through the observation period, averaging 35 000 to 50 000 customers per week (which could go up to 80 000–90 000 customers during busy weeks) and the vast majority of customers are from Luxembourg or neighbouring countries, sales being limited to the Luxembourg territory. The online player base is of around 4 000 a week and is 100% Luxembourg resident. For its draw-based games, the National Lottery has established collaborations with foreign/international lotteries (e.g. Euro Millions, Lotto), in order to offer larger potential winning pools to its customers. The instant games (in the form of scratch-cards) are all domestic only.

Insight Box 8: Ad hoc lotteries

Ad hoc lotteries are organised in Luxembourg at the municipal and national levels according to article 2 of the 1977 Gambling Law. All lotteries must be dedicated, partially, or entirely, to charity purposes.

Most lotteries are organised at the local level and approved by one of the 100 municipalities, if they are expected to generate less than EUR 12 500. They are unlikely to generate significant proceeds given the low threshold in place. Assuming conservatively that each municipality authorizes three ad hoc lotteries a year for average revenues of EUR 6 000, total revenues generated by local ad hoc lotteries would reach EUR 2 million per year.

Above the expected revenue level of EUR 12 500, lotteries must be approved by the MoJ. Overall, the amounts involved for these national ad hoc lotteries are limited. Between 2021 and 2024, 24 lotteries were authorized at the national level, selling tickets for a global amount of EUR of almost 1 200 000 (nearly EUR 300 000 on average per year). Furthermore, authorisations granted by the MoJ provide that 40% of the generated revenue is distributed as wins to the participants.

10.3.5. Legal and accounting professionals supervised by the AED

AT A GLANCE

Most relevant TF stage:

[144] National Lottery data.

☐ Raising ☒ Moving ☐ Using ☐ Non-relevant

Products and activities rather suitable for:

☐ Lone actors, small cells and FTFs with small TF needs

☒ International organisations and other terrorist actors with larger TF needs

At the product level (SNRA)

Overall, the 2022 SNRA concludes that TF risk related to the services provided by legal and accounting professionals does not differ from ML risk considering their potential to hide the illegal origin of funds. The 2022 SNRA assessed the TF risk of services provided by these professionals as "High".

At the sub-sector level (NRA)

The inherent TF risk of legal and accounting professionals under AED supervision is assessed to be "High" with key vulnerabilities stemming in from sub-sector fragmentation, products and activities (including TCSPs), exposure to international business, and clients.

Sector	Sub-sectors	2026 NRA: Inherent risk
Legal and accounting professions supervised by the AED	Accountants	High
	Professional directors and business centres	High

343. In case these professionals are providing TCSP activities, they are globally known to be particularly vulnerable to ML/TF. Indeed, as other professionals providing TCSP services, they might be abused to hide the illegal origin or destination of the funds or the true BO.

10.3.5.1. Accountants

344. Through the observation period, the total number of accountants remained stable at around 630, on average. Whereas top-five players generated 35% of the market turnover in 2024 (i.e., EUR 395 million), top 100 players accounted for 79% of the said turnover. Considering the important number of players and the moderate degree of market concentration, the sector is assessed to bear some fragmentation.

10.3.5.2. Professional directors and business centres

345. In 2021 (2020), the AED registered 688 (627) certified directors for VAT purposes. The market became more fragmented with top-five players generating 59% of total market turnover in 2020 compared to 20% in 2021. The turnover linked to those professionals amounted to EUR 38 million (EUR 54 million) in 2021 (2020)[145].

346. Through the observation period there were, on average, around 60 business centres supervised by the AED, with top-five players generating slightly more than 50% of total turnover in

[145] AED data.

2024, compared to around 40% between 2021 and 2023. Overall, business centres supervised by the AED accounted for a total annual turnover of around EUR 54 million, on average[146].

10.4. Legal and accounting professions supervised by SRBs

AT A GLANCE

Lawyers, notaries, and accountants face medium to high inherent risk linked to their roles in corporate structuring, real-estate transactions and legal-arrangement management, where complex structures can conceal beneficial ownership and the origin/destination of funds.
Auditors present medium inherent TF risk, while court bailiffs and casinos present low inherent TF risk.

SNRA

Overall, the 2022 SNRA concludes that TF risk related to the services provided by these professionals does not differ from ML risk considering their potential to hide the illegal origin of the fund. The 2022 SNRA assessed the TF risk of services provided by these professionals as "high".

NRA

The 2026 NRA assesses the TF risks of services offered by legal and accounting professionals for each sub-sector under the "products/activities" dimension. The table below provides the inherent risk levels for the sub-sectors falling within the AML/CFT supervision of the different SRBs:

Sector	Sub-sectors	2026 NRA: Inherent TF risk
Legal and accounting professions supervised by SRBs	Lawyers	Medium
	Notaries	High
	Court bailiffs *("huissiers de justice")*	Low
	Audit profession[147]	Medium
	Chartered professional accountants *("experts-comptables")*	High

10.4.1. Lawyers

AT A GLANCE

The sub-sector inherent TF risk level is "Medium".

Most relevant TF stage:

☐ Raising ☒ Moving ☐ Using ☐ Non-relevant

Products and activities rather suitable for:

[146] AED data.
[147] In this document, the term "audit profession" covers statutory auditors ("*réviseurs d'entreprises*"), approved statutory auditors (*réviseurs d'entreprises agréés*), audit firms ("*cabinets de revision*") and approved audit firms ("*cabinets de révision agréés*").

☐ Lone actors, small cells and FTFs with small TF needs

☒ International organisations and other terrorist actors with larger TF needs

The structure stands out as the main risk factor of this sub-sector followed by the international dimension of the profession and the number (volume) of mandates served. The ownership structure as well as the products and services offered by those professionals were considered to bear lesser TF risk.

347. Over the observation period, the number of lawyers registered with the *Barreau de Luxembourg* (OAL) is large and increasing with 3 587 registered lawyers spread into 708 law firms in 2024, in comparison to 3 078 registered lawyers and 554 law firms in 2021. The *Barreau de Diekirch* (OAD) counted 29 members in 2024 and 25 law firms. Most law firms are owned or controlled by a Luxembourgish BO, with less than 30% being owned or controlled by a foreign BO based in the EU in 2024.

348. Around 37% of OAL members were employed by the ten largest law firms and 573 out of the 708 (i.e. 80%) law firms employed 10 or less lawyers in 2024. In this context, it is also noteworthy to mention that the degree of fragmentation is not only considerable in terms of players on the market, but also in terms of financial viability of the different types of law firms.

349. During the observation period, around 50% of law firms offered services falling within the scope of the 2004 AML/CFT Law. Nonetheless, most lawyers focus predominantly on litigation and legal services and on legal mandates to a lesser extent. Those activities generally represent a lower risk for TF. Due to Luxembourg's important financial sector, Luxembourg's largest law firms are specialised in banking, corporate tax, mergers and acquisitions, private equity, investment funds and litigation legal services.

350. TCSP activities are globally known to be particularly vulnerable to ML/TF, as professionals delivering these activities might be abused to hide the illegal origin of the funds or the true beneficial owner. Especially the involvement of a lawyer may add respectability and credibility to an activity, a valuable feature that could be abused by criminals. With respect to TF specifically, it should however be noted that these services are more likely to be abused by more sophisticated actors (organized groups) with important financial needs rather than by lone actors and smaller organisations considering their low financial requirements and the licit origin of their funds.

351. As already noted in the 2025 NRA of ML, only a small share of OAL law firms (around 10% between 2021 and 2024) provide TCSP services, with most of them offering domiciliation services and/or directorship services. Furthermore, these services accounted for a minimal share (less than 1%) of total generated turnover. Between 2022 and 2023, no OAD member and OAD law firm performed TCSP activities. In 2024, one of the 25 OAD law firm provided TCSP services, representing less than 10% of its turnover.

Insight Box 9: Complementarity of information provided in the 2025 NRA of money laundering for services offered by lawyers

Considering that the TF risk with regard to services offered by lawyers has common features with the ML risk, please refer to the 2025 NRA ML (section 6.4.1. on the vulnerability of the lawyer profession and section 6.6.1. on TCSP activities) for further information.

352. In line with the international openness of Luxembourg's economy, lawyers serve an international, but predominantly European clientele[148]. However, the exposure towards countries that were selected for analysis for the purposes of this report under section 6 (i.e. TJs) appears to be limited:

- Out of the law firms offering services falling into the scope of the 2004 AML/CFT law (61 entities), 18% declared having clients that are domestic legal persons having activities and/or assets (i) related and/or (ii) located in TJs, representing 684 clients in 2024;
- Out of the law firms offering services falling into the scope of the 2004 AML/CFT law (48 entities), 18% declared having clients that are foreign legal persons having activities and/or assets (i) related and/or (ii) located in TJs, representing 818 clients in 2024.

353. In terms of exposure to clients residents in a TJ, OAL law firms counted 95 natural persons and 969 BOs in 2024. In line with the analysis of flows performed and the conclusions drawn under section 10, there is no evidence to suggest that the nature and volume of these flows pose a material threat in terms of TF to the profession.

354. The number of OAL law firms having clients with higher risk factors was situated around 10% in 2022 and 2023 but decreased to approximately 6% in 2024. In terms of materiality, more than 80% of them noted that those clients represented less than 10% of their total volume of clients.

355. Findings from the OAL "annual mandatory AML/CFT general questionnaire" suggested that the higher the turnover linked to activities in scope of the 2004 AML/CFT Law, the higher their estimated risk". Among the OAL law firms falling within the scope of the 2004 AML/CFT Law, most of them (and all of the concerned OAD law firms) declared generating between 1% and 10% of their turnover from the said activities.

356. The vast majority of members (both lawyers and law firms) of the OAD do not offer services falling within the scope of the 2004 AML/CFT law and if so, it's a small part of their activities. Only one member of the OAD had activities inherently in scope of the 2004 AML/CFT during the observation period.

357. Finally, the majority of contacts and entry into business relationships were made through direct contacts, decreasing the TF vulnerability linked to distribution channels.

[148] Here, this term includes EU Member States and 31 territories / countries such as Switzerland, Liechtenstein, UK, Monaco, Ukraine, Iceland, Norway, Albania, Andorra, Belarus, Bosnia-Herzegovina, North Macedonia, Montenegro, Moldova, Serbia and territories (even outside of Europe) administered by these countries (mainly the UK).

10.4.2. Notaries

AT A GLANCE

The sub-sector inherent TF risk level is "High".

Most relevant TF stage:

☐ Raising ☒ Moving ☐ Using ☐ Non-relevant

Products and activities rather suitable for:

☐ Lone actors, small cells and FTFs with small TF needs
☒ International organisations and other terrorist actors with larger TF needs

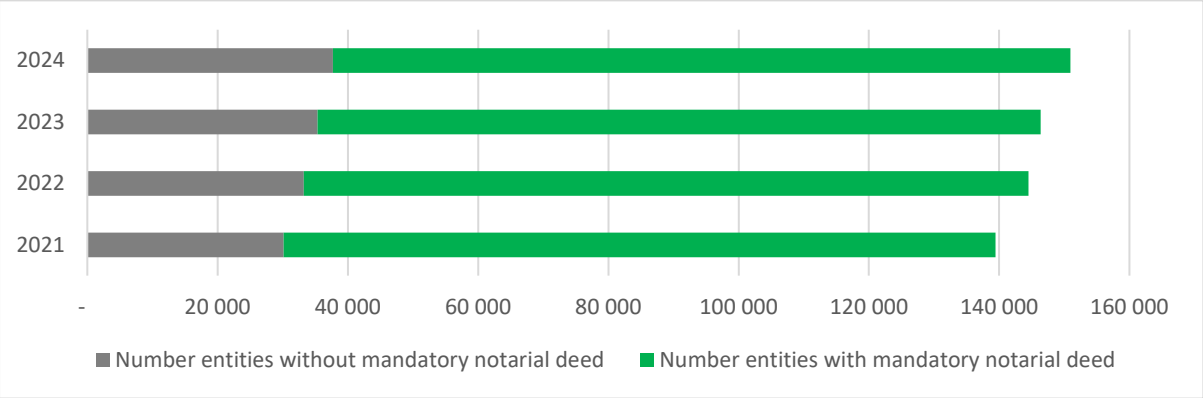
Sub-sector size and international exposure of some notaries' offices are the key vulnerabilities driving TF inherent risk for notaries.

358. The number of notaries is fixed at 36 by the Law of 9 December 1976 on the organisation of the notarial profession. Although the number of notaries has remained unchanged since the 2020 NRA, eight new notaries were appointed between 2021 and 2024 due to an equivalent number of retirements. It was estimated that the number of employees in these 36 notarial offices fluctuated between 250 and 350[149].

359. As explained in detail in the VRA on ML/TF risks of legal persons and legal arrangements[150], some legal acts can only be performed by notaries. For instance, a notarial deed is required to incorporate some types of legal persons and most real estate transactions require the intervention of a notary. Some of these activities are considered high-risk by the FATF (e.g. real estate transactions, purchase of shares and other participations).

360. The following graph represents the total number of entities registered with the RCS with and without notarial deed throughout the observation period of this NRA.

Figure 16: Number of legal persons registered with the RCS, situation as of end 2021–2024[151]



[149] CdN data.
[150] MoJ, *ML/TF vertical risk assessment on legal persons and legal arrangements,* 2022, link.
[151] LBR data.

361. Although the share of entities created by notarial deed has slightly decreased during the observation period, at least 75% of Luxembourg legal persons were registered by notarial deed.

362. Compared to 2021, the number of total real estate mortgage transcriptions with the AED decreased from around 29 700 to less than 22 000 transcriptions in 2024[152,153]. In view that most real estate transcriptions required the intervention of a notary, it is considered that this is a fair indicator of notaries' activities in terms of volume.

363. Generally speaking, it is considered that corporate law activities tend to be more international than real estate or family law related activities. Most notarial deeds set up in Luxembourg concerned private individuals residing in Luxembourg with international companies playing a minor role. Consequently, these notaries primarily serve local and national clients within a variety of civil law fields, which are deemed to be exposed to lower TF risk than those offices more active in international corporate activities, transactions implying larger cash flows, etc. The number of notaries reporting that corporate law forms the largest part of their activities increased during the observation period (they represented less than 20% notaries in 2021–2022, and around 35% of notaries in 2023–2024). Indeed, the number of notaries reporting that corporate law forms the largest part of their activities increased in 2023 even though the volume of corporate law transactions remained unchanged in that year, explained by the decrease in real estate activities. However, the number of corporate law transactions then decreased drastically in 2024.

364. Considering that notaries do not provide TCSP activities and the level of expertise and planning required to involve notaries in the setting up of legal persons and/or sale of real estate transactions, their services are not particularly attractive for straightforward TF purposes, but rather for more sophisticated actors.

365. Nevertheless, there is a significant portion of international clientele in some notarial offices, especially in the ones that are specialized in business acts[154]. Hence, a conservative scoring for the "international business" criterion was applied.

10.4.3. Court bailiffs

AT A GLANCE

The sub-sector inherent TF risk level is "Low".

Most relevant TF stage:

☐ Raising ☐ Moving ☒ Using ☐ Non-relevant

Products and activities rather suitable for:

☒ Lone actors, small cells and FTFs with small TF needs
☐ International organisations and other terrorist actors with larger TF needs

[152] AED, *Rapport d'activité 2021 de l'Administration de l'enregistrement, des domaines et de la TVA,* 2021, link, 2022, link, 2023, link and 2024, link.
[153] At present, a more granular breakdown of notaries' activities is not available to determine which acts relate to real estate transactions with monetary consideration and which do not.
[154] CdN data.

366. The number of Court bailiffs is capped at 19 by the Law of 4 December 1990 on the organisation of Court Bailiffs.

367. Court bailiffs are subject to the 2004 AML/CFT Law when conducting public actions:

- Sales related to bankruptcies: requested by trustees in order to liquidate the debtor's assets and repay the body of creditors.
- Sales at the request of the Asset Management Office (AMO): these have grown in recent years.
- Forced sales: organized to sell assets seized during the enforcement of court judgments.
- Voluntary sales: when an owner requests the sale of their movable property (for example, in the context of an inheritance; certain public entities may also use this procedure).

368. The number of bailiffs active in this activity remains stable since 2018 at around 12.

369. Since 2024, more detailed statistics show that 70% of auction proceeds come from bankruptcy-related sales or sales requested by the AMO. It therefore seems unlikely that someone would use this channel to finance terrorist activities.

370. In order to assess whether bidders could use goods acquired at these auctions to commit terrorist acts, it should be noted that to participate in a public auction, identification and proof of the origin of funds are mandatory. Furthermore, goods that are sold by bailiffs are second hand and available in other businesses and marketplaces. It is, therefore, generally easier to obtain similar goods through commercial channels or from private individuals.

371. In conclusion, the goods sold at auction are easily accessible through other means and do not have any particular characteristics that would make them a preferred vector for financing terrorism.

10.4.4. Audit profession[155]

AT A GLANCE

The sub-sector inherent TF inherent risk level is "Medium".

Most relevant TF stage:

☐ Raising ☒ Moving ☐ Using ☐ Non-relevant

Products and activities rather suitable for:

☐ Lone actors, small cells and FTFs with small TF needs

☒ International organisations and other terrorist actors with larger TF needs

As for ML, sub-sector size, international exposure and significant number of audit clients are the key vulnerabilities driving TF inherent risk for the audit profession. However, products and activities do not appear to be particularly suitable for TF purposes. Moreover, TCSPs activities, that are deemed higher risk of ML and TF represent a minor share of total activities of the audit profession and flows with weak AML/CFT measures geographies and exposure to clients that are PEP are rather limited.

[155] In this document, the term "audit profession" covers statutory auditors *("réviseurs d'entreprises")*, approved statutory auditors *("réviseurs d'entreprises agréés"),* audit firms *("cabinets de revision")* and approved audit firms *("cabinets de révision agréés").*

372. The description of the size and structure of the sector given in 2025 NRA ML remain valid as of end 2024: the sector remains sizable and moderately fragmented.

373. Overall, it should be noted that services provided by statutory auditors are not, in a sense, relevant for lone actors, small cells and FTFs. Statutory auditors' core activities relate to assurance services such as audit and review of annual accounts of legal persons. As for ML, these activities are considered to be low TF risk. Furthermore, statutory auditors generally intervene at a second stage in the process (post facto review of annual accounts or historical data). In a similar vein, assurance and related services (e.g. accounting, compliance and regulatory services) represented 82% of the total turnover and 85% of their clients as a whole in 2024. TCSP activities, which are deemed to be higher risk from a ML and TF point of view, represented a minor share of total activities (they represented less than 0,80% of statutory auditors total turnover and were provided to 1,34% of their clients in 2024), which decreases audit profession's vulnerability to TF related to products and services.

374. Statutory auditors predominantly served a regional clientele with 91% (92%) of them being registered or residing in the *"Grande region"* in 2024 (2023). In a similar vein, BOs of audit firm clients were mainly resident in EU countries (69% in 2024, 68% in 2023), the UK (9,2% in 2024, 9,4% in 2023), the USA (6,6% in 2024, 8% in 2023) and Switzerland (6% in 2024 and 2023). Exposition to BOs residing in jurisdictions targeted for analysis represented 3% in 2024 (2,47% in 2023) and represent mostly T4 and T6 countries.

375. The number of clients amounted to around 35 500 in 2024 (34 700 in 2023) for the whole profession. (Approved) audit firms' clients were mainly represented by Luxembourg *Sociétés commerciales* (84% in 2024 and 2023) from both the financial and non-financial sector. The number of BOs of legal persons clients of the audit profession who were PEPs represented 3,2% of the total number of BOs reported by the audit profession in 2024 (3,4% in 2023).

376. Moreover, the share of clients represented by sectors known to be more vulnerable to TF is very low, as for example:

- PI and EMI (0,13% in 2024, 0,11% in 2023);
- crowdfunding service providers (one client declared for the whole profession in 2024, none in 2023).

377. Furthermore, less than 0,5% of audit firms' clientele had a business activity which is related to one of the riskier business sectors listed in Appendix IV of the 2004 AML/CFT Law throughout the observation period.

10.4.5. Chartered professional accountants

AT A GLANCE

The sub-sector inherent TF inherent risk level is "High".

Most relevant TF stage:

☐ Raising ☒ Moving ☐ Using ☐ Non-relevant

Products and activities rather suitable for:

☐ Lone actors, small cells and FTFs with small TF needs

☒ International organisations and other terrorist actors with larger TF needs

As for ML, sub-sector structure, international exposure and volume are the key vulnerabilities driving TF inherent risk for chartered professional accountants.

Although TCSPs activities, deemed higher risk from a ML and TF perspective are widely provided by a number of chartered professional accountants (CPAs), the related generated revenue is relatively minor. Moreover, these services are generally not provided on a stand-alone basis but rather in combination with other core services. This enables CPA to have a more exhaustive and broader understanding of their clients and thus limiting to some extent TF risks.

378. The structure of the profession remains large and fragmented with over 1 200 professionals spread across 568 entities (CPA firms) and 90 independent professionals. Although the exact number of OEC members employed by one of the four largest firms varies on a monthly basis due to new registrations, radiations and staff turnover, around 30% of registered CPAs are employed by one of these firms. The profession includes also a high number of small CPA firms, although their total revenue is limited. Large CPA firms account for the biggest share of revenue generated by the sector.

379. It is generally presumed that the largest CPA firms offer international business services, although some smaller firms also serve an international clientele. Belgium, France and Italy are the most prevalent countries of residence of CPA's clients. More than 60% of CPA's had at least one BO residing in a non-EU country and 48% of CPAs had among their clients at least one BOs from risky jurisdictions. Nevertheless, these clients represent 2% of the total client base[156].

380. CPAs serve more than 110 000 clients, including over 800 offshore companies, almost 700 NPOs, and around 150 foundations. *Soparfis* are the most common type of clients served by CPA, accounting for around a third of the total client base, followed by commercial or industrial companies (around 28%) and natural persons (almost 20%). Around 30% of CPAs have clients that are PEPs, they represent less than 1% of the total client base, posing a moderate risk[157].

381. TCSP activities are globally known to be particularly vulnerable to ML/TF, as professionals delivering these activities might be abused to hide the illegal origin of the funds or the true BO. In the case of TF, TCSP activities might be also abused to hide the illegal destination of the funds. As already highlighted in the 2025 NRA ML, CPAs play a key gatekeeper and intermediary role for many transactions presenting a high risk. Indeed, CPAs provide a significant amount of TCSPs activities, which are considered high risk from a ML/TF perspective. Domiciliation services seem to be the most prevalent TCSP offering; however, for the firms who do provide this service, the revenue generated from it often represents less than 10% of their total turnover. CPA firms generally do not provide TCSP activities as a stand-alone service, but rather in combination with core CPA activities, which provides them broader oversight of their clients' activities, and thus limiting risks to some extent. Activities offered by TCSPs are not suitable for lone actors, small cells and FTFs considering their low financial requirements and the licit origin of their funds.

[156] OEC 2024 RBA questionnaire (data as of end 2023).
[157] OEC 2024 RBA questionnaire (data as of end 2023).

10.5. Legal persons and legal arrangements

AT A GLANCE

Legal persons and legal arrangements present medium-high to high inherent TF risk, reflecting the potential for shell companies, limited partnerships and other corporate vehicles to be used to obscure beneficial ownership and route TF funds through opaque holding structures. Luxembourg's RBE transparency framework mitigates this exposure, but cross-jurisdictional chains and BO opacity remain recurring TF risk amplifiers.

SNRA

Legal persons ("companies"):

At the EU level, the SNRA 2022 considers the overall level of TF risk for companies as medium.

In terms of TF threats, the SNRA 2022 states that there have been instances where companies have been abused for TF purposes. Funds generated by criminal activities have been laundered through cash enterprises, such as licensed premises and security companies or in the form of "loans" to businesses. These were often fronted by persons with no obvious affiliations to terrorist groups and whose involvement in terrorist financing was found after investigation.

In terms of vulnerability, the SNRA notes that, although there has been little evidence of their misuse for TF purposes, risks of trade-based terrorism financing are likely to materialize as terrorist groups increasingly adopt the operational methods of organised crime groups.

Legal arrangements ("trusts"):

In general, there is little evidence to date that trusts and other type of legal arrangements have been misused for the purpose of financing terrorism. Possibly due to the costs associated with setting up these arrangements, they do not appear to be particularly attractive to groups that carry out TF activities. The configuration of fiduciary structures does not allow the rapid management or disposition of funds – that usually accompanies TF activities – and demands a series of requirements to be carried out – which makes it difficult to use these structures for TF purposes. Therefore, the TF threat relating to legal arrangements is considered lowly/moderately significant (level 1/2).

The assessment of the TF vulnerabilities posed by legal arrangements has been considered together with ML in the SNRA, as there are no indications that vulnerabilities vary in type or intensity according to the type of misuse (ML or TF). Therefore, the TF vulnerability relating to legal arrangements is considered significant (level 3).

NRA

Sector	Sub-sectors	2026 NRA: Inherent risk
Legal persons and legal arrangements	*Sociétés commerciales*	High
	Sociétés civiles	Medium
	NPOs (as per FATF definition) [158] carrying out primarily international activities – ASBLs and *Fondations*	High

[158] See section 10.6 for a more granular view of the inherent TF risk of the NPO sub-sector.

NPOs (as per FATF definition) carrying out international and local activities – ASBLs and *Fondations*	Medium
NPOs (as per FATF definition) carrying out local activities – ASBLs and *Fondations*	Low
Other legal persons	Medium
Domestic *Fiducies*	High
Foreign trusts	High

10.5.1. Legal persons

AT A GLANCE

The sub-sector inherent TF risk level is "High".

- For *Sociétés commerciales*, risk drivers relevant to ML such as size, ownership/structure and volume of clients are also relevant for TF, although products and activities appear less vulnerable for TF than for ML.
- Key vulnerabilities of NPOs with international activities are products/services and the geography where these products/services are provided.

Most relevant TF stage:

☒ Raising ☒ Moving ☐ Using ☐ Non-relevant

Products and activities rather suitable for:

☐ Lone actors, small cells and FTFs with small TF needs
☒ International organisations and other terrorist actors with larger TF needs

424. All legal persons incorporated in Luxembourg must be registered with the RCS as per the 2002 RCS Law. With respect to the situation at the end of the observation period, the total number of legal persons has risen to 150 942 (8% increase from 139 430 legal persons as of 31 December 2021).

382. By broad category of legal persons, *Sociétés commerciales* increased the most, with 10 773 additional entities. Within this category, SARLs and *Société en commandite spéciale* contributed the most to this increase with respectively 2 296 and 4 743 additional entities. On the other hand, SAs decreased by 1 693. *Sociétés civiles* increased by 172 to reach 6 017 entities. Within the non-profit sector, the number of ASBLs (out of which only a portion fall within the FATF NPO definition) increased by 543 to reach 9 000, while the number of *Fondations* (most of which fall within the FATF NPO definition) remained stable just below 200. Other legal persons also remained fairly stable at around 3 000 entities.

383. In terms of structure of the Luxembourg legal persons landscape, the situation has been rather stable for the last years with around 88% of *Sociétés commerciales*, 4% of *Sociétés civiles*, 6% of non-profit legal persons (*ASBLs* and *Fondations*) and 2% of other legal persons.

Table 12: Luxembourg legal persons by legal form and category, 2020–2024

	Situation date									
Legal form	31/12/2020	P%	31/12/2021	P%	31/12/2022	P%	31/12/2023	P%	31/12/2024	P%
Commercial companies	**121 918**	**88%**	**121 916**	**87%**	**126 485**	**88%**	**128 265**	**88%**	**132 689**	**88%**
Société cooperative	141	0%	149	0%	147	0%	148	0%	152	0%
Société cooperative européenne	-	0%	-	0%	-	0%	-	0%	1	0%
Société cooperative organisée comme une SA	114	0%	114	0%	132	0%	138	0%	139	0%
Société anonyme	36 533	26%	32 392	23%	31 110	22%	29 794	20%	30 699	20%
Société à responabilité limitée	73 226	53%	74 461	53%	77 531	54%	78 532	54%	79 757	53%
Société à responabilité limitée simplifiée	3 284	2%	4 150	3%	4 801	3%	5 343	4%	5 973	4%
Société par actions simplifiée	185	0%	212	0%	249	0%	273	0%	305	0%
Société européenne	41	0%	56	0%	55	0%	51	0%	44	0%
Société en commandite par actions	1 951	1%	2 087	1%	2 218	2%	2 326	2%	2 422	2%
Société en commandite simple	1 697	1%	1 849	1%	1 955	1%	1 997	1%	2 009	1%
Société en commandite spéciale	4 579	3%	6 304	5%	8 148	6%	9 538	7%	11 047	7%
Société en nom collectif	167	0%	142	0%	139	0%	125	0%	141	0%
Civil companies	**5 478**	**4%**	**5 845**	**4%**	**6 065**	**4%**	**6 068**	**4%**	**6 017**	**4%**
Société civile	5 478	4%	5 845	4%	6 065	4%	6 068	4%	6 017	4%
ASBLs	**8 504**	**6%**	**8 457**	**6%**	**8 717**	**6%**	**8 806**	**6%**	**9 000**	**6%**
Association sans but lucratif	8 504	6%	8 457	6%	8 717	6%	8 806	6%	9 000	6%
Fondations	**218**	**0%**	**193**	**0%**	**192**	**0%**	**193**	**0%**	**192**	**0%**
Fondation	218	0%	193	0%	192	0%	193	0%	192	0%
Other legal persons	**3 096**	**2%**	**3 019**	**2%**	**3 027**	**2%**	**3 041**	**2%**	**3 044**	**2%**
Association d'assurance mutuelle	6	0%	6	0%	6	0%	6	0%	6	0%
Société créée selon la loi du 28 mars 1997	1	0%	1	0%	1	0%	1	0%	1	0%
Société créée selon la loi du 24 mars 1989	1	0%	1	0%	1	0%	1	0%	1	0%
Société d'investissement à capital variable (SICAV)	1 175	1%	1 136	1%	1 099	1%	1 080	1%	1 074	1%
Société européenne d'investissement à capital variable (SICA	1	0%	1	0%	1	0%	1	0%	1	0%
Groupement d'intérêt économique	80	0%	82	0%	88	0%	92	0%	88	0%
Groupement européen d'intérêt économique	59	0%	58	0%	60	0%	59	0%	59	0%
Association agricole	110	0%	86	0%	88	0%	88	0%	89	0%
Association épargne-pension	10	0%	10	0%	10	0%	11	0%	9	0%
Etablissement public	118	0%	123	0%	128	0%	131	0%	138	0%
Fonds commun de placement	1 530	1%	1 505	1%	1 477	1%	1 461	1%	1 440	1%
Fonds d'investissement alternatif réservé	2	0%	2	0%	2	0%	2	0%	2	0%
Mutuelle	3	0%	8	0%	18	0%	32	0%	34	0%
Fonds de titrisation	-	0%	-	0%	48	0%	76	0%	102	0%
Total	139 214	100%	139 430	100%	144 486	100%	146 373	100%	150 942	100%

384. The ability to be used as complex structures is a key vulnerability of legal persons, also with regards to TF. In this regard, the presence of corporate shareholders and corporate managers/directors in legal persons may contribute to this complexity and thus pose obstacles to transparency and enhance the exposure to TF in two ways:

- From the point of view of the origin of the funds: when TF funds are sourced from illegal activities that are blended (or not) to proceeds from legitimate activities, obstacles to transparency may make it difficult to detect the illicit origin funds and disrupt the TF flow;
- From the point of view of the destination of the funds: obstacles to transparency may make it challenging to detect that the illicit ultimate destination of the funds that are either raised, stored, managed or moved by legal persons.

385. Basic information registered in the RCS shows that corporate owners were more prevalent in *Sociétés commerciales* than in *Sociétés civiles*[159].

386. Evidence from the RCS suggests that the presence of corporate managers/directors in Luxembourg legal persons is less common. Corporate managers/directors were more prevalent in *Sociétés commerciales* and much more limited in other categories of legal persons (*Sociétés civiles*, "Other legal persons") and specially in ASBLs and *Fondations*, where the number of legal persons with only natural persons as managers/directors was very close to 100%[160].

[159] RCS data as of 31 December 2023 provided by the LBR.
[160] RCS data as of 31 December 2023 provided by the LBR.

387. BO information[161] of legal persons must be registered with the *Registre des bénéficiares effectifs* (RBE) as per the 2019 RBE Law. As of end 2024, the compliance rate with this obligation was close to 100% for *Sociétés commerciales*, *Fondations*, and "Other legal persons" and slightly lower for ASBLs, but concerns the whole population of ASBLs and not only those falling under the FATF definition of NPO, and *Sociétés civiles*[162].

388. Information registered with the RBE as of 31 December 2024 confirms the international nature of BOs in the corporate environment in Luxembourg (see section 2), specifically with regards to *Sociétés commerciales* and "Other legal persons".

- From the legal person point of view:
  - By category of legal person, the higher percentage of legal persons with all Luxembourg residents are ASBLs, and *Sociétés civiles* and *Fondations*. *Sociétés commerciales*[163] and "Other legal persons" appear to have the least percentage of legal persons with all BOs being Luxembourg residents.
- From the BO point of view:
  - Altogether, 51% of registered BOs were Luxembourg residents, 29% were EU residents and the remaining 20% were residents outside the EU.
  - The "Other legal persons" category is shown to have the highest level of non-resident BOs, mostly explained by the presence of non-residents in *Fonds communs de placement* (FCPs[164]).
  - Non-resident BOs in S*ociétés commerciales* represented a significant share, driven by the presence of non-resident BOs in *Sociétés anonymes* and in *Sociétés à responsabilité limitée,* which were the most prevalent legal forms of *Société commerciale* in Luxembourg.
  - For the remaining types of legal persons, BOs are mostly national residents.

389. As explained in detail in section 8.2.1, BO registrations for persons residing in TJs represent 4% of total number of BOs and SMO registrations for persons residing in TJs are very limited (0,4%).

390. With respect to products and activities, the following table summarises the sectoral activity split per category of legal person as of 31 December 2024.

[161] Note that in the following section, SMOs are included in BO statistics unless otherwise specified.
[162] Data provided by the LBR. Closed bankruptcies are not taken into account.
[163] *Sociétés commerciales* also show a higher vulnerability with regards to non-resident shareholder/partnership than *Sociétés civiles*, as explained in MoJ, *Legal persons and legal arrangements ML/TF vertical risk assessment*, 2022, link.
[164] Although FCPs have no legal personality, they are registered as "Other legal persons" in the RCS. Please note that FCPs can be created through private deed.

Table 13: Sectoral split of legal persons registered with RCA following NACE codes as of end 2024 – top-three sector per category highlighted in orange[165]

Sector	*Sociétés commerciales*	*Sociétés civiles*	ASBLs	*Fondations*	"Other legal persons"
Agriculture, forestry and fishing	188	123	7	-	35
Mining and quarrying	13	-	-	-	-
Manufacturing	951	3	4	-	3
Electricity, gas, steam and air conditioning supply	212	140	1	-	5
Water supply	66	-	2	-	14
Construction	6 964	35	-	-	6
Wholesale and retail trade	10 218	7	2	-	28
Transportation and storage	1 716	4	1	-	4
Accommodation and food service activities	3 725	5	19	-	-
Information and communication	3 755	1	95	-	35
Financial and insurance activities	77 982	725	8	1	2 299
Real estate activities	5 817	3 473	5	2	17
Professional, scientific and technical activities	9 573	656	69	4	62
Administrative and support service activities	3 470	627	80	-	20
Public administration and defence	3	-	33	4	60
Education	640	3	165	10	16
Human health and social work activities	550	15	524	40	48
Arts, entertainment and recreation	540	34	2 085	7	19
Other service activities	1 392	-	4 692	82	35
Activities of extraterritorial organisations and bodies	1	-	1	-	-

[165] As of end 2024, the NACE code allocation for some legal persons (less than 5%) was pending. Consequently, the total of number of entities shown in this table is inferior to the total number of legal persons registered as of 31 December 2024 (i.e. 150 942) with the RCS. Nonetheless, the overall split shown above is deemed to remain valid.

391. The table above shows that almost 59% of *Sociétés commerciales* are active in the financial and insurance sector, which is in line with Luxembourg's context (see section 2). *Sociétés commerciales* are far less active in other sectors in percentage terms (wholesale and retail trade: 7,7%); professional, scientific and technical activities: 7,2%; construction activities: 5,2%) but still important in terms of number of entities[166].

392. Almost 60% of *Sociétés civiles* are largely active in real estate activities[167], which are globally considered as high risk from a ML perspective, but may also be exposed to TF as terrorist financiers may invest in real estate to place or store funds for later use.

393. "Other legal persons" were mostly active in the financial and insurance sector[168], which is explained by the fact that FCPs and *Sociétés d'investissement à capital variable* (SICAVs) used in the collective investment industry are included in this broad category.

394. With regard to the non-profit sector, it is worth noting that the information in the table above is given for illustrative purposes only, as it concerns all ASBLs and *Fondations* registered with the RCS, irrespective of being identified to fall under FATF Recommendation 8 definition as "NPOs". The activities, along with the geographical scope of activity analysis of Luxembourg NPOs falling under FATF definition is included in section 10.6.

10.5.2. Legal arrangements

AT A GLANCE

The sub-sector inherent TF risk level is "High".

Key TF risk drivers are ownership/legal structure (referring to beneficial ownership and legal features of legal arrangements), product and activities and geography.

Most relevant TF stage:

☒ Raising ☒ Moving ☐ Using ☐ Non-relevant

Products and activities rather suitable for:

☐ Lone actors, small cells and FTFs with small TF needs
☒ International organisations and other terrorist actors with larger TF needs

395. With regards to products and activities, *Fiducies* and other similar legal arrangements are inherently asset holding entities as they separate legal ownership from the beneficial ownership of the assets[169]. Although this characteristic of legal arrangements has been identified as a recurring vehicle

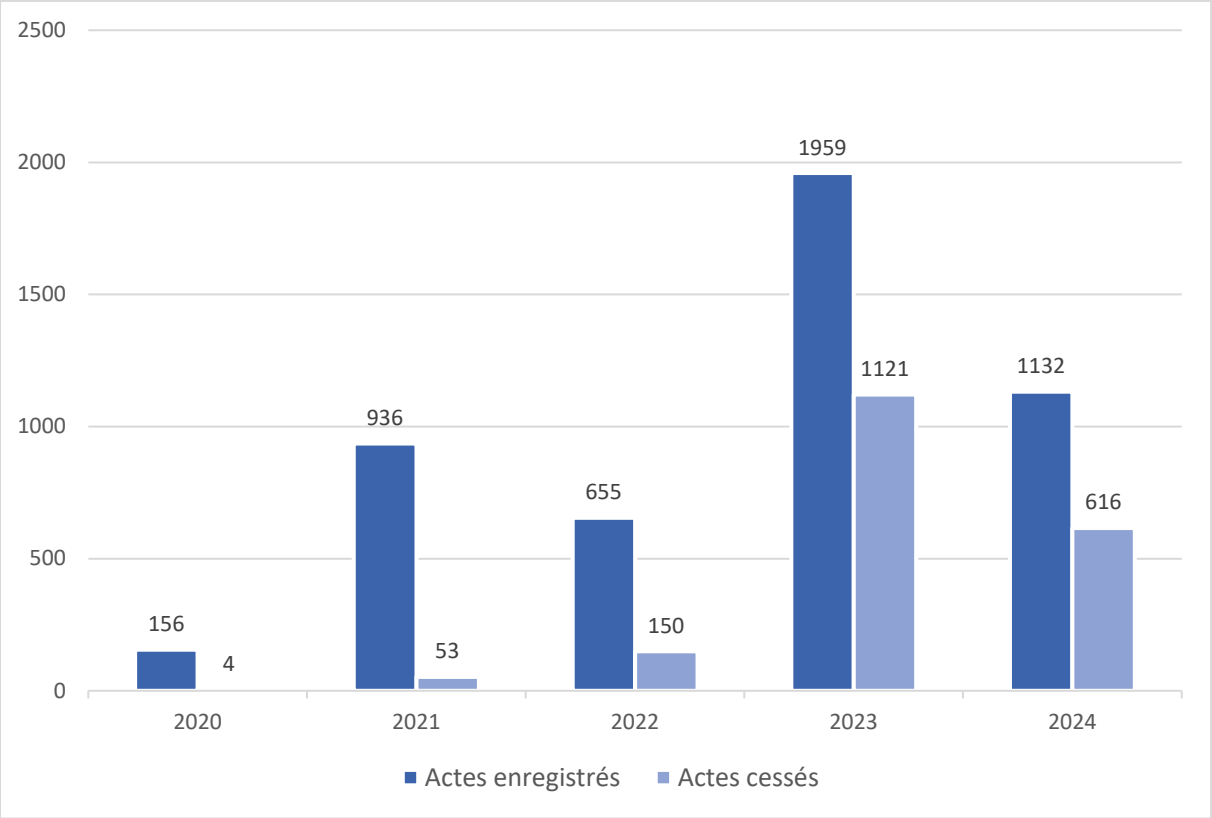
[166] Note that for 3,7% of *Sociétés commerciales* as of 31 December 2024 NACE codes are unknown.
[167] Note that for 12,6% of *Sociétés civiles* as of 31 December 2024 NACE codes are unknown.
[168] Note that for 13,7% of "Other legal persons" as of 31 December 2024 NACE codes are unknown.
[169] MoJ, *Legal persons and legal arrangements ML/TF vertical risk assessment*, 2022, link (section 5.1.2.2).

used in ML schemes globally, there is little evidence to date that trusts and other type of legal arrangements have been misused for the purpose of TF[170], as explained above.

396. In Luxembourg, legal arrangements comprised domestic *fiducies* and foreign trusts[171]. Except for the number of entities (*fiducies* represent 85% of legal persons registered in Luxembourg and foreign trusts, 15%), both *fiducies* and foreign trusts shared the same key vulnerabilities to TF.

397. The RFT went live in the second half of 2020. Figure 17 below shows the evolution of legal arrangements registered *"actes enregistrés"* and ceased *"actes cessés"* during the year and the following table next page shows the number of legal arrangements active at year end. The below graph shows that the population process is ongoing and dynamic as legal arrangements are subject to multiple revisions throughout their life cycle. The regular number of legal arrangements registered and ceased evidence that users are well informed about their obligations.

Figure 17: RFT registrations over the period 2020–2024[172]



[170] European Commission, *[Working Document] – Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities*, 2022, link.
[171] A detailed description, examples and related key legislation is provided in the LPs/LAs VRA, section 3.4 (pages 23-25), link.
[172] Registered *("Actes enregistrés")* vs. ceased *("Actes cessés")*, AED.

Table 14: RFT registrations over the period 2020–2024[173]

Year	Registered	Ceased	Modified	Actives as of 31 December	Actives as of 31 December (cumulative)
2020	156	4	2	152	152
2021	936	53	26	883	1 053
2022	655	150	89	505	1 540
2023	1 959	1 121	238	838	2 378
2024	1 132	616	134	516	2 894
Total as of 31 December 2024	**4 838**	**1 944**	**489**	**2 894**	**2 894**

398. There were 2 894 active *fiducies* and trusts managed in Luxembourg registered with the RFT as of 31 December 2024 (152 as of end 2020; 1 035 as of end 2021; 1 540 as of end 2022; 2 378 as of end 2023). As of end 2024, 85% of registered legal arrangements were domestic *fiducies* and 15% were trusts (managed by regulated trustees/fiduciary)[174].

399. Generally, it is acknowledged that these arrangements can have very complex structures, as they usually do not have (legal) owners, but parties with different roles, rights and obligations[175]. From a geographical point of view, beneficial ownership structure is diverse and quite stable since end 2021, observation period, even if the share of Luxembourg residents has decreased by 5%[176]. As of end 2024, Luxembourg residents represent approximatively 25% of registered BOs (30% as of end 2021) and residents in other EU countries represent 42% (41% as of end 2021). With respect to resident in non-EU countries (33% as of end 2024, 38% as of end 2021), nearly 10% are UK residents (7% as of end 2021), almost 5% are residents in Switzerland (same percentage as of end 2021) and 18% in other non-EU countries (17% as of end 2021). As explained in detail in section 8.2.1., BO registrations for persons residing in TJs represent 6% of total number of BOs registered in the RFT. Nevertheless, there were no BO resident in a high-risk jurisdiction subject to a call for action by FATF[177].

10.6. Non-profit organisations

AT A GLANCE

FATF definition of NPO:

As explained in the interpretative note to recommendation 8, the FATF has adopted a functional definition of an NPO, which refers "to a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works"."

[173] AED.
[174] AED.
[175] OECD – IDB, A beneficial Ownership Implementation Toolkit, 2019, page 12.
[176] Data from the RFT as of end 2023 and end 2024.
[177] FATF, High-Risk Jurisdictions subject to a Call for Action–25 October 2024, link.

Pursuant to the FATF's interpretive note to Recommendation 8, these NPOs are particularly at risk of terrorist financing abuse.

Identification of the NPO FATF subset:

As explained in section 8.2.3, in Luxembourg, legal persons in the non-profit sector may take the form of ASBLs or *Fondations.* Luxembourg identifies those ASBLs and *Fondations* falling under FATF definition in a regular basis. As of end 2024, the NPO FATF-subset is considered to count around 1 000 ASBLs and *Fondations* (i.e. approximately 10% of all ASBLs and *Fondations* registered in the RCS).

SNRA:

For NPOs collecting or transferring funds the estimated level of TF risk is considered as significant (High), although it is considered to be less significant for NPOs receiving institutional funding (Low).

TF risk levels of Luxembourg NPO FATF subset sub-categories are provided below. Main risk drivers are, for all sub-categories, the type of activities provided (collecting and distributing funds) and geography, for those sub-categories providing these categories abroad, potentially in conflict zones.

Sub-sector[178]	**Sub-categories of FATF NPO**[179]	**2026 NRA: Inherent risk**
NPOs (as per FATF definition) carrying out primarily international activities – ASBLs and *Fondations*	ASBLs without UP status or without the DNGO accreditation carrying out primarily international activities	High
	ASBLs and *Fondations* with the DNGO accreditation carrying out primarily international activities	High
NPOs (as per FATF definition) carrying out international and local activities – ASBLs and *Fondations*	ASBLs without UP status or without the DNGO accreditation carrying out international and local activities	Medium
	ASBLs with the UP status and *Fondations* carrying out international and local activities	Medium
NPOs (as per FATF definition) carrying out primarily local activities – ASBLs and *Fondations*	ASBLs without the UP status carrying out primarily local activities	Low
	ASBLs with the UP status and *Fondations* carrying out primarily local activities	Low

400. For the years 2022–2024, the AML/CFT Directorate of the MoJ identified the sub-set of ASBLs and *Fondations* falling within the scope of FATF's NPO definition and classify the resulting subset into risk categories. The analysis was based on the review of the NPOs legal forms, additional statutes and accreditations and sector of activity and geographical scope as deferred from their statutory purpose or name of the entity.

401. In Luxembourg, a NPO may take the legal form of an ASBL or a *Fondation*. In addition, ASBLs may be granted with a public utility status *"utilité publique"* (ASBL UP) by the MoJ and both ASBLs and

[178] As per NRA taxonomy.
[179] As per the more granular risk classification following 2022, 2023 and 2024 Desk top analysis of NPOs by the MoJ.

fondations may be accredited as "non-governmental organisation for development" (DNGO) by the MoFA.

Table 15: Luxembourg non-profit associations by legal form and status

	Legal form	Additional status	Observations
Luxembourg non-profit associations (whole population)	ASBL	/	/
		UP	the UP status is granted by MoJ
		DNGO	the DNGO accreditation is granted by MoFA
	Fondation	/	the *Fondation* legal form is subject to MoJ approval

402. It should be noted that all DNGO were considered to fall within the FATF NPO subset. This status is granted by the MoFA to organisations active in the field of development cooperation and more particularly in the implementation of programmes and projects for the benefit of populations of developing countries. Once the DNGO status approved, specific approved projects are co-financed by the MoFA and donations to NPOs with DNGO status are tax deductible. Considering this, these NPOs are likely to engage in development and humanitarian aid abroad and are likely to collect (both from donors and from the MoFA) and disburse a substantial amount of funds to projects abroad. Following this, NPOs with DNGO status are considered within the FATF NPO subset and to have an international dimension.

403. Furthermore, the great majority ASBLs UP status are also considered to fall within the FATF NPO definition. ASBLs that engage in philanthropic, social, religious, scientific, cultural, artistic, educational, sporting or tourist activities in the general interest may apply to obtain the UP status. As for the DNGO status, they are likely to receive donations and distribute funds for such activities, as these are tax deductible.

404. Overall, it should be noted that, as for any legal person, the statutory purpose of the NPOs may be large to allow some flexibility to carry out any ancillary activity or to expand its geographical scope without modifying the articles of association. For instance, a purely local NPO providing education aid in Luxembourg may include in its statutory purpose that it may also conduct this activity abroad. Also, a local sports club (in principle not a FATF NPO) may indicate that it can also participate in charitable works in Luxembourg or abroad, and in such a case it would be considered a FATF NPO. The identified "FATF NPOs" are, therefore, to be considered as an estimate at the high end.

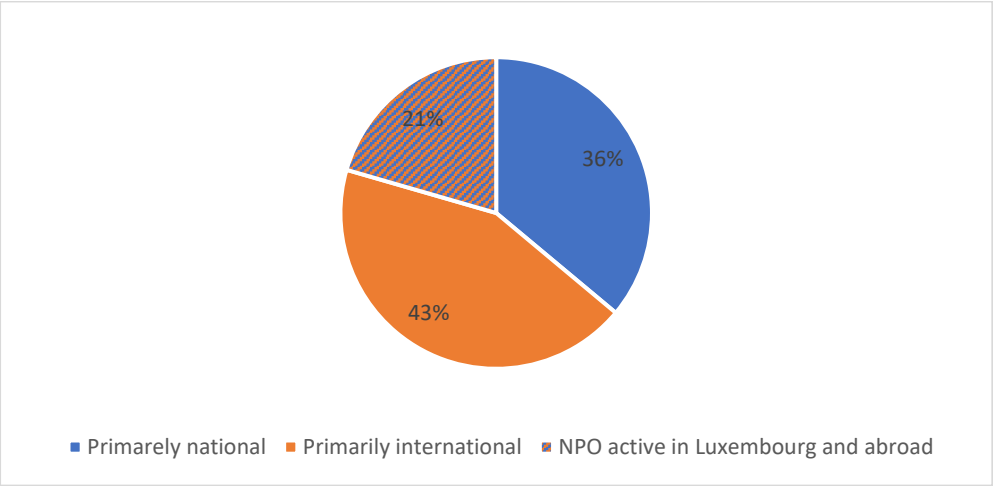
10.6.1. FATF NPO subset and legal form

405. During the observation period of this report, an average of around 9 000 ASBLs and *Fondations* were registered with the RCS. Among those, less than 11% were considered to fall within the FATF NPO sub-set. On average, this FATF NPO subset was composed for 87% of ASBLs and 13% of *Fondations*. From another perspective, around 10% of all ASBLs and 66% of all *Fondations* fell within the said subset.

10.6.2. Geographical activities analysis

406. The pie-chart below depicts the geographical scope of NPOs assessed as falling within the analysed subset. As the repartition remains stable throughout the observation period, the chart below reflects the situation in 2024.

Figure 18: Geographical scope of activities of the FATF NPO subset, 2024



407. From the graph above, it can be concluded that most Luxembourg NPOs are primarily engaged abroad (43%), followed by those having national activities (36%). Around 20% of NPOs within the FATF subset were identified having activities both in Luxembourg and abroad.

408. The orientation towards activities abroad may be explained by the inherent interest of NPOs to carry out projects in less developed countries, the country's relatively small population (approximately 672 000 in 2024), the international structure of Luxembourg's society and the limited territorial size of the Grand-Duchy itself. As about 47% of Luxembourg's residents are foreigners[180], some FATF NPO aim to fund project in their country of origin. Other residents may also have an interest to create NPOs that help newcomers to integrate and at the same time maintain their culture in Luxembourg.

409. Overall, most FATF NPOs are engaged in social work without accommodation (about 28% of NPOs falling within the sub-set). However, beyond this category, the activities of FATF NPOs differ depending on the geographical scope of activities (national vs. international). Indeed, development projects (including relief aid) are prevalent in FATF NPOs carrying activities abroad, whereas religious and NPOs related to culture, health, and social work with accommodation are more prevalent in FATF NPOs carrying activities in Luxembourg. To note that for 59 religious NPOs out of 104 in the FATF NPO subset (vs. 59% in 2023), the activities are rather related to or at least include the financing of the maintenance of buildings or organs in Luxembourg as their statutory purpose.

410. FATF NPOs with international activities potentially carry out their activities in Africa (and especially sub-Saharan Africa), South and South-East Asia and East Europe.

411. Overall, it appears that most FATF NPOs (in case where the statutory object allowed for identification) were active in countries that present strategic deficiencies in their AML/CFT regimes on

[180] STATEC, La démographie luxembourgeoise en chiffres – Edition 2024, link.

top of humanitarian needs and ecological threats (i.e. with most TJ identified being T1 and T2 countries). Indeed, the very nature and geographical scope of the activities of NPOs (carrying out development and humanitarian projects in developing countries) make them prone to maintain flows with such geographies. Thus, and as explained in section 8.2.2, for NPOs the link to TJs is not with regards to "ownership" (residence of BOs) but with regards to the geography where the activities of these NPOs are carried out, especially with regards to T1 and T2 countries, making NPOs active internationally more vulnerable with regards to criteria "geography/flows with weak CFT geographies".

412. Globally, FATF and the Egmont Group signalled that legitimate NPOs that operate in foreign jurisdictions (especially in high-risk environments) are at risk of having their funds or goods abused at the point of distribution by the partner organisation or the charity.

413. Overall, the FATF acknowledges that NPOs operating in high-risk jurisdictions tend to be most exposed to TF risks when they are subject to minimal or no oversight since very little is known about their operations and might be less aware of potential TF risks. In addition to that, NPOs operating in high-risk areas can also face higher exposure when there are only a few (or no) regulated financial services to conduct their operations and must, therefore, rely on informal financial channels which come often at the cost of no due diligence processes and lesser traceability.

414. As noted throughout the report and as already highlighted in the 2022 TF VRA, organisations linked to terrorists or terrorist groups have been known to create false appeals to raise money (sham organizations). In most cases, donations are made by the public in the belief that the money will be used to fund genuine charitable activities. However, occasionally the donors are aware of the true destination of the funds and use the humanitarian cover to avoid raising suspicion. The use of crowdfunding, P2P payments and crowdfunding and other online payment platforms have gained in significance. The TF stage likely to take place in Luxembourg with regards to domestic NPOs is raising TF funds (Luxembourg residents' donations to NPOs carrying out development humanitarian projects abroad) for third countries. No such cases have yet been identified by the CRF for Luxembourg NPOs, but the vulnerability exist.

415. There may also be a heightened TF risk associated with religious NPOs, particularly those operating within populations that terrorist entities actively target.

11. Cross sector vulnerabilities

416. The following means are likely to be exploited by terrorist organisations and actors with the potential to cause harm by raising, moving, storing, or using funds or other assets for terrorist purposes. Such means can also be used in combination with each other or with other more traditional means, or simultaneously by terrorists, violent extremists, or TF sponsors. Cash, crypto-assets, crowdfunding and underground banking will be further analysed below.

11.1. Cash

417. It is observed that cash remains a prevailing modus operandi among terrorist organisations and actors. Indeed, cash is anonymous, universally accepted and difficult to trace. In particular:

- It can be easily transported cross-borders by travellers, especially in porous jurisdictions where borders are not subject to controls when entering or exiting or where controls are weak;
- Terrorist actors might also transport cash below the EUR 10 000 threshold per person in Europe to avoid the obligation for declaration;
- It is observed that terrorist organisations or actors exploit legitimate or informal cash-intensive businesses, such as retail shops, grocery stores, markets, filling stations, transport and trading companies. They use the revenue generated to finance their activities;
- Proceeds of illicit activities used for TF purposes can be in the form of cash. For example, in kidnapping cases, the ransoms are generally required in cash; in extortion activities, fees are also being required in cash; in corruption, cash is prevailing[181];
- Cash is often used to purchase prepaid cards which are also an anonymous payment instrument which can be easily transported or given freely to anyone for subsequent use, including for the purchase of goods and services;
- Cash is the dominant means used in informal payment systems (HOSSP).

11.2. Crypto-assets

418. It is globally observed that terrorist organisations and actors use crypto-assets, especially to raise funds. Based on their analysis of onchain flows, "TRM Labs" has notably identified that terrorist organisations and their supporters demonstrate more sophistication in their use of crypto-assets[182]. Transactions in crypto-assets are indeed anonymous/pseudo-anonymous, instant and irreversible. The main typologies identified are the following:

- Terrorist groups have used social media platforms to publicly share their crypto wallet addresses (often self-hosted wallet) and provide instructions on how to make donations. Also, messaging systems have recently been used to call for donations;
- Crypto-assets are used as a means of payment to pay for goods and services on the Darknet including material that can be used for TF purposes;

[181] Sourced from FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025, link, §123, 125 and 130.
[182] TRM Labs | Agents and intelligence to fight crime.

- Crypto-assets may also be withdrawn in cash from crypto-ATMs or exchanged to fiat currency mainly *via* unlicensed exchanges and subsequently be withdrawn. The received funds are then used to support terrorist activities;
- Criminals use privacy coins such as Dash and Monero to ensure anonymity, and they often use self-hosted wallets for direct funding or fundraising purposes. In addition, the use of "mixers" (e.g. software that obscure the history and origin of crypto-assets through them) in the chain of the transactions) increases the difficulty to trace crypto-assets transactions. As regards the crypto-assets used, a shift is noted with an increasing use of stablecoins (notably USDT).

419. Authorities indicate that there is a growing use of crypto-assets (including stablecoins), although it remains limited.

11.3. Crowdfunding

420. The 2022 SNRA states that "the assessment of the terrorist financing vulnerability related to crowdfunding shows that the sector cannot be assessed in isolation", citing notably the multitude of possible crowdfunding models (e.g. investment-based, loan-based or donation- based), the fact that certain crowdfunding models and intermediaries are unregulated due to the applicable European legal framework being heterogenous, the cross-border nature of transactions, and the potential use of virtual assets.

421. Unregulated donation-based crowdfunding platforms present a higher inherent risk of misuse for terrorist financing purposes as these platforms are currently outside the scope of financial institutions and of prudential and anti-money laundering supervisors[183], pending the entry into force of the AMLR on 10 July 2027. Furthermore, in Luxembourg, no entity has been granted a license under Regulation (EU) 2020/1503 on European Crowdfunding Service Providers for business yet[184].

11.4. Underground banking and HOSSP

422. Unregulated banking systems, mainly Hawala and other similar service providers (HOSSPs), facilitate terrorist actors to move funds around the world under the supervisory radar. Underground banking and HOSSPs[185] are non-formal financial systems, which are used to transfer money through a

[183] European Commission, *SNRA*, 2022, link.

[184] Regulation (EU) 2020/1503 applies to the provision of investment and lending-based crowdfunding services. It does not apply to other crowdfunding models, such as donation- or reward-based crowdfunding platforms. Furthermore, the regulation only applies to crowdfunding services provided to non-consumer project owners and to offers which do not exceed EUR 5 million calculated over a period of twelve months.

[185] According to the FATF General Glossary definition, Hawala and other similar service providers are considered a subset of MVTS. Their classification varies across jurisdictions, depending on the legal framework. They may operate as licensed/registered entities or as an unregulated or even illegal remittance mechanisms. Although the term "Hawala" is commonly used in several countries, it is not universally recognised. Therefore, for the purpose of this report, the term "Hawala and Other Similar Service Providers (HOSSP)" will be used. HOSSPs are characterised by the services they offer rather than their regulatory status. What distinguishes them from other money transmitters is their reliance on non-bank settlement methods, including settlement via trade and cash, as well as prolonged settlement period. See: FATF, The Role of Hawala and Other Similar Service Providers in ML/TF (2013), page 9.

network of mediators ("hawaladars") and are widespread in the Middle East, several regions of Africa and South Asia[186].

423. Transactions carried out *via* underground banking systems or HOSSP constitute an increasing challenge, due to the lack of traceability of these money flows.

[186] Sourced from FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025, link, §141.

12. Emerging risks

424. Emerging risks in Luxembourg are shaped largely by the country's highly internationalised financial ecosystem, its strong reliance on digital payment infrastructures, and the growing sophistication of terrorist actors in exploiting both traditional and innovative financial channels. While the overall level of terrorist activity within the country remains low, the exposure arises mainly from misuse of financial services and cross-border payment chains, rather than from domestic threats.

425. A first major area of emerging risk relates to the continued relevance of cash and its convergence with digital financial services. Despite technological advances, cash remains a dominant modus operandi for terrorist actors due to its anonymity, ease of transport, and global acceptability. In Luxembourg, this risk is amplified by the ability to inject cash into the formal financial sector and subsequently move funds cross-border. Key vulnerabilities include:

- Use of cash deposits followed by ATM withdrawals in other jurisdictions.
- Cash couriers transporting amounts below declaration thresholds to avoid detection.
- Exploitation of cash-intensive legitimate businesses (e.g. retail, transport, trading companies).
- Purchase of prepaid cards with cash, allowing anonymous onward use (although in Luxembourg, as seen in section 10.1.1, no retail and business bank, nor entity operating online, offer anonymous prepaid cards or products and services linked to anonymous prepaid cards.
- Reliance on cash in informal value transfer systems (although indicators and intelligence suggest that such systems currently could be present or operate within and through Luxembourg to a limited extent).

426. A second and increasingly important emerging risk concerns digital fundraising and financial innovation, particularly crypto-assets, crowdfunding, and innovative payment instruments. Terrorist actors are showing increasing sophistication in combining these tools, often leveraging social media platforms. While still limited in scale, the use of virtual assets is growing and presents challenges due to speed, anonymity, and complexity. Notable risk vectors include:

- Use of crypto-assets (including stablecoins and privacy coins) for donations, payments, and ransomware-related TF.
- Exploitation of donation-based crowdfunding campaigns often framed as humanitarian or charitable causes.
- Use of virtual IBANs (vIBANs), which can obscure the final beneficiary through long intermediary chains.
- Instant payments, which increase the speed of fund availability and reduce intervention windows, despite existing safeguards.

427. Finally, complex financial and trade-related services, alongside broader cyber-enabled criminal activity, represent a medium but evolving risk. Trade finance services, while limited in scale in Luxembourg, remain vulnerable due to documentation complexity, multiple intermediaries, and exposure to high-risk corridors. In parallel, authorities highlight the growing convergence between cyber-enabled fraud, organised crime, and terrorist financing. Emerging trends include:

- Over- or under-invoicing, forged trade documents, and use of shell companies in trade finance.
- Increasing detection of TF-linked transactions involving crypto-assets and cash couriers.

- AI-enabled cyber fraud schemes operated by transnational criminal networks, whose illicit proceeds may be redirected to terrorist causes.

428. Overall, emerging TF risks in Luxembourg are less about new products or activities and more about the evolving misuse of existing financial infrastructures, requiring enhanced coordination, cross-sectoral awareness, and continued adaptation of supervisory and investigative tools.

13. Mitigating factors analysis

429. Luxembourg's AML/CFT framework relies on five pillars, namely i) national strategy and coordination, ii) prevention and supervision, iii) detection, iv) prosecution, investigation and asset recovery, and v) international cooperation. The following sections develop the specific mitigating measures developed by Luxembourg to combat TF. These measures mitigate the inherent risk detailed in the previous sections and result in the residual risk levels provided in section 14.

13.1. National strategy and coordination

430. The Inter-ministerial Steering Committee for the Fight against Money Laundering and Terrorist Financing (ISC)[187] sets the high-level national policy and draws up a multi-annual AML/CFT strategy that sets out the main guidelines for combating ML/TF and defines high-level strategic objectives. The multi-annual AML/CFT strategy is presented to the Government Council for validation, showing a political commitment to combat ML and TF at the highest level. The ISC elaborated the 2025-2026 AML/CFT strategy. It was adopted by the Government Council in February 2025 and consisted of four strategic priorities in AML/CFT.

i. Promote effective understanding and communication of ML/TF risks and further develop information sharing between the public and private sectors, including operational information
ii. Optimize AML/CFT supervision by reforming its architecture through the creation of a new public authority and harmonize supervisory practices through an integrated approach.
iii. Improve the operational effectiveness of investigative and prosecuting authorities, as well as asset management and recovery, in particular by leveraging technological innovation in the criminal justice chain and strengthening the effectiveness of procedures
iv. Strengthen the role of registry managers and pool technological tools, continue efforts to ensure the transparency of legal persons and identify abuses of PM/CJ

431. The National prevention committee (NPC) is chaired by the national AML/CFT coordinator and is composed of operational members, such as representatives of the supervisory authorities (CSSF, CAA and AED), SRBs (OAL, OAD, CdN, CdH, IRE and OEC), the CRF, the investigation and prosecution authorities and of the private sector. The high-level strategic objectives of the AML/CFT strategy are implemented by these operational actors in different working groups in accordance with their respective competences and areas of expertise. The NPC also allows the gathering of institutional players on the one hand and representatives of the private sector on the other around a multidisciplinary round table.

432. The Executive Secretariat of the NPC and the ISC supports these two Committees in coordinating the implementation of the AML/CFT national strategy. The national AML/CFT coordinator reports to the Government on the progress made in implementing the national AML/CFT strategy.

[187] The ISC is chaired by the national AML/CFT coordinator and gathers representatives of the MoJ, MoF, MoE, the Ministry of Internal Security and the MoFA.

13.2. Prevention and supervision

433. This section provides a high-level view of specific CFT preventive and supervision measures and initiatives.

13.2.1. CSSF

434. As supervisor, the CSSF plays an important TF preventative role with regards to the financial sector. Its preventative role is twofold: first, performed at market entry, and then, during its daily supervision.

13.2.1.1. Market entry controls

435. The CSSF applies strict market entry controls to prevent criminals and their associates from accessing financial sector professionals under its AML/CFT supervision and to ensure that all relevant licensed or registered professionals meet common sets of minimum standards at market entry and continue to do so on an ongoing basis. These requirements are defined in various sectoral laws and in article 2 (4) of the 1998 CSSF Law[188].

436. As part of the licensing/authorization or registration process, the CSSF conducts Fit and Proper assessments on BOs, shareholders and persons of the management bodies (supervisory and day-to-day management) or key function holders where relevant. Those assessments are completed both when granting a licence/authorization/registration and at any subsequent change in those positions.

437. In addition, a specific CFT-related measure taken by the CSSF is the daily screening of above-mentioned persons against lists including UN, EU, and other terrorist lists.

438. The CSSF also cooperates with different national authorities for that purpose, e.g. CSSF reaches out on a risk-based approach with other relevant authorities to ensure there is no adverse information on the persons subject to the Properness assessment. The CSSF might also contact international authorities, where applicable.

439. Moreover, the CSSF assesses the envisaged activity and the purpose of establishing a business in Luxembourg in order to detect whether the professional could be used or abused for terrorist financing activities.

13.2.1.2. Supervision

440. The CSSF uses a wide range of supervisory activities to verify compliance by the professionals under its supervision with AML/CFT obligations, including those obligations related to targeted financial sanctions (including CFT-related targeted financial sanctions) and to countermeasures against certain jurisdictions called for action by the FATF.

[188] The CSSF also ensures that natural or legal persons known to have direct or indirect ties other than strictly professional with organised crime do not take direct or indirect control of natural or legal persons under its supervision, whether as BOs, by acquiring a significant or controlling interest, by holding a management function or otherwise. As part of this role, the CSSF assesses whether directors and senior management personnel are fit and proper, which includes an assessment of their expertise and integrity.

441. In the context of counter-terrorist financing, the following measures are highlighted, they need to be read together with actions taken by CSSF's internal CFT Task Force as detailed further below:

Annual Survey on Financial Crime

- The CSSF uses i.a. the annual AML/CFT questionnaire to monitor the effectiveness of supervised professionals' mitigating measures. During the observation period of the NRA (i.e. 2021-2024), over 1 500 professionals completed the questionnaire annually. The mandatory completion of the questionnaire is enforced by the CSSF.
- The annual AML/CFT questionnaire is composed of two parts, one pertaining to inherent risk and a second to mitigating measures. It includes, for example, specific questions on the type of clients (including legal arrangements), country risk, PEPs and TF-related questions, both general and sector-specific. In particular, it constitutes a tool allowing the CSSF to identify whether the professionals have assessed their exposure to TF.

Regular exchanges with professionals including TF topic

- CSSF off-site supervisory teams hold on a regular basis bilateral meetings with professionals including those having a higher ML/TF residual risk. They meet their Chief Compliance Officers and include TF risk on the agenda. Also, TF topic can be discussed by the CSSF with several professionals from the same sector at the same time, in order to have insights on how the TF risk is assessed and mitigated.

Analysis of professionals' annual ML/TF risk assessment

- As part of their off-site supervisory measures, CSSF off-site teams review the annual ML/TF risk assessment completed by professionals e.g. to identify possible shortcomings related to TF.

Follow-up on country risk information

- The CSSF follows up with professionals that would have incorrectly classified countries to ensure remediation[189].
- Based on the CSSF's on-site inspections, compliance with obligations in relation to high-risk countries including countries with a higher TF risk exposure is broadly consistent across the different professionals under the CSSF's supervision.
- In recent years, there have been few notable compliance failures relating to enhanced due diligence process for clients from high-risk countries including countries with a higher TF risk exposure. In these cases, the CSSF acted quickly to ensure that the identified deficiencies were remediated.

On-site control plan, TF specificities

- TF is covered in the on-site control plan in the following testing phases:
    - Review of procedures: An assessment of the professional's procedures is performed to ensure that procedures in place cover TF risks. The procedures are required to mention the obligation to detect persons, entities or groups involved in a transaction

[189] CSSF internal data (responses to AML/CFT questionnaire), 2025. The CSSF has a country risk rating tool in place to challenge classifications by professionals.

or business relationship subject to prohibitions or restrictive measures in financial matters in the context of the fight against TF (including, notably, EU and ministerial regulations lists) and the obligation to inform the competent authorities as soon as possible.

- Management Interview: A kick-off meeting with the professional's AML/CFT (Chief) Compliance Officer and/or the member of management in charge of AML/CFT (where applicable) provides a first overview on how TF risks have been considered by the professional in its control framework.
- Risk Assessment and Risk Appetite: The risk self-assessment, which is linked to the risk appetite and risk strategy, approved by the management and by the Board of Directors of the entity, assesses the risks of TF it faces and describes the controls in place to mitigate those risks. The entity is expected to have considered, inter alia, the SNRA, the NRA and the relevant sub-sector specific risk assessments which are published on the CSSF website.
- Review of a sample of client files: For a sample of client files, a know your customer (KYC) review is performed in order to verify whether the professional has correctly identified and verified the identity of its client, obtained information on the nature and purpose of the business relationship, on the origin of the funds and the types of transactions for which the business relationship is solicited so that it has a sound knowledge of its client and the transactions envisaged (detailed information value). An analysis of movements that occurred on the account within a selected period is also performed to ensure those movements do not give rise to suspicions of TF.

13.2.1.3. Remediation and enforcement

442. The CSSF has all the supervisory and investigatory powers needed, as provided for in the 2004 AML/CFT Law, the 2020 Sanctions Implementation Law and in various sectorial laws, for the purpose of carrying out its duties.

443. The CSSF identifies deficiencies, assesses their nature and severity, and chooses appropriate supervisory activities or measures. First, the CSSF identifies deficiencies through on-site and off-site supervision. The CSSF then groups identified deficiencies within defined AML/CFT themes (e.g. governance, customer due diligence, etc.) and assesses their severity. Based on the assessment of the nature and severity of identified deficiencies, the CSSF selects the appropriate supervisory activities (meetings or calls with senior managers or directors, requests for the CSSF on-site inspections, requests for on-site inspections by external auditors) or supervisory measures. Supervisory measures can have different forms and include observation letters, injunction letters and enforcement measures (warnings, reprimands, administrative fines, temporary bans, withdrawals or suspensions of authorisation and public statements).

444. Nonetheless, on several occasions, the CSSF has identified general breaches in relation to requirements on transaction monitoring, enhanced due diligence measures and "name matching" controls, which ultimately may include a TFS-related component. These deficiencies have been sanctioned or, if of minor importance, administrative measures have been issued, requiring for adequate remediation by the professional.

13.2.1.4. Regulation and information

445. The CSSF-supervised professionals play an important role in preventing access by terrorist actors to the financial sector and its activities and are required to assess TF risks (including circumvention risks) they are exposed to, prevent TF to materialise, to identify potential TF attempts or commitment and to report these cases to the CRF. If links to TFS lists are identified, professionals must immediately freeze the funds and report to the MoF with the CSSF in copy.

446. The 2012 CSSF Regulation, *inter alia*, specifies applicable TFS requirements, notably by introducing screening on the investment side and provide requirements related to the controls put in place for the purpose of TFS[190].

447. The CSSF has taken measures to promote a clear understanding of ML/TF risks and AML/CFT obligations among professionals under its supervision through: (1) publication of AML/CFT guidance; (2) organisation and participation in industry events; (3) direct collaboration with the private sector; (4) risk assessments; (5) feedback as part of supervisory activities; and (6) broader communications. Specific initiatives that should be noted in the context of CFT include:

- Publication on a regular basis of the latest FATF statements concerning high-risk jurisdictions for which enhanced vigilance measures and, where appropriate, countermeasures are required and jurisdictions under increased monitoring of the FATF
- Publication of expectations in annual activity report. The CSSF has also established dedicated pages on its website (International financial sanctions) with all relevant details (regulations, guidance, forms, FAQs, etc.) on TF and TFS;
- AML/CFT Conferences organised by the CSSF or contribution to conferences organised by other authorities. In November 2024 a specific Preventing TF Seminar took place (see Insight Box 10)[191];
- Exchange with the MoF and reception of information from professionals under the supervision of the CSSF regarding the freezing measures taken by them pursuant to the TFS regimes.
- Exchanges with the private sector during AML/CFT Expert Working Groups (Banking sector, Collective investment sector, and Specialised PFS);
- Discussion of CFT risks and challenges during bilateral meetings with AML/CFT Compliance Officers, where relevant;
- Involvement of professionals in risk assessments: the CSSF has published three sub-sector risk assessments, and four updates of those including dedicated sections on TF risks[192] to which professionals or representative associations have participated; they also participated to the NRA and topical VRAs.

[190] See for example articles 33, 34 (2), 38 and 39 (1a), link.
[191] Looking back on the Preventing Terrorism Financing Seminar by the CSSF and the CRF, in association with the ABBL and ALFI, of 8 November 2024 – CSSF.
[192] See dedicated section « Risk assessment » under "Documentation" of the page Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) – CSSF.

Insight Box 10: Seminar dedicated to Preventing Terrorism Financing in November 2024

The CSSF, the CRF, the ABBL and the ALFI organised a seminar dedicated to Preventing Terrorism Financing in November 2024[193] to assist the private sector to better understand terrorist threats and TF risks in Luxembourg. The conference was opened to all financial sector professionals.

Subsequently, the CSSF off-site supervision Banking department included information on the exposure to TF during the annual joint conference with the ABBL held on 24 April 2025.

During both conferences, the message that the patterns of TF are specific and that, consequently, it is highly recommended to assess the TF risk separately form ML risk, has been shared with the attending Banks. The CSSF also recommends that the Banks document their analysis in a separate section of their business wide risk assessment considering the principle of proportionality.

Based on the latest information collected through the annual Survey on Financial Crime, the CSSF has noted good progresses. All entities confirmed they have assessed TF risks: 11% have performed a dedicated risk assessment and 43% have documented their analysis in a separate section. Among the 46% that have assessed/documented the TF risk exposure jointly with ML risk exposure, 43% have a low exposure to TF risk and 85% belongs to a sub-sector assessed to have a lower risk exposure according to the 2022 VRA TF.

13.2.1.5. Internal Task Force "Counter-Terrorism Financing"

448. In 2023, the CSSF decided with the support of its AML/CFT Steering Committee, to set up a task force dedicated to the subject of Counter-Terrorism Financing (the "CTF Task Force") reporting to its AML/CFT Working Group. The Task Force is composed of representatives of AML/CFT off-site departments, on-site inspection departments and of the Financial Crime Prevention department. In line with the 2025-2026 National AML/CFT Strategy and the findings of Luxembourg's 4th Round FATF Mutual Evaluation Report, its objective is to strengthen the CSSF's and the private sector's understanding and awareness of TF risks in order to ultimately mitigate them more efficiently.

449. A roadmap has been established by the CTF Task Force detailing an action plan, actions which are monitored and checked for progress at least on a quarterly basis by the members of the Task Force. Ongoing progress is also reported to the CSSF AML/CFT Steering Committee. The roadmap has been built around the pillars of the CSSF AML/CFT strategy and includes, among others, the following CFT actions:

(1) Understanding of risks: definition of Key Risk Indicators enabling to follow up on the TF risk exposure of the sectors under the supervision of the CSSF, and completion of deep-dive TF risk analyses for sectors with the highest inherent TF risk exposure according to the 2022 TF VRA (notably the banks and the payment and e-money institutions).
(2) Regulation and information (including awareness): a dedicated section on TF risk has been included in the latest ML/TF sub-sector risk assessments published by the CSSF on private banking (2023), collective investment sector (2025) and Specialised PFS providing corporate services (2026). TF-related guidance was also shared for example through publications in CSSF's Newsletter, or i.a. during the annual sectorial AML/CFT conferences organised by the CSSF, the Public-Private Partnerships, and the 2024 CFT-dedicated conference.

[193] Preventing Terrorism Financing Seminar, 8 November 2024, link

(3) Supervision: TF thematic reviews were completed, where deemed necessary. For example, a sample of Specialised PFS providing corporate services[194] were reviewed regarding (i) the assessment of TF risks, (ii) a sample testing of beneficial owners of clients residing in higher risk jurisdictions, and (iii) an analysis of TF risk exposure of clients having NPOs within their shareholder structures. Also, additional questions dedicated to TF risks were incorporated in the annual Financial Crime Survey and addressed to all professionals falling under the AML/CFT supervision of the CSSF.

(4) National/international exchanges: bilateral exchanges on best practices regarding TF risk assessment and supervisory approaches with other jurisdictions and the Luxembourg CRF. Also, relevant contributions have been completed to the vertical and national risk assessments on this topic.

(5) Training: attendance end of 2025 to a TF training held by the CRF for CSSF agents only and set up of TF-related training sessions dedicated to CSSF agents.

450. The CTF Task Force maintains its efforts to follow-up on the exposure of the financial sector entities under the supervision of the CSSF, to identify and understand the evolving TF-related typologies and contribute to the national efforts in terms of awareness.

13.2.2. Other supervisory authorities and SRBs

451. For the other supervisory authorities (CAA, AED) and SRBs (CdN, CdH, OEC, OAL/OAD, IRE), AML/CFT mitigation rests on layered licensing and fit-and-proper regimes, mandatory annual or biennial AML/CFT questionnaires driving risk-based supervision, mandatory continuing training and active outreach, maturing private-sector controls, credible onsite/offsite inspection programmes backed by disciplinary referrals and material administrative fines, and goAML reporting underpinned by close cooperation between authorities.

Insight Box 11: Mitigating factors overview

- **CAA supervised sectors:** Mitigation measures are very similar to those of the CSSF, notably with regard to Market entry controls, AML/CFT Questionnaire, on-site control plan, TF specificities, remediation and enforcement, as well as with regard to regulation and information. Mitigation rests on rigorous fit-and-proper testing, daily database screening, an annually updated risk matrix, intensive sector outreach (including dedicated TF awareness sessions) and active risk-based supervision. Supervised sectors are mature; ongoing focus is on TF-specific risk assessment, transaction monitoring and intermediary outreach.
- **AED supervised sectors:** Mitigation rests on sustained outreach (newsletters, conferences with professionals), an active onsite/offsite inspection programme, and a robust enforcement record.
- **OAL/OAD supervised sectors:** Mitigation combines a strict access regime, annual screening of all lawyers, mandatory annual AML/CFT questionnaires and active risk-based supervision and disciplinary follow-up.

[194] Refer to pages 23 to 35 of the following presentation: Looking back on the 2026 CSSF AML/CFT Conference for Specialised PFS – CSSF.

- **IRE supervised sectors**: Mitigation combines demanding market-entry requirements, mandatory continuing AML/CFT training, regularly updated IRE professional standards, annual risk-based questionnaires, an active onsite programme, and disciplinary follow-up.
- **OEC supervised sectors:** Mitigation rests on double market-entry controls (general business permit obtained by the MoE plus OEC approval), professionalised onsite controls by dedicated staff, sustained training and outreach.
- **CdN supervised sectors:** Mitigation rests on demanding market-entry controls, annual AML/CFT questionnaires and active supervision.
- **CdH supervised sectors:** Mitigating combines a strict access regime and annual coverage of professionals through an AML/CFT questionnaire.

13.2.3. Oversight of NPOs

452. Luxembourg NPOs rely on preventive measures put in place by the service providers they use, for example, on transaction monitoring systems put in place by banks when performing bank wire transfers. Some Luxembourg NPOs engaged in development and humanitarian projects abroad have implemented specific CFT controls, for example, name screening systems such as WorldCheck, to evaluate risk levels of their partners and beneficiaries of funds, but this applies to a small share of entities.

453. Furthermore, Luxembourg NPOs carrying out development and humanitarian projects abroad may apply to obtain DNGO status from the MoFA in order to receive subsidies to fund or co-fund their projects and programmes abroad. Given that the MoFA subsidises DNGOs, it performs checks on these organisations and their projects to ensure the appropriate use of government funds. Through their TF risk assessment methodology, the MoFA conducts TF risk assessments on accredited DNGOs on an annual basis. This TF risk assessment is carried out in the first stage using information obtained through an off-site monitoring tool, via a yearly questionnaire. The analysis is complemented by information gathered from annual reports, audits, evaluations, field visits by the MoFA or external bodies, and other sources. This oversight has a positive impact on reducing the TF exposure of these NPOs. The results of the assessment serve as a tool for the MoFA to determine a strategy or plan to monitor the DNGOs to prevent their potential abuse for TF purposes. In addition, when necessary, the MoFA may decide to implement targeted mitigation measures to reduce or manage TF risks. Furthermore, the MoFA continuously works to improve the DNGOs understanding of TF risk through training sessions, information sessions, and the general conditions document, which describes the risk-based approach applied to their oversight.

454. ASBLs with the UP status and *Fondations* benefit from additional oversight. *Fondations* must undergo a stringent creation process. They must be established by notarial deed and undergo a licensing procedure involving, among other things, the submission of a three-year activity plan and budget, a review of their statutes, and fit and proper assessments of founders and board members. The final approval for the creation of a foundation is granted by Grand-Ducal decree. Following their establishment, fit and proper assessments of board members must be renewed at least every five years. ASBLs may apply for public utility status once they meet the conditions laid down by law. These conditions are broadly similar to those applicable to *Fondations*. However, while *Fondations* must demonstrate their public benefit purpose *ex ante* as part of the creation process, ASBLs seeking public utility status must demonstrate *ex post* that they pursue a public interest objective through their activities.

455. More generally, all ASBLs and *Fondations* are required to file their annual accounts with the RCS. Public utility ASBLs and *Fondations* are, however, subject to additional reporting and oversight requirements. They must have their annual accounts audited by an approved statutory auditor, and the auditor's report must be filed and published together with the annual accounts in the RCS. Once established or recognised as being of public interest, both *Fondations* and ASBLs with public utility status are subject to ongoing supervision by the MoJ. In particular, amendments to their articles of association are subject to review by the MoJ.

456. In addition, all NPOs are subject to a supervisory mechanism under which donations and testamentary gifts exceeding the legal threshold require prior authorisation from the MoJ.

13.3. Detection by the CRF

457. The *Cellule de renseignement financier* (CRF) is the national authority responsible for receiving and analysing suspicious transactions and activity reports (STR/SAR) and other information on events that could involve ML, associated predicate offences or TF. The CRF is an independent agency headed by magistrates who operate independently and autonomously[195].

458. In particular, it receives and analyses:

- Suspicious transaction and activity reports transmitted by a professional subject to the AML/CFT legislation as provided by article 5, paragraph 1, a) of the 2004 AML/CFT Law; and
- Information communicated by other AML/CFT competent authorities pursuant to article 74-2 (4) of the amended law of 7 March 1980 on the judiciary organisation.

459. The CRF disseminates, spontaneously and upon request, the results of its analysis and any other relevant information when there are reasonable grounds to suspect ML, associated predicate offences or terrorist financing, to the national judicial authorities, to the national AML/CFT competent authorities, as well as to its foreign counterparts.

460. The CRF cooperates with its foreign counterparts in accordance with the principles developed by the Egmont Group and, for cooperation at the European level, in accordance with the requirements of the Fourth Directive (Directive EU 2015/849 of the European Parliament and of the Council of 20 May 2015).

461. The CRF's analytical function is twofold:

- The operational analysis which focuses on individual cases and specific targets or on appropriately selected information, depending on the type and volume of information received and the expected use of the information after their dissemination; and
- The strategic analysis which focuses on identifying ML/TF related typologies, trends and patterns based on the exploitation of data in order to gain an in-depth understanding of the ML/TF risks, threats and vulnerabilities faced by Luxembourg and secondly to share the strategic intelligence gathered with relevant parties at national and international level.

462. With the amendment of the Law of 16 July 2016 on the organisation of controls on the cross-border transportation of cash (2021 Cash Control Law), magistrates of the CRF have the power to

[195] Note that the CRF is under the administrative authority of the General State Prosecutor's Office.

freeze funds upon suspicion (for instance, following receipt of a suspicious transaction report (STR) or following cooperation with other FIUs) for an unlimited period of time. The CRF has also direct and indirect access to a wide range of databases and have significant IT capabilities (including a secure channel for STR filing and various analytical tools).

463. As per the 2004 AML/CFT Law, all professionals, their directors and employees have the obligation to report suspicious transactions and activities, including attempted suspicious transactions, regardless of the amount of the transaction, to the CRF[196].

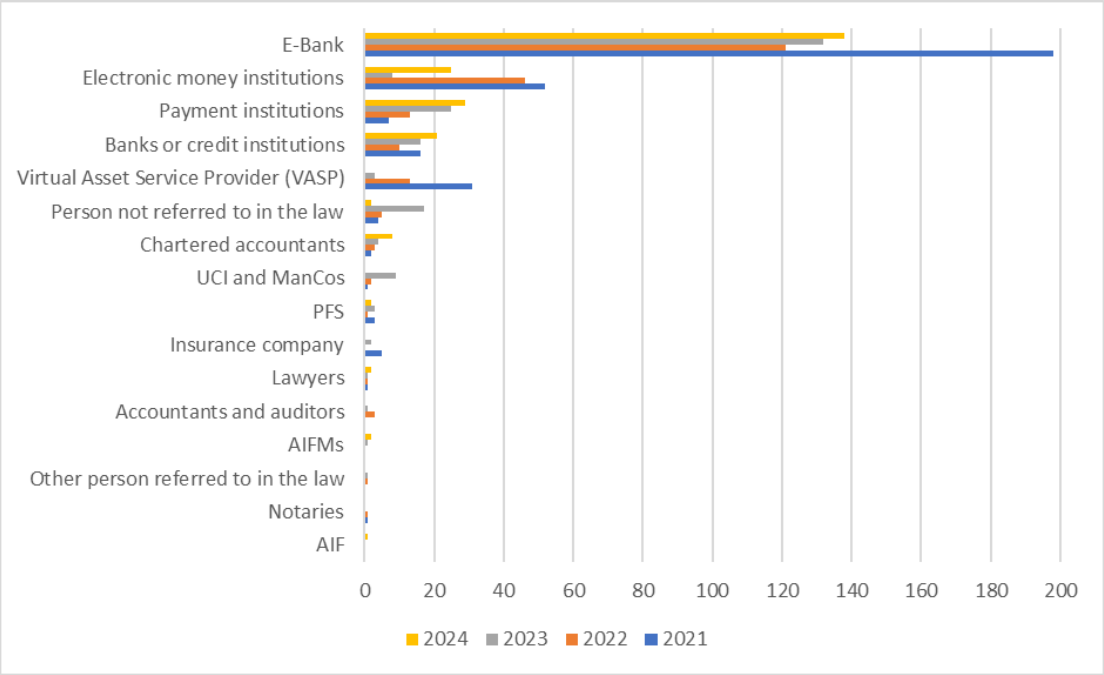
13.3.1. Analysis of suspicion reports

464. Professionals subject to the 2004 AML/CFT Law report suspicions of TF to the CRF. Two specific report formats are available, depending on whether suspicions are related to specific transactions (terrorist financing transactions report or TFTR) or not (terrorist financing activity report or TFAR).

465. The CRF has a dedicated team composed of operational and strategic analysts, as well as magistrates, focused on TF matters. The team participates in weekly operational meetings at the national level, engages in strategic discussions, and is actively involved in international trainings and projects (see detail below).

466. Throughout the observation period, the majority of the TF-related reports were filed by e-banks. Their share has, however, decreased since 2019, along a relative increase of TF-related reports filed by e-money institutions since 2023 and DNFBPs since 2020.

Figure 19: Filed TFARs/TFTRs per type of reporting entities, 2021–2024[197]

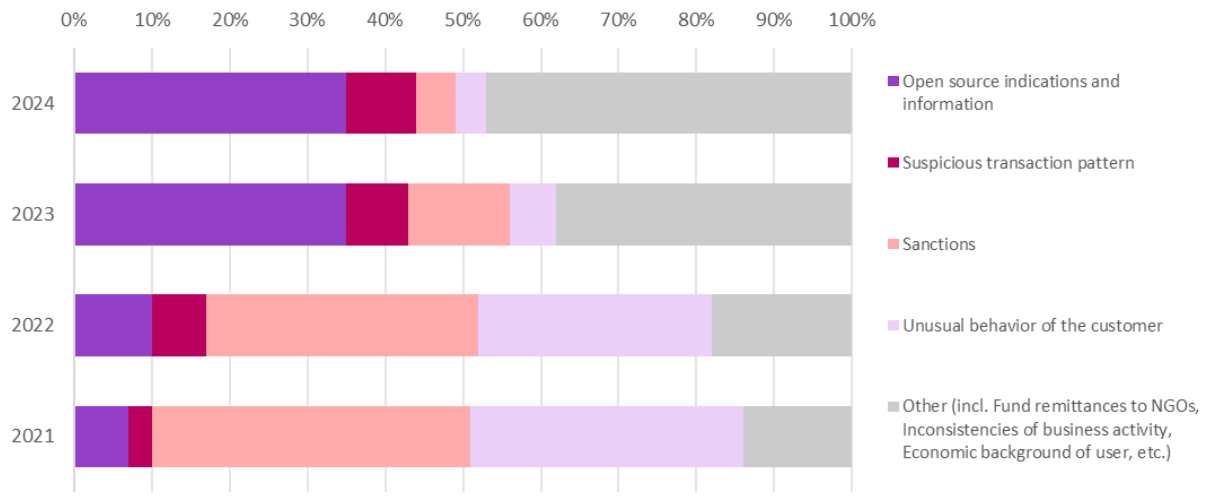


[196] Note that in 2021, 5 048 obliged entities were registered with goAML, 7 720 in 2022, 10 417 in 2023 and 12 210 in 2024. The increase is due to enhanced supervisory actions and awareness raising activities of supervisors and the CRF.

[197] CRF data. Note that e-Bank is an internal classification used in goAML, referring to specific reporting entities with a banking and/or EMI and/or PI and/or other types of licenses.

467. As mentioned previously, almost one third of TF-related reports filed in 2023 and 2024 were based upon open-source information, including terror-related adverse media or sanctions, usually generated from name screening alerts. Suspicious media posts and related contents are playing a relatively growing role in TF suspicions from reporting entities.

Figure 20: Evolution of main TF risk indicators from filed TFARs/TFTRs from 2017 to 2024 (October)



468. The CRF considers that the quality of the information received as generally good. This conclusion is based on analyses carried out by CRF specialists and feedback received from other competent national administrations and authorities, and feedback received from foreign FIUs.

13.3.2. International cooperation

469. As noted previously, the CRF disseminates, spontaneously and upon request, the results of its analysis to the national judicial authorities, to the national AML/CFT competent authorities, as well as to its foreign counterparts.

470. International CFT cooperation is of paramount importance given Luxembourg's open economy and presence of an international financial centre. Given the potential consequences of the threat of terrorism and TF, Luxembourg authorities aim to immediately disseminate any information to the relevant foreign authority and to provide immediate response to requests for cooperation received from a foreign authority.

471. At the strategic level, the CRF actively participates in numerous international meetings and trainings organised by the FATF, the EGMONT Group, Europol and Interpol, with the aim of enhancing terrorism and TF risk understanding, preparing strategic analysis documents such as typologies and indicators for professional guidance. Furthermore, the CRF organises bilateral meetings with those FIUs. Thus, the CRF maintains both active and passive cooperation.

472. Luxembourg law does not require the CRF to enter into any special agreement for it to be allowed to exchange financial information related to ML, associated predicate offences or TF with

other FIUs[198]. However, a number of foreign FIUs are bound by the obligation of a prior agreement and the CRF has therefore signed memoranda of understanding with foreign FIUs.

473. At a more operational level, cooperation between the CRF and foreign FIUs may be spontaneous or following a request from any FIUs.

474. Whenever a link with another jurisdiction is identified, the CRF systematically exchanges all relevant information with the relevant foreign FIU. Dissemination to foreign FIUs may take the form of spontaneous dissemination or of a fully-fledged international cooperation. The latter is used when there is the slightest indication of imminent danger, or the loss of funds that could be used for TF purposes, or if the CRF intends to initiate additional analyses in Luxembourg.

Table 16: Number of incoming and outgoing requests of information from and to FIUs, 2021–2024 (spontaneous and requests of information)

	2021	2022	2023	2024
Incoming requests of information	**136**	**136**	**144**	**125**
- *Requests of information*	*131*	*135*	*140*	*116*
- *Spontaneous*	*5*	*1*	*4*	*9*
Outgoing requests of information	**327**	**247**	**263**	**253**
- *Requests of information*	*106*	*171*	*142*	*49*
- *Spontaneous*	*221*	*76*	*121*	*204*

475. During the observation period, the overall majority (almost 90%) of incoming T/TF requests of information originated from European FIUs, with France accounting alone for around 60% of total requests received during the observation period, followed by Germany and Belgium, with 13% and 3% of requests. Incoming T/TF requests from FIUs from TJ were very limited, representing around 2% of the total 541 requests received.

476. During the observation period, the overall majority (around 75%) of total outgoing T/TF requests of information were addressed to European FIUs, with Germany being the destination country for around 33% of total request sent by the CRF, followed by France (16% of total requests) and to a lesser extent by Austria and Belgium (representing each around 5%). With regard to requests being addressed to non-European FIUs, the UK received most requests (around 15% of total requests). Outgoing requests to TJs were very limited, representing around 2% of total requests that were sent.

477. Feedback provided by foreign FIU's is essential to improve the quality of reports and the CRF strives to improve upon this feedback, in particular, by participating in different working groups within the EGMONT Group.

13.3.3. Outreach and training

478. Considering the ever-evolving landscape of TF and the cross-border nature of Luxembourg's financial centre, magistrates and analysts of the CRF plays an active role in initiatives striving to keep abreast of the lasted trends, typologies in the matters of FT. In this regard, the CRF intervenes and

[198] Article 74-5(1) of the Law on the Organisation of the Judiciary.

participated in conferences organized by international bodies such as FATF, no money for terror, or the Egmont group.

479. In a similar vein, CRF analysts dedicated to the matter of TF contribute to international projects and workstreams initiated by the FATF, or the Egmont Group to further elaborate typologies and guidance with regard to TF. As such, CRF analysts were project member of FATF's Comprehensive update on TF risks and of the EFIPPP Lead TF-Workstream 2023/2024/2025: Financing of Terrorist Organization: Typologies & Red Flags.

480. At a national level, the CRF intervenes, together with supervisory authorities and SRBs, regularly at dedicated TF-trainings, workshops and conferences.

481. The CRF also produces and disseminates to reporting entities via goAML the following documents:

- Terrorist financing fundraising campaigns in the context of the terrorist attacks on Israel on 7 October 2023 (26 October 2023)
- Financing of terrorist organizations – List of indicators (8 December 2023).

13.4. Investigations triggered by information taken from mutual legal assistant requests

482. The State Prosecutor analyses mutual legal assistance (MLA) requests and may decide to open a national investigation on the grounds of the information contained in the MLA request if a link with a reporting entity in Luxembourg is found. In all of these cases, the State Prosecutor informs the CRF and requests a financial analysis from the CRF.

483. With the exception of the MLA requests from Kosovo and Switzerland (2 requests out of 46), they all originated from EU Member States with half of them being from Germany (i.e. 23). Belgium and France addressed 5 requests each to the Luxembourg authorities.

484. Compared to requests received by the CRF (cf. Table 16), it can be observed that the number of requests received by Luxembourg judicial authorities is lower than those received by the CRF from its foreign counterparts. This is explained by the fact that those received by the CRF intend to obtain intelligence related to cases where the suspicion of terrorism or TF is still vague, while MLA requests seek to gather evidence in investigations that are already much more advanced. As mentioned in the beginning of this section, the State prosecutor may decide to initiate a national investigation and request a financial analysis from the CRF on the basis of the information contained in an MLA request. During the observation period, two national cases were opened based on information contained in MLA requests relating to terrorism or terrorist financing.

13.5. Prosecution, investigation and asset recovery

13.5.1. State prosecutor

485. In cases of terrorism and TF, the State Prosecutor at the District Court of Luxembourg leads and directs the work of the SPJ. Within this mission, the State Prosecutor is granted the same powers as conferred to a judicial police officer.

486. As shown in the insight box below, and pursuant to article 11 of the 1980 Judiciary Organisation Law, the State Prosecutor's Office at the District Court of Luxembourg is composed of 47 magistrates (one State Prosecutor, 4 Deputy State Prosecutors, 10 Principal Substitutes, 16 First Substitutes and 16 Substitutes) as of end 2024. Four magistrates deal with terrorism and TF cases. For the financial part of the investigations, they can rely on the support from their colleagues of the economic and financial crime department.

Insight Box 12: Law of 24 July 2024

The Law of 24 July 2024 set the framework for a three-year recruitment plan for magistrates in Luxembourg and created 94 vacancies. Among the 32 vacancies that were created for the 2024–2026 period, the magistrates within the Luxembourg District Court, 22 additional positions are dedicated to the Luxembourg's State Prosecutor's Office, as shown in the table below.

Table 17: Number of magistrates allocated to the Luxembourg's State Prosecutor's Office

	16/09/23–16/09/24	16/09/24–15/09/25	16/09/25–15/09/26	16/09/26–15/09/27
State Prosecutor	1	1	1	1
Deputy State Prosecutor	3	4	4	4
Principal Substitutes	7	10	13	16
First Substitutes	14	16	18	20
Substitutes	14	16	18	20
Total	**39**	**47**	**54**	**61**

487. The policy of the State Prosecutor is to order investigations at the earliest stages of terrorism or TF. The aim is to ensure that all information received is properly analysed to prevent these crimes from occurring. However, the action of the authorities at such an early stage makes it difficult to distinguish between potential cases of TF and potential cases of terrorism. Nevertheless, the financial aspect of every potential terrorism case is systematically analysed. The actions to be taken by the authorities may be discussed during the monthly coordination meetings described in section 13.5.5.

488. As described in detail in the next section, investigations are entrusted to the SPJ. Whenever there are any indications of TF, the State Prosecutor's Office informs the CRF of the existence of the case and requests a screening of the person(s) under investigation. The State Prosecutor's Office obtains feedback through an analysis report. In consultation with the State Prosecutor, CRF analysts may also interact directly with the SPJ.

13.5.2. Investigative judge

489. With the introduction of the Law of 24 July 2024 (see Insight Box 12), the District Court of Luxembourg counts one Chief investigative judge and 18 investigative judges in 2024. Two investigative judges (including the Chief investigative judge) deal with matters related to terrorism and three investigative judges (including the Chief investigative judge) with matters related to TF.

490. In cases where a certain number of formal investigations have revealed more specific indications of crime, the State Prosecutor entrusts an investigative judge with the follow-up of an investigation. This is in particular the case if coercive measures, such as house searches or arrests, have to be carried out.

491. Considering Luxembourg's international exposure and position as international financial centre, some evidence with respect to terrorism or TF might be located abroad. In some cases, investigative judges might seek legal assistance for international cooperation on a regular basis. Between 2021 and 2024, 24 MLA requests were sent out by Luxembourg investigative judges in matters of terrorism and TF. Among those, around one third were addressed to Luxembourg's neighbouring countries, one third to other EU Member States and one third to non-EU Member States (including one request to a T6 TJ).

13.5.3. Judicial Police Service

492. Investigations relating to the financing of terrorism or to terrorism (that may potentially have a terrorist financing component) respectively fall within the domain of competence of two distinct units within the SPJ, namely:

- a dedicated team of specialized investigators within the Anti-Money Laundering Section of the Economic and Financial Crime Department (SPJ-AB) for investigations relating to the financing of terrorism. It should be mentioned that 5 investigators have built up the know-how necessary for FT investigations, however every investigator in the SPJ-AB unit (amounting to 32 investigators as of September 2025) is capable to lead an FT investigation;
- the Anti-Terrorism Unit of the Organised Crime Department (SAT) for investigations relating to terrorism. The SAT currently comprises 11 investigators and 3 analysts, all of whom are judicial police officers and have many years of experience in the fight against terrorism.

493. The split between the T and TF investigations and the assignment of these investigations to two different units came into effect in July 2023. It should however be noted that both units closely cooperate with each other, and that the heads of the aforementioned units participate in regular meetings.

494. Since the perpetrators of terrorist and TF offences act very cautiously and operate in closed circles, it is usually difficult to determine the exact scope and intent of their statements and actions. At the beginning of an investigation, it is usually impossible to determine whether there are sufficient elements to substantiate the terrorist or TF offence.

495. With every investigation for terrorism, the financial dimension is systematically investigated by the SPJ. Indeed, it is generally accepted that the radicalised individual may, in an early stage manifest this radicalisation by financially supporting terrorist causes through the transmission of money amounts, even if only small amounts. For this reason, no minimum threshold is required to start TF

investigations. The financial information collected either confirms evidence of TF or is used as elements to support terrorism investigations. The SPJ conducts financial investigations within its own capacity or with the support of the CRF.

496. Throughout the observation period (2021–2024), 5 cases of TF (and other related offences) were allocated to either the SPJ-AB or SPJ-SAT unit. In this context, 6 Luxembourg residents were investigated. Bank transfers were identified to be the principal means of TF activity according to the TF cases investigated by the SPJ-AB, followed by credit cards, e-money and cash.

497. If a FI has been involved in a possible TF case, the SPJ-AB systematically verifies whether compliance with AML/CFT professional obligations has been ensured. If shortcomings are identified, coordination activities involving the exchange of non-operational information with the supervisory authorities concerned (CSSF/CAA) or a criminal investigation for non-compliance with professional obligations under the 2004 AML/CFT are envisaged.

498. With regards to trainings and knowledge sharing, it is worth mentioning that:

- SAT investigators participate mainly in trainings organized by foreign counterparts (BKA, CEPOL) and are actively involved in multiple working groups ("analysis projects") coordinated by Europol (AP Hydra, AP Travelers, AP Dolphin, AP Check the Web). Police cooperation also exists at the level of Interpol.
- SPJ-AB investigators specialized in TF investigations attended a dedicated FT training organized by the FBI in 2024, as well as the "Counter Terrorism Financing (CFT) Advanced" training organized by the House of Training, a foundation created in 2015 on the initiative of the Luxembourg Chamber of Commerce and the Luxembourg Banker's Association (ABBL). In addition to that, these investigators also participated in the biannual meetings of the "Counter Terrorism Financing Investigators network (CTFIN for TF specialized units) as coordinated by the European Commission.

499. The SPJ is continuously engaged in bilateral or multilateral cooperation via *inter alia* EUROPOL's "Secure Information Exchange Network Application" (SIENA) or INTERPOL for all types of criminal offence, including the financing of terrorism and terrorism).

13.5.4. Prosecutions and convictions

500. The first prosecution and conviction for terrorism took place in Luxembourg in 2021. Nevertheless, there have been no prosecutions or convictions for TF in Luxembourg up to 2024.

13.5.5. National CFT cooperation and coordination

501. As noted previously, the CRF disseminates, spontaneously and upon request, the results of its analysis to the national judicial authorities and to the national AML/CFT competent authorities.

502. National cooperation between the Public Prosecutor's Office and supervisory authorities is based on article 23 of the Code of criminal procedure. To strengthen that cooperation, the bill of law 8705 which transposes Directive (EU) 2024/1619, includes provisions regarding the cooperation between the CSSF and the CAA, and the State Prosecutor's Office, particularly where acts that could give rise to administrative sanctions could also be subject to criminal penalties.

503. The following table shows the number of intelligence reports transmitted by the CRF, both spontaneously and on the basis of cooperation, related to terrorism and TF. It thus illustrates the cooperation between the CRF and the prosecution authorities.

504. Considering that only a small share of cases has a direct link with Luxembourg, the number of cases sent to the judicial authorities and the SPJ is relatively low. These cases have been investigated but did not lead to sufficient evidence to support TF prosecution.

505. Furthermore, it should be noted that there is a high level of cooperation between national competent authorities (for instance, monthly coordination meetings) and the permanent collaboration between CRF analysts and the members of the SAT in order to assess the grounds and the merits of a suspicion reported by a professional. On a more purely operational level, cooperation between CRF analysts and police officers is very frequent. These exchanges can occur during meetings or phone conversations, or via the goAML message board.

506. Investigators of the SAT and SPJ- AB unit participate at the monthly “COS” meetings together with the judicial authorities and the SRE. Furthermore, SAT investigators also meet the SRE on a monthly basis (usually before the “COS” meetings).

14. Residual terrorist financing risk

507. The residual risk level is used to identify areas where Luxembourg remains exposed to TF risk once the effect of mitigating measures are taking into account. It thus serves as a basis to develop and prioritize strategic actions, which can be undertaken to further strengthen Luxembourg's AML/CFT framework and further reduce the TF risk. The table below provides an overview of the inherent residual risk by subsector assessed in this NRA update.

Table 18: Inherent and residual risk levels

Sector	Sub-sector	2026 NRA: Inherent TF risk	2026 NRA: Residual TF risk
Banks	Retail and business banks	High	Medium
	Entities operating online	High	Medium
	Wholesale, corporate and investment banks	Medium	Low
	Private banking	Medium	Low
	Custodians and sub-custodians (incl. Central Securities Depositories)	Medium	Low
Investment sector	Investment firms authorized to carry out the services of investment advice and portfolio management[199]	Medium	Low
	Investment firms authorized to carry out the services of reception and transmission of orders in relation to one or more financial instruments and of execution of orders on behalf of clients[200]	Medium	Low
	Investment firms authorized to carry out activities of dealing on own account, of underwriting of financial instruments and/or placing of financial instruments on a firm commitment basis and of placing financial instruments without a firm commitment basis[201]	Low	Very low
	Collective investments	Medium	Low
	CSSF-supervised pension funds	Very Low	Very low
Money value or transfer services (MVTS)	Payment institutions (PIs)	High	Medium
	E-money institutions (EMIs)	High	Medium
	Agents and e-money distributors acting on behalf of PIs/EMIs established in other European Member States	Medium	Medium
VASPs		High	Medium
Specialised PFSs	Specialised PFSs providing corporate services	Medium	Low
	Professional depositaries	Low	Very low
	Support PFSs	Very low	Very low

[199] In the 2020 NRA: "Wealth and asset managers".
[200] In the 2020 NRA: "Brokers and broker-dealers (non-banks)".
[201] In the 2020 NRA: "Traders / market-makers".

Sector	Sub-sector	2026 NRA: Inherent TF risk	2026 NRA: Residual TF risk
Support PFSs and other specialised PFSs[202]	Other specialised PFSs		
Market operators		Low	Low
Insurance	Life insurance	Medium	Low
	Non-life insurance	Low	Low
	Reinsurance	Low	Low
	Intermediaries	Low	Very Low
	Professionals of the insurance sector (PSAs)	Very Low	Very Low
	CAA-supervised pension funds	Very Low	Very Low
Real estate agents and developers	Real estate agents *(agents immobiliers)*	Medium	Medium
	Real estate developers *(promoteurs immobiliers)*	Medium	Medium
Freeport operators		Medium	Low
Dealers in goods	Precious metals/jewellers/clocks	Medium	Low
	Car dealers	High	Medium
	Art/Antiques	Medium	Medium
	Luxury goods (e.g. *"maroquinerie")*	Medium	Medium
Gambling service providers	Casino	Low	Very Low
	National lottery	Low	Very Low
Legal and accounting professions supervised by the AED	Accountants	High	Medium
	Professional directors and business centres	High	Medium
Legal and accounting professions supervised by SRBs	Lawyers	Medium	Low
	Notaries	High	Medium
	Court bailiffs *(huissiers de justice)*	Low	Low
	Audit profession[203]	Medium	Low
	Chartered professional accountants *(experts-comptables)*	High	Medium
Legal persons and legal arrangements	*Sociétés commerciales*	High	Medium
	Sociétés civiles	Medium	Low
	Other legal persons	Medium	Medium

[202] Analysis covered in NRA vulnerability section; Support PFSs & other specialised PFSs assessed on aggregate due to very low risk.

[203] In this document, the term "audit profession" covers statutory auditors ("*réviseurs d'entreprises"*), approved statutory auditors ("*réviseurs d'entreprises agréés"*), audit firms ("*cabinets de revision"*) and approved audit firms ("*cabinets de révision agréés"*).

Sector	Sub-sector	2026 NRA: Inherent TF risk	2026 NRA: Residual TF risk
	Domestic *Fiducies*	High	High
	Foreign trusts	High	High
NPOs (as per FATF definition) carrying out primarily international activities – ASBLs and *Fondations*	ASBLs without UP status or without the DNGO accreditation carrying out international activities	High	High
	ASBLs and *Fondations* with the DNGO accreditation carrying out international activities	High	Medium
NPOs (as per FATF definition) carrying out international and local activities – ASBLs and *Fondations*	International and local activities: ASBLs without UP status or without the DNGO accreditation carrying out international and local activities	Medium	Medium
	International and local activities: ASBLs with the UP status and *Fondations* carrying out international and local activities	Medium	Medium
NPOs (as per FATF definition) carrying out local activities – ASBLs and *Fondations*	ASBLs without the UP status	Low	Low
	ASBLs with the UP status and *Fondations*	Low	Low

Appendix A Methodology

A.1. Threat assessment: selection of jurisdictions targeted for analysis and tier classification

1. Since the TF VRA 2022, the NRA process includes the analysis of financial and non-financial flows. With respect to the present NRA on TF specifically, the analysis of financial and non-financial flows is aimed to identify, understand and evaluate the TF threat stemming from large movements of funds that transit the financial centre and that may potentially be linked to terrorist activities mainly elsewhere, in view that Luxembourg has not experienced any completed terrorist attack nor have any established terrorist group on its soil.

2. The starting point of the analysis is to establish a list of jurisdictions targeted for the analysis (the so called "target jurisdictions" (TJs)), containing countries being significantly impacted by terrorist attacks and/or presenting strategic deficiencies within their CFT framework. Whereas countries that are geographically located within regions that are particularly impacted by terrorism are presumed to be exposed to all the three stages of TF, countries with strategic deficiencies are mainly exposed to the raising and moving stages of TF. Consequently, countries that are both affected by the presence of international terrorist organisations and by strategic deficiencies within their CFT framework, are particularly exposed to a TF threat.

3. Credible, objective and reliable data sources were used to draw the country list, namely the Global Terrorism Index 2023 (GTI 2023) and the results of the 4th round of FATF/FSRBs mutual evaluation reports. The country list takes a broad approach, including countries that fit at least one of the following criteria:

   - Terrorist impact dimension: countries with worst GTI 2023 scores for counties located within the world regions most affected by terrorism (MENA and Sub-Saharan Africa region[204]);
   - TF dimension: countries subject to a call for increased monitoring by the FATF and that were assessed having a low or moderate effectiveness level for immediate outcome 9 (IO.9) during the 4th round of mutual evaluations.

4. In a second step, the selected 56 countries were categorized into six different tier groups for analytical purposes. Once determined which tier presents the most representative financial and non-financial links with Luxembourg, a more detailed and in-depth analysis on the most relevant countries was performed on the materiality and potential risk exposure they may represent.

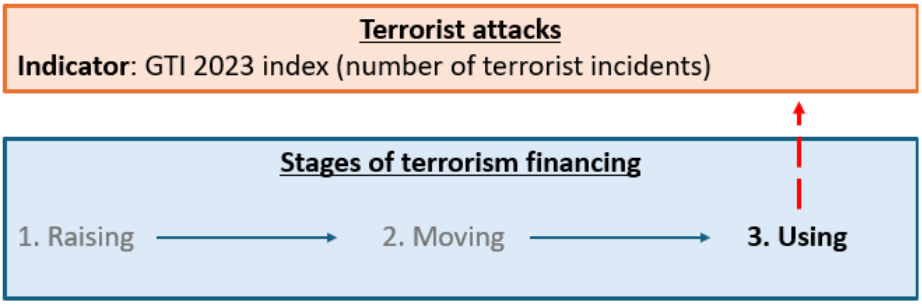
A.1.1. Terrorism approach: leveraging the Global Terrorist Index

5. First, countries most impacted by terrorist attacks were identified. The following figure depicts the link between terrorist attacks and the different stages of terrorism. Should terrorist attacks involve a financing component, it is in the using stage where those financing needs are exploited in order to execute such attacks. Nevertheless, it is important to point out that not all terrorist attacks leave

[204] For the MENA region, countries with a GTI score over 0,0 were selected; for the Sub-Saharan region, which contains more counties, the threshold was set to 0,2 not to overstate the sample.

a financing trail. However, all TF initiatives strive to finance, to some extent, the execution of hypothetical terrorist attacks.

Figure 21: Linking terrorist attacks with the different TF stages

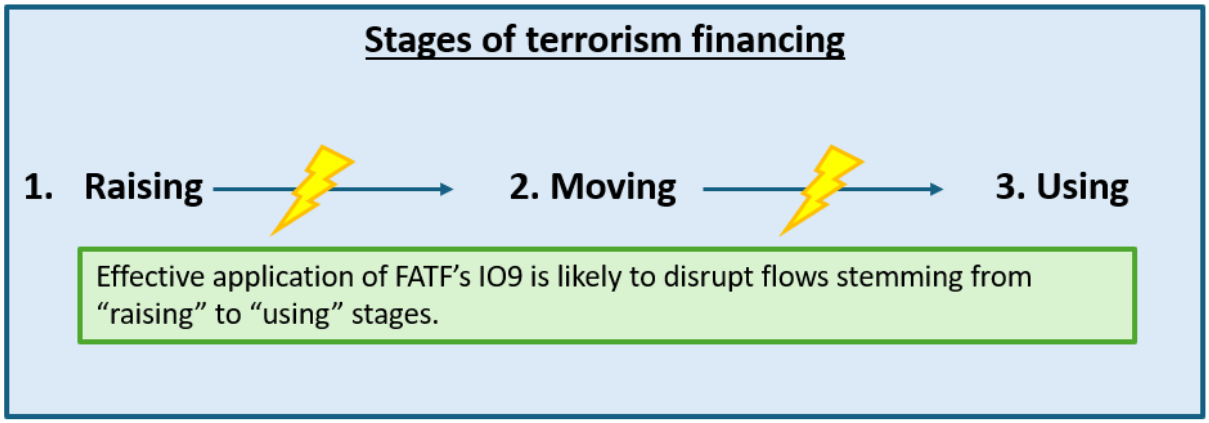


6. The GTI 2023 developed by the Institute for Economics & Peace counts the number of terrorist attacks over a period of five years and scores each country on a scale from 0 (no impact from terrorism) to 10 (highest measurable impact of terrorism). Consequently, the more terrorist attacks occur in a specific country, the higher the GTI 2023 score. The two regions most affected by terrorism and where ISIL and its affiliates are mostly active are Sub-Sahara Africa and the MENA region. However, ISIL and its affiliates are also present in Asia.

A.1.2. Terrorist financing approach: leveraging the results of the FATF mutual evaluations

7. The previous section explained the link between terrorist attacks and TF (notably the using TF stage). It also determined the countries that are most at risk of suffering a terrorist attack. Note that, depending on the effectiveness of the respective national CFT regimes, the vulnerability of these countries to TF related to terrorist attacks on their soil may be mitigated at different degrees.

Figure 22: reversed TF process and effective CFT regimes



8. Thus, countries that were assessed to be "Highly Effective" with respect to Immediate Outcome 9 (IO9) – TF investigation and prosecution during the FATF's 4th Round mutual evaluations were not considered as TJs for the purpose of this report. Indeed, highly effective CFT regimes deter TF activities and disrupt flows, as depicted in the figure above.

9. On the other hand, following a "TF approach" based on the results of the 4th cycle of mutual evaluations, countries with a "Moderate" (ME) or "Low Effective" (LE) rating in IO9 were identified. Based on this list, countries included in the FATF's "increased monitoring" list were selected under the "TF approach". Note that countries analysed within the "Terrorism approach" and that were not subject to a mutual evaluation are included for coherence purposes.

10. Overall, 37 countries were selected for analysis pursuant to a "TF approach" (IO9). Among those, more than half of them (21) were also selected for analysis pursuant to the "Terrorism approach" (GTI 2023 score).

A.1.3. Jurisdictions targeted for analysis: categorisation into tier groups

Overall, 56 countries were selected for the purpose of the analysis in this report, with:

- 21 being selected following both approaches (GTI 2023 and IO9)
- 19 being selected following a T-approach (GTI 2023)
- 16 being selected following a TF approach (IO9)

11. Indeed, as noted previously, countries that are geographically located within regions that are particularly impacted by terrorism are presumed to be exposed to all the three stages of TF, countries with strategic deficiencies are mainly exposed to the raising and moving stages of TF. Consequently, countries that are both affected by the presence of international terrorist organisations and by strategic deficiencies within their CFT framework, are particularly exposed to a TF threat.

12. The following table visualises the process followed in order to elaborate the countries subject to analysis. Considering that these countries were selected on the basis of different criteria and the implications of these criteria on their potential exposure towards the different stages of TF, they were further categorised into six different tier groups.

Table 19: Approach used to categorise TJ into tier groups

	Jurisdictions selected following a…		
	…both T and TF approach	**… only a T approach**	**… only a TF approach**
Criteria	GTI score 2023 and result of the 4th round of ME	GTI score 2023	Result of the 4th round of ME (IO9)
Relevant TF stages	Raising, moving, using	Raising, moving, using	Raising, moving
Tier groups	Tier 1 and Tier 2	Tier 3 and Tier 4	Tier 5 and Tier 6
Number of countries identified	21 TJs	19 TJs	16 TJs

Tier 1 and Tier 2

13. As noted above, 21 countries were selected based on the GTI 2023 and IO9 criteria. Among these countries, the GTI 2023 score varies between 0,83 (presenting a very low impact of terrorism) and 8,161 (presenting a very high impact of terrorism). In a similar vein, some of these countries were allocated a ME rating with regards to their CFT efforts whereas others were allocated a LE.

Furthermore, some countries were not subject to a mutual evaluation process. Taking into account these factors, these 21 countries are divided into two different tiers, namely T1 and T2.

14. As the GTI 2023 score ranges from 0 to 10, with 10 presenting the score of countries most impacted by terrorism, the effectiveness results obtained in the context of the mutual evaluation process, were translated into scores varying from 0 to 10. This allows for comparability of the GTI scores and FATF effectiveness ratings.

Table 20: Numerical score of effectiveness rating

Effectiveness rating	Numerical score
High level of effectiveness (HE)	0
Substantial level of effectiveness (SE)	2,5
Moderate level of effectiveness (ME)	5
Low level of effectiveness (LE)	7,5
Not assessed (NA)	10

15. As such, it is presumed at this stage that countries with the highest average rating of the GTI 2023 score and the effectiveness rating of IO9 are most vulnerable at being abused for TF purposes. In order to categorize these 21 countries evenly into two groups, the first ten countries with the highest average score were allocated into T1 and the remaining eleven into T2.

Tier 3 and Tier 4

16. As noted earlier, 19 countries were selected solely because of their GTI 2023 score. Their categorization into Tier 3 and Tier 4 depends on the result of their GTI 2023 score.

Tier 5 and Tier 6

17. Finally, the remaining 16 countries were selected on the basis of their mutual evaluation's results. In order to classify these countries, ratings allocated to IO9 were considered as well as their ratings with regard to IO1 (risk understanding), IO2 (international cooperation), and IO4 (preventive measures). It should be noted that this tier rating is based solely on their effectiveness rating.

18. As for step 1, the effectiveness levels were transformed into numerical scores.

A.2. Vulnerabilities assessment

Table 21: Scorecard of assessment criteria for sectorial vulnerabilities

Dimension	Sub-dimension	Examples of indicators/data
Structure	Size	• Revenue/turnover and profit • Assets • Assets under management
	Fragmentation/complexity	• Number of institutions • Level of concentration (e.g. top-five entity assets as a % of the market)
Ownership/ legal structure	Ownership/ legal structure	• % ownership by foreign BOs (of which from countries on the TJs list) • % of entities with foreign mother
Products/ activities	Products/activities	• % of products or activities susceptible to TF (e.g. % revenue from products/activities)
Geography	International business	• % of international business (e.g. in clients' revenue, assets, transactions)
	Flows with weak AML/CFT measures geographies	• % of high-risk geographies based on the TJs list (e.g. in clients' revenue, assets, transactions)
Clients/ transactions	Volume	• Number of clients • Total number (stock) • New clients per year (flow)
	Risk	• % high-risk clients (based on supervised entities' internal models) • % PEPs (over time): domestic vs. foreign and residing in TJs
Channels	Channels	• Type of interaction: % face-to-face, indirect (e.g. online), via intermediaries

Table 22: Inherent risk scorecard – individual risk ratings

Risk rating against criteria	Risk levels
1	Very Low
2	Low
3	Medium
4	High
5	Very High

Table 23: Inherent risk scorecard risk – overall inherent risk outcome

Average between		
Lower bound	**Higher bound**	**Risk levels**
1,00	1,80	Very Low
1,80	2,60	Low
2,60	3,40	Medium
3,40	4,20	High
4,20	5,00	Very High

A.3. Mitigating factors and residual risk

Table 24: Scorecard of impact criteria for mitigating factors

Dimension	Criteria	Information/data used (examples)
Market entry controls	Market entry	• Licenses/registrations – number of applications received, processed, approved, rejected
	Breaches	• Number of licenses/registrations breaches identified/remediated
Understanding of ML/TF risks and AML/CFT obligations	Understanding of TF risks and AML/CFT obligations	• Annual questionnaires • Risk assessments (e.g. entity level, sub-sector risk assessments) • Internal trainings • Supervisors' publications on ML/TF risks in the sector
	Regulation & information	• Type of supervisor (e.g. association, ministry, dedicated supervisor) • Regulation communication to the sector (e.g. circulars) • Education to private sector (e.g. publications, trainings, etc.)
Prevention / Private sector controls	TF controls in place	• CDD/KYC approach, aligned with risk level, number of customers declined based on CDD • Transaction monitoring approach, aligned with risk level, number of alerts generated, handled and STRs reported
	Internal supporting structures	• Formalised policies, procedures and controls, clearly articulating the risk-based AML/CFT approach • Member of management body responsible for compliance with AML/CFT obligations
Supervision & Enforcement	Level of supervision	• Number and type of inspections (on-sites and off-sites) • Supervisor procedures formalised and up to date
	Enforcement	• Remedial actions imposed (i.e. number of sanctions and other actions) • Outcomes of remedial actions (i.e. number of deficiencies remediates)
Detection, Prosecution & Asset recovery	STRs/SARs	• Number of STRs and SARs issued by subsector and predicate offences • Quality of STRs and SARs issued by subsector and predicate offences

Figure 23: Residual risk calculation

Inherent risk scorecard risk – overall inherent risk outcome

Inherent risk (i.e. in the absence of controls)

Avg. between Lower bound	Higher bound	Risk levels
1.00	1.80	Very Low
1.80	2.60	Low
2.60	3.40	Medium
3.40	4.20	High
4.20	5.00	Very High

−

Mitigating factors scorecard – overall impact on residual risk outcome

Mitigating factors

Avg. between Lower bound	Higher bound	**Outcome** (mitigating factors in place)	Impact on residual risk
1.00	1.80	Limited or no mitigating factors	0
1.80	2.60	Some mitigating factors	-0.5
2.60	3.40	Significant mitigating factors	-1
3.40	4.20	High mitigating factors	-1.5
4.20	5.00	Very high mitigating factors	-2

=

Residual risk — *Same as inherent risk scores*

As an example, a given sub-sector "X" could have:

- Inherent risk score of 3,8 (average across the inherent risk criteria). This corresponds to a level of "High" inherent risk;
- Mitigating factors score: 2,1 (average across the residual risk criteria). This corresponds to an outcome of "some mitigating factors in place" and hence to a reduction of inherent risk by -0,5.
- Residual risk score: 3,8-0,5 = 3,3, which corresponds to a residual risk outcome of "Medium".

Appendix B List of tables, figures, case studies and insight boxes

B.1. List of tables

Table 1: Residual TF risk, summary by (sub-)sector 5
Table 2: EU27 vs. Luxembourg real GDP growth, 2020–2024 10
Table 3: Net year-ending FDI position of Luxembourg by partner (in millions of EUR), 2021-2024 12
Table 4: FDI position (inward stock) by top-ten partner (in millions of EUR), 2021-2024 12
Table 5: FDI position (outward stock) by top-ten partner (in millions of EUR), 2021-2024 12
Table 6: Methodology – key definitions 17
Table 7: International cooperation CRF, 2021–2024 data 39
Table 8: Approach used to categorise TJs into tier groups 47
Table 9: Financial flows to and from TJs, overview: amounts between parenthesis represent million euros as of end 2024 (in the case of balances) or for 2024 (in the case of flows) 48
Table 10: Luxembourg TF threat level 54
Table 11: Average number and value of transactions, 2021–2024 72
Table 12: Luxembourg legal persons by legal form and category, 2020–2024 105
Table 13: Sectoral split of legal persons registered with RCA following NACE codes as of end 2024 – top-three sector per category highlighted in orange 107
Table 14: RFT registrations over the period 2020–2024 110
Table 15: Luxembourg non-profit associations by legal form and status 112
Table 16: Number of incoming and outgoing requests of information from and to FIUs, 2021–2024 (spontaneous and requests of information) 131
Table 17: Number of magistrates allocated to the Luxembourg's State Prosecutor's Office 133
Table 18: Inherent and residual risk levels 137
Table 19: Approach used to categorise TJ into tier groups 142
Table 20: Numerical score of effectiveness rating 143
Table 21: Scorecard of assessment criteria for sectorial vulnerabilities 144
Table 22: Inherent risk scorecard – individual risk ratings 145
Table 23: Inherent risk scorecard risk – overall inherent risk outcome 145
Table 24: Scorecard of impact criteria for mitigating factors 146

B.2. List of figures

Figure 1: Annual current account of Luxembourg (in millions of euros; BPM6 methodology) 10
Figure 2: Terrorist financing stages 22
Figure 3: TF vs. ML 22
Figure 4: FT activity of FTFs according to their location 24
Figure 5: Number of terrorist attacks in the EU by ideology, 2021–2024 34
Figure 6: Number of arrests in the EU by ideology, 2021–2024 34
Figure 7: Share of terrorist attacks in Luxembourg's neighbouring countries, split by ideology 35
Figure 8: Share of arrests in Luxembourg's neighbouring countries, split by ideology 36
Figure 9: Main ideologies observed per year from filed TFARs/TFTRs (2023–2024), in % 39
Figure 10: Number of BO registered with the RBE 49

Figure 11: Number of SMO registered with the RBE 50
Figure 12: Number of BO registered with the RFT, 2024 50
Figure 13: Number of clients served by Luxembourg VASP, 2021–2024 75
Figure 14: Total turnover generated by dealers in goods (in EUR million), 2021–2024 90
Figure 15: Concentration rates: share of revenues generated by top-five entities (per category), 2021–2024 91
Figure 16: Number of legal persons registered with the RCS, situation as of end 2021–2024 98
Figure 17: RFT registrations over the period 2020–2024 109
Figure 18: Geographical scope of activities of the FATF NPO subset, 2024 113
Figure 19: Filed TFARs/TFTRs per type of reporting entities, 2021–2024 129
Figure 20: Evolution of main TF risk indicators from filed TFARs/TFTRs from 2017 to 2024 (October) 130
Figure 21: Linking terrorist attacks with the different TF stages 141
Figure 22: reversed TF process and effective CFT regimes 141
Figure 23: Residual risk calculation 147

B.3. List of case studies

Case study 1: Luxembourg suspect using layering techniques to collect and move funds for an FTF in Syria 24
Case study 2: SPJ investigation into a Non-Profit Association 30
Case study 3: Use of credit cards and e-money accounts and payments to facilitate TF in Luxembourg 58
Case study 4: Use of funds 59

B.4. List of insight boxes

Insight Box 1: Editing and reposting material from media outlets of terrorist groups 30
Insight Box 2: Terrorist situation in Luxembourg's neighbouring countries 35
Insight Box 3: Luxembourg: the fight against terrorism and violent extremism 36
Insight Box 4: TF indicators 40
Insight Box 5: Complementarity of information provided in the 2025 update of the Collective Investment Sub-Sector Risk Assessment 68
Insight Box 6: Looking ahead: transition from VASPs to CASPs under MiCAR and potential implications in TF risk 75
Insight Box 7: Non-life insurance TF assessment (cyber, kidnap/ransom and marine) 82
Insight Box 8: Ad hoc lotteries 93
Insight Box 9: Complementarity of information provided in the 2025 NRA of money laundering for services offered by lawyers 97
Insight Box 10: Seminar dedicated to Preventing Terrorism Financing in November 2024 125
Insight Box 11: Mitigating factors overview 126
Insight Box 12: Law of 24 July 2024 133

Appendix C Glossary

Acronym	Definition
ABBL	The Luxembourg Bankers' Association
ACD	*Adminisration des Contributions Directes*
ADA	*Administration des Douanes et Accises*
AED	*Administration de l'Enregistrement et des Domaines*
AI	Artificial intelligence
AIFM	Alternative investment fund manager
AML/CFT	Anti-money laundering and counter-terrorist financing
AMO	Asset Management Office
ARO	Asset Recovery Office
ASBL	*Association sans but lucratif*
ATM	Automated teller machines
AuM	Assets under management
BCL	*Banque centrale du Luxembourg*
BO	Beneficial owner
CAA	*Commissariat aux Assurances*
CDD	Customer due diligence
CdH	*Chambre des Huissiers de Justice*
CdN	*Chambre des Notaires*
CPA	Chartered professional accountants
CRF	*Cellule de renseignement financier*
CSD	Central Securities Depositories
CSSF	*Commission de Surveillance du Secteur Financier*
DNFBP	Designated non-financial businesses and professions
DNGO	Development non-governmental organisation
EBA	European Banking Authority
EMI	E-money institution
EPPO	European Public Prosecution Office
EU	European Union
FATF	Financial Action Task Force
FCP	*Fonds commun de placement*
FDI	Foreign Direct Investment
FI	Financial institution
FIU	Financial intelligence unit
GDP	Gross Domestic Product
GGR	Gross Gaming Revenue
HOSSP	Hawala and other similar service providers
IRE	*Institut des Réviseurs d'Entreprises*
ISC	Inter-ministerial Steering Committee for the Fight against Money Laundering and Terrorist Financing
KYC	Know your customer

Acronym	Definition
KYT	Know your transaction
LBR	Luxembourg Business Registers
LGX	Luxembourg Green Exchange
LHSH	Luxembourg High Security Hub
LPs/LAs VRA	Legal persons and legal arrangements ML/TF vertical risk assessment
LuxSE	Luxembourg Stock Exchange
ManCo	Management Companies
ML	Money laundering
MLA	Mutual legal assistance
MoE	Ministry of Economy
MoF	Ministry of Finance
MoFA	Ministry of Foreign and European Affairs, Defence, Development Cooperation and Foreign Trade
MoJ	Ministry of Justice
MVTS	Money value transfer service
NPC	National Prevention Committee on money laundering and terrorist financing
NPO	Non-profit organisations
NRA	National Risk Assessment
OAD	*Ordre des Avocats de Diekirch*
OAL	*Ordre des Avocats de Luxembourg*
OEC	*Ordre des Experts-Comptables*
P2P	Peer-to-peer
PEP	Political exposed person
PFS	Professional of the financial sector
PSA	Professional of the insurance sector
PSP	Payment Service Provider
RBE	*Registre des bénéficiaires effectifs*
RCS	*Registre de Commerce et des Sociétés*
REA	Real estate agents
RED	Real estate developers
RFT	Register of *fiducies* and trusts
SARL	*Société à responsabilité limitée*
SICAV	*Société d'investissement à capital variable*
SMO	Senior management official
SNRA	Supranational assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities
SRB	Self-regulatory body
STR	Suspicious transaction report
TCSP	Trust and corporate service provider
TF	Terrorist financing
UCITS	Undertaking for collective investment in transferable securities
UP	*Utilité publique*

Acronym	Definition
VASP	Virtual asset service provider
vIBAN	Virtual IBAN